Computer Forensics Investigation Process

Module 02

Computer Forensics Investigation Process

The computer forensics investigation process is a methodological approach of preparing for an investigation, collecting and analyzing digital evidence, and managing the case from the reporting of the crime till the case's conclusion. This process takes place in a computer forensics lab.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The rapid increase of cyber-crimes has led to development of various laws and standards that define cyber-crimes, digital evidence, search and seizure methodology, evidence recovery and investigation process. The investigators must follow a forensics investigation process that comply with local laws and established precedentsand any deviation from the standard process may jeopardize the complete investigation. As digital evidence is fragile in nature, a proper and thorough forensic investigation process that ensures the integrity of evidence is critical to prove a case in a court of law. The investigators must follow a repeatable and well documented set of steps such that every iteration of analysis gives the same findings, otherwise the findings of the investigation can be invalidated during the cross examination in a court of law.

Hence, as a computer forensic investigator, it is important to have knowledge of the process involved during a forensic investigation, such as collecting the digital evidence, building a computer forensics lab, recovering the deleted data, etc.

Lab Objectives

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

- Recovering deleted file 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.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

Lab Environment

This lab requires:

- A system running with **Windows Server 2012** virtual machine.
- A system running with **Windows 10** virtual machine.
- A web browser with an Internet access.
- Administrative privileges to run tools.

Lab Duration

Time: 80 Minutes

Overview of the Computer Forensics Investigation Process

A computer forensic expert should be well-versed in how to use various tools for data recovery. By using tools such as EaseUS Data Recovery Wizard, MD5 Calculator, and HashCalc, it is possible to recover files that have been deleted even from a device's recycle bin, make a duplicate, and check the checksums to compare with the original data.

A computer forensics lab (CFL) is a designated location for conducting computer-based investigations on collected evidence. It is an efficient computer forensics platform that is able to investigate any cybercrime event. In a CFL, the investigator analyzes media, audio, intrusions, and any type of cybercrime evidence obtained from the crime scene.

Many organizations build a forensics lab to prevent unauthorized access to sensitive information. The information that comes from the laboratory can help in determining the guilt or innocence of a person or a corporation.

TASK 1

Overview

Lab Tasks

Recommended labs to assists in computer forensic investigation process:

- Recovering Data using the **EaseUS Data Recovery Wizard**.
- Performing Hash, Checksum, or HMAC Calculations using the **HashCalc**.
- Generating MD5 Hashes using **MD5 Calculator**.
- Viewing Files of Various Formats using the **File Viewer**.
- Handling Evidence Data using the **P2 Commander**.
- Creating a Disk Image File of a Hard Disk Partition using the **R-drive Image Tool**.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab

1

Recovering Data Using the EaseUS Data Recovery Wizard

EaseUS Data Recovery Wizard recovers deleted files, even if you've emptied the Recycling Bin or deleted them directly (and provided they haven't been securely deleted with multiple passes).

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

For instance, a finance manager in a reputable company modifies the financial data of the company and transfers the company's funds to his personal account. In order to conceal the evidence, he permanently deletes the original files from his computer using **Shift+Del**. The company then hires a computer forensic expert to investigate on the issue. The investigator recovers the deleted files by using the EaseUS Data Recovery Wizard data recovery software.

The investigator has to duplicate the evidence, as the original data shouldn't be tampered with, if the evidence is going to be presented in court. As a part of the digital validation of the duplicated evidence, the investigator uses a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. The unique number is referred to as a "digital fingerprint."

Lab Objectives

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

The objective of this lab is to help students understand and perform data file recovery using the EaseUS Data Recovery Wizard tool.

Lab Environment

This lab requires:

- A computer running **Windows 10** virtual machine.
- Administrative privileges to install and run tools.
- A web browser with an Internet connection.

- EaseUS Data Recovery Wizard, located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Data Recovery Tools\EaseUS Data Recovery Wizard**.
- You can also download the latest version of **EaseUS Data Recovery Wizard** at http://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm.
- Kindly note that, if you decide to download the latest version, then the screenshots shown in this lab might differ.

Lab Duration

Time: 15 Minutes

Overview of EaseUS Data Recovery Wizard

Take a snapshot (a type of quick backup) of your machine before each lab, because if something goes wrong, you can go back to it.

EaseUS Data Recovery Wizard, data recovery software, will recover deleted files that have been emptied from the Windows Recycle Bin or have been lost due to the formatting or corruption of a hard drive, a virus or Trojan infection, or an unexpected system shutdown or due to software failure. It can recover data from hard drives, USB drives, memory cards, and other storage devices.

Lab Tasks

1. Log on to **Windows 10** virtual machine.

TASK 1

Install and Launch EaseUS Data Recovery Wizard

2. Navigate to **Z:\CHFIv9 Module 02 Computer Forensics Investigation Process\Data Recovery Tools\EaseUS Data Recovery Wizard**, double-click **drw_free.exe**, select a language (English) and follow the wizard driven installation steps to install the application.

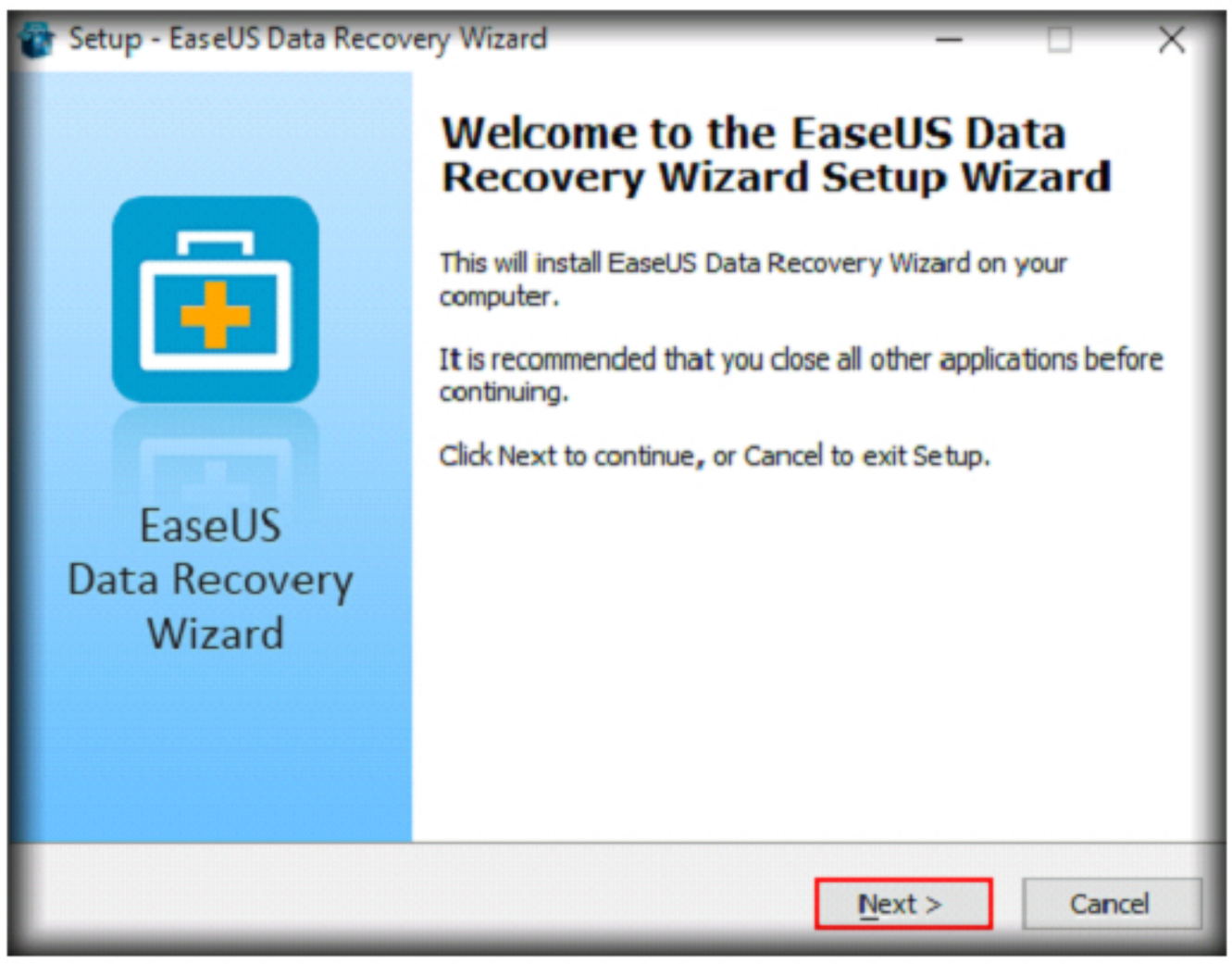

FIGURE 1.1: EaseUS Data Recovery Wizardsetup wizard

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

If a **User Account Control** pop-up appears, click **Yes**.

If a **Windows Security** dialog-box appears, enter the credentials of Windows Server 2012 virtual machine and then click **OK**.

3. In the final step of installation, ensure that **Launch EaseUS Data Recovery Wizard** option is checked, uncheck **Participate in the Customer Experience Improvement Program** option and click **Finish**.

Professional data recovery software for:

1. Deleted files
2. Lost files
3. Formatted disks
4. RAW disks
5. Missing drive letters
6. Windows reinstalls

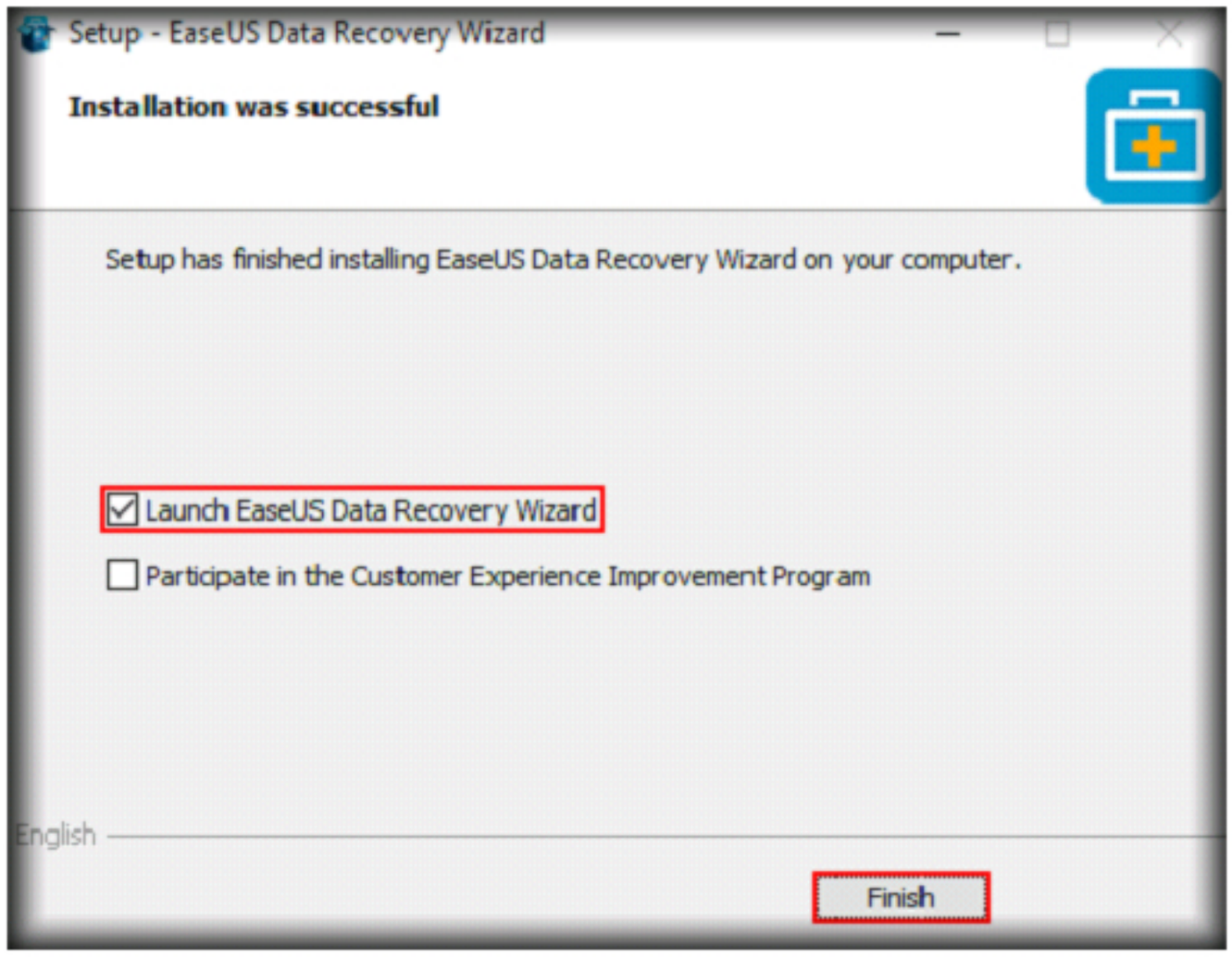

FIGURE 1.2: EaseUS Data Recovery Wizard setup wizard

4. A EaseUS webpage appears in the default web browser, close it.
5. **EaseUS Data Recovery Wizard** appears along with a pop-up. **Close** the pop-up and click on **Next** in the wizard.

