Digital Forensics Lab Report

Name: KARTHIKEYAN G

Roll Number: **CB.SC.P2.CYS24008**

Digital Forensics Lab

Lab – 1

Objective

The objective of this lab is to provide an overview of the tools used in the forensic investigation process. This includes knowledge of the following tasks:

- Recovering deleted files from the evidence.
- Generating hashes and checksum files.
- Calculating the MD5 value of the selected file.
- Viewing files of various formats.
- Handling evidence data.
- Creating a disk image file of a hard disk partition.

Recovering Data using the EaseUS Data Recovery Wizard

Step 1: Installation

Install the *EaseUS Data Recovery Wizard*.

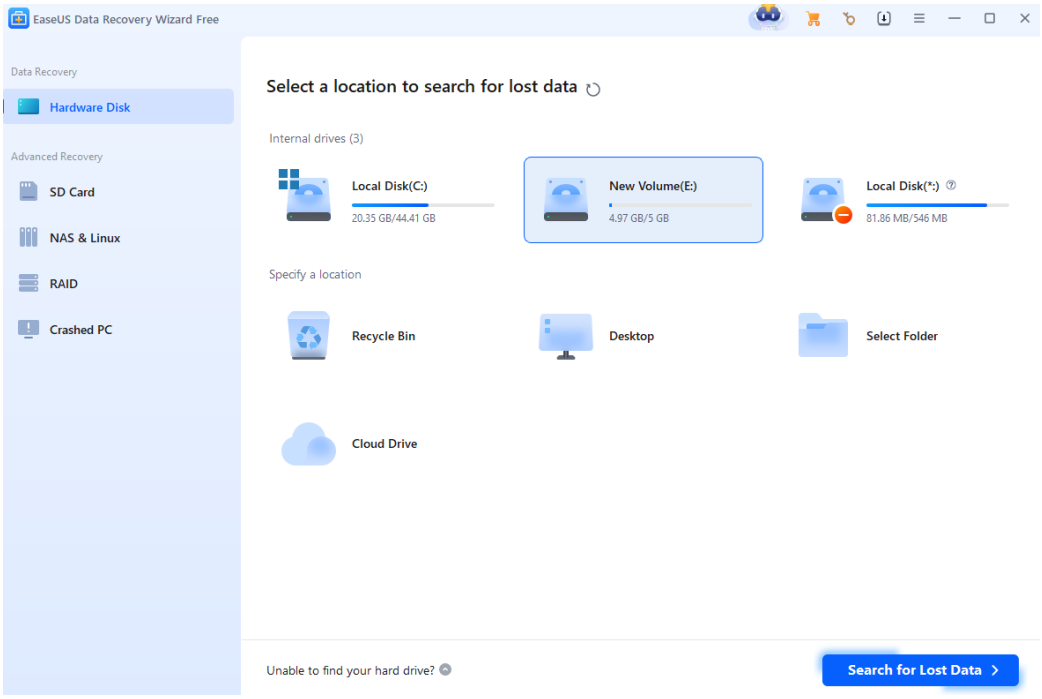

Figure 1: EaseUS Installation

Step 3: Recovery

The deleted files were found.

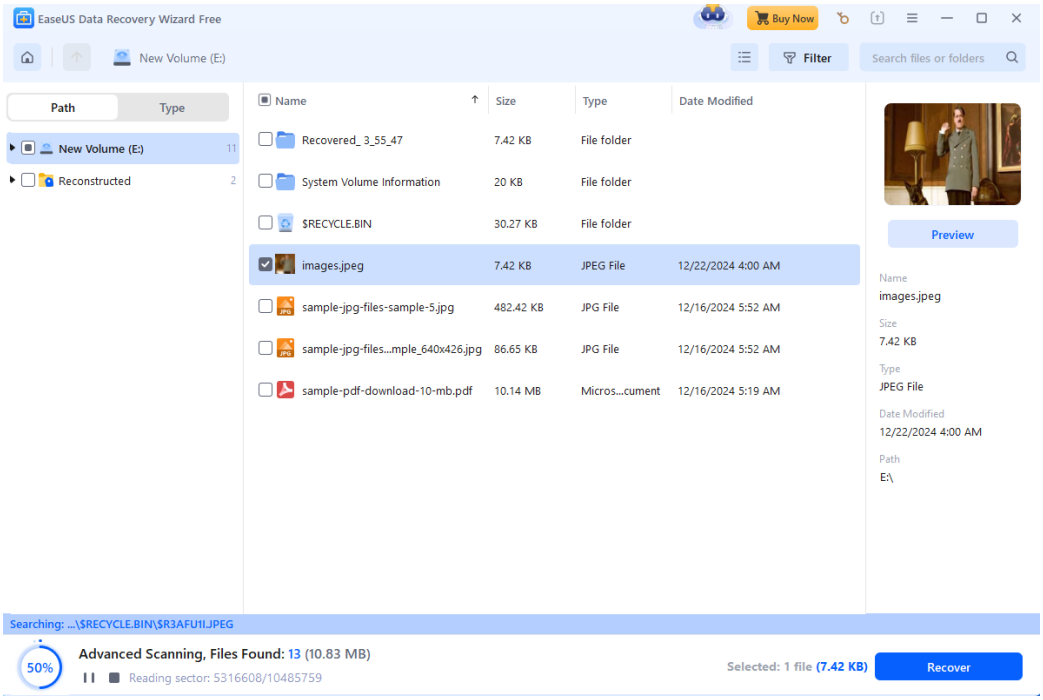

Figure 2: Deleted files found during the scan

Successfully recovered the deleted image.

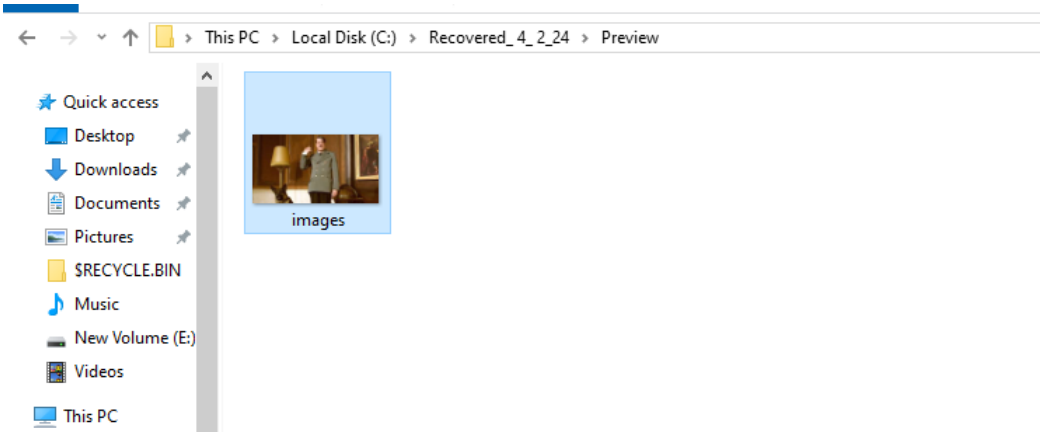

Figure 3: Recovered image

Performing Hash, Checksum, or HMAC Calculations Using HashCalc

Step 1: Installation

Install *HashCalc*.

