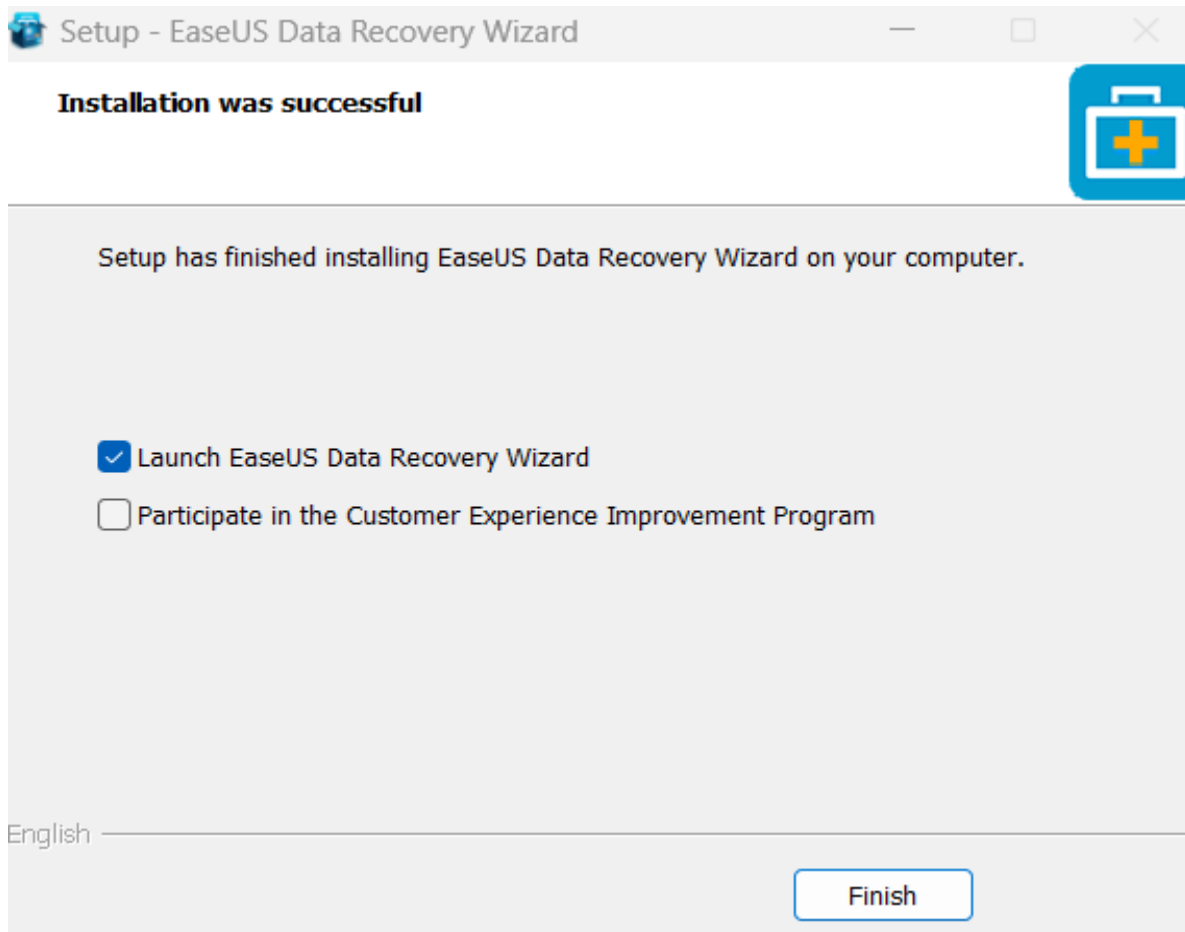
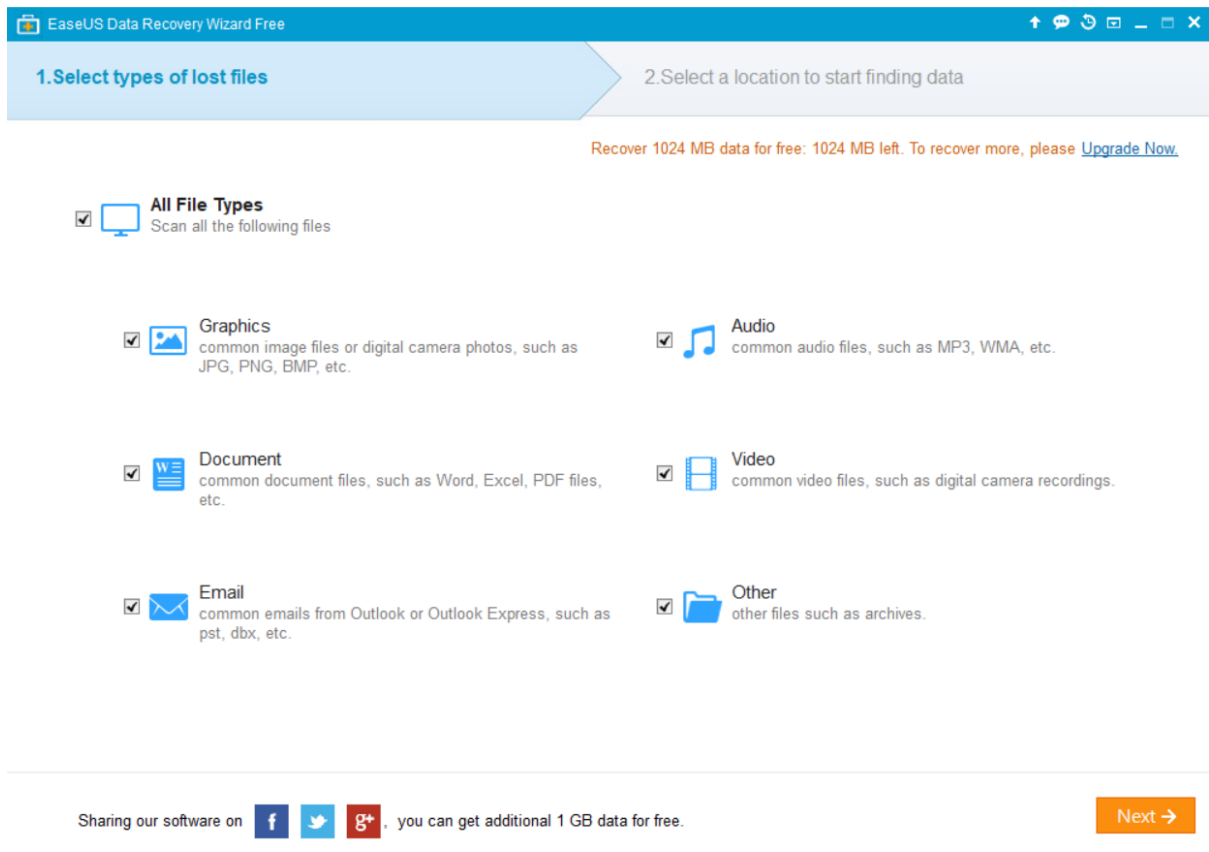


LAB1

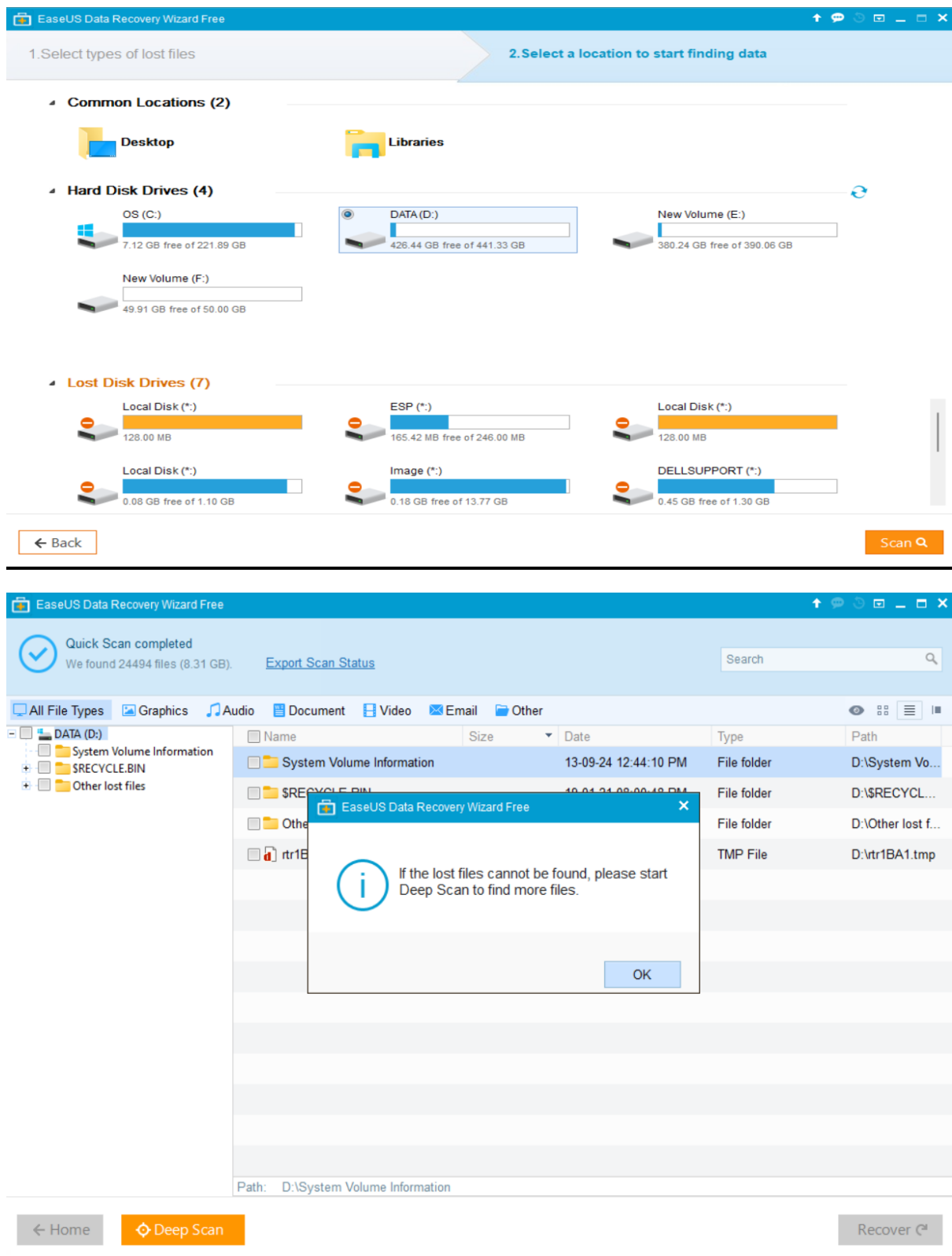
Recovering Data Using the Easeus Data Recovery Method

Objective: To understand and perform data file recovery using EaseUs Data Recovery Wizard Tool.

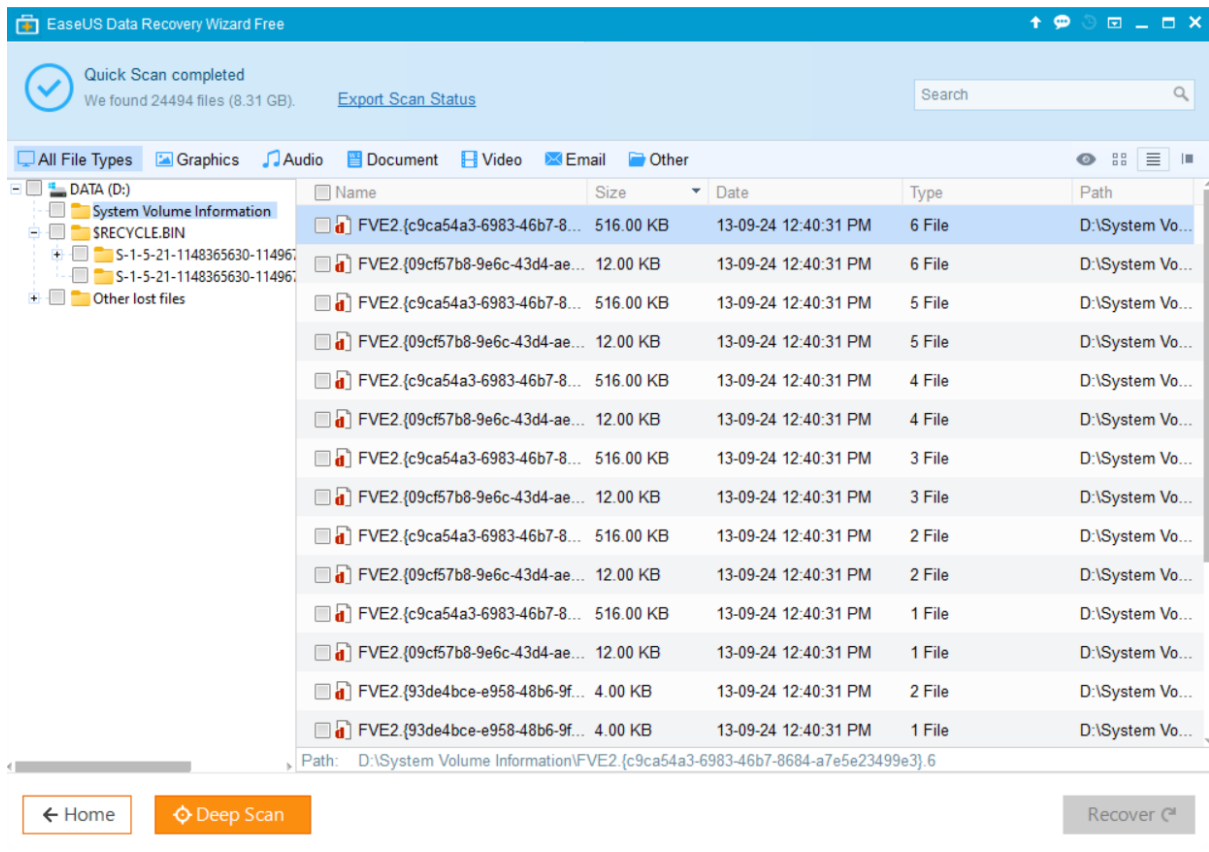




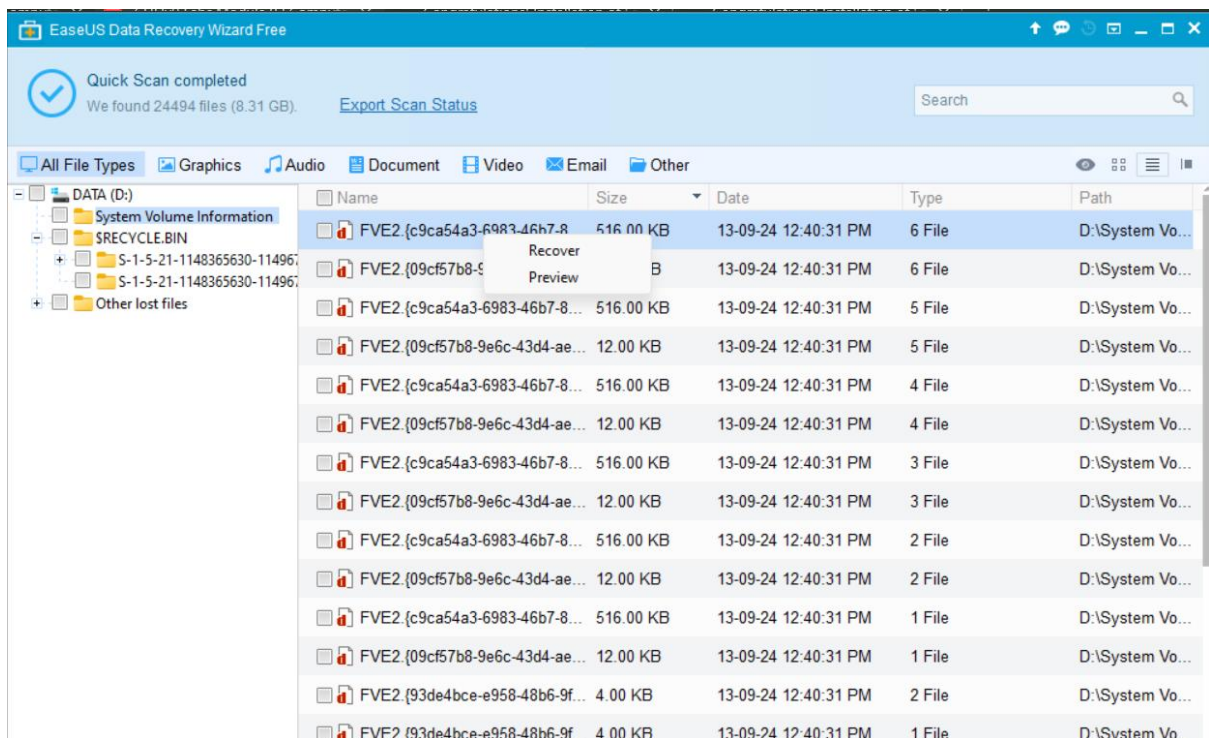
Scan this drive and begins to display the contents of the drive along with the data that have been deleted.