EaseUS Data Recovery Wizardis designed specifically to allow home and business users to quickly and simply recover data.

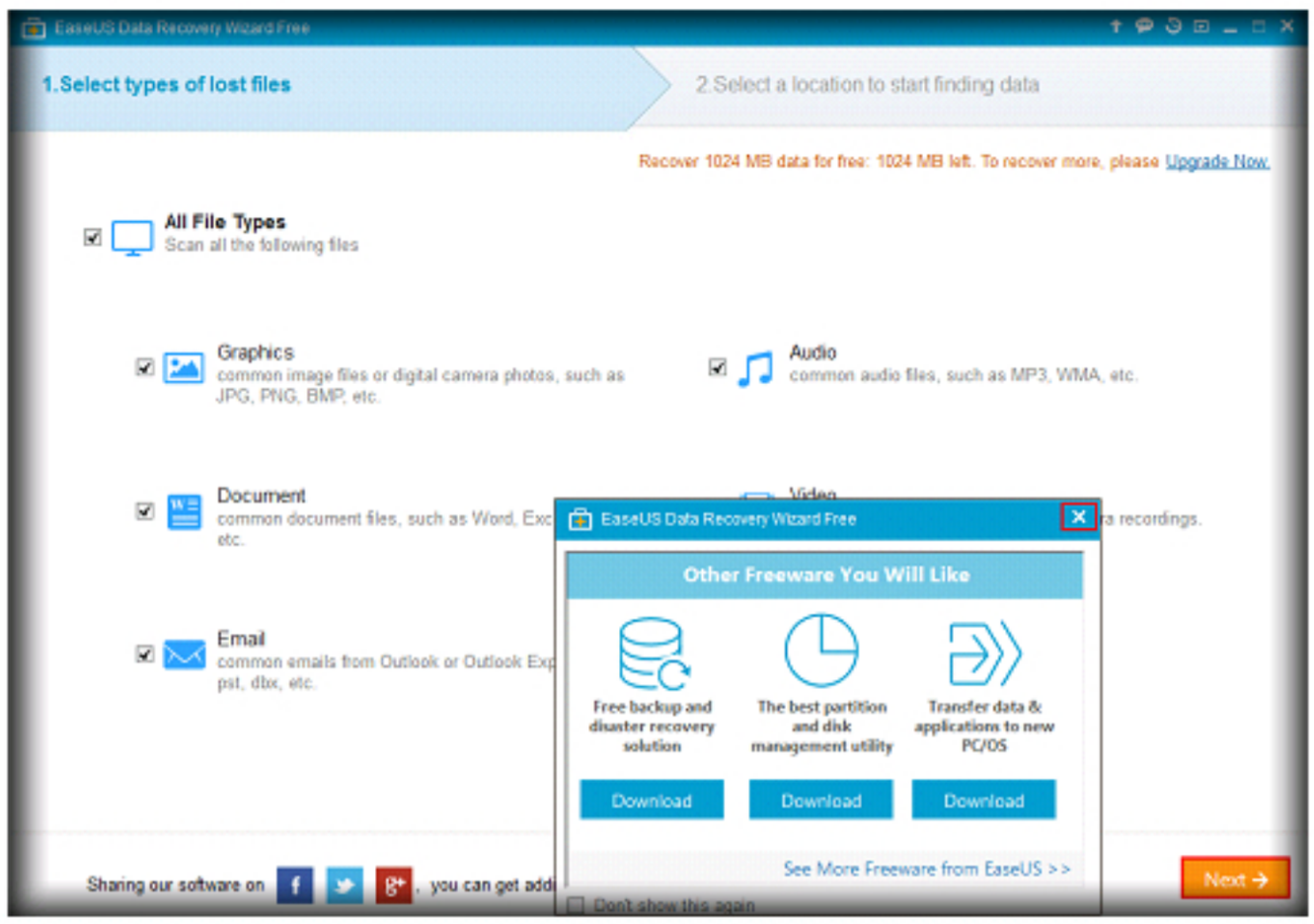

FIGURE 1.3: EaseUS Data Recovery Wizard

6. Next step of the wizard appears displaying the **Common Locations** and **Hard Disk Drives**. Select **D drive** and after that click **Scan**.

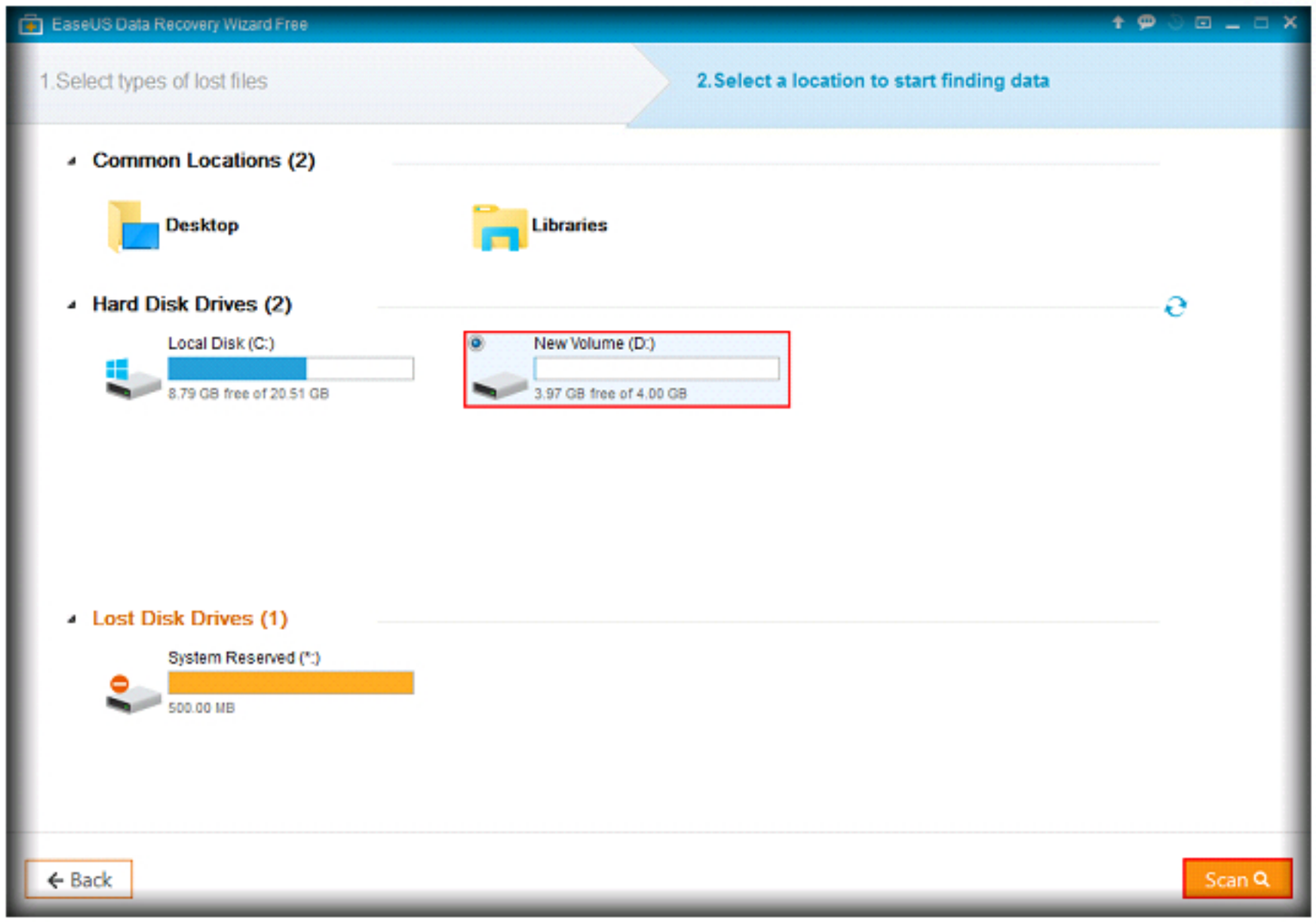

FIGURE 1.4: EaseUS Data Recovery Wizard location screen

7. The application begins to scan the drive and begins to display the contents of the drive, along with the data that has been deleted.
8. On completion of the scan, a pop-up appears; click **OK** to close the pop-up.
9. The file system of **D drive** appears in the left pane, displaying the files present in the drive (if any), along with the deleted files (denoted by the letter **d**) as shown in the following screenshot:

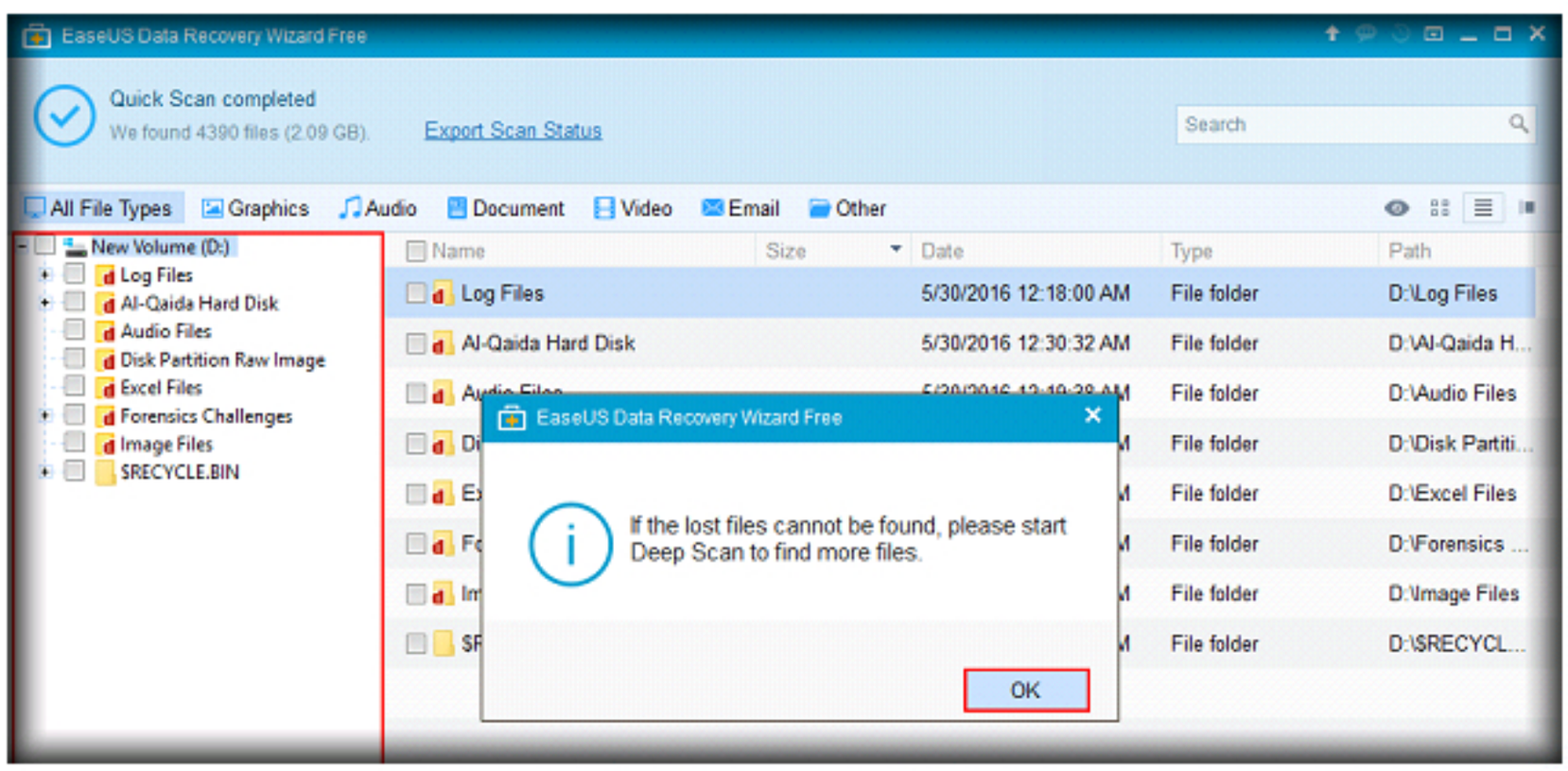

FIGURE 1.5: EaseUS Data Recovery Wizard All File Types screen

10. To view the deleted files inside a folder which contains sub-folders, you need to expand the nodes pertaining to each directory, until you find a directory that contains files.
11. In this lab, the deleted contents of the directory **top_files** located in**\Al-Qaida Hard Disk\Al-Qaida Articles\x_files** are viewed.