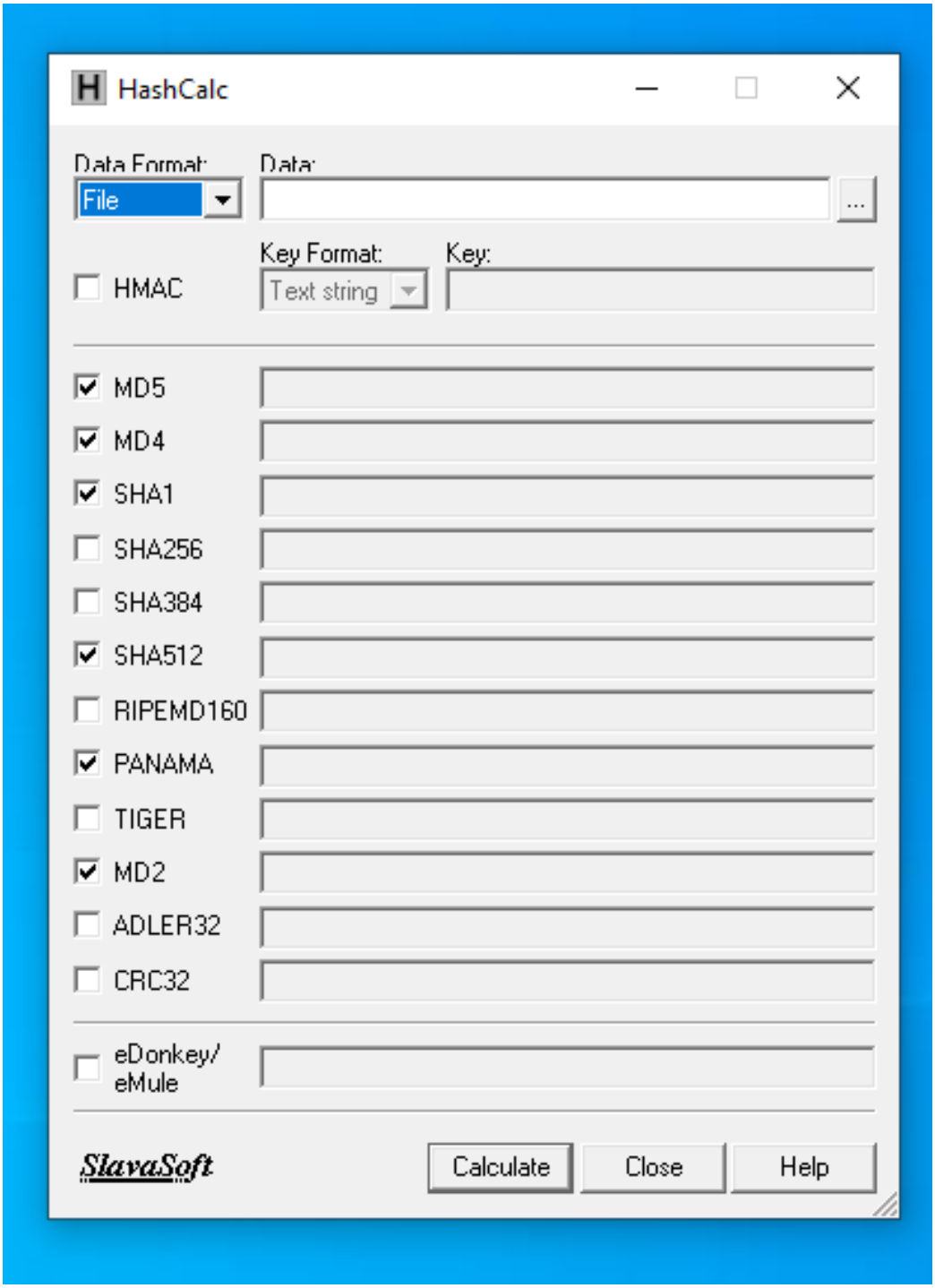

Figure 4: HashCalc Installation

Step 2: Hash Calculations

Use the recovered image from the previous step as the evidence file. Calculate its hash values.