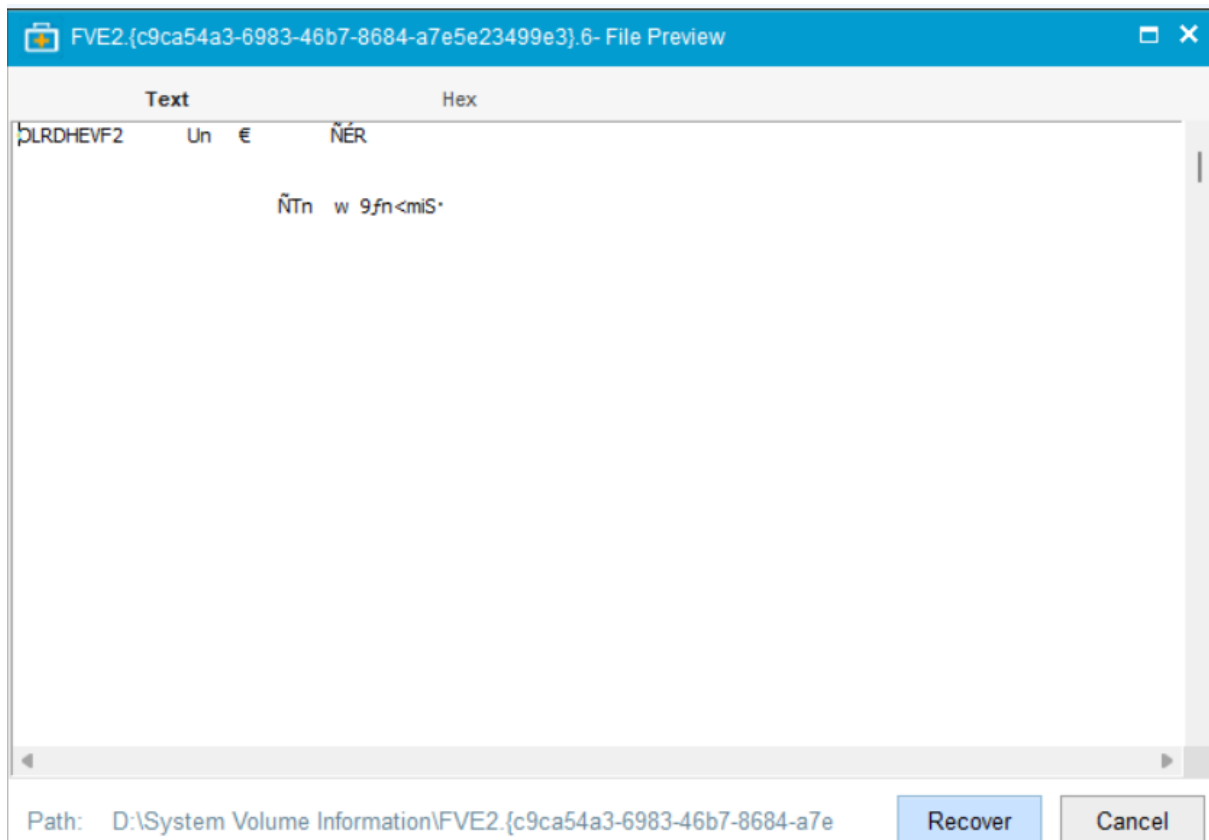


From this we can identify the deleted files.

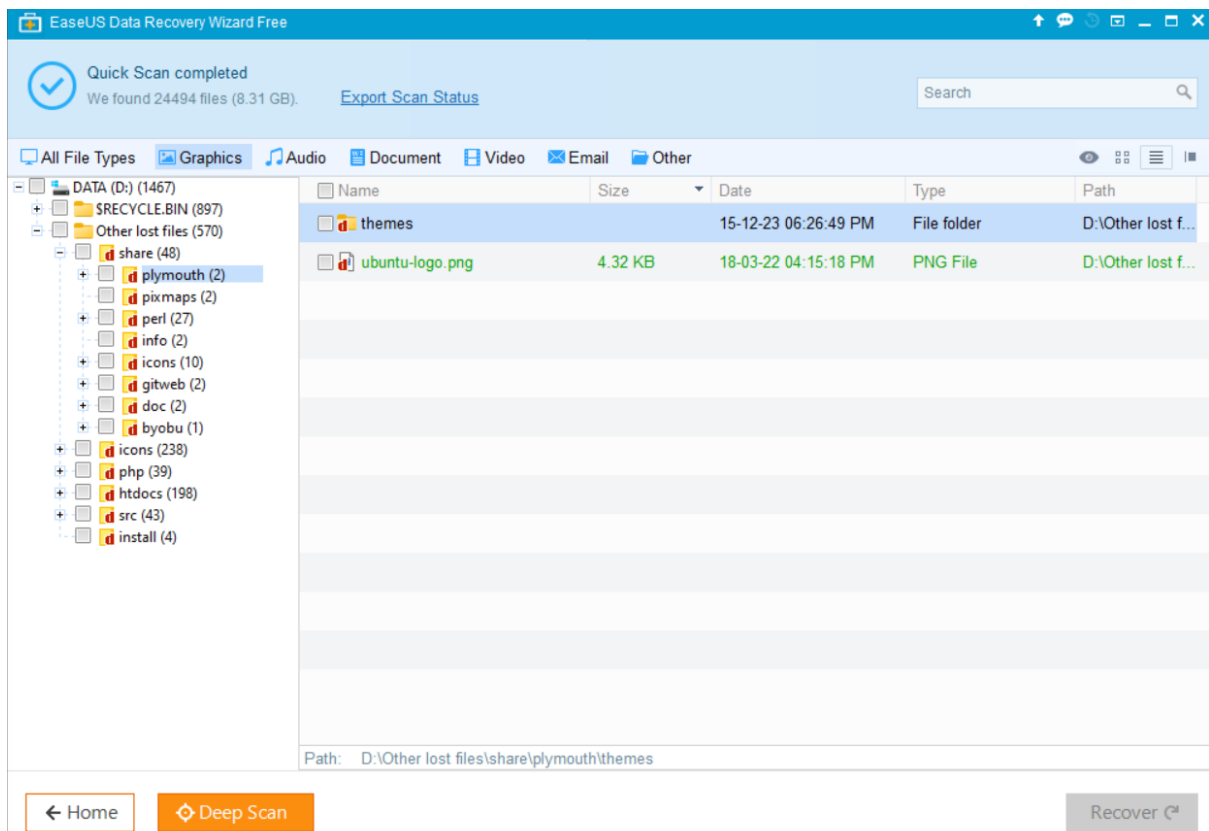


To view the file click preview. then we can see the contents of file.

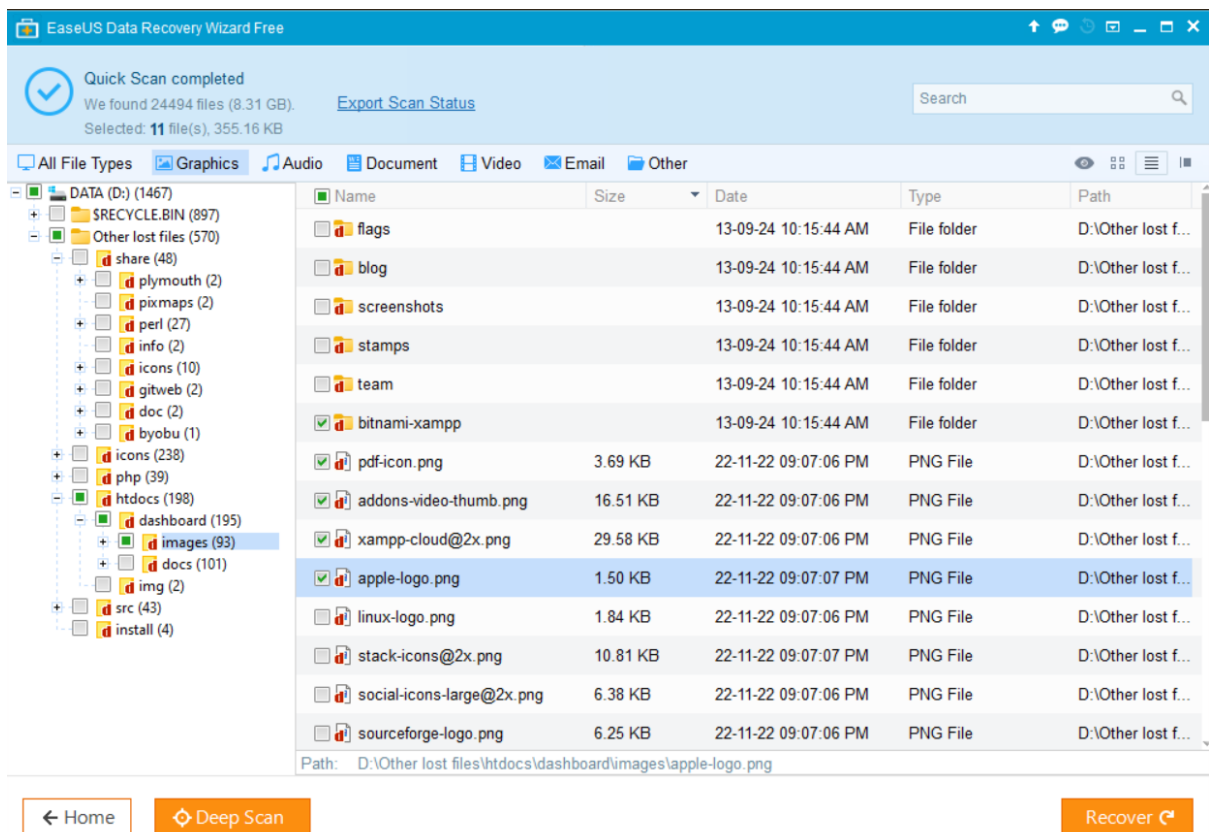




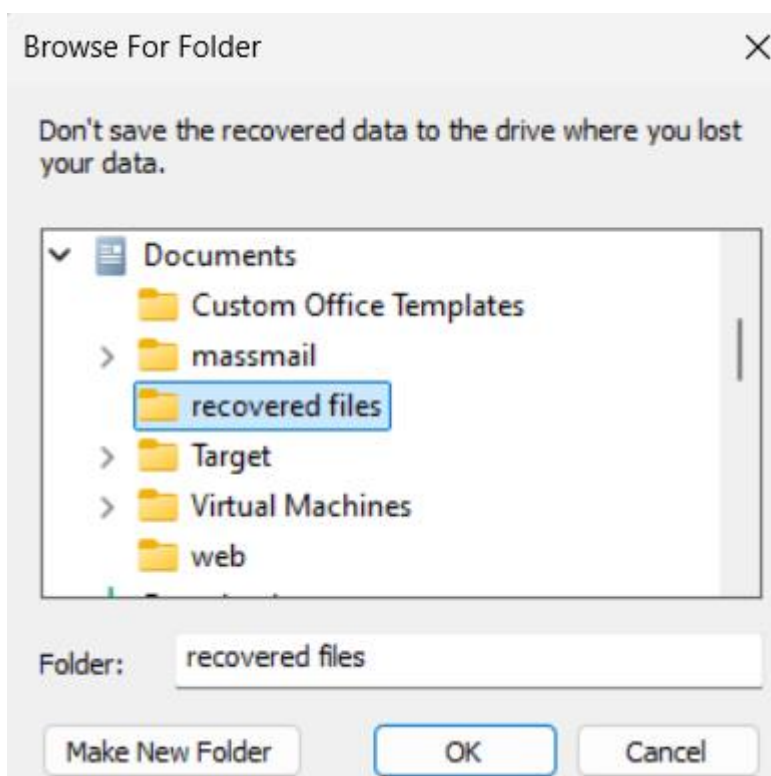
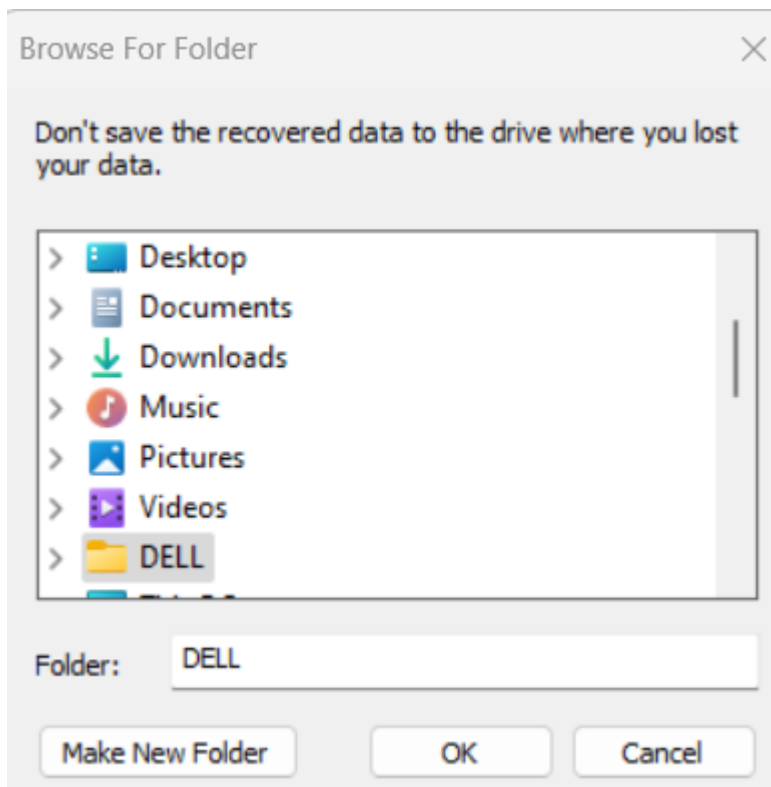
To view the files containing images format click graphics.