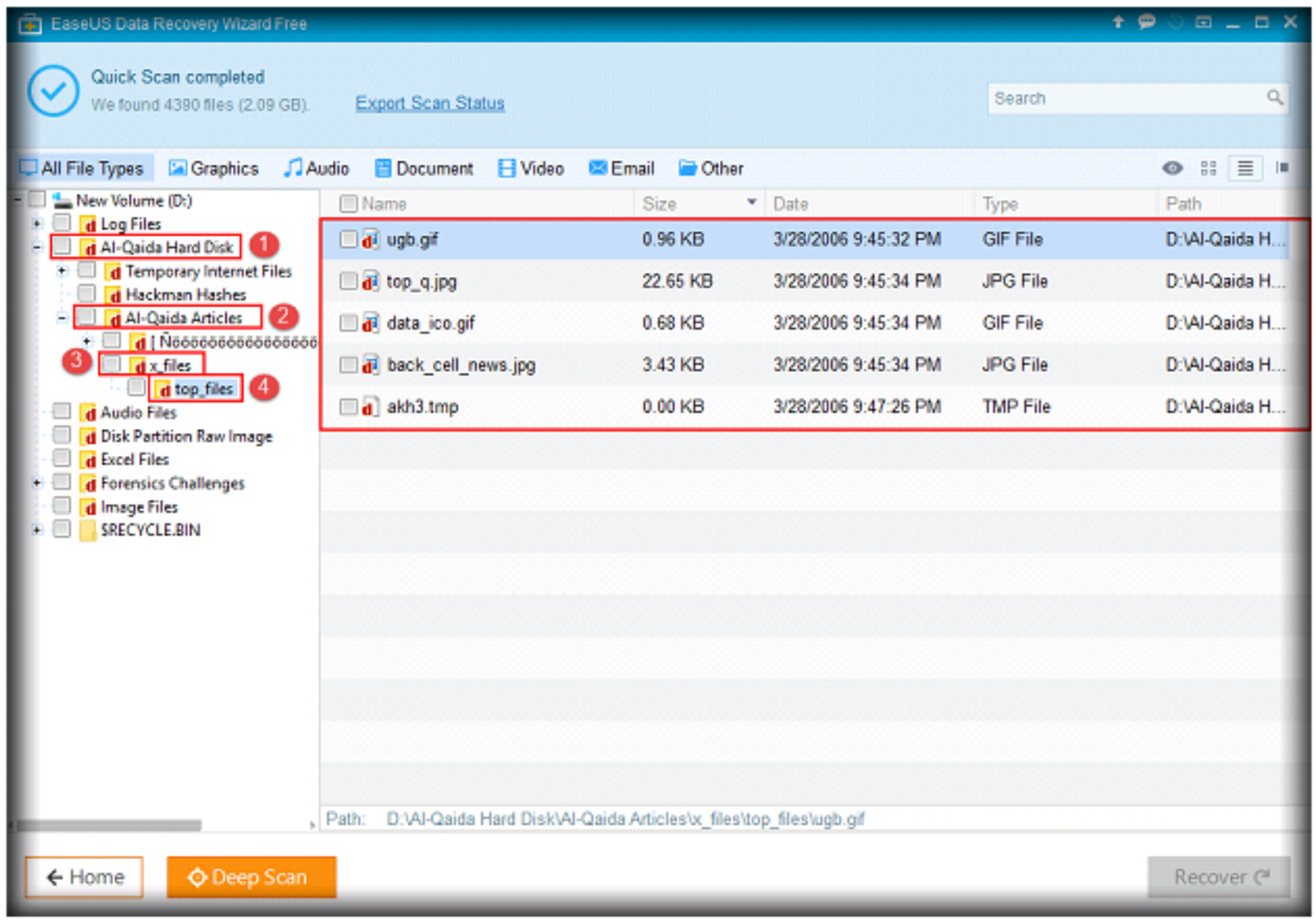

FIGURE 1.6: EaseUS Data Recovery WizardAll File Types screen

12. To view the deleted file, right-click on the respective file and click **Preview**.

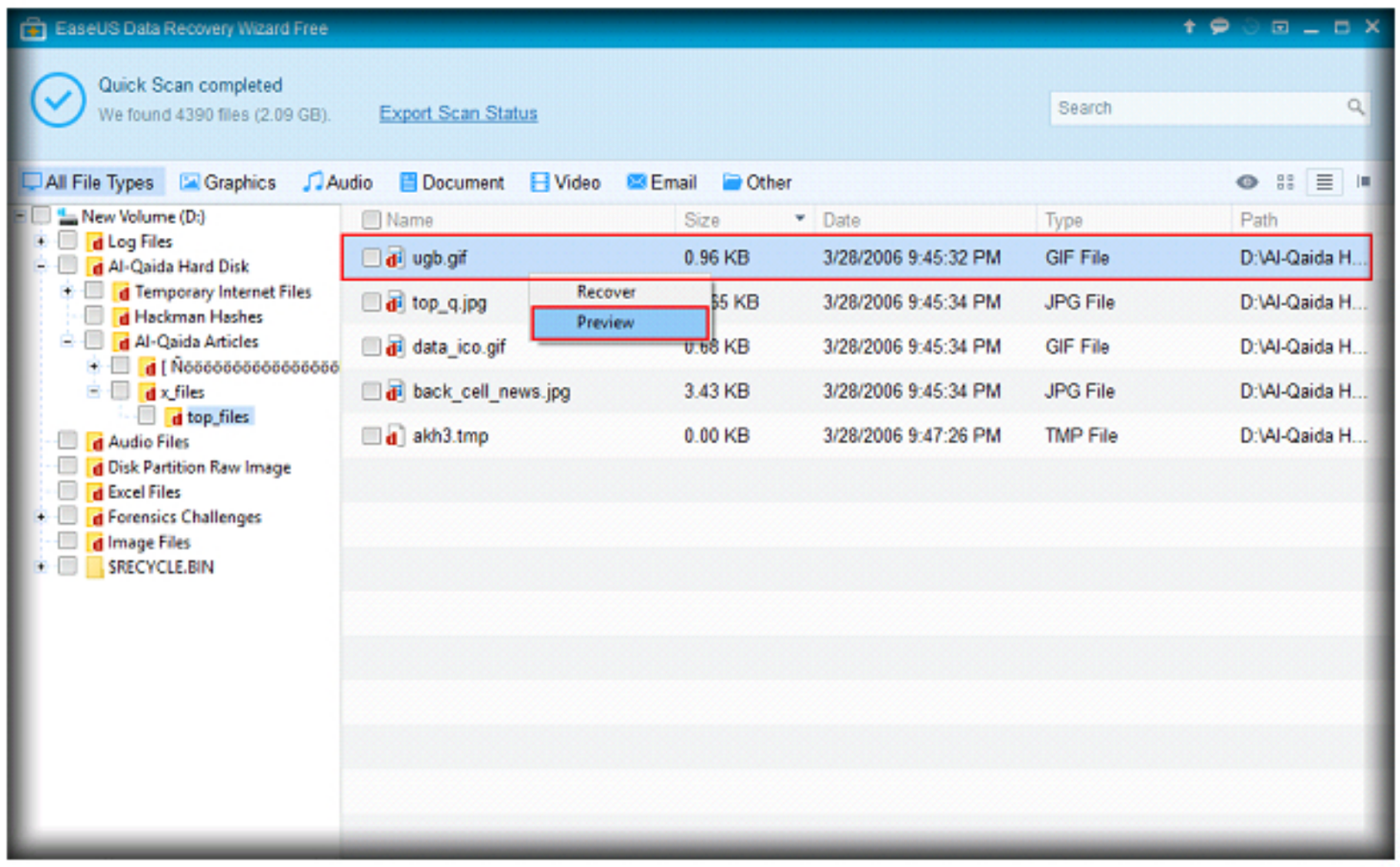

FIGURE 1.7: EaseUS Data Recovery WizardAll File Types screen

13. The preview of the file appears as shown in the following screenshot:

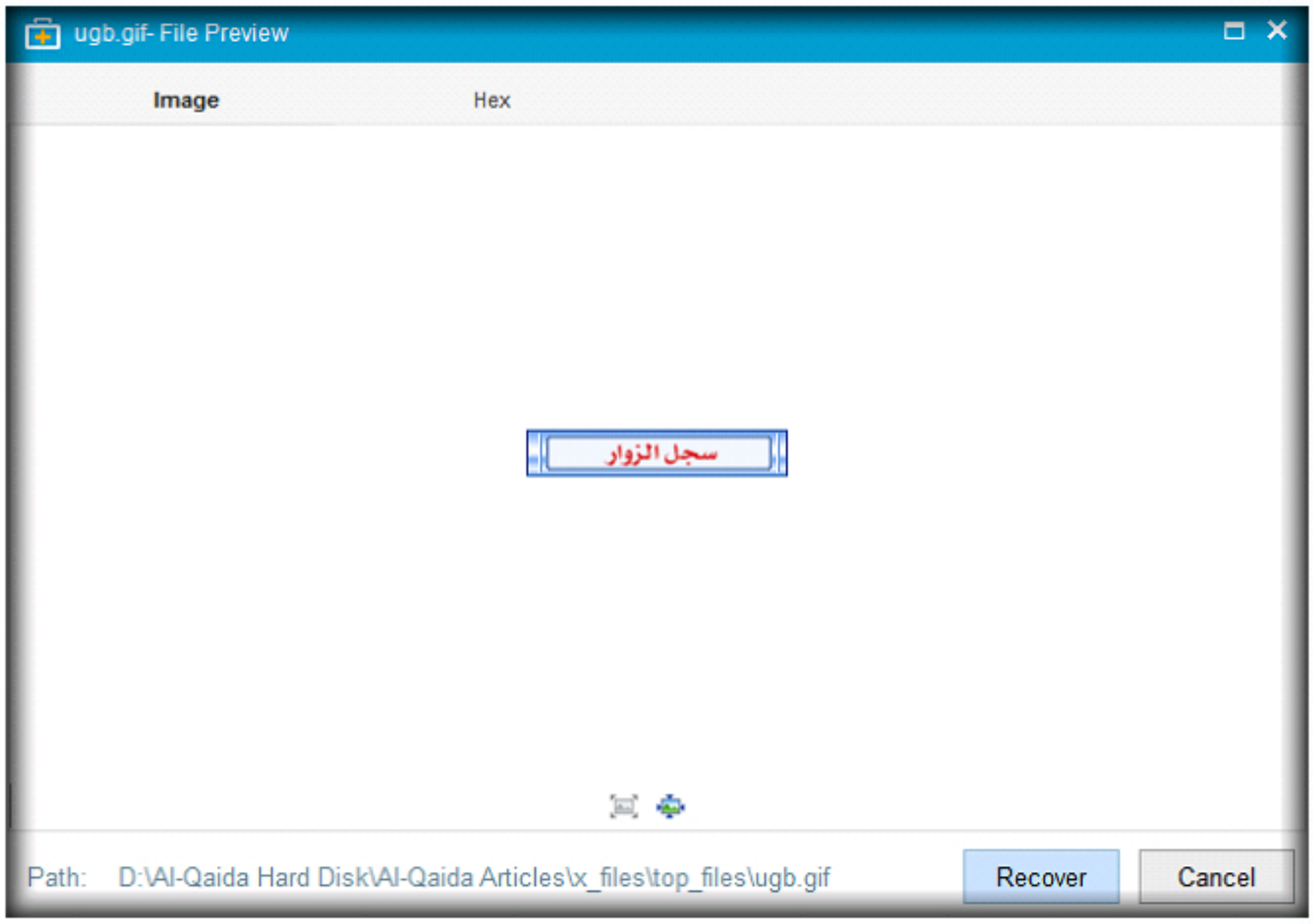

FIGURE 1.8 File preview

14. Click **Cancel** to view the other deleted files.

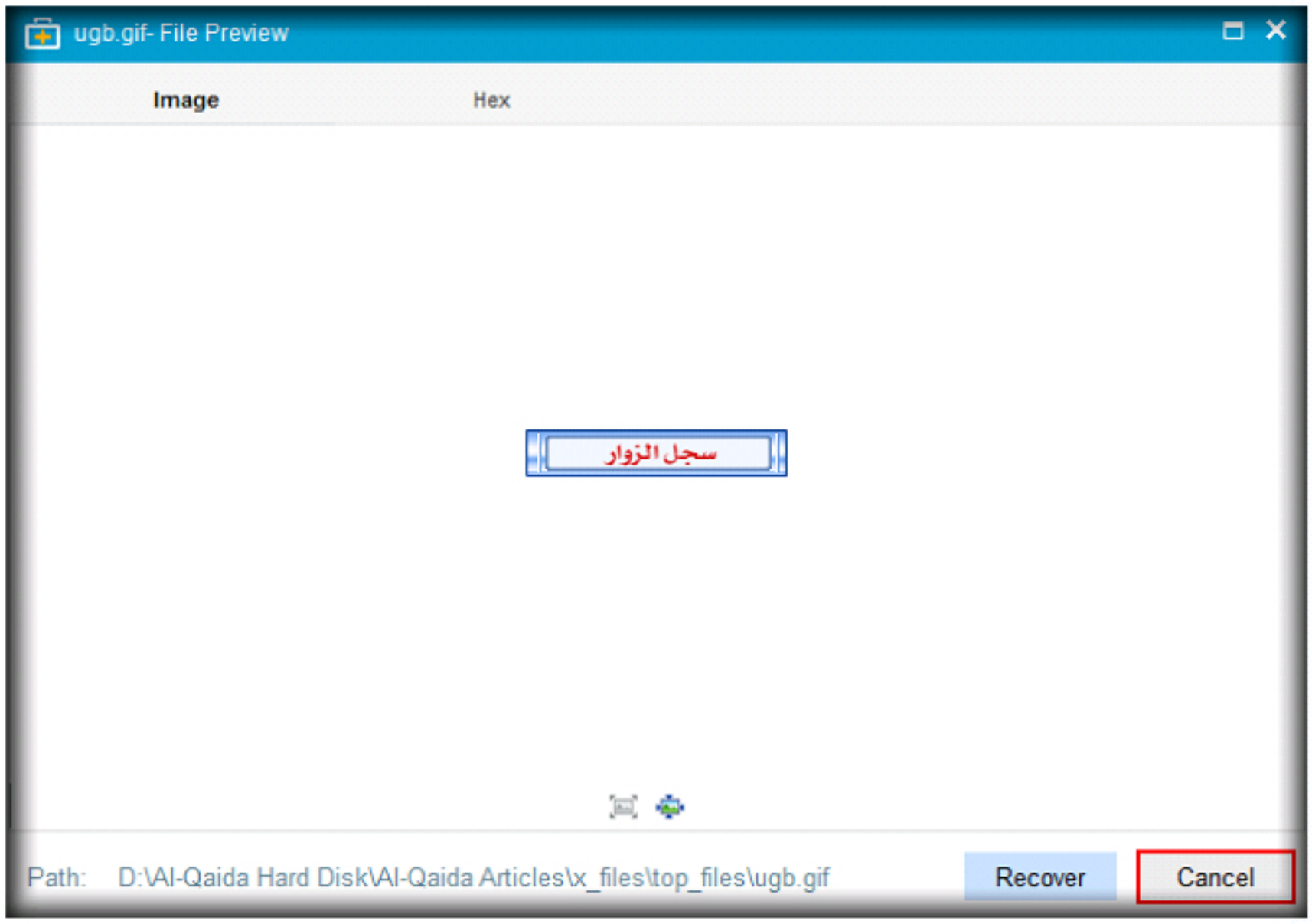

FIGURE 1.9: File preview

15. To view the files pertaining to image format, click **Graphics** tab and then, select a folder. The images present in the folder appear in the right-pane as shown in the following screenshot:

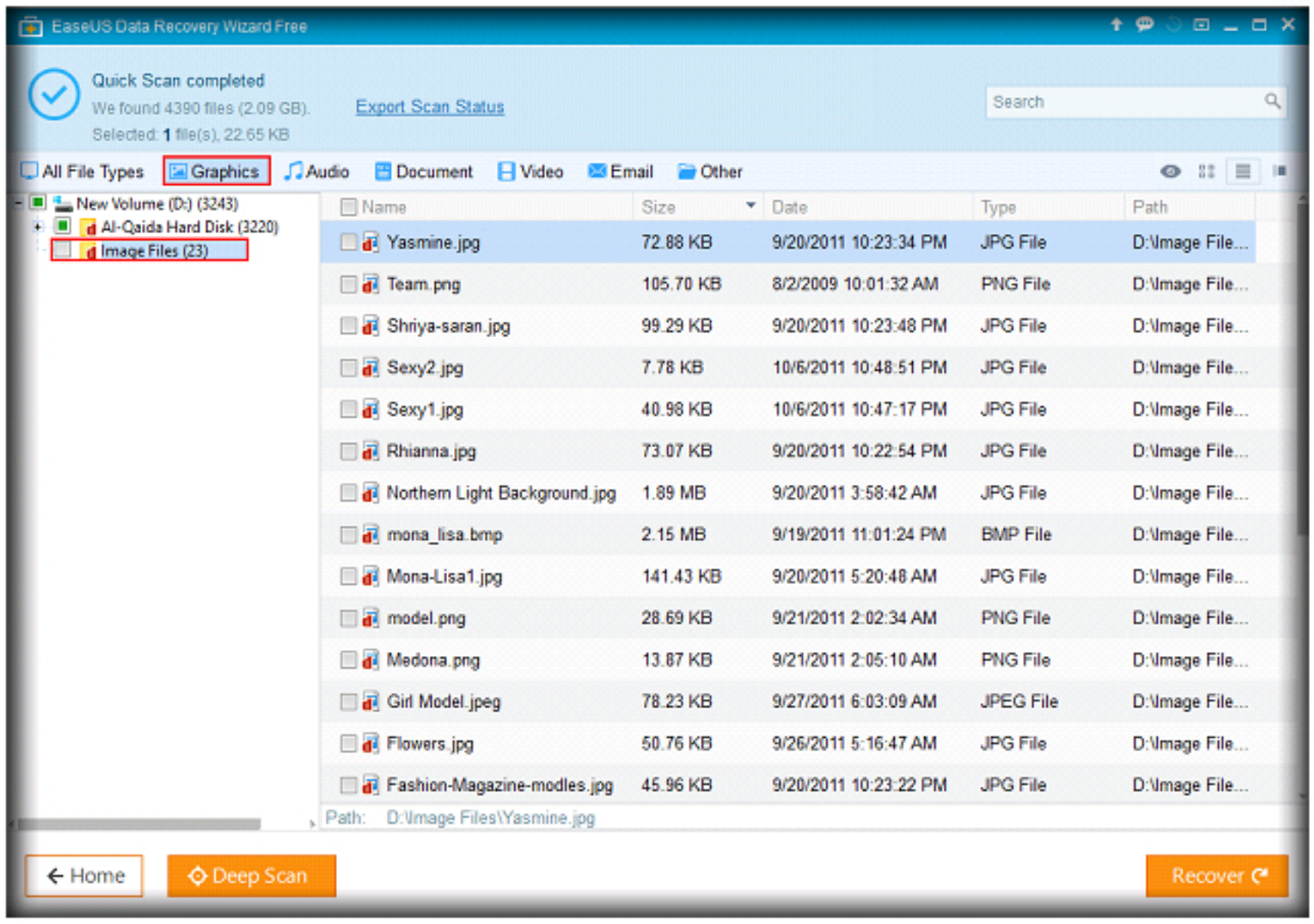

FIGURE 1.10: EaseUS Data Recovery WizardGraphics screen

16. To recover a single or multiple files, select the file/files of your choice and click **Recover**. In this lab, files present in **Image Files** folder are being recovered.