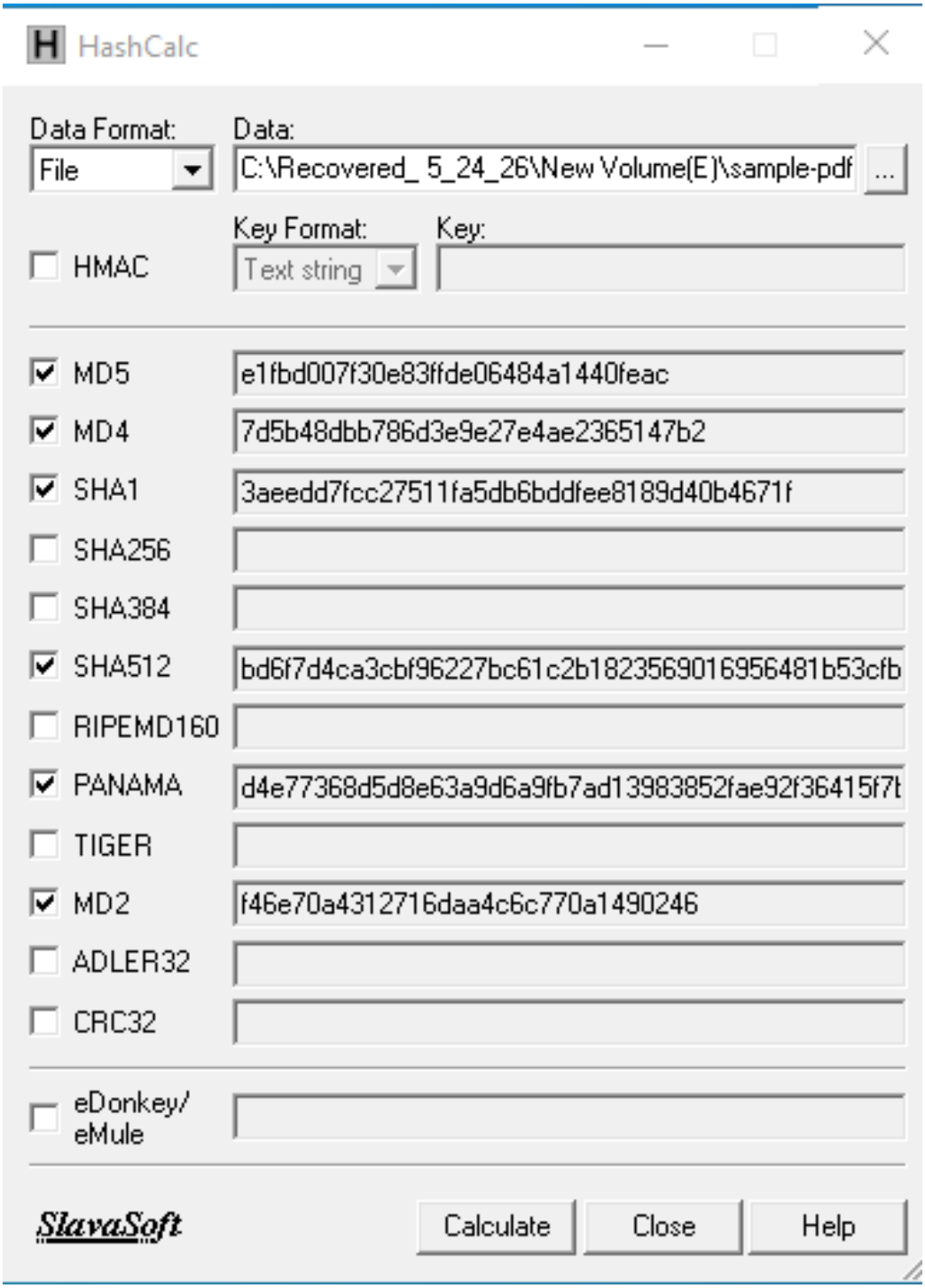

Figure 5: Calculated hash values

Step 3: HMAC Calculation

Calculate a keyed-Hash Message Authentication Code (HMAC) for the image.

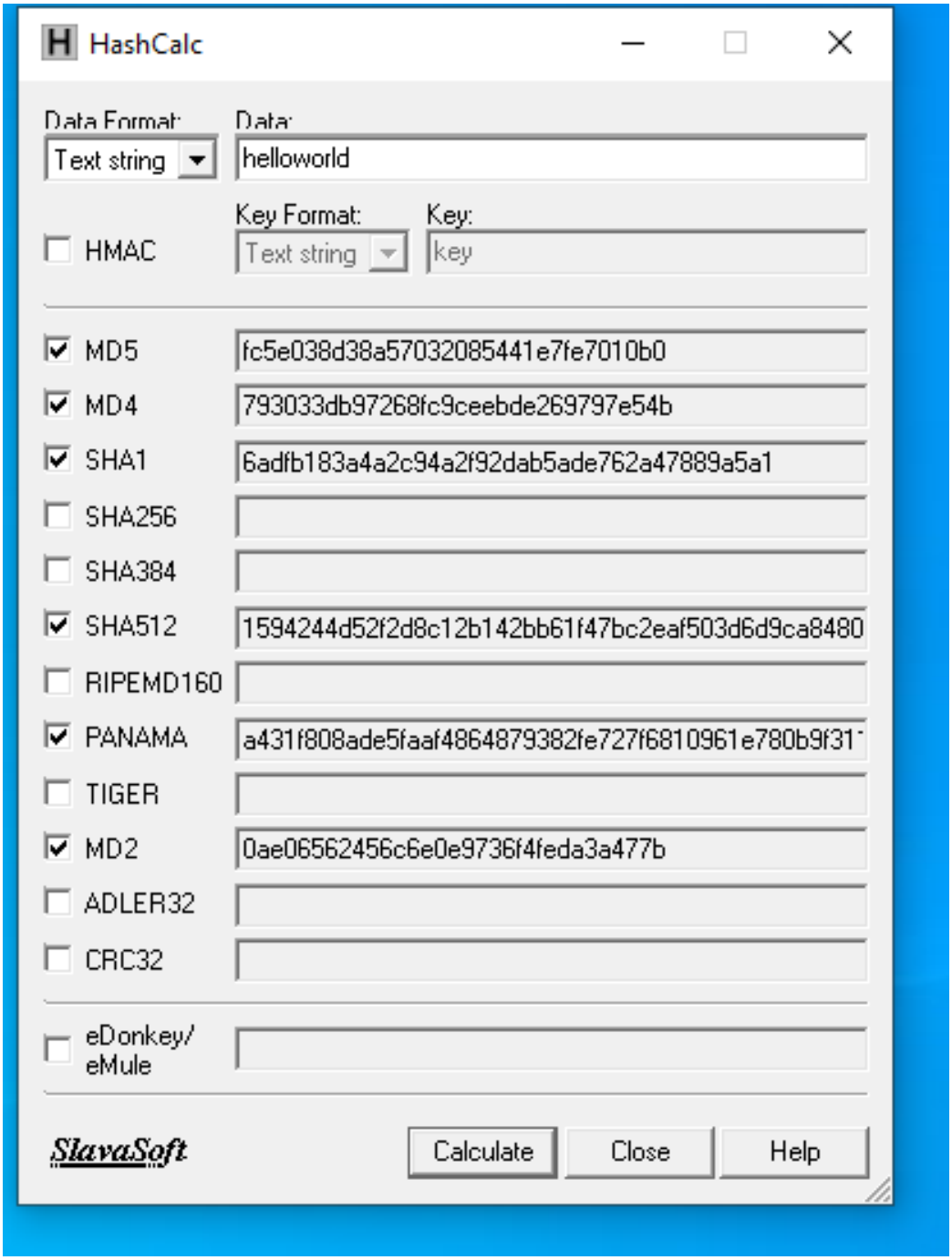

Figure 6: HMAC values calculated for the evidence

Step 4: String Hashing

Calculate the hash value for a string.