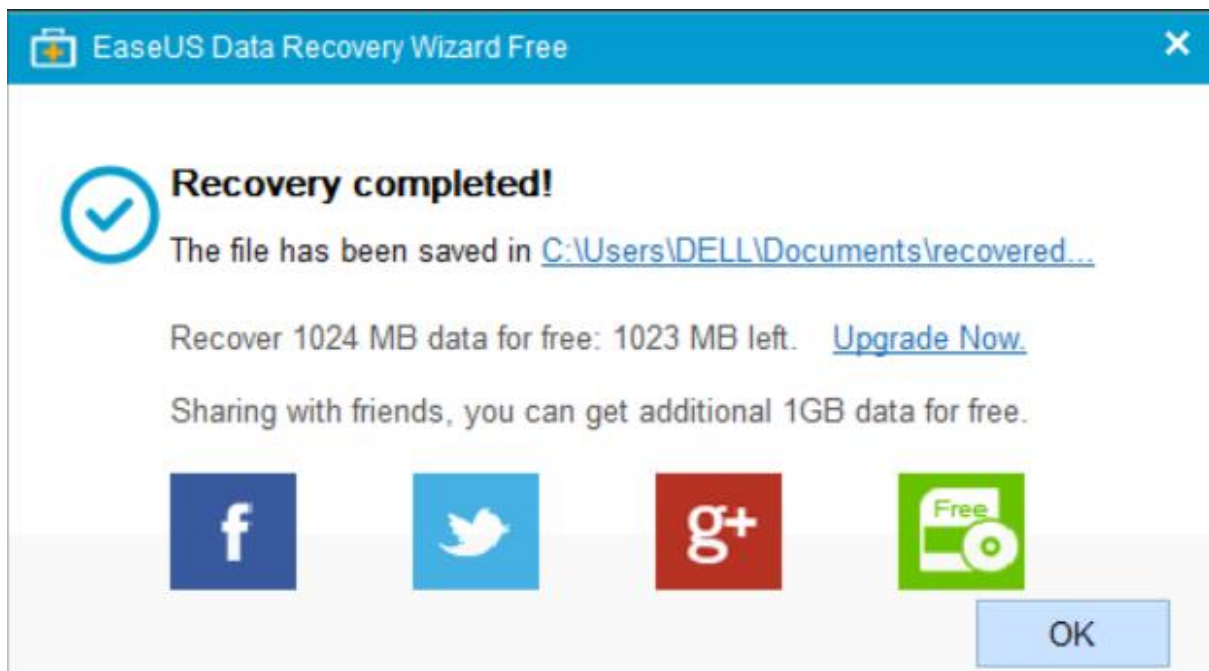


Here recovered multiple files I want.

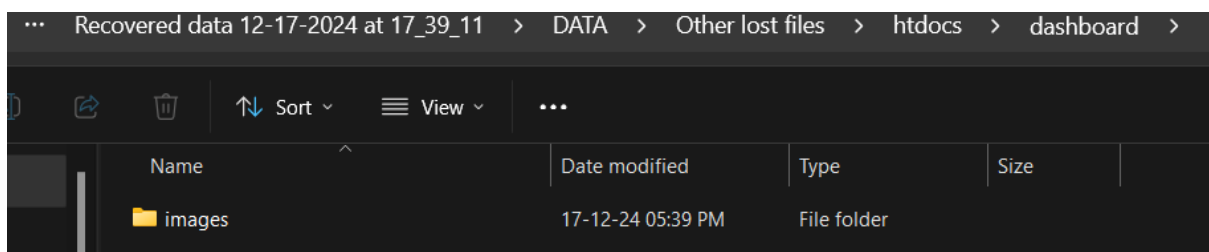
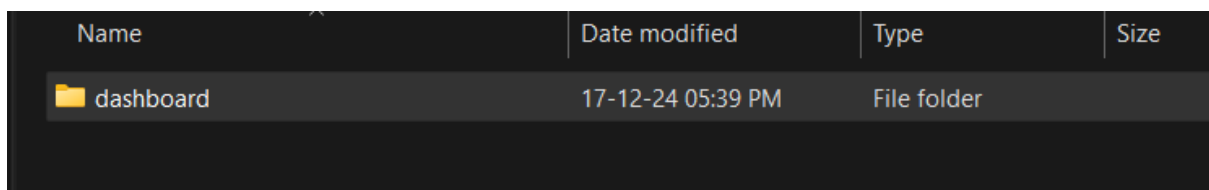
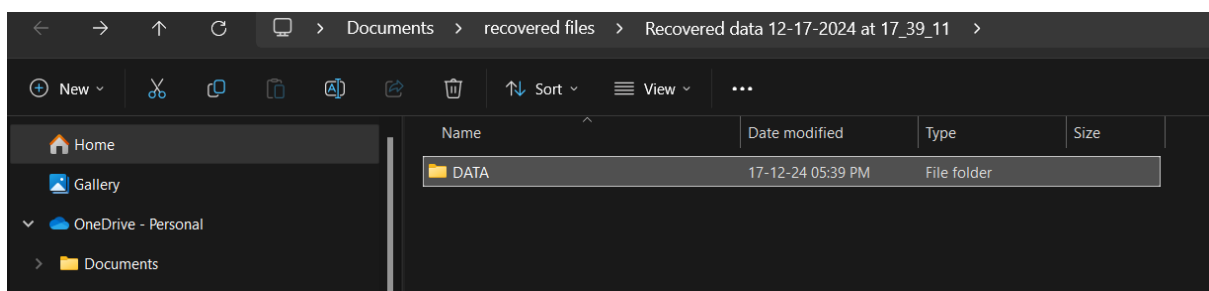


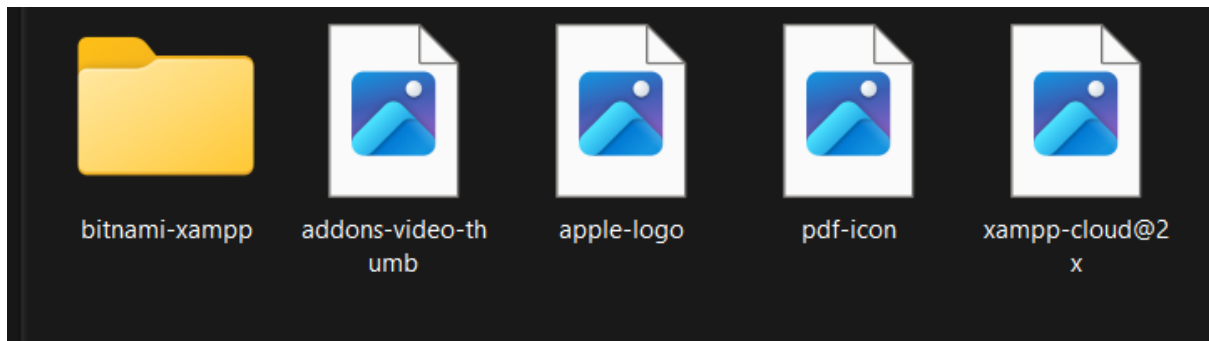
After that to store this files chose a location.





Now it is visible in my documents.





LAB-2

Performing Hash, Checksum, or HMAC Calculations Using the Hashcalc

Objective: This lab will show how to encrypt data and how to use it. Furthermore, it will teach how to:

- Use the encrypting command
- Generate hashing and checksum files.



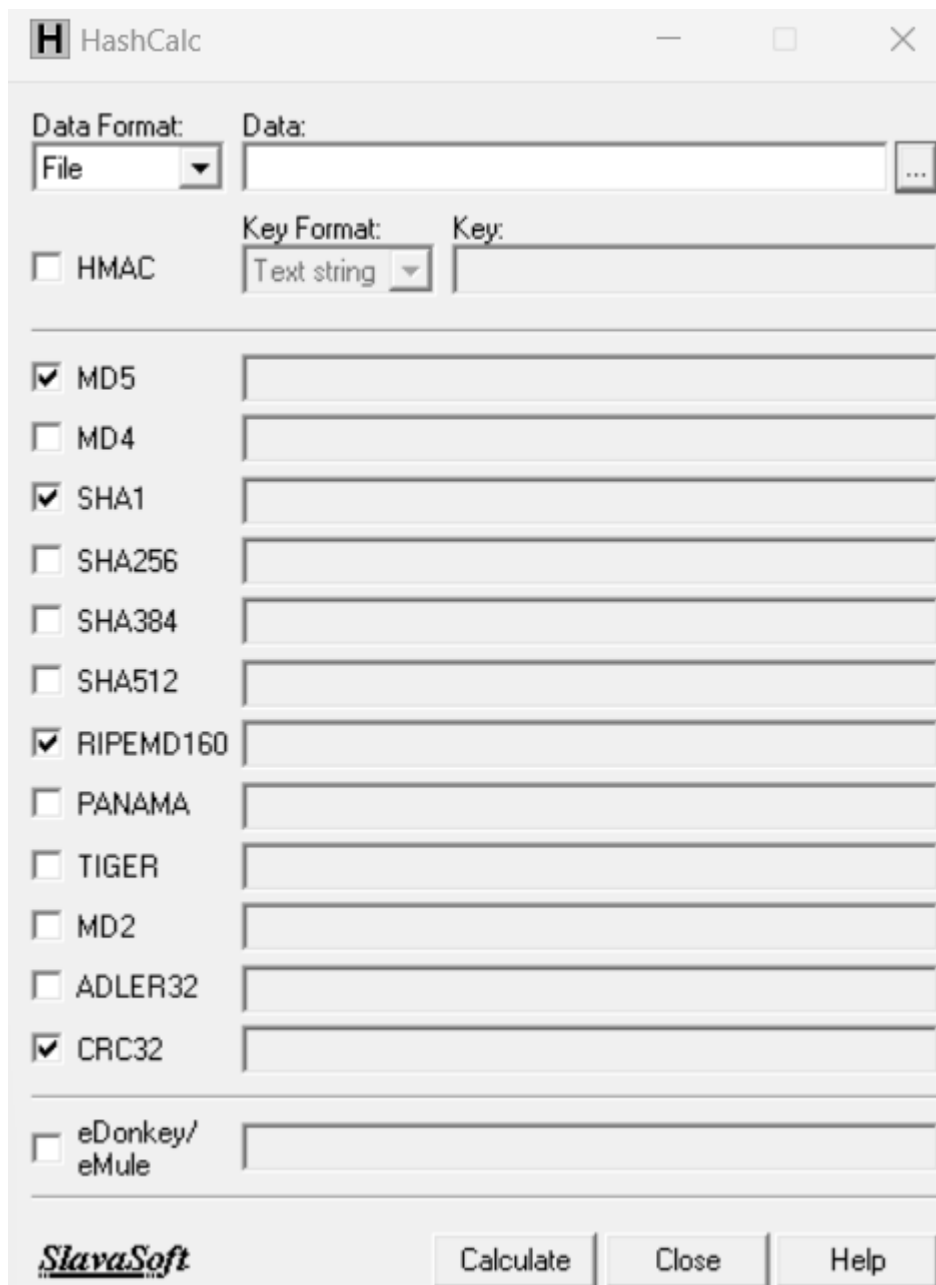
Completing the HashCalc Setup Wizard

Setup has finished installing HashCalc on your computer. The application may be launched by selecting the installed icons.

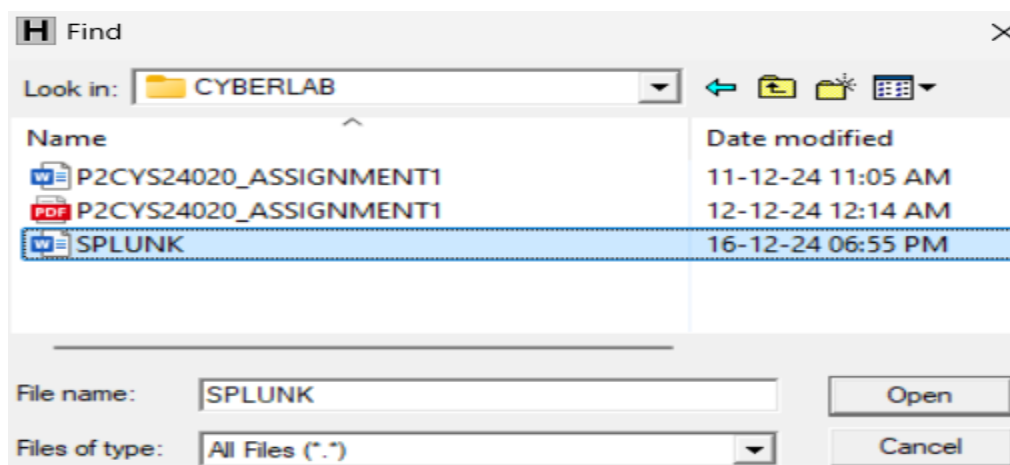
Click Finish to exit Setup.