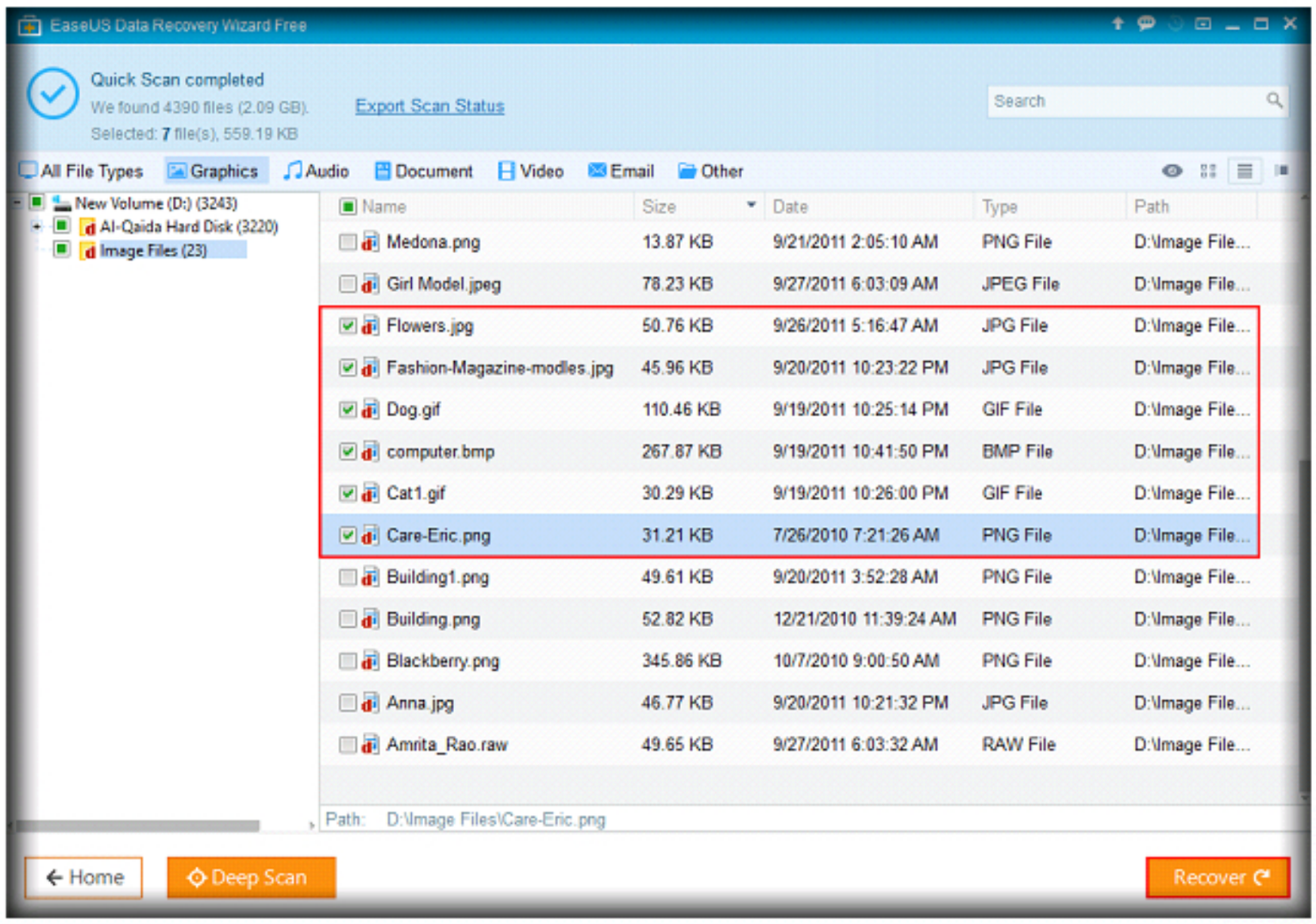

FIGURE 1.11: EaseUS Data Recovery WizardGraphics screen

17. A **Browse For Folder** window appears. You need to choose a location to store the recovered files.
18. So, navigate to **Documents**, create a folder named **Recovered Files** and then click **OK**.

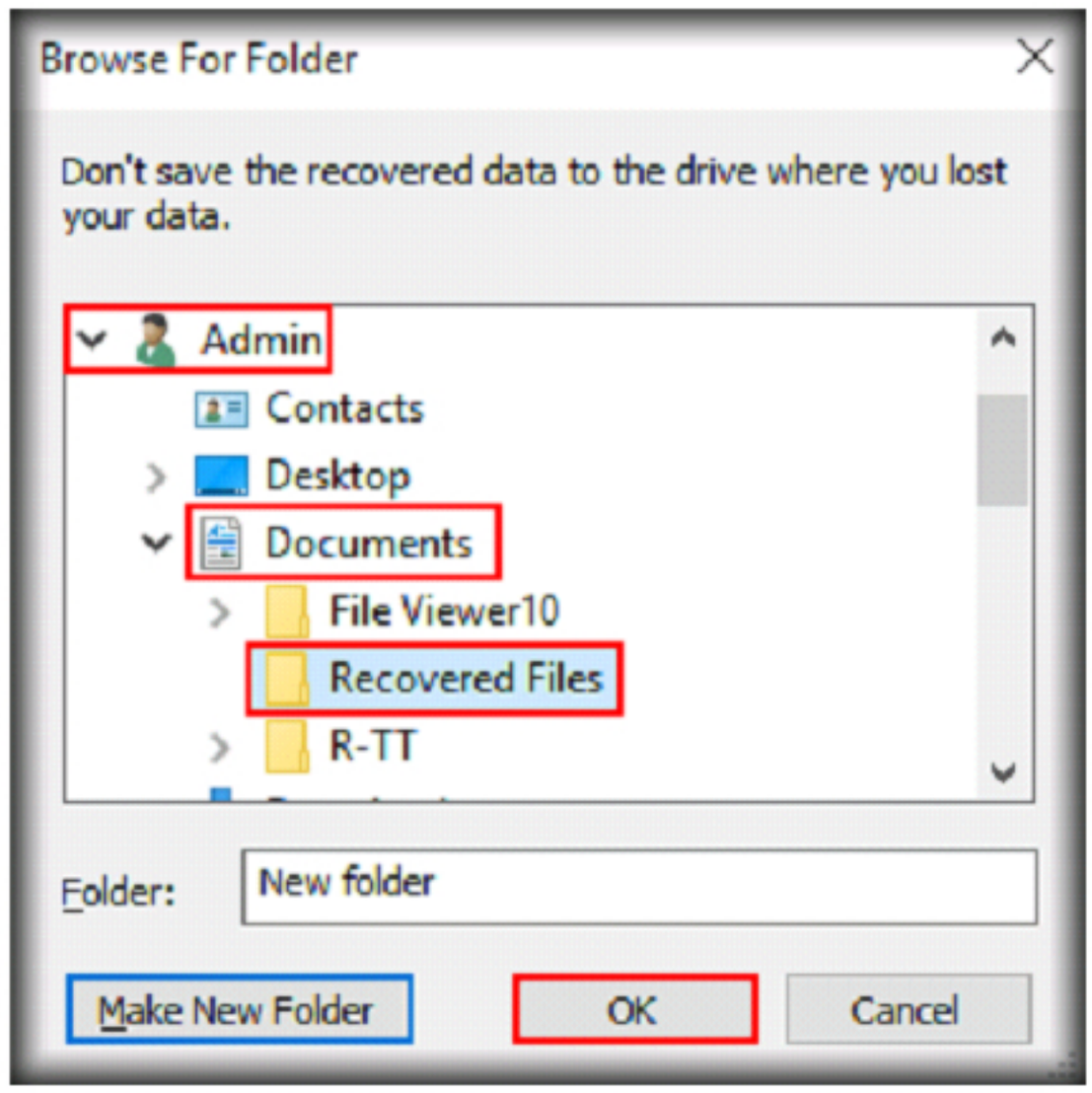

FIGURE 1.12: Browse for folder screen

19. EaseUS Data Recovery application recovers the files to **Recovered data [date] at [time]/New Volume** as shown in the following screenshot:

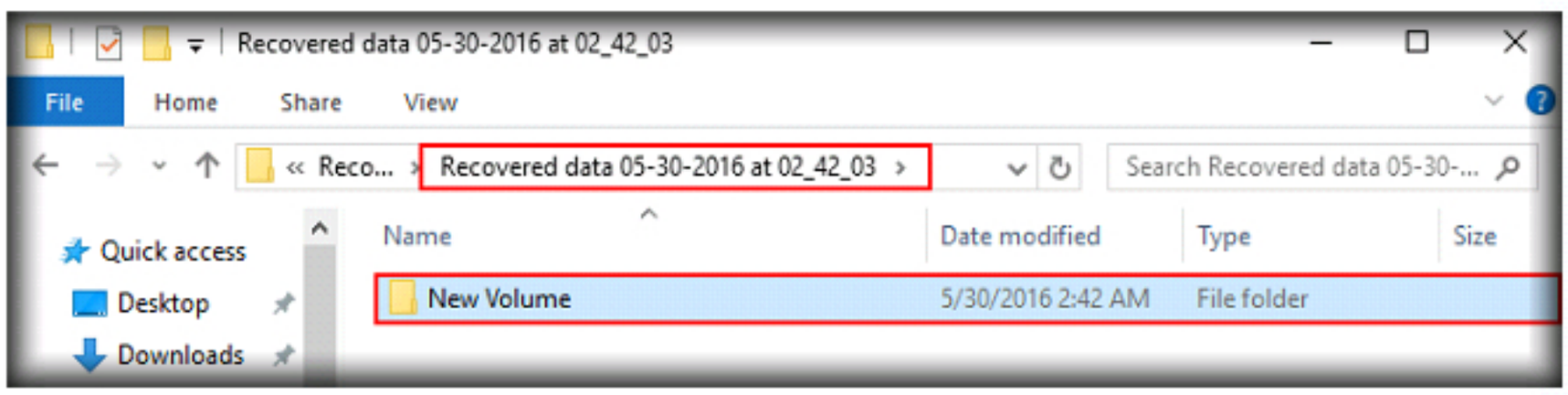

FIGURE 1.13: Recovered data [date] at [time]/New Volume Folder

20. Open the **New Volume** folder. The New Volume folder contains folder **Image Files** folder, from where we have recovered the deleted files as indicated in step no. 16.Open this folder.