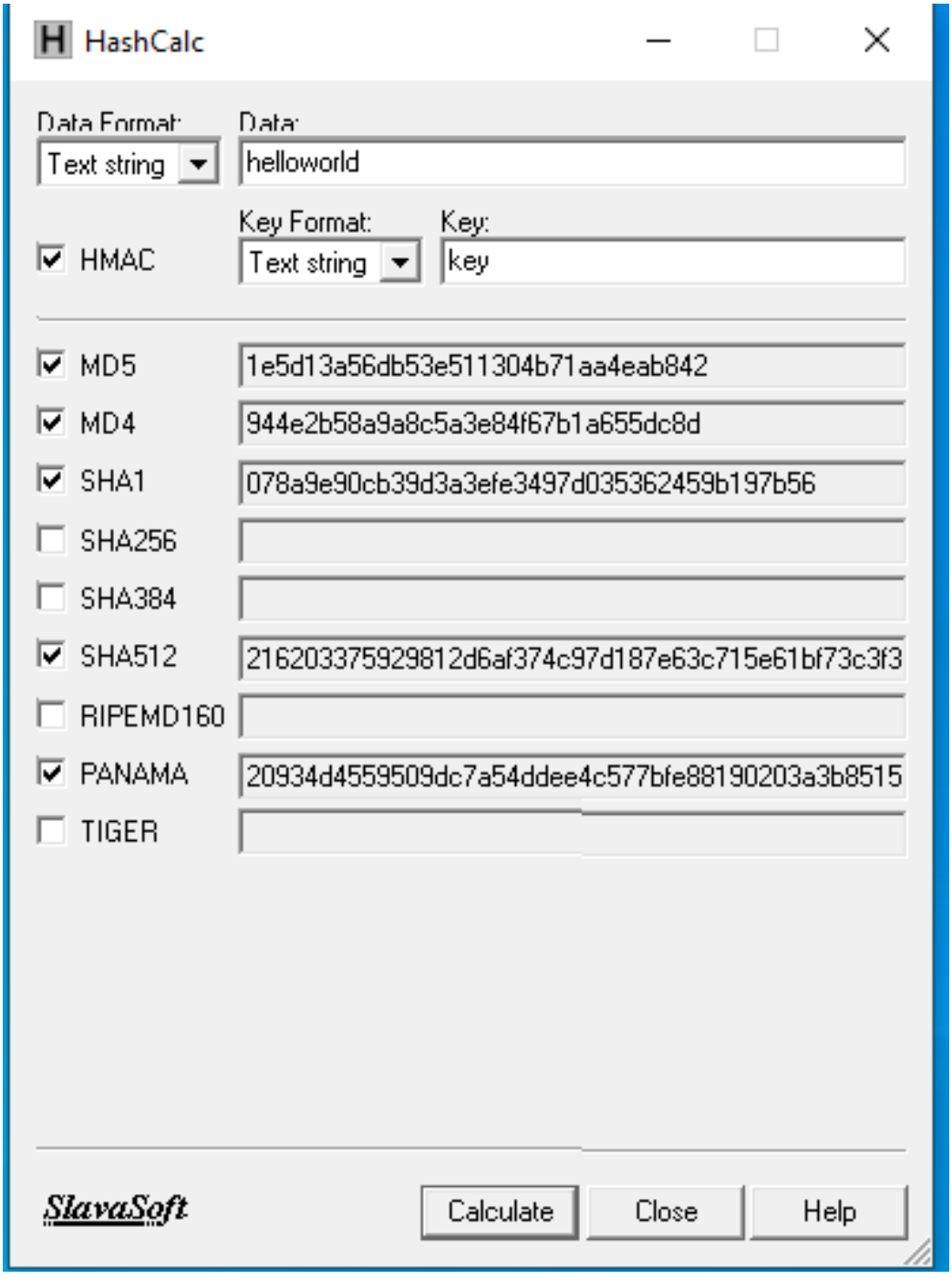

Figure 7: String hash values

Generating MD5 Hashes Using MD5 Calculator

Step 1: Installation

Install the *MD5 Calculator*.

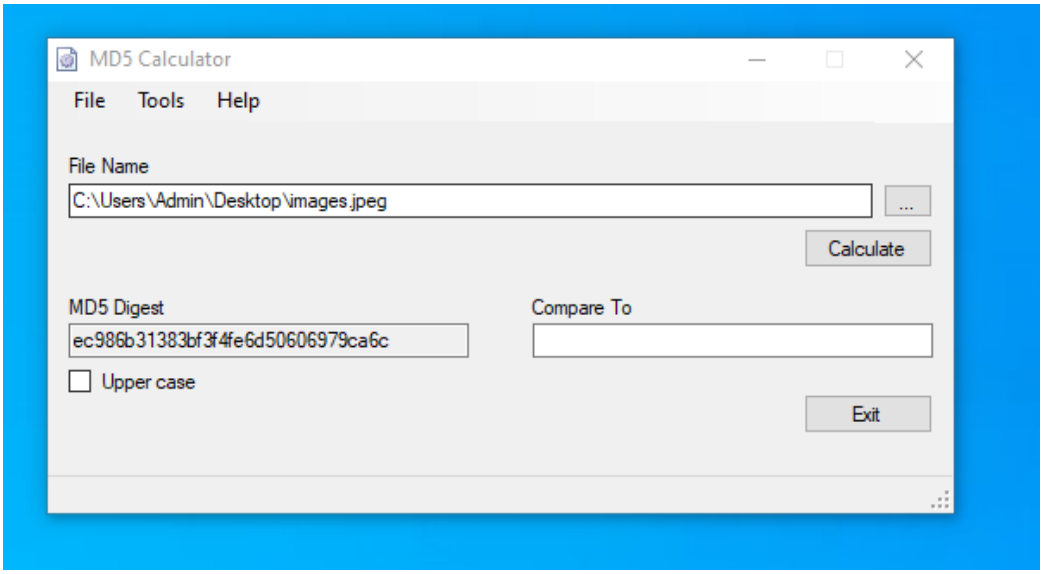

Figure 8: MD5 Calculator Installation

Step 2: MD5 Digest

Open the evidence image file and calculate the MD5 Digest.

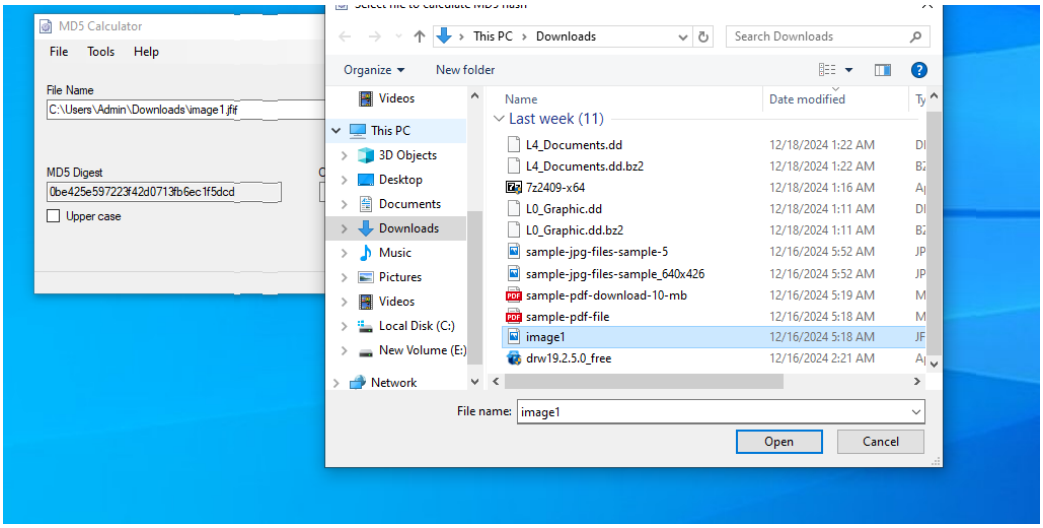

Figure 9: MD5 Digest for the evidence image

Viewing Files of Various Formats Using File Viewer

Step 1: Installation

Install the *File Viewer*.