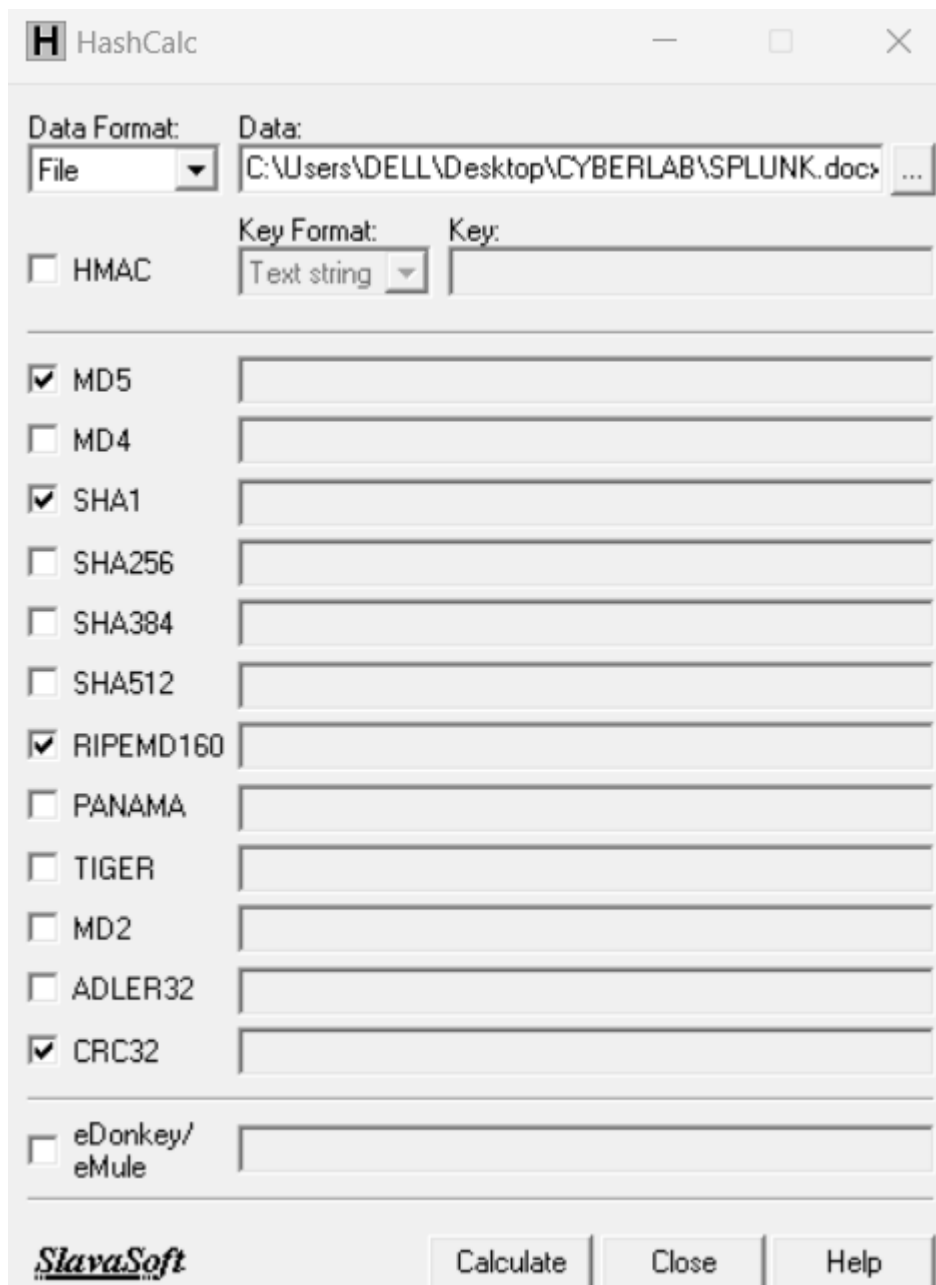
- ☐ View the README file
- ☒ Launch HashCalc

Finish



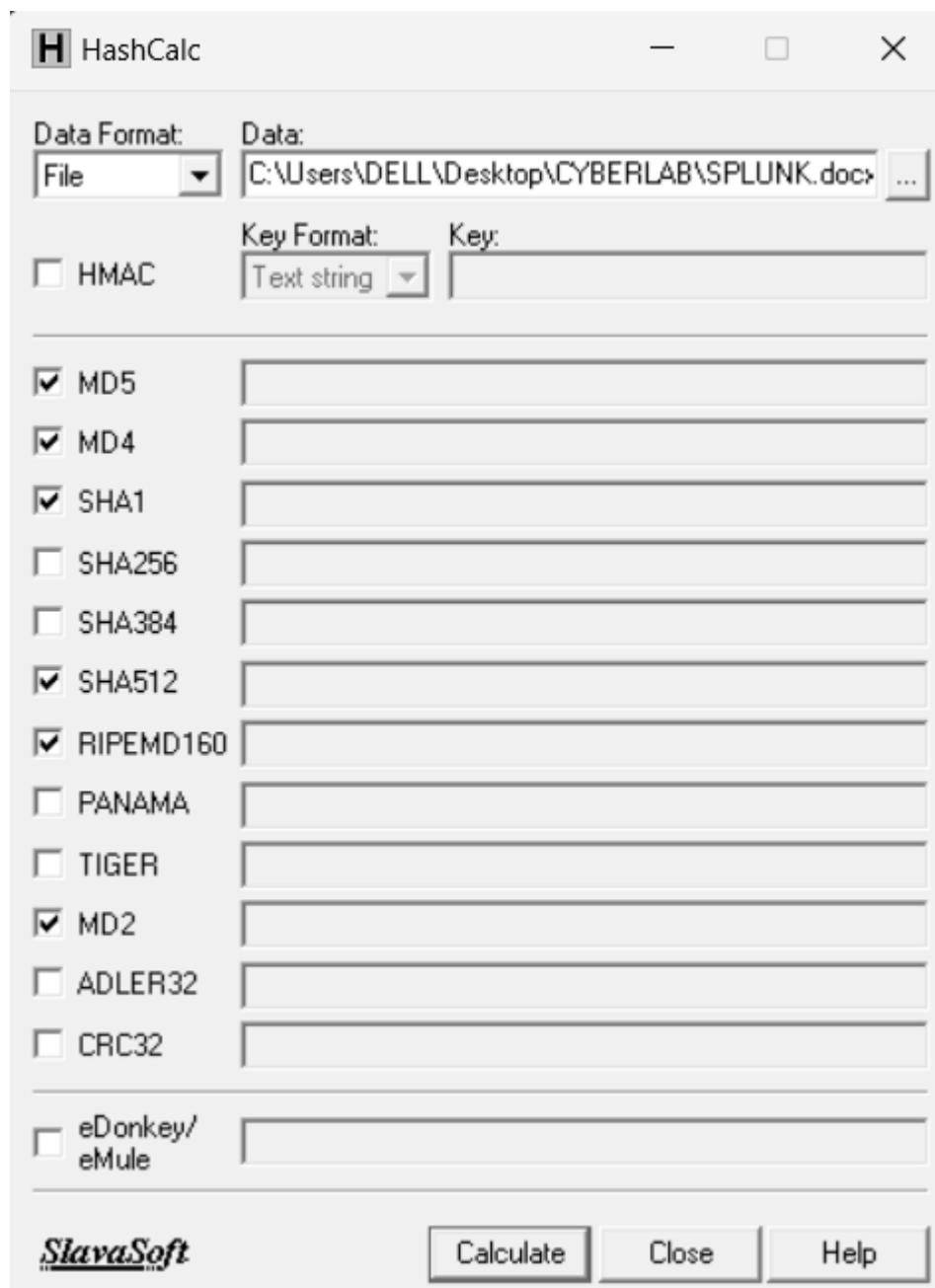
Here we can select the file whose hash value need to be calculated.



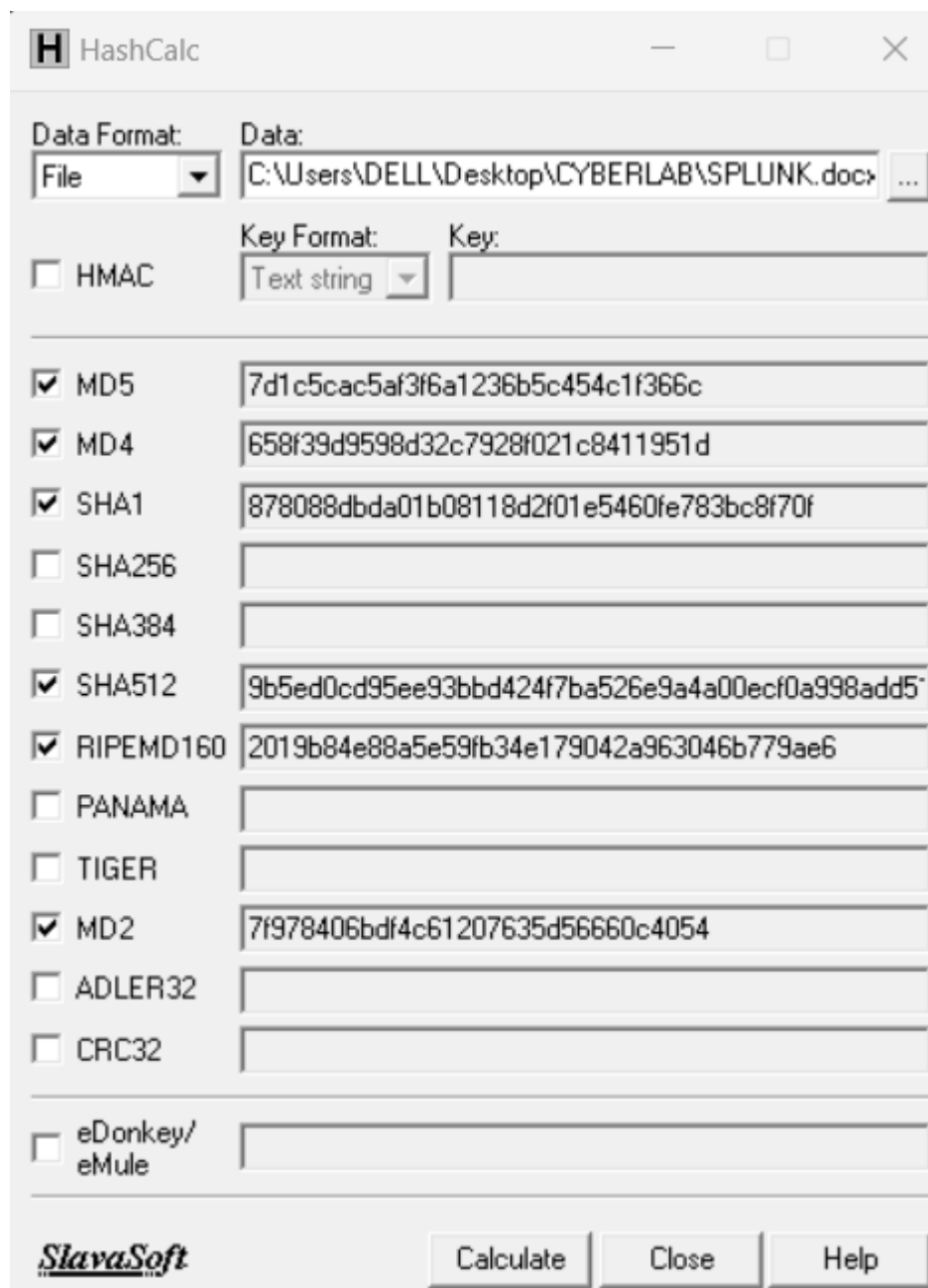


To calculate the message digest/checksums for the data, the HMAC box must be unchecked.

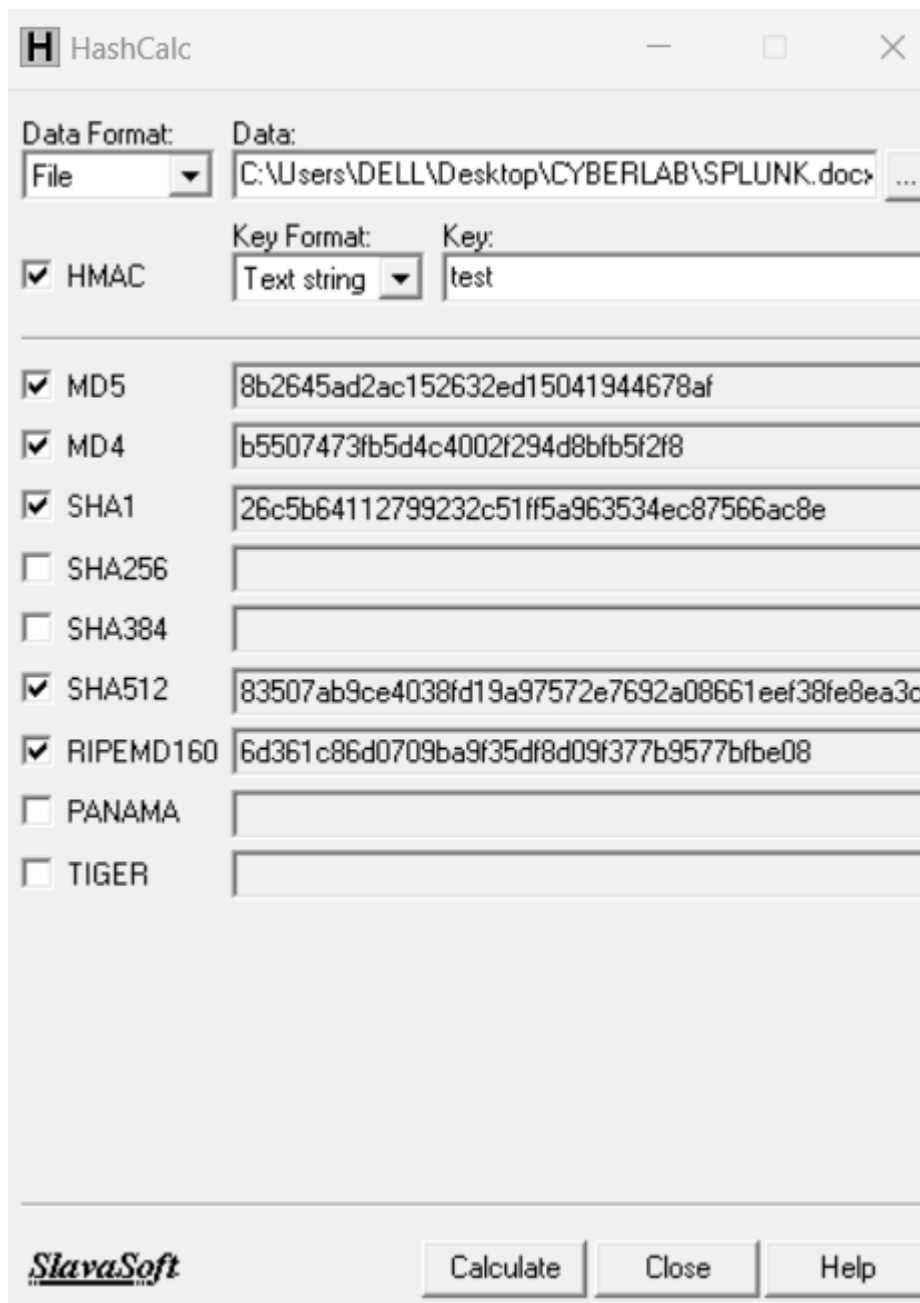
Then chose the algorithm use for calculations.



Then the hash value will be displayed for the selected file as shown in the following screenshot.