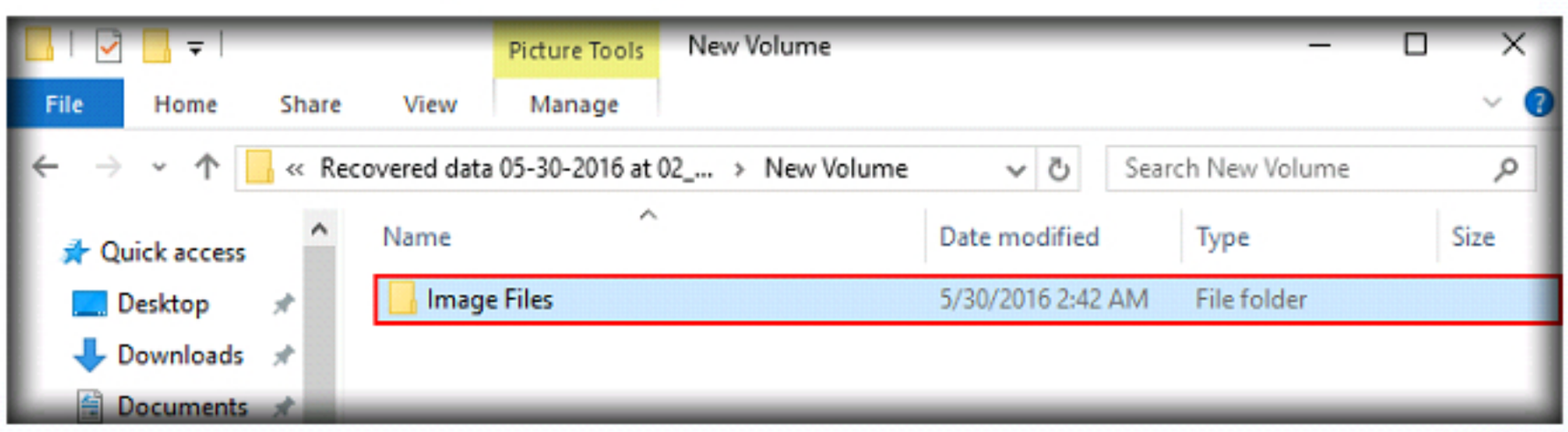

FIGURE 1.14: New Volume Folder

21. The files are successfully recovered as shown in the following screenshot:

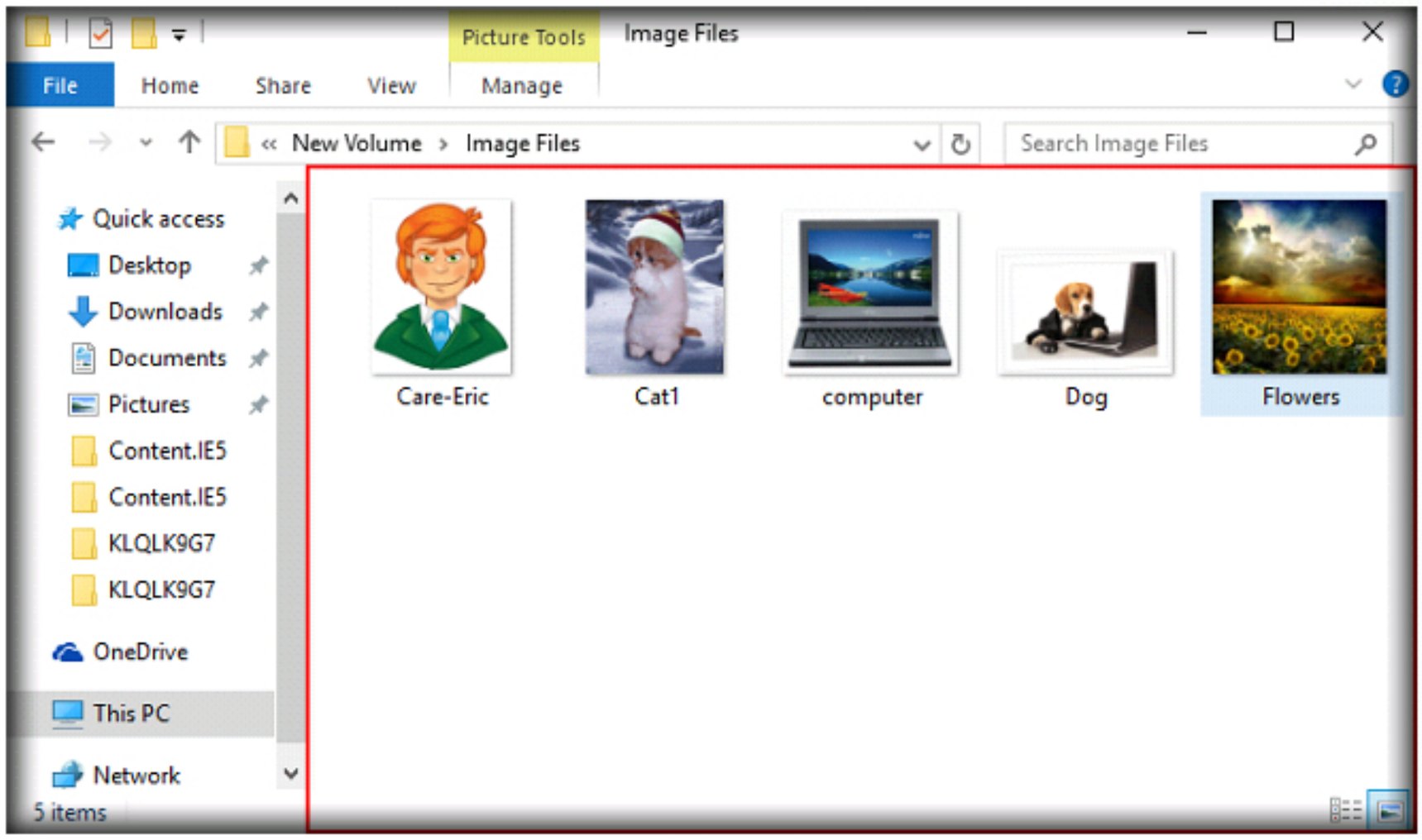

FIGURE 1.15: Image files

22. Switch to EaseUS Data Recovery Wizard, and close the pop-up that contains the status of the recovery.

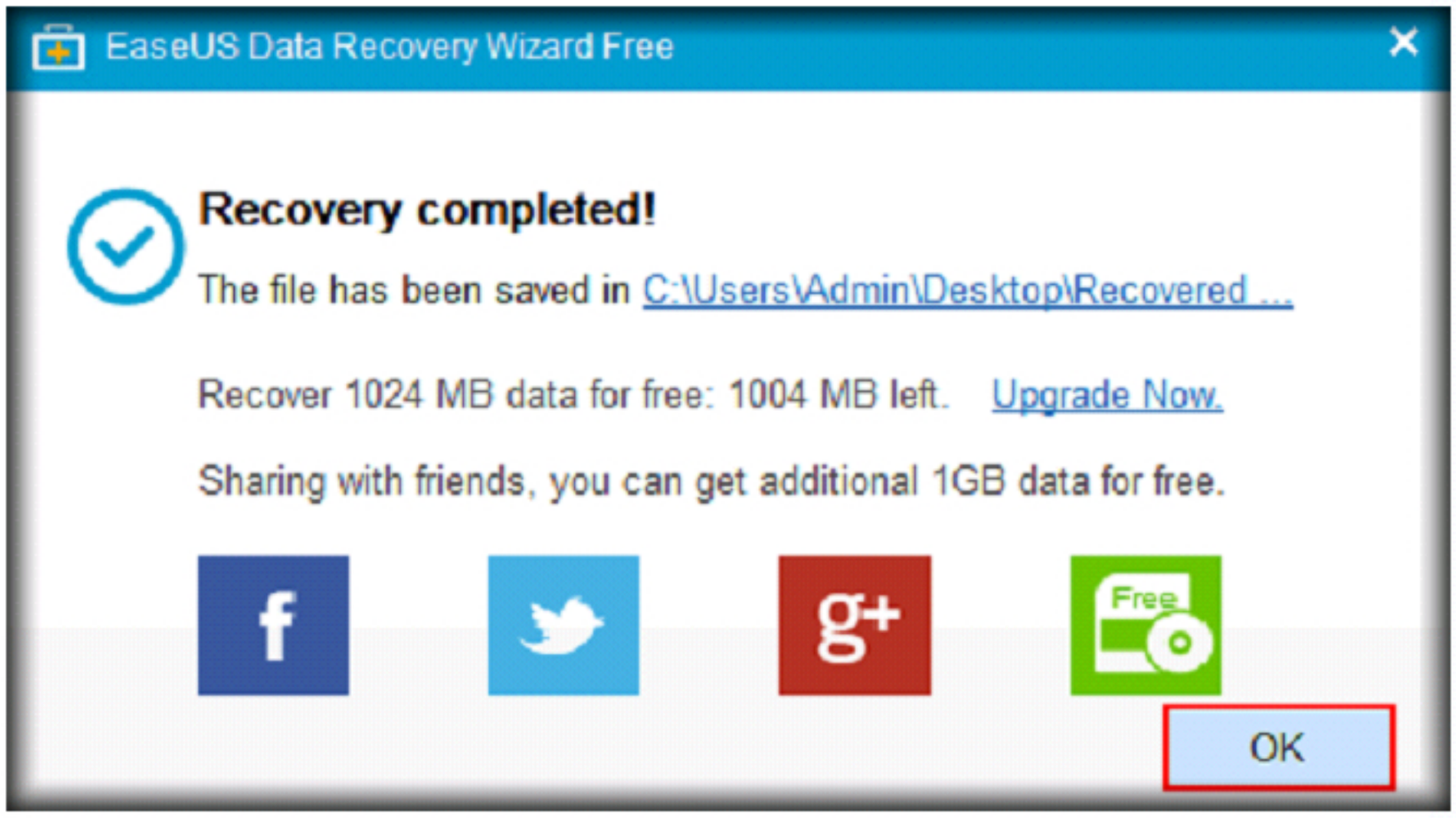

FIGURE 1.16: Recovery completed screen

23. This way, you may also view files of other formats and recover them. In some cases, the application may fail to find all the deleted files. In such cases, you may need to perform a deep scan on the respective disk drive/folder.

Lab Analysis

Analyze and document the results related to this lab exercise. Submit your opinion and experiences with the EaseUS Data Recovery Wizard.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Performing Hash, Checksum, or HMAC CalculationsUsing the HashCalc

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in eDonkey and eMule tools.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A multi-national company has undergone a network attack and has called forensics investigator to look into the issue. The investigator found some codes that seem to be familiar and needs to cross-check for their availability across a malware database. The major problem here is that the code is huge and uses pretty big storage capacity, making it difficult for search. Therefore, the investigator uses hash values of the code to find their traces in the database.

To be an expert computer forensic investigator, one must have sound knowledge of the tools used to compute hashes and check checksums.

Lab Objectives

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

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

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

This lab requires:

- A computer running **Windows Server 2012** virtual machine.
- Administrative privileges to run tools.
- HashCalc located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\HashCalc**.
- You can also download the latest version of **HashCalc** from the link http://www.slavasoft.com/hashcalc.
- Please note that, if you are willing to download the latest version, the screenshots and steps shown in this lab might differ.

Lab Duration

You can download HashCalc from www.slavasoft.com

Time: 10 Minutes

Overview of HashCalc

HashCalc allows you to compute message **digests, checksums,** and **HMACs for files**, as well as for **text and hex strings**. It offers a choice of 13 of the most popular hash and checksum algorithms for calculations.

Lab Tasks

TASK 1

Launching HashCalc

1. Login to **Windows Server 2012** virtual machine.
2. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** to find the evidence files for this lab.

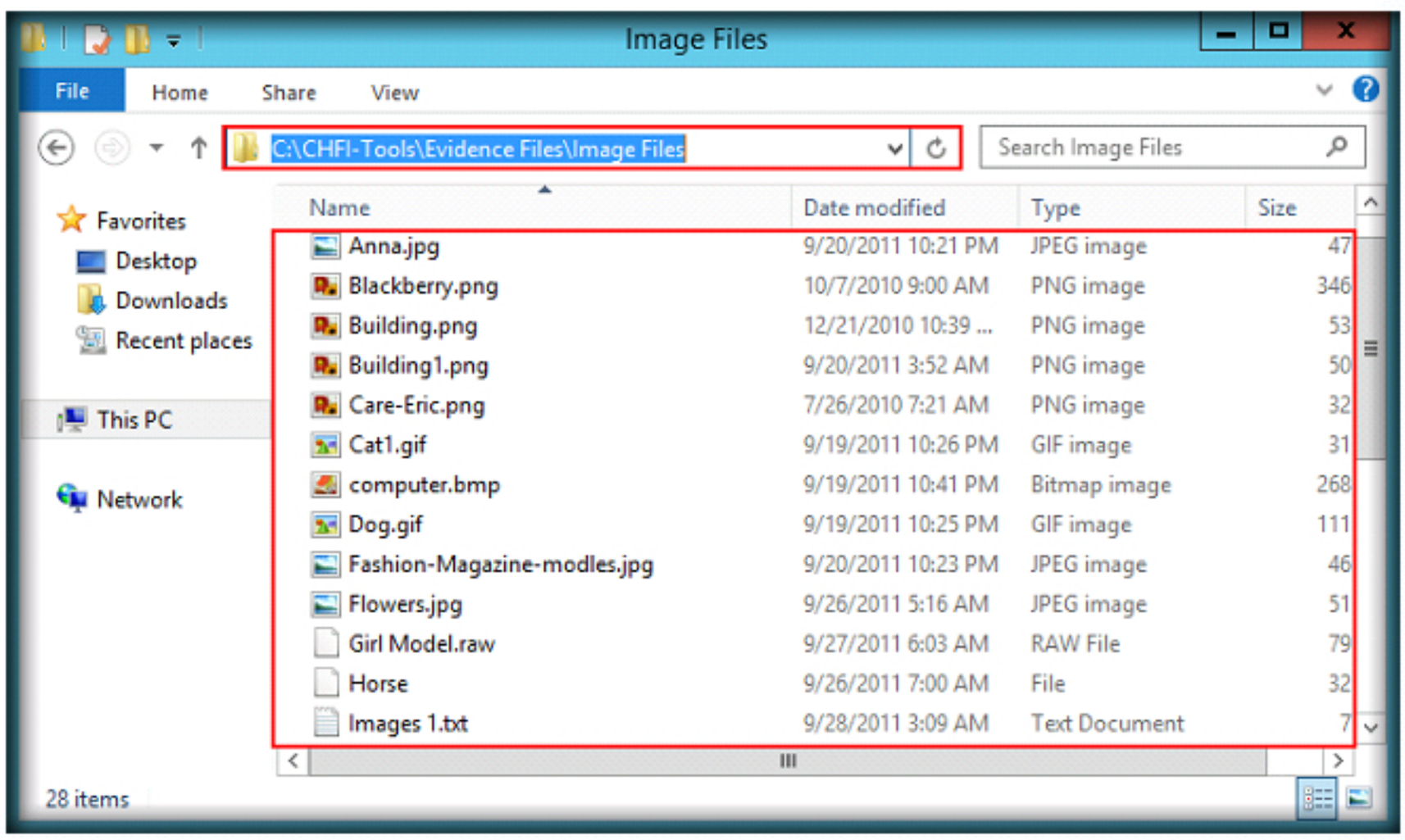

FIGURE 2.1: Evidence file

3. Navigate to **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\HashCalc**, then double-click on **setup.exe** and follow the wizard-driven installation steps to install the application.

   Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

A fast and easy-to-use calculator that allows you to compute message digests, checksums, and HMACs for files, as well as for text and hex strings.

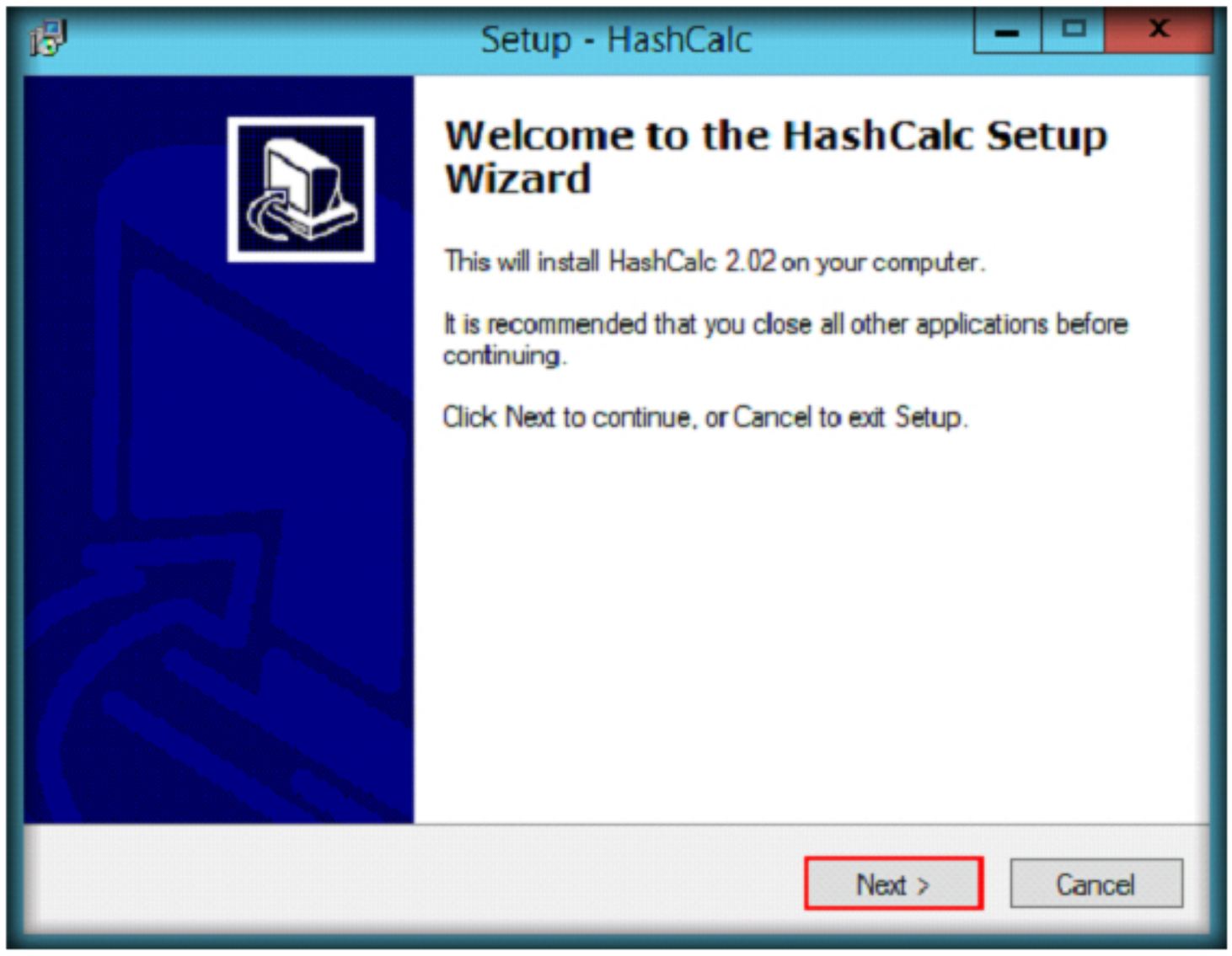

FIGURE 2.2: HashCalc Setup Wizard

4. In the final step of installation, uncheck **View the README file** option, check **Launch HashCalc** option and click **Finish**

HashCalcSupports 12 well-known and documented hash and checksum algorithms: MD2, MD4, MD5, SHA-1, SHA-2(256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, CRC32.

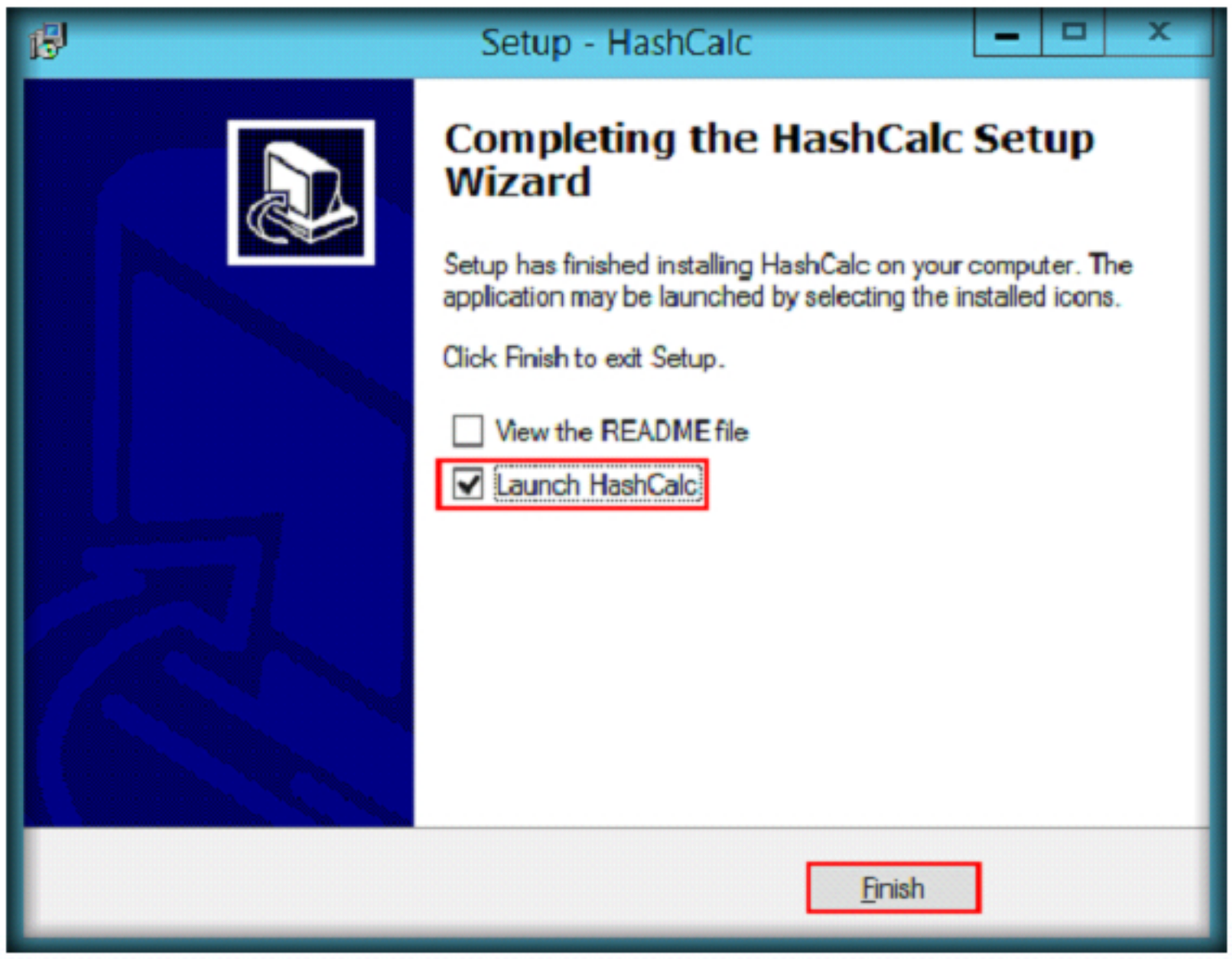

FIGURE 2.3: HashCalc Setup Wizard

5. The **HashCalc** application's main window appears as shown in the following screenshot:

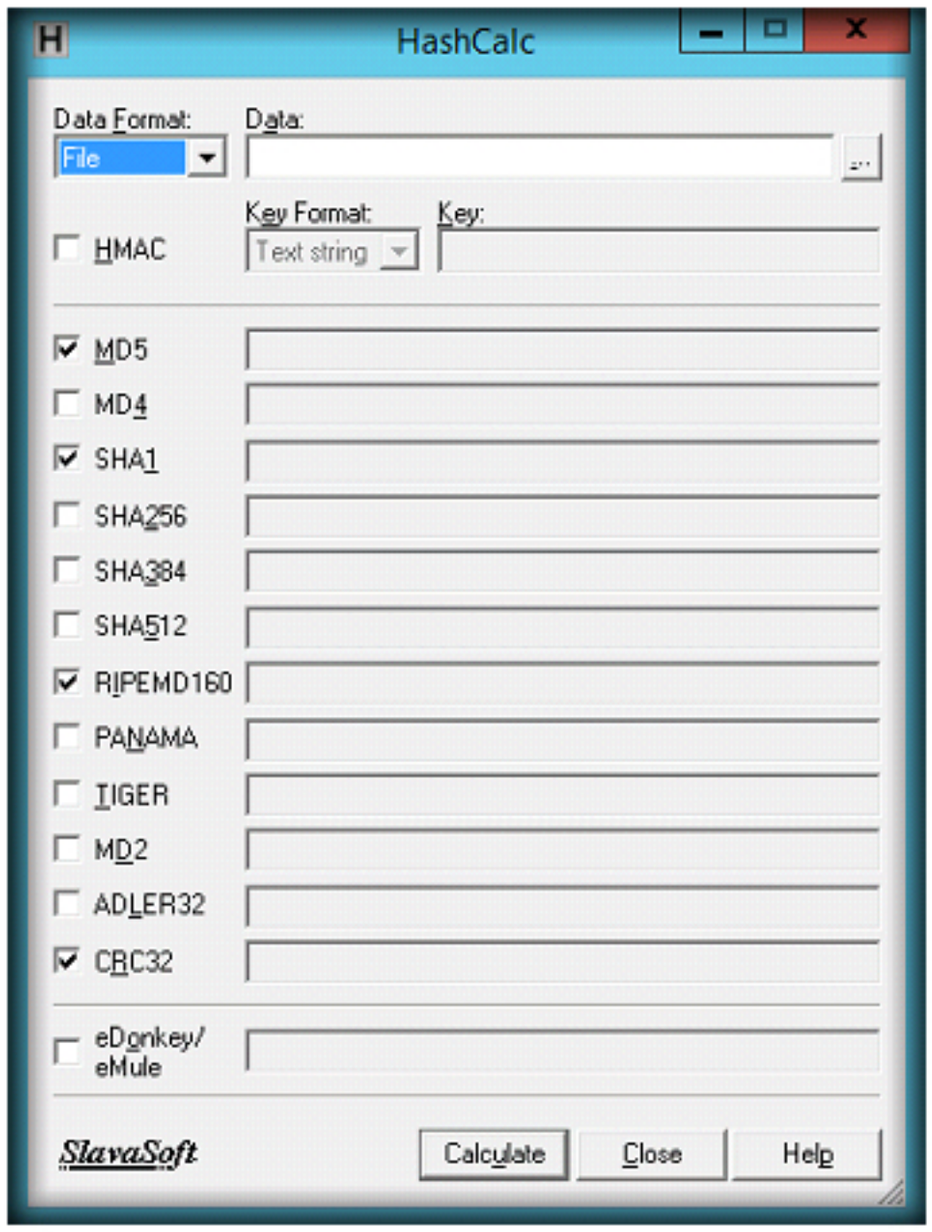

FIGURE 2.4: HashCalcmain window

Works with large file sizes. It has been tested on file sizes up to 15 GB.