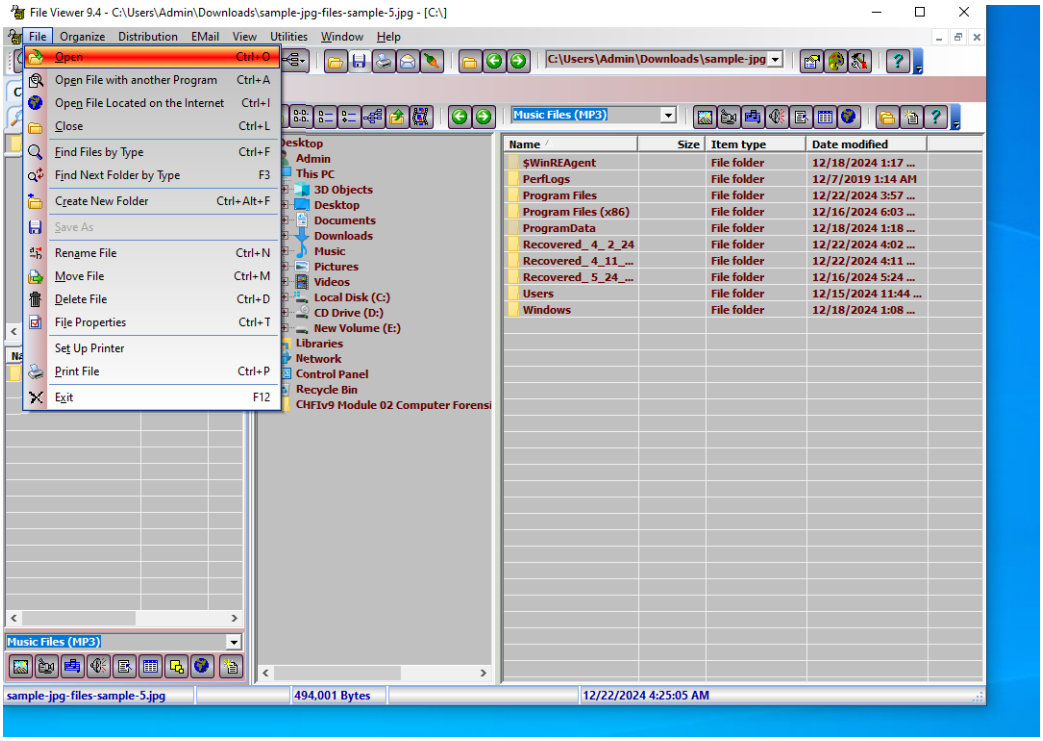

Figure 10: File Viewer Installation

Step 2: Viewing Files

Open the evidence image file and view its properties.

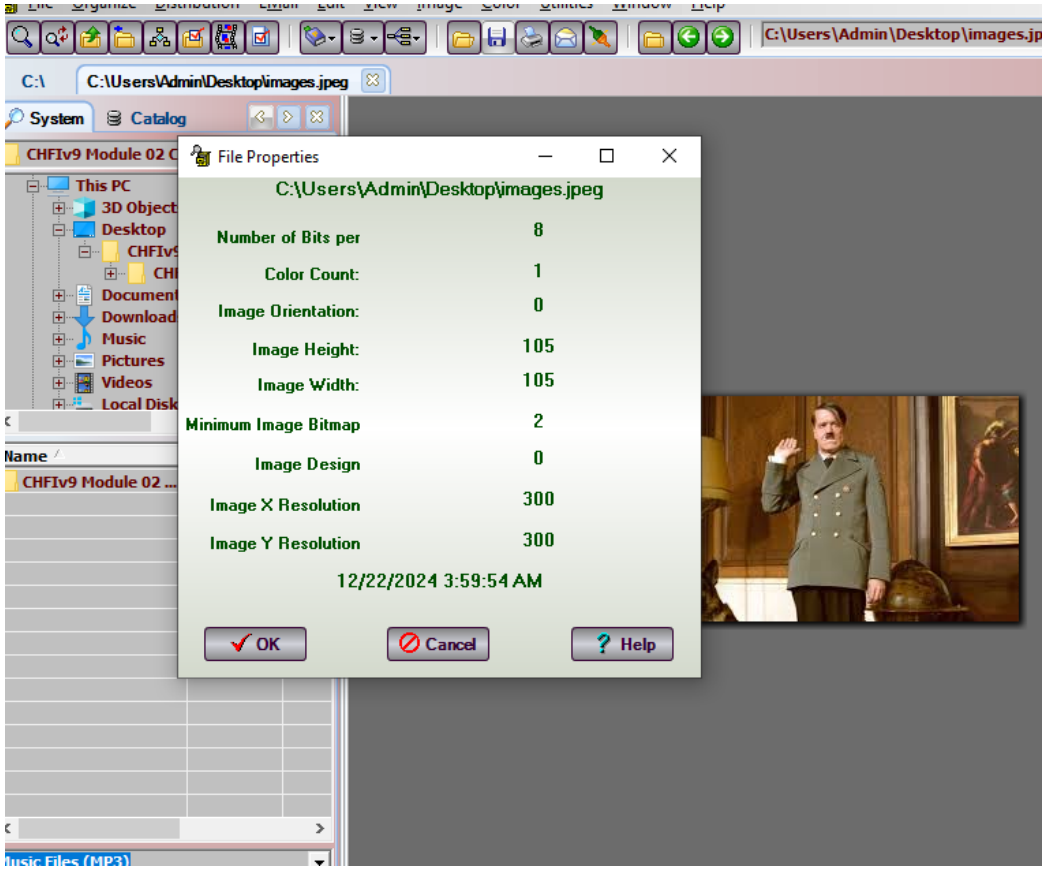

Figure 11: Viewing properties of the evidence image

Handling Evidence Data Using FTK

Step 1: Installation

Install *FTK*.

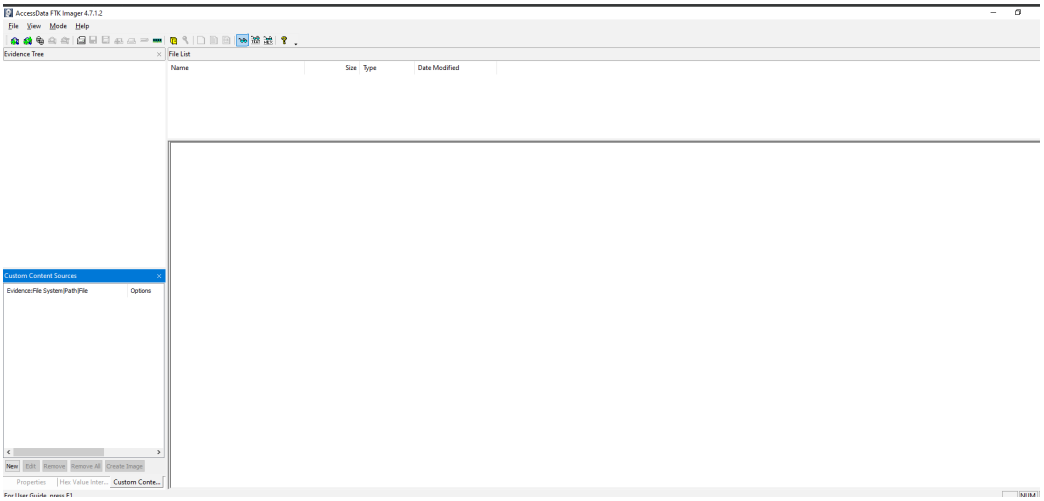

Figure 12: FTK Installation

Step 2: Creating a Case

Create a new case. (Continuation pending due to a missing evidence file.)