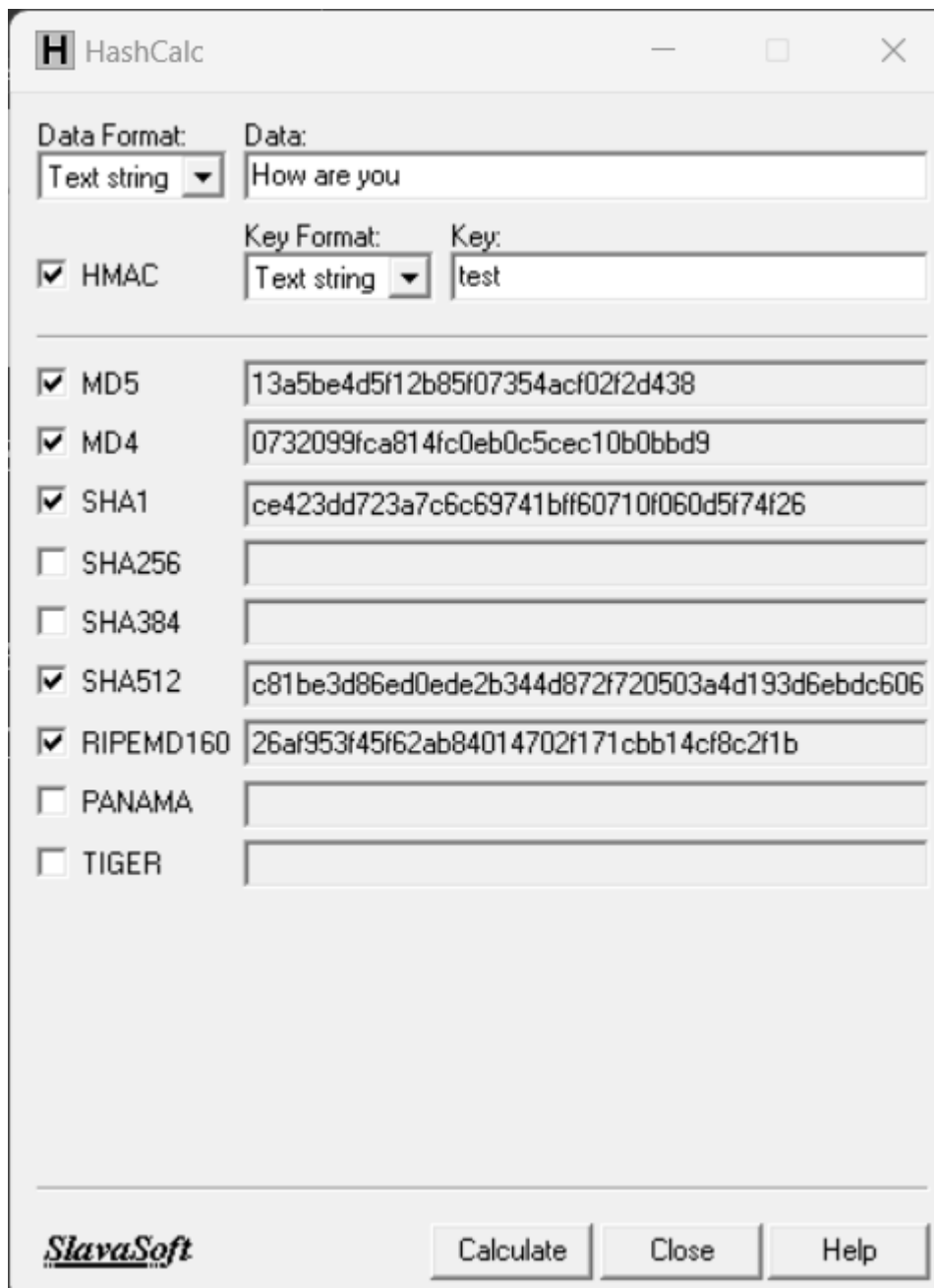


To calculate the keyed-hash message authentication code for the data:
Select key format ,key, and algorithm. Then it calculates the hashes of
the specified file and displays them



Both the windows contains MD5 hash values(with key and without key).

For calculating hash for text string, we can select data format as text string and enter the text. And then select the algorithms.



LAB-3

Generating MD5 Hashes using MD5 Calculator

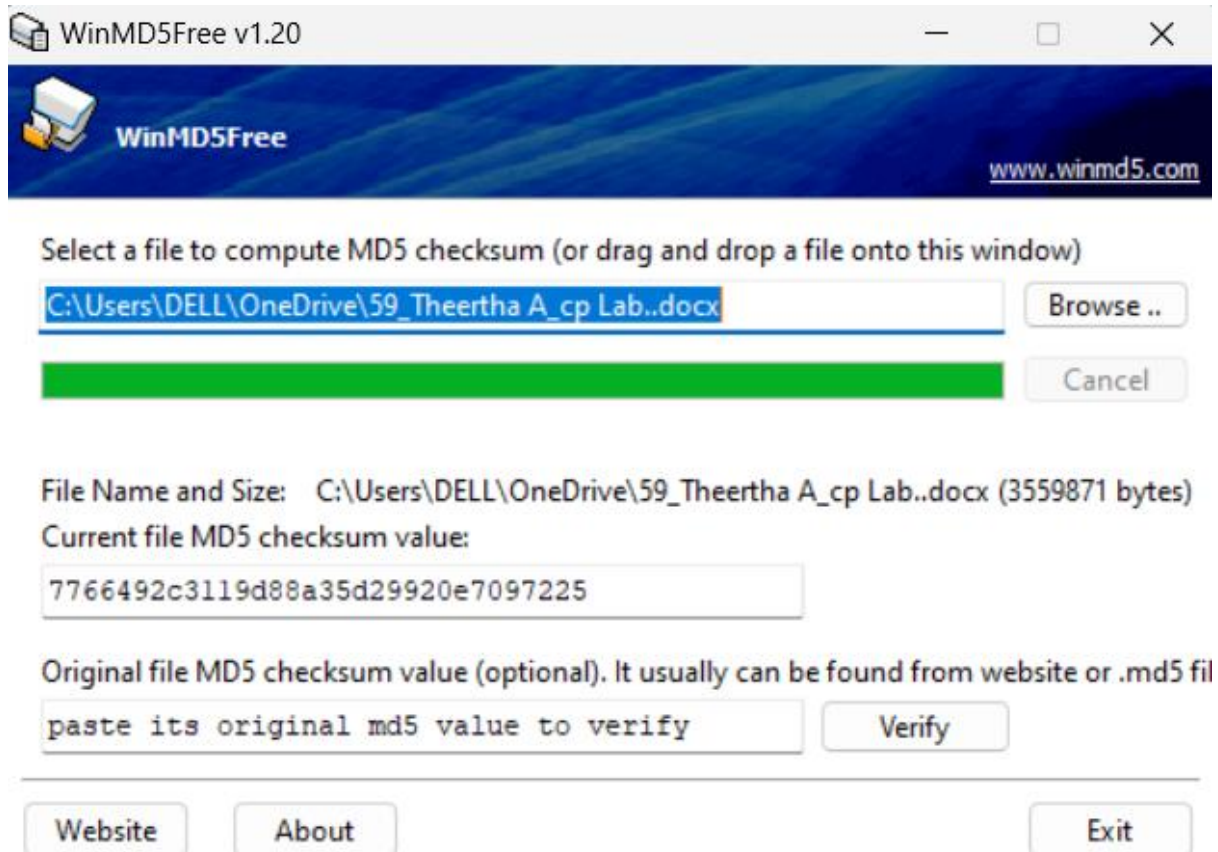
Objective:

This lab will give experience encrypting data and show you how to do it. It will teach how to:

- Use encrypting command.

- Calculate the MD5 value of selected files.

Launch the MD5 Calculator. Use the **Browse** button to choose the file want to generate an MD5 hash for. Once the file is selected, the MD5 hash will be displayed in the "MD5 Checksum" field.



LAB-4

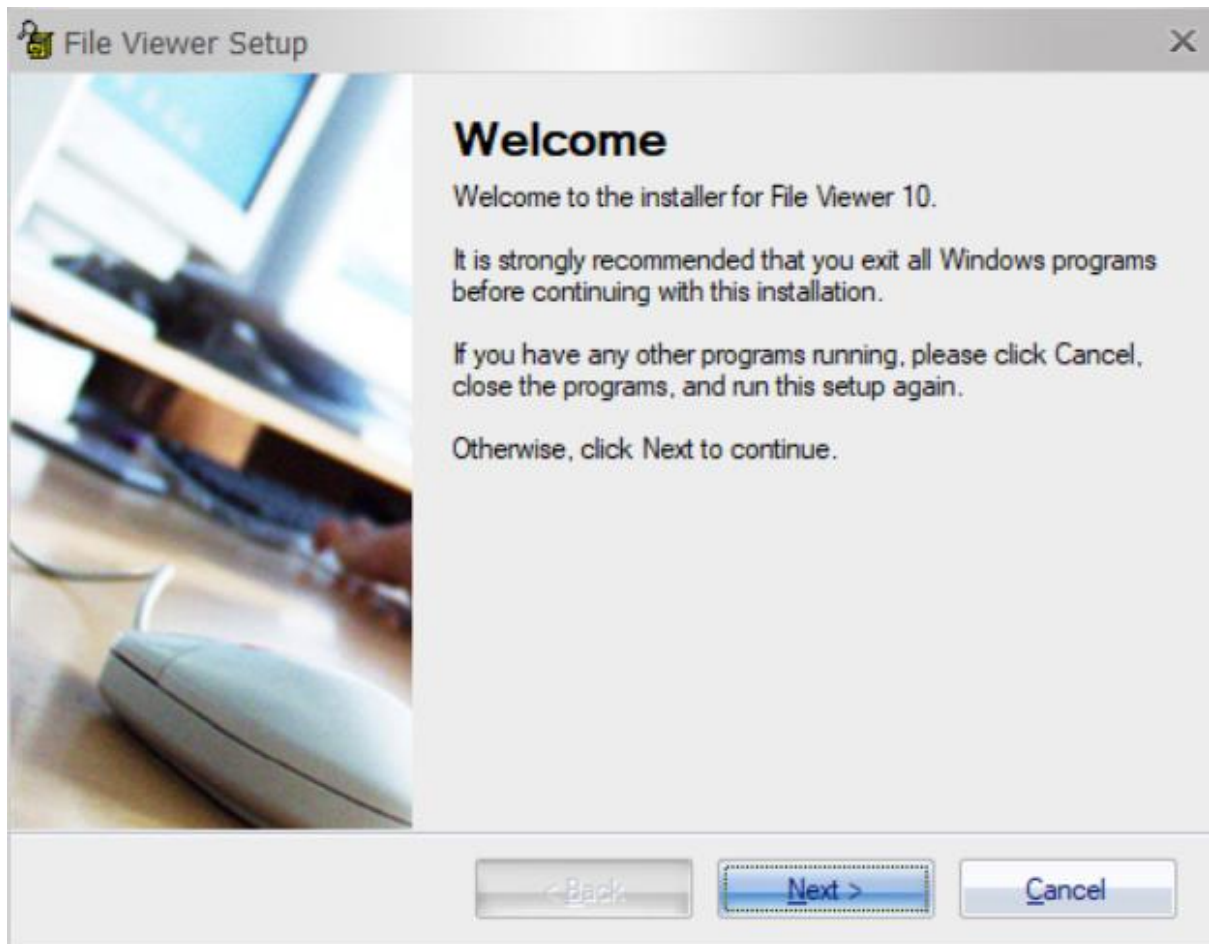
Viewing Files of various Formats using the File viewer

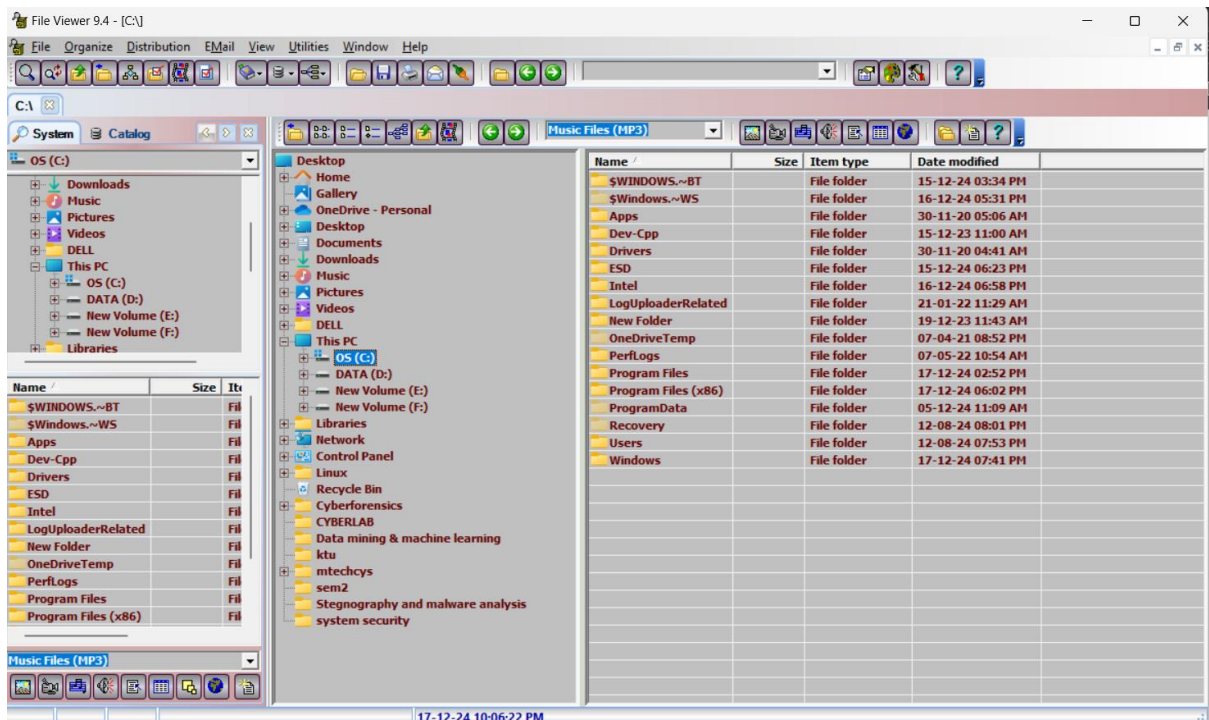
Objective:

The objective of this lab is to learn and perform file viewing with the help of file viewer. File viewer is used for:

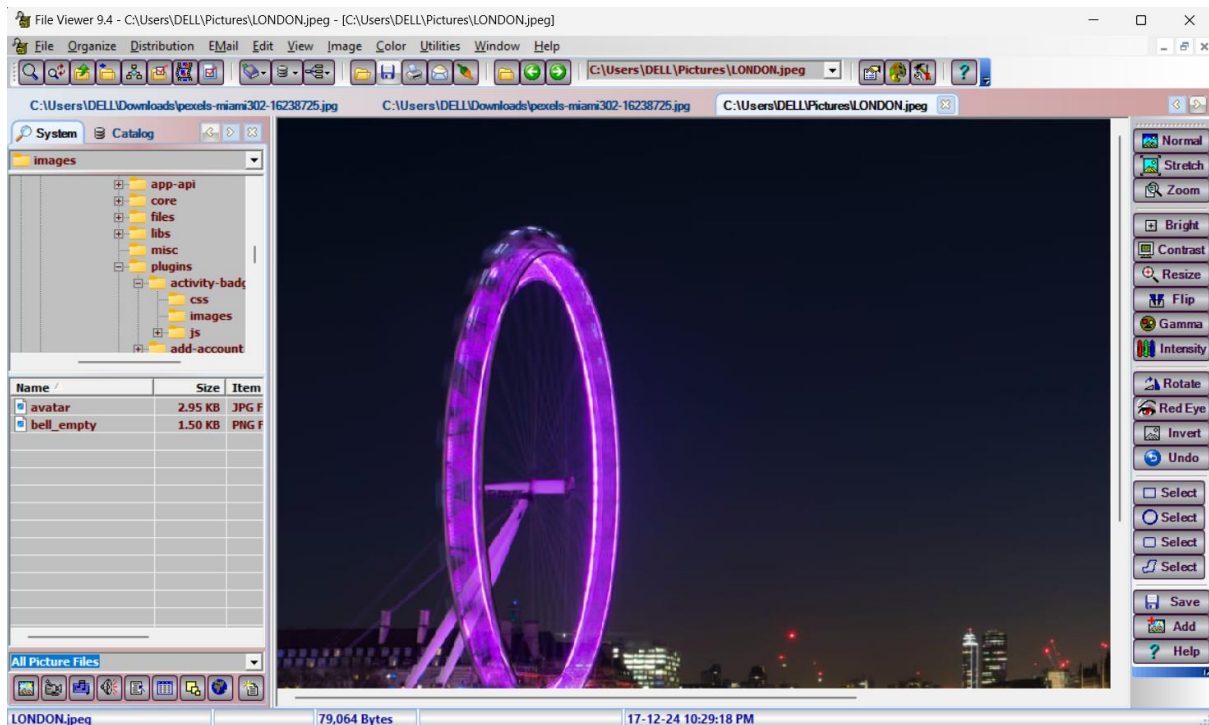
- Viewing files of various formats.
- Quickly locating the files needed.