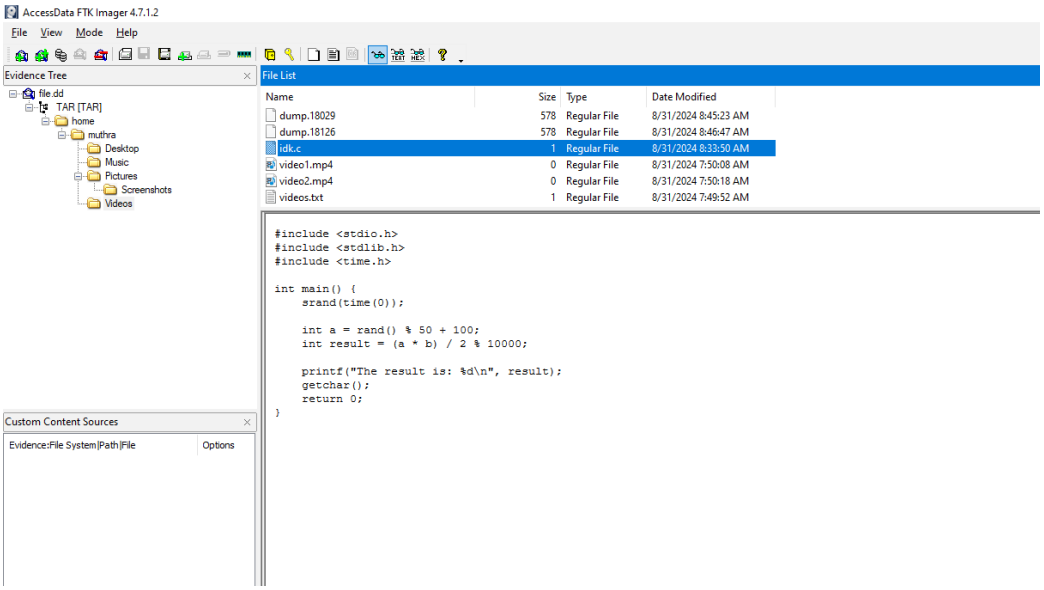

Figure 13: Creating a new case in FTK

Creating a Disk Image File Using R-Drive Image

Step 1: Installation

Install *R-Drive Image*.

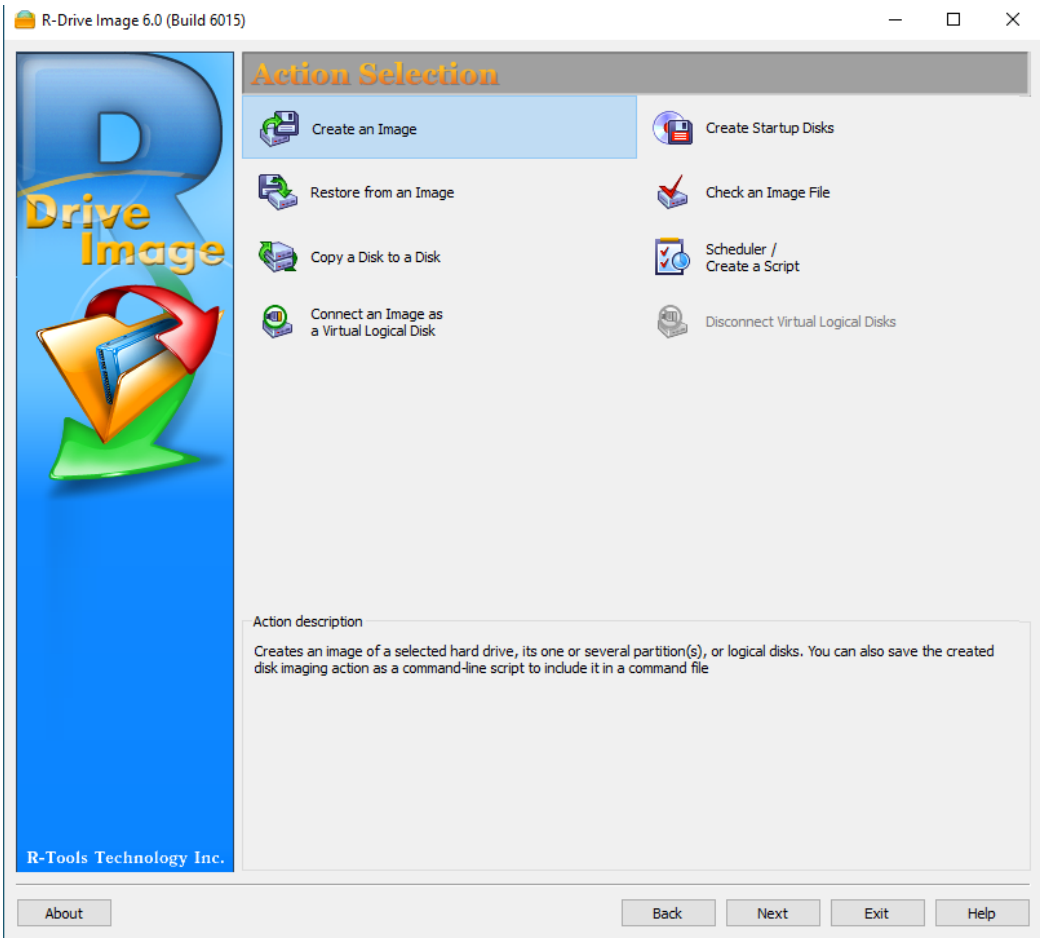

Figure 14: R-Drive Image Installation

Step 2: Selecting the Source Drive

Launch the R-Drive Image application. Select the E drive as the source drive for imaging.