File viewer is a disk and file utility for windows based machines that helps to quickly locate ,view, print, organize, and exchange files over the internet using windows email components.

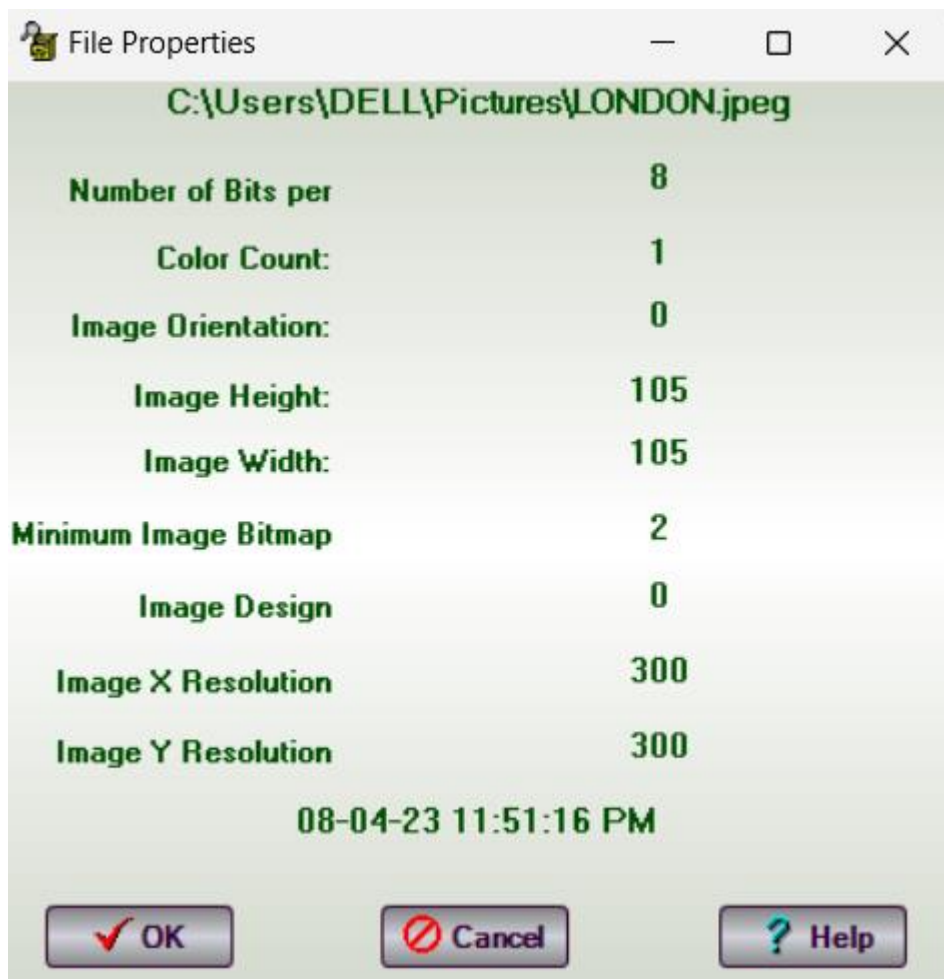




Use the "File" > "Open" option in the menu. Browse to the location of the file to view, and select it.



In file->file properties we can see the various properties of selected image.



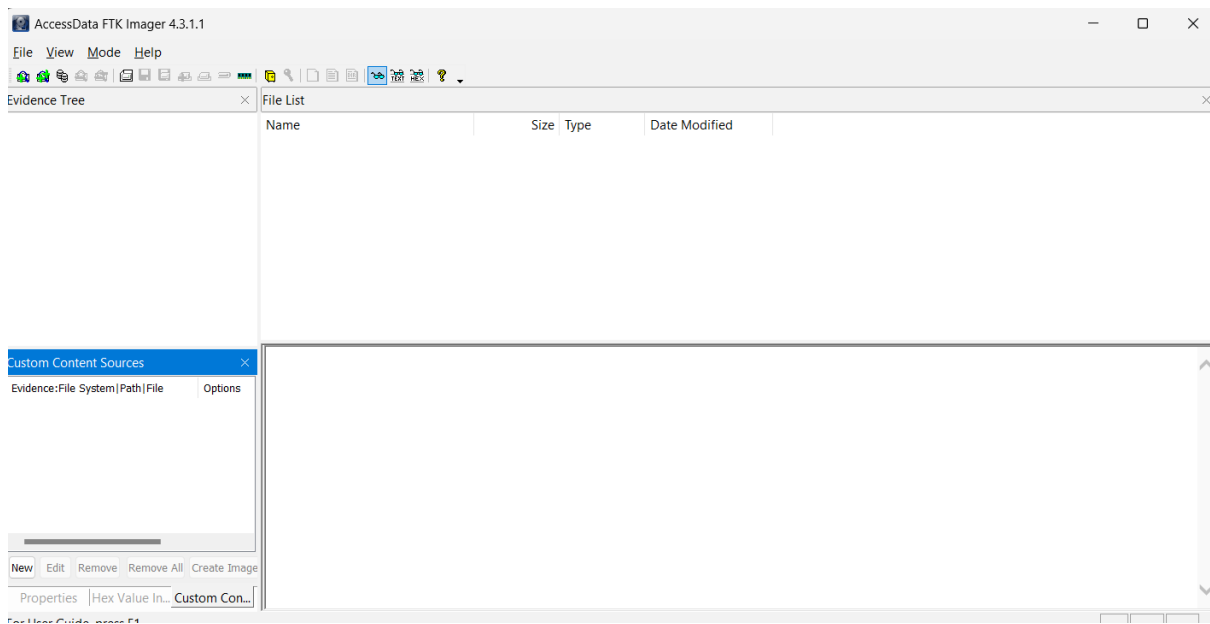
LAB-5

Handling Evidenc Data Using the FTK Imager

FTK Imager is an open-source software by AccessData that is used for creating accurate copies of the original evidence without actually making any changes to it. The Image of the original evidence is remaining the same and allows us to copy data at a much faster rate, which can be soon be preserved and can be analyzed further. The FTK imager also provides the inbuilt integrity checking function which generates a hash report which helps in matching the hash of the evidence before and after creating the image of the original Evidence.

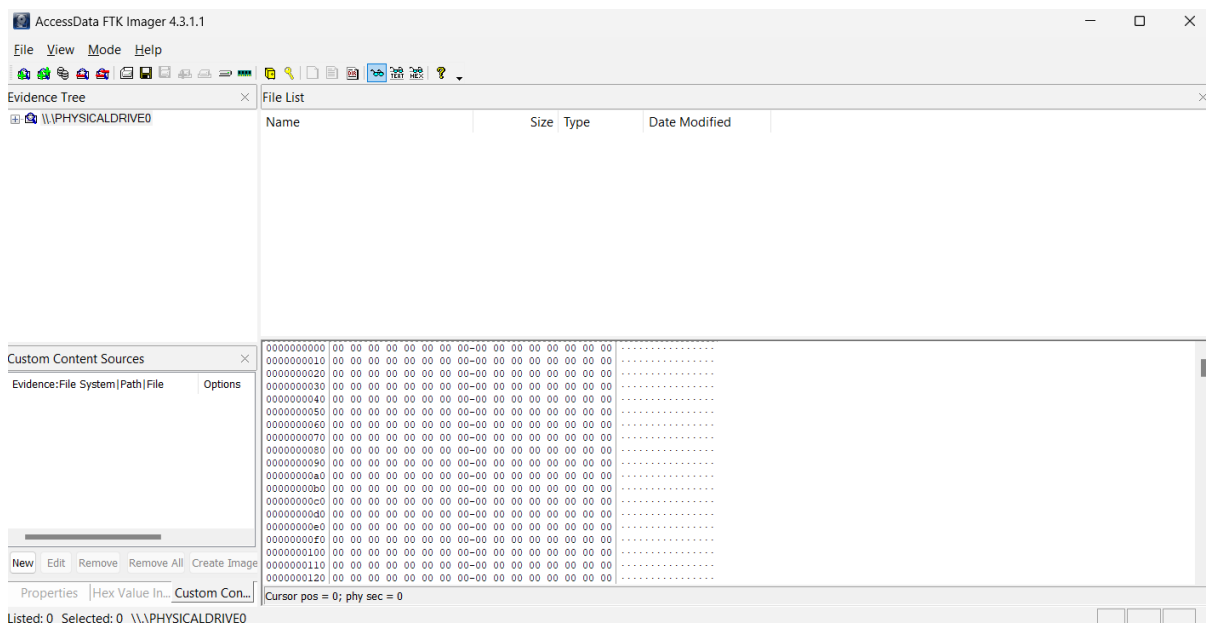
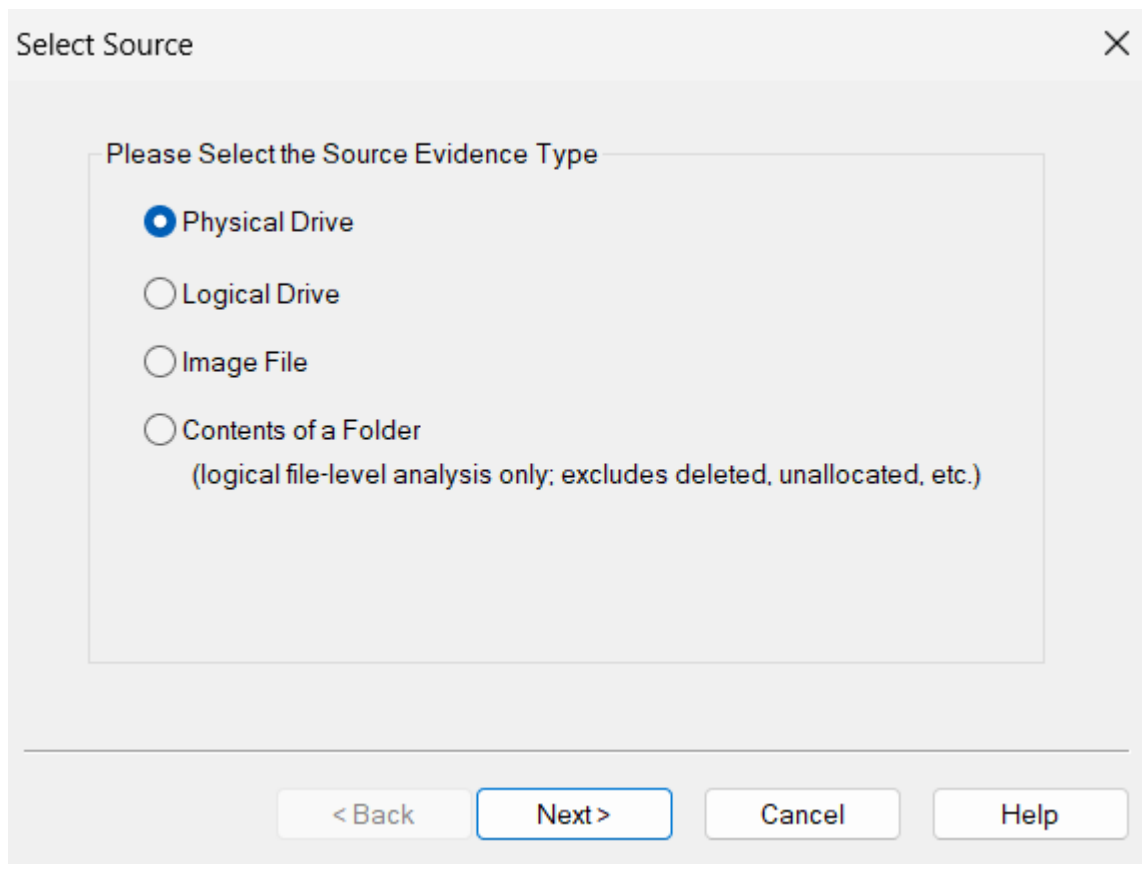


Open FTK Imager by AccessData after installing it, and we will see the window pop-up which is the first page to which this tool opens.



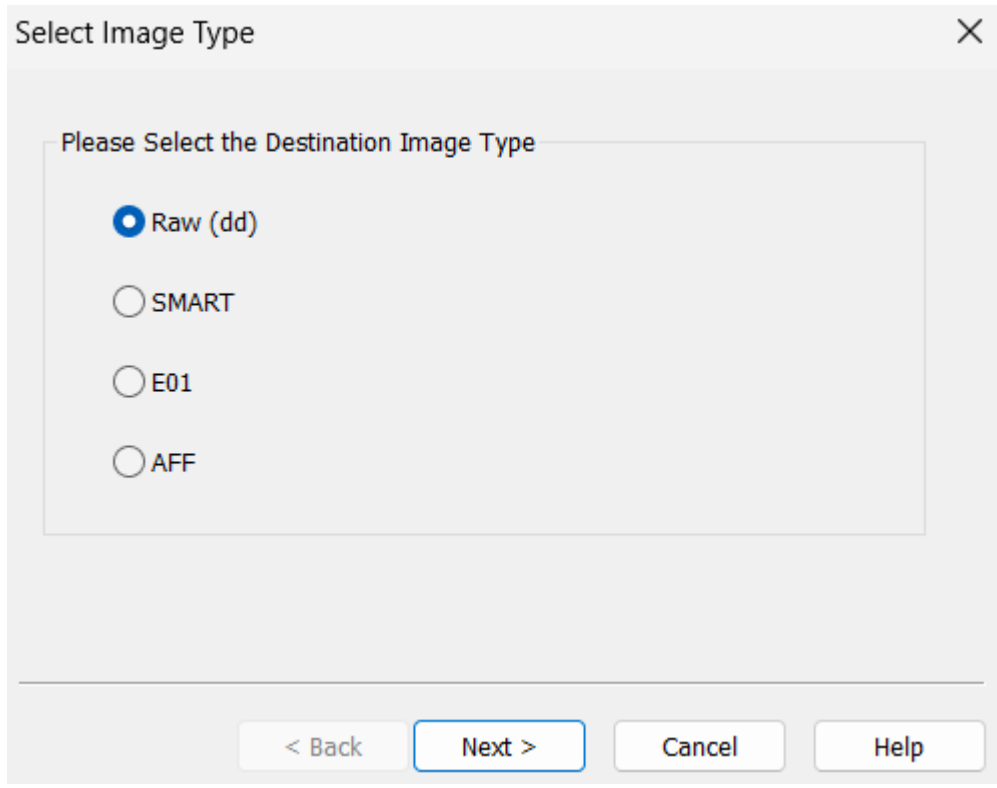
Now, to create a Disk Image. Click on File > Create Disk Image.