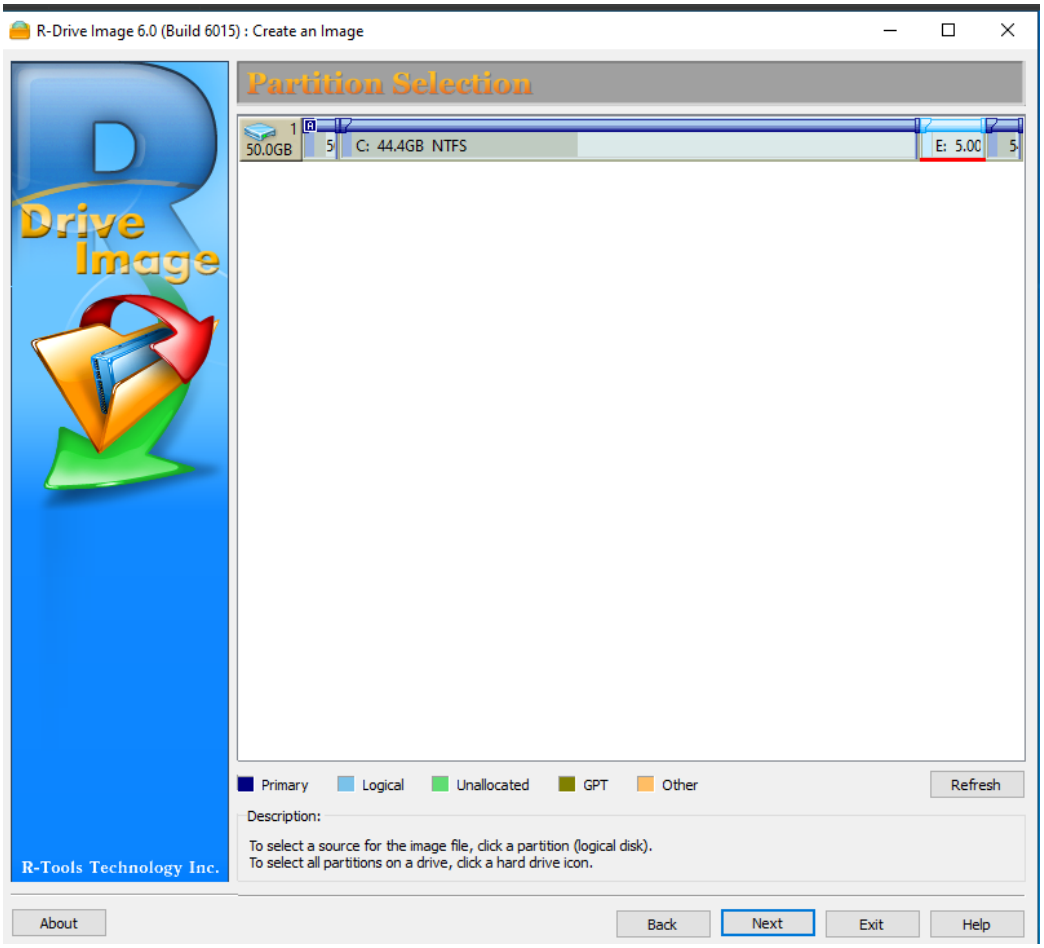

Figure 15: Selecting the E drive as the source

Step 3: Configuring Image Settings

Specify the location to save the disk image file. Choose the desired compression level and partition settings.

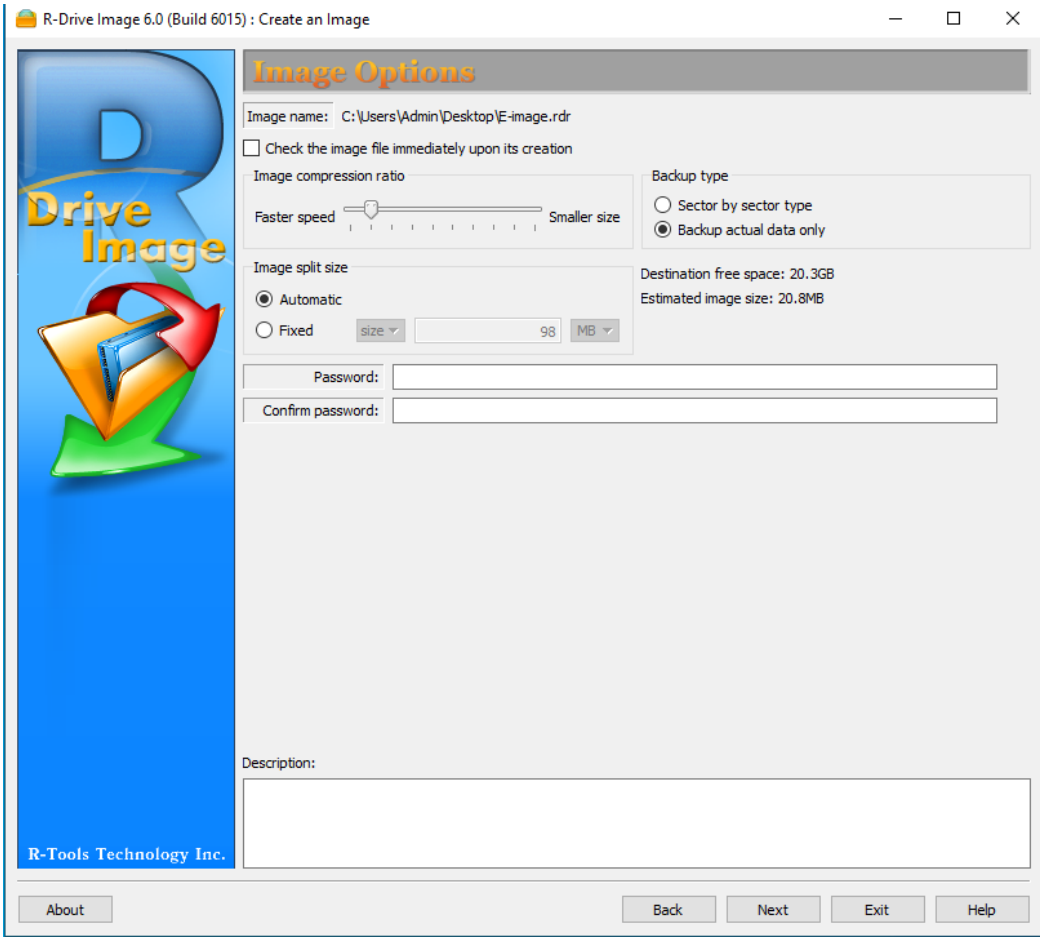

Figure 16: Configuring disk image settings

Step 4: Starting the Imaging Process

Review the settings and start the disk imaging process. Monitor the progress through the status bar.

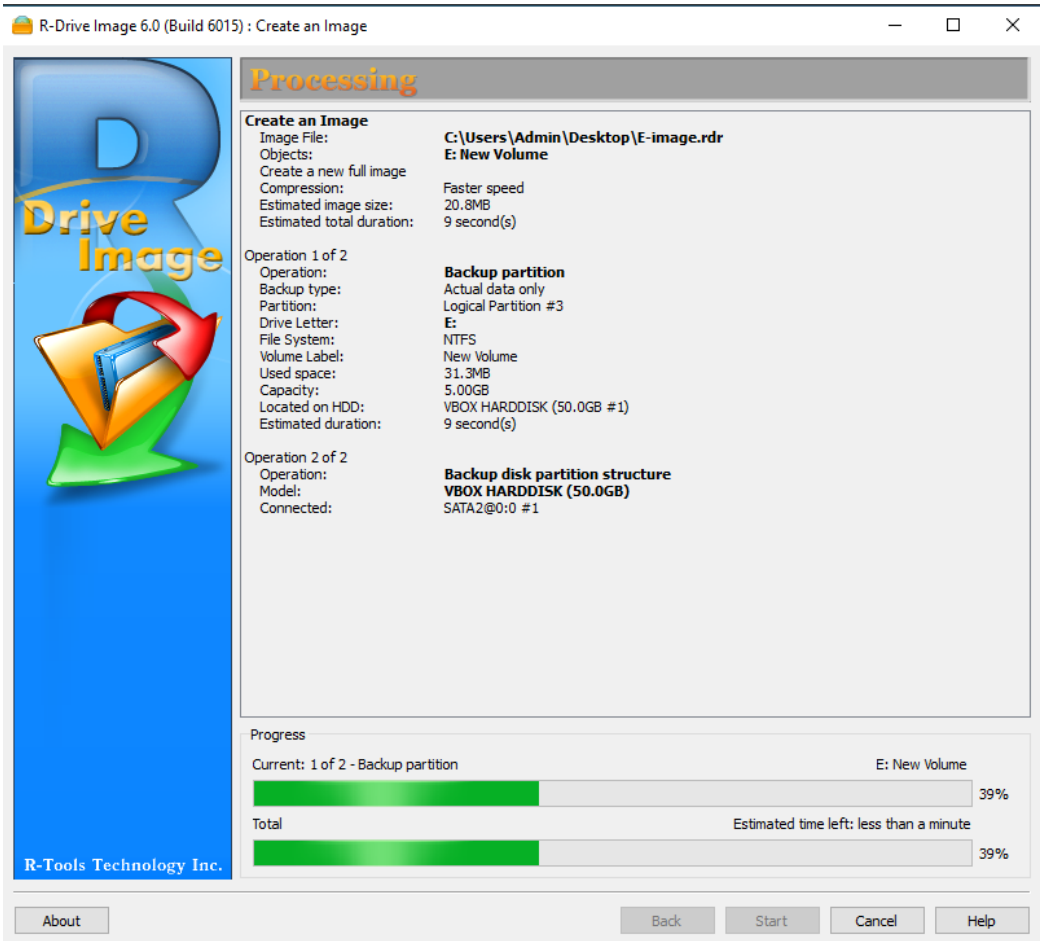

Figure 17: Disk imaging process in progress

Step 5: Verifying the Disk Image

Once the process is complete, verify the integrity of the created disk image by using the built-in verification tool in R-Drive Image.

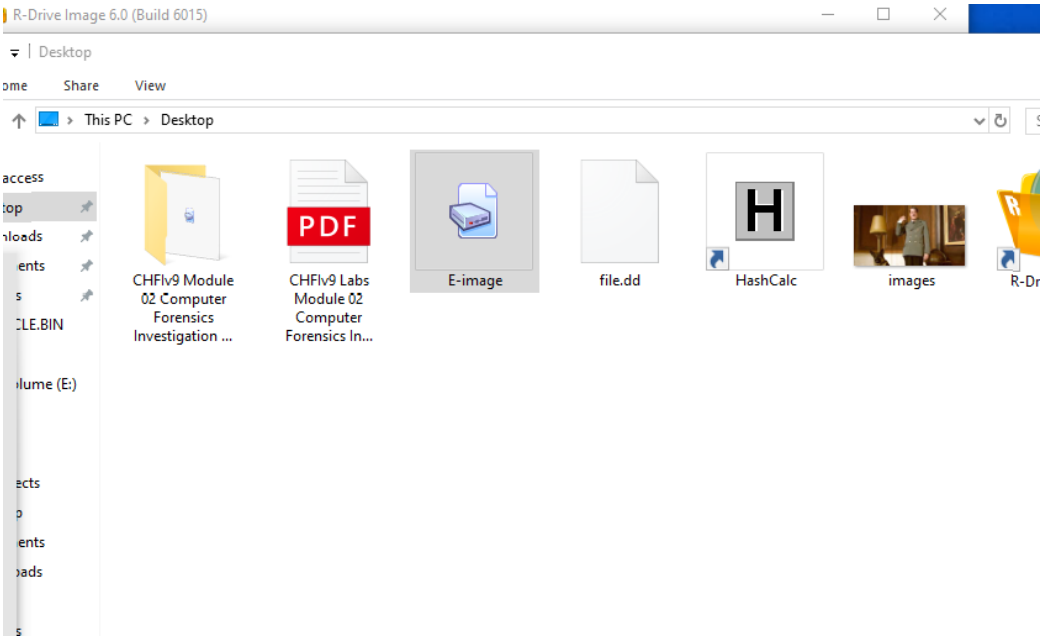

Figure 18: Verifying the disk image for integrity

Step 6: Completing the Process

After verification, confirm that the disk image file has been saved to the designated location. Record its metadata for future use.

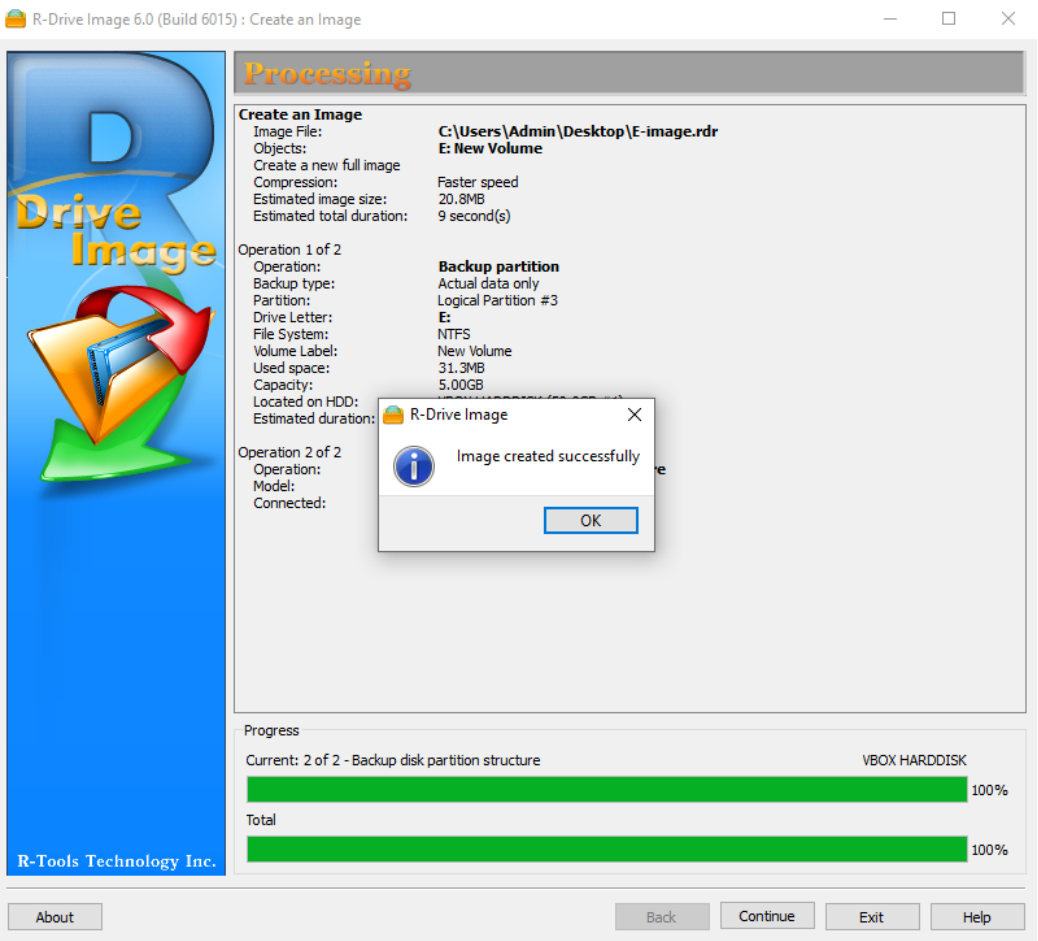

Figure 19: Disk image creation process completed