A Physical Drive is the primary storage hardware or the component within a device, which is used to store, retrieve, and organize data.

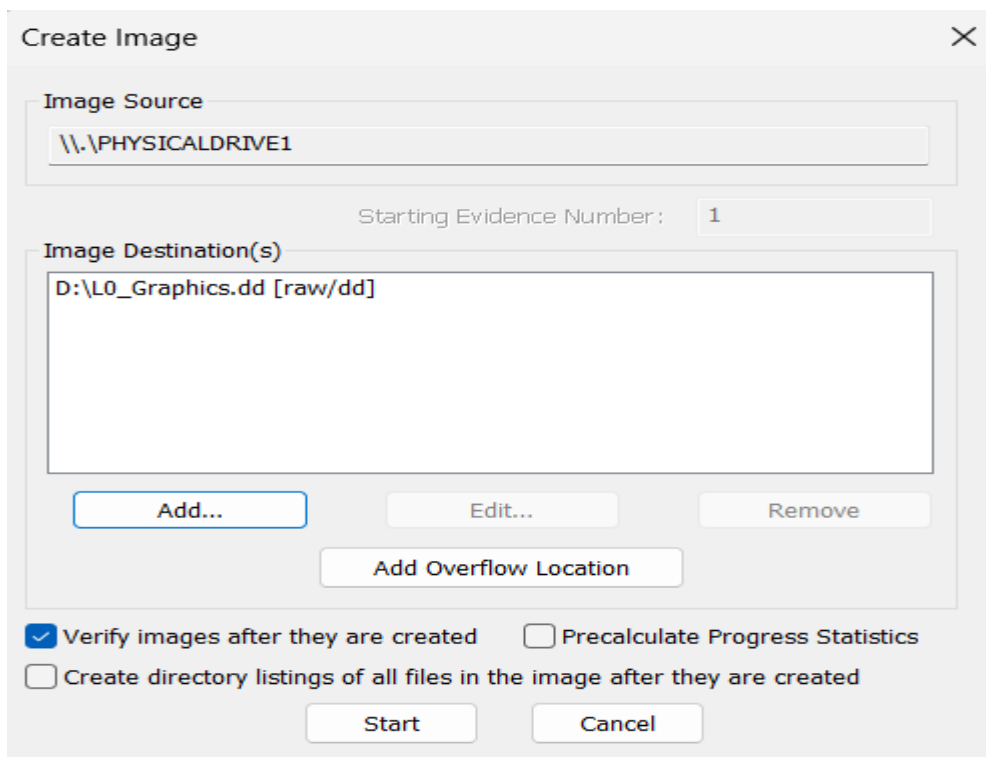


Now choose the source of drive that want to create an image copy of.

Add the Destination path of the image that is going to be created. From the forensic perspective, It should be copied in a separate hard drive and multiple copies of the original evidence should be created to prevent loss of evidence.



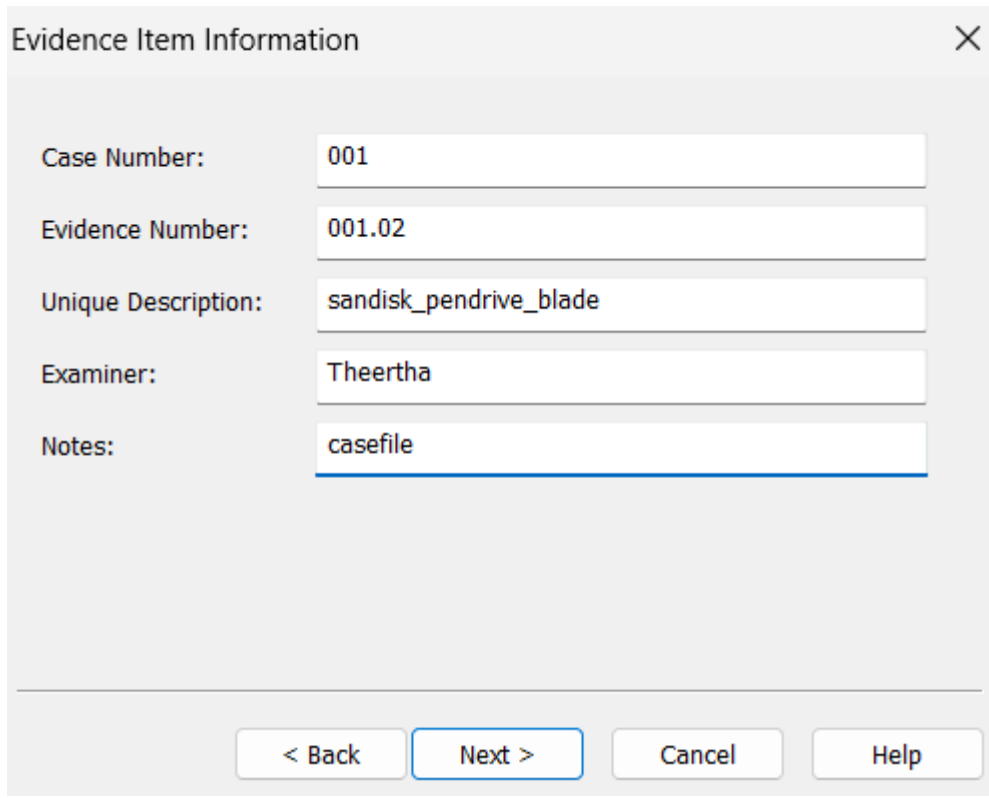
The 'Select Image Type' dialog box features a title bar with a close button (X). The main area is titled 'Please Select the Destination Image Type' and contains four radio button options: 'Raw (dd)' (selected), 'SMART', 'E01', and 'AFF'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.



The 'Create Image' dialog box has a title bar with a close button (X). It contains several fields and options: 'Image Source' with the text '\\.\PHYSICALDRIVE1', 'Starting Evidence Number' with the value '1', and 'Image Destination(s)' with the text 'D:\L0_Graphics.dd [raw/dd]'. Below these are three buttons: 'Add...', 'Edit...', and 'Remove'. A fourth button, 'Add Overflow Location', is positioned below the 'Image Destination(s)' list. At the bottom, there are two checked checkboxes: 'Verify images after they are created' and 'Create directory listings of all files in the image after they are created'. There are also two unchecked checkboxes: 'Precalculate Progress Statistics' and 'Start'. The 'Start' and 'Cancel' buttons are at the very bottom.

Raw(dd): It is a bit-by-bit copy of the original evidence which is created without any additions and or deletions. They do not contain any metadata.

Now, add the details of the image to proceed.

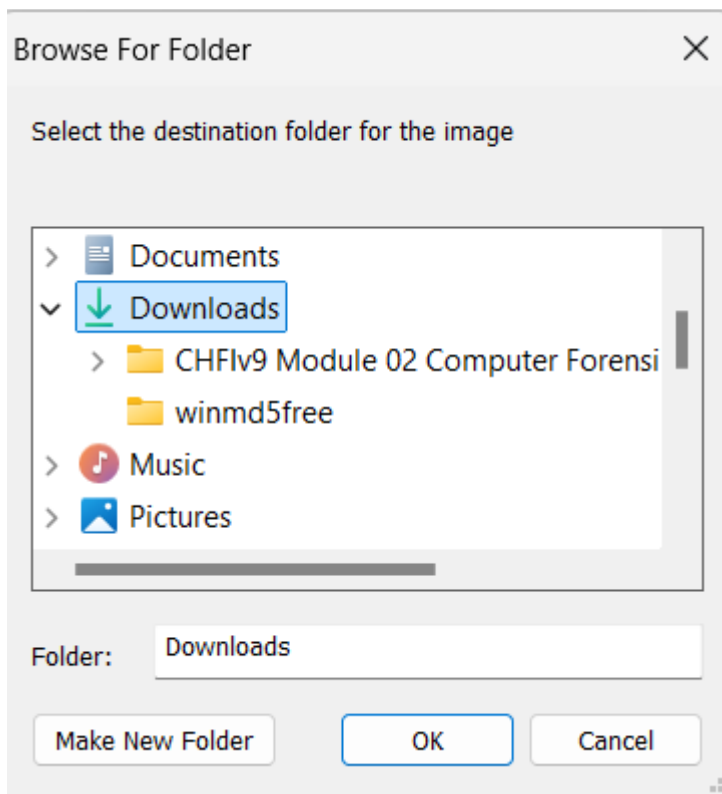


The 'Evidence Item Information' dialog box contains the following fields and values:

Field	Value
Case Number:	001
Evidence Number:	001.02
Unique Description:	sandisk_pendrive_blade
Examiner:	Theertha
Notes:	casefile

At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Now finally add the destination of the image file, name the image file and then click on Finish.



The 'Browse For Folder' dialog box shows the following structure:

- Select the destination folder for the image
- Folder list:
 - > Documents
 - ▼ Downloads (selected)
 - > CHFlv9 Module 02 Computer Forensi
 - > winmd5free
 - > Music
 - > Pictures
- Folder: Downloads
- Buttons: Make New Folder, OK, Cancel

Select Image Destination ✕

Image Destination Folder
C:\Users\DELL\Downloads\L0_Graphic.dd Browse

Image Filename (Excluding Extension)
L0_Graphic.dd

Image Fragment Size (MB) 4500
For Raw, E01, and AFF formats: 0 = do not fragment

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

Use AD Encryption ☐

< Back Finish Cancel Help

Once added the destination path, we can now start with the Imaging and also click on the verify option to generate a hash.

Create Image

×

Image Source

\\.\PHYSICALDRIVE1

Starting Evidence Number :

1

Image Destination(s)

D:\L0_Graphics.dd [raw/dd]

Add...

Edit...

Remove

Add Overflow Location

☒ Verify images after they are created

☐ Precalculate Progress Statistics

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

Start

Cancel

Creating Image...

—

□

×

Image Source:

\\.\PHYSICALDRIVE1

Destination:

D:\L0_Graphics.dd

Status:

Image created successfully

Progress

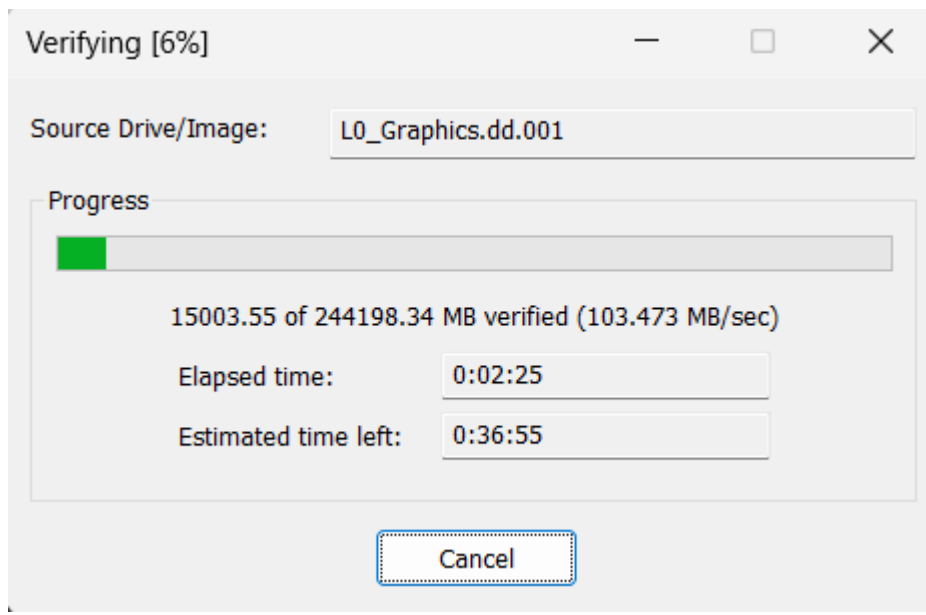
Elapsed time:

0:40:27

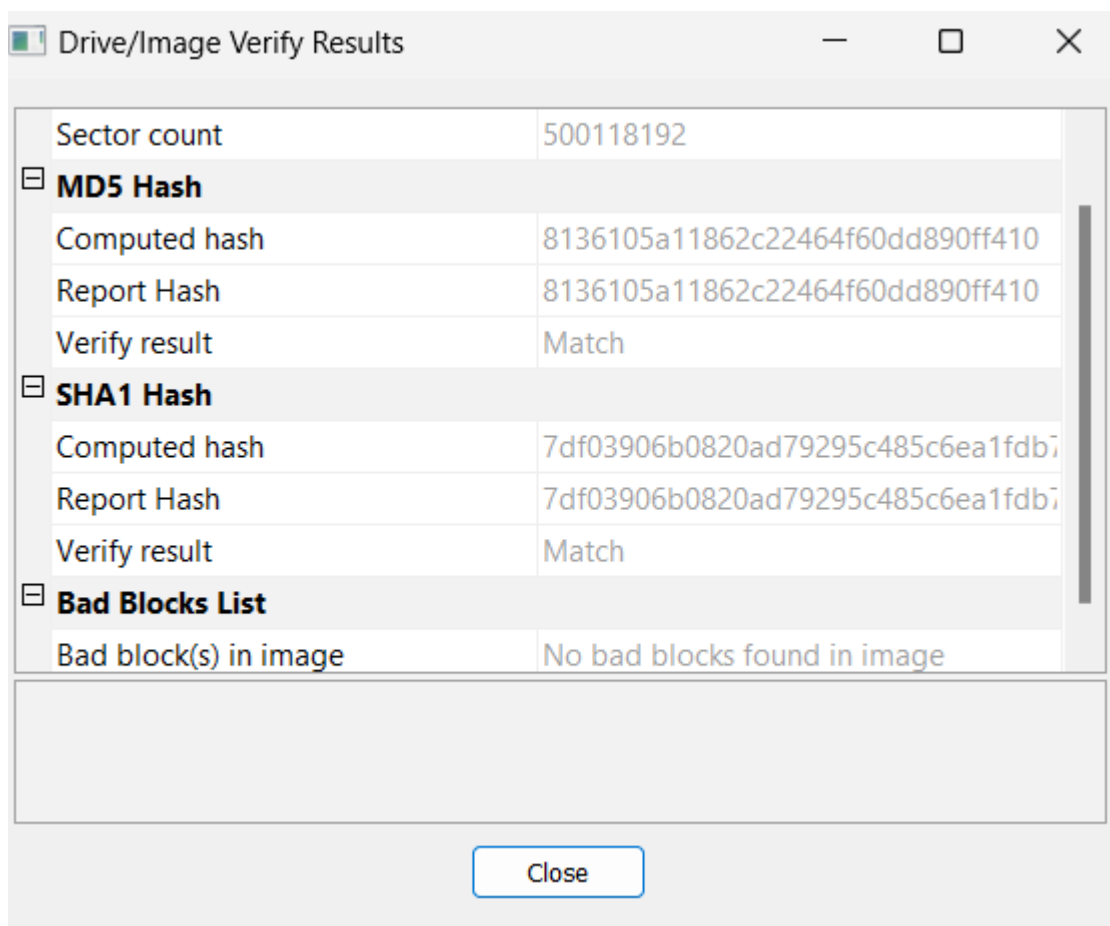
Estimated time left:

Image Summary...

Close



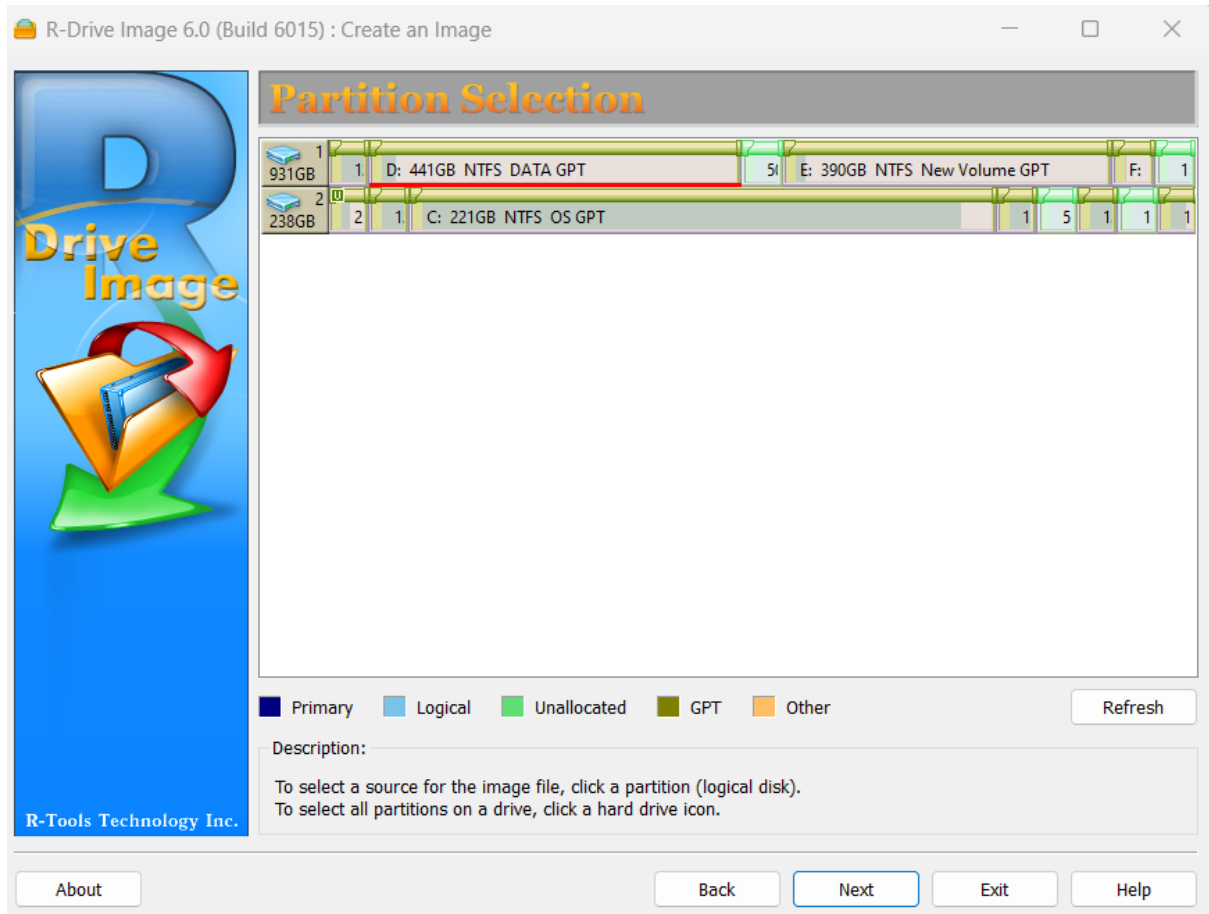
After the image is created, a Hash result is generated which verifies the MD5 Hash, SHA1 Hash, and the presence of any bad sector.



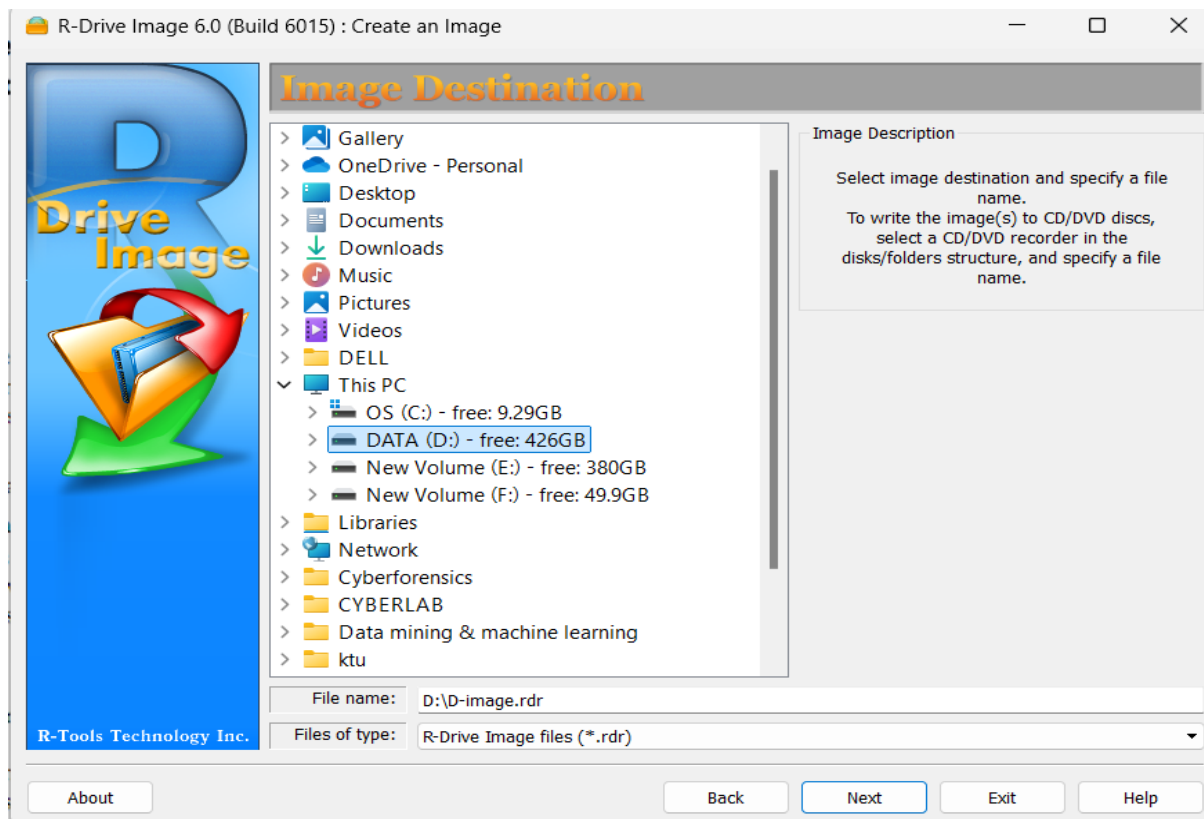
LAB-6

Creating a Disk Image File of a Hard Disk Partition Using the R-drive Image

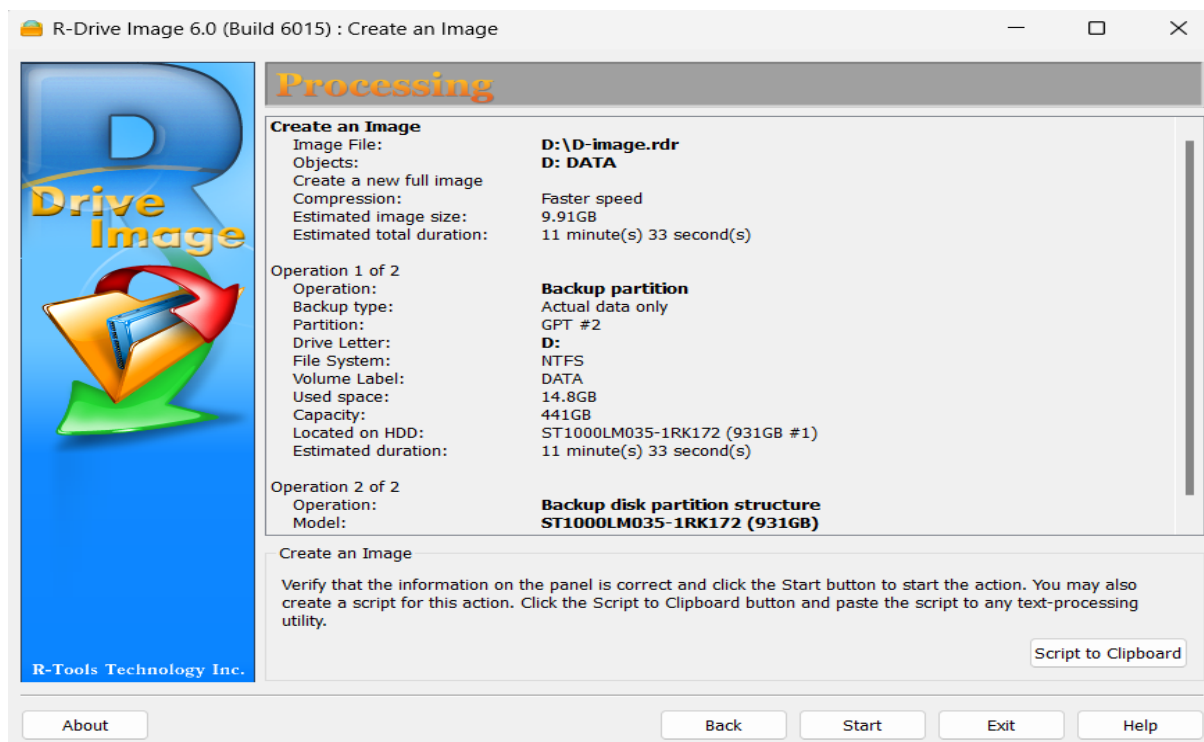
Launch the software. On the main menu, click on "Create an Image".



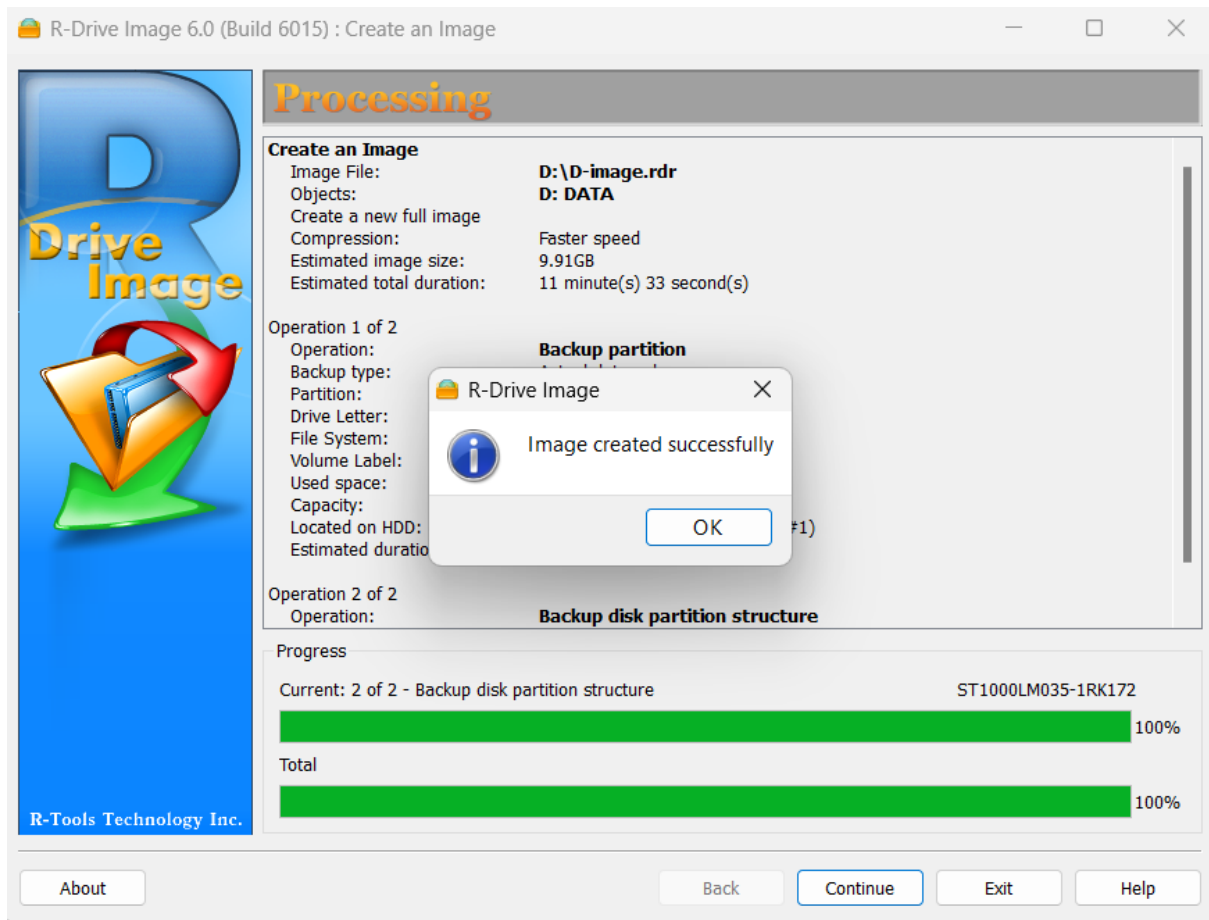
Choose the hard disk or specific partition you want to image. Specify where to save the image file. This can be on another partition, an external drive, or network location. Assign a name to the image file. Click Next.



Choose the level of compression for the image file (None, Normal, or High). Higher compression reduces file size but takes more time.



click Start to begin creating the disk image. Wait for the process to complete. The time taken depends on the size of the partition and the level of compression chosen.



After the image is created, click continue then that folder will be visible.