TASK 2

Selecting Evidence File

6. In the **Data Format** drop-down list, select file format as **File** and click the ellipsis button associated with the **Data** field to select the file.

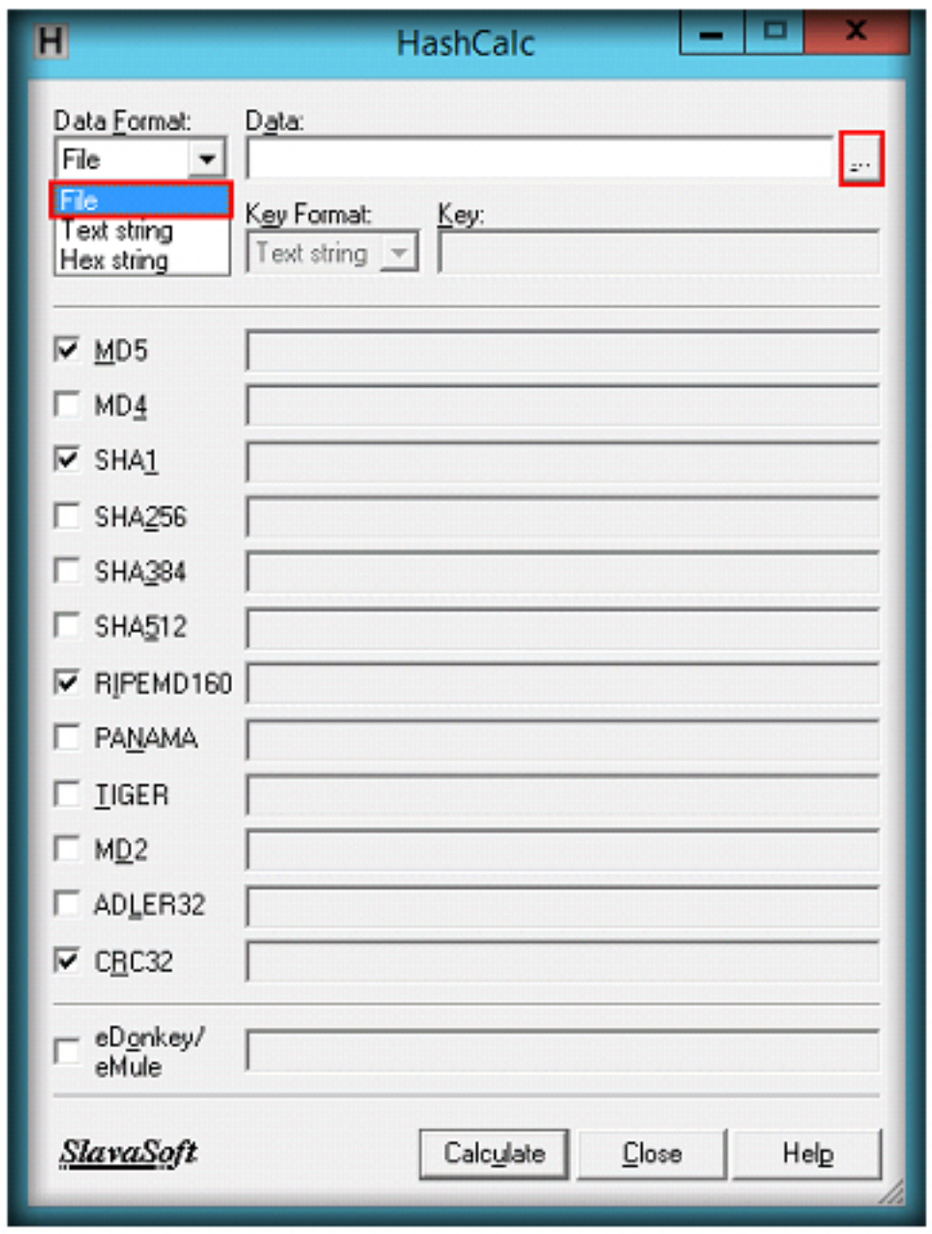

FIGURE 2.5: HashCalcdata format options

7. **Subsequently**, **Find** window appears, navigate to **C:\CHFI-Tools\Evidence Files\Image Files**. In this location, you need to select an evidence file, whose hash value needs to be calculated. In this lab, we have selected **Blackberry.png**. Once you select the file, click **Open**.

Support of 2 modes of calculations: HASH/CHECKSUM and HMAC.

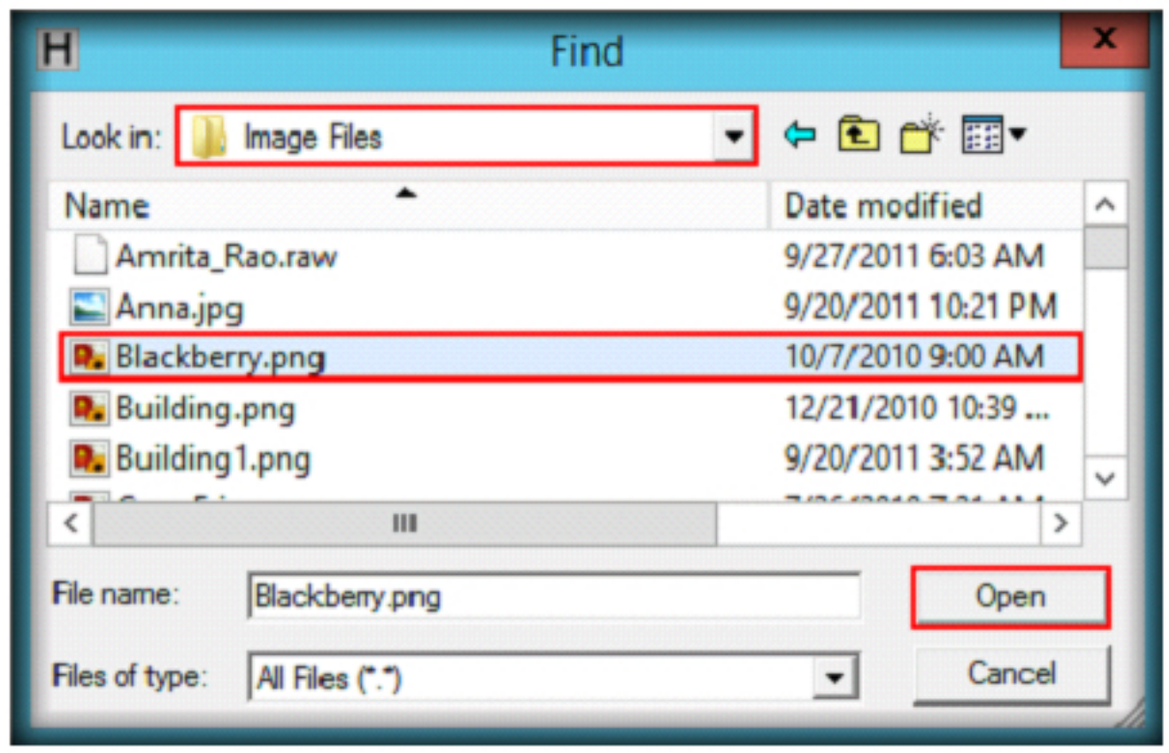

FIGURE 2.6: Selecting evidence file in D drive

8. The selected file will be displayed in the **Data** field.

HashCalc Calculates hash/checksum and HMAC for files of any type, including music, audio, video, image, icon, text, compression, etc., with the extensions: .mp3, .wav, .avi, .mpg, .midi, .mov, .dvd, .ram, .zip, .rar, .ico, .gif, .pif, .pic, .tif, .tiff, .txt, .doc, .pdf, .wps, .dat, .dll, .hex, .bin, .iso, .cpp, .dss, .par, .pps, .cue, .ram, .md5, .sfv, etc.

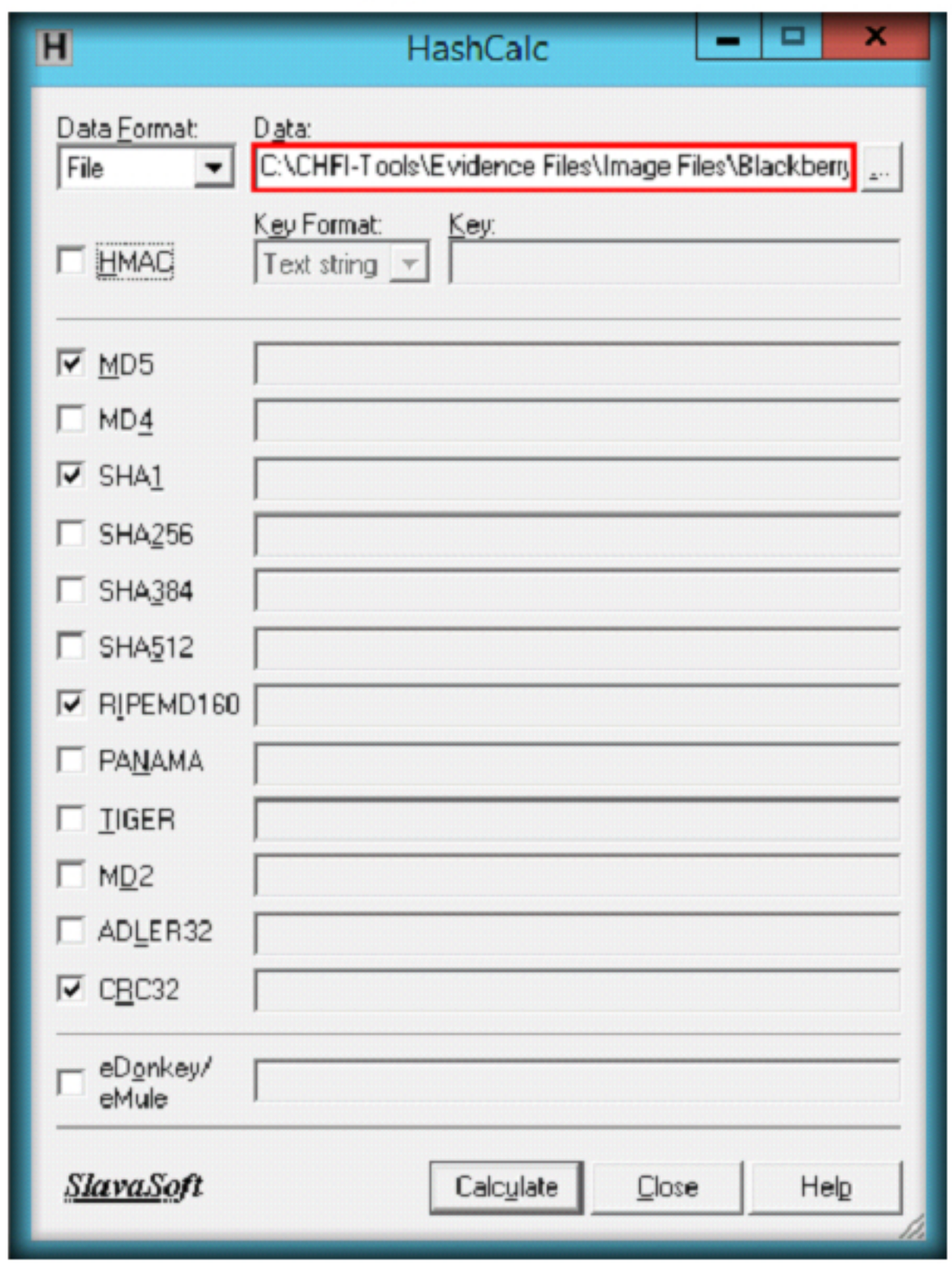

FIGURE 2.7: HashCalc window

Note: To calculate the message digests/checksums for the data, the **HMAC** box must be unchecked.

TASK 3

Selecting Algorithms

9. Select the algorithms you want to use for calculations by checking the boxes with the appropriate names, and then click the **Calculate** button.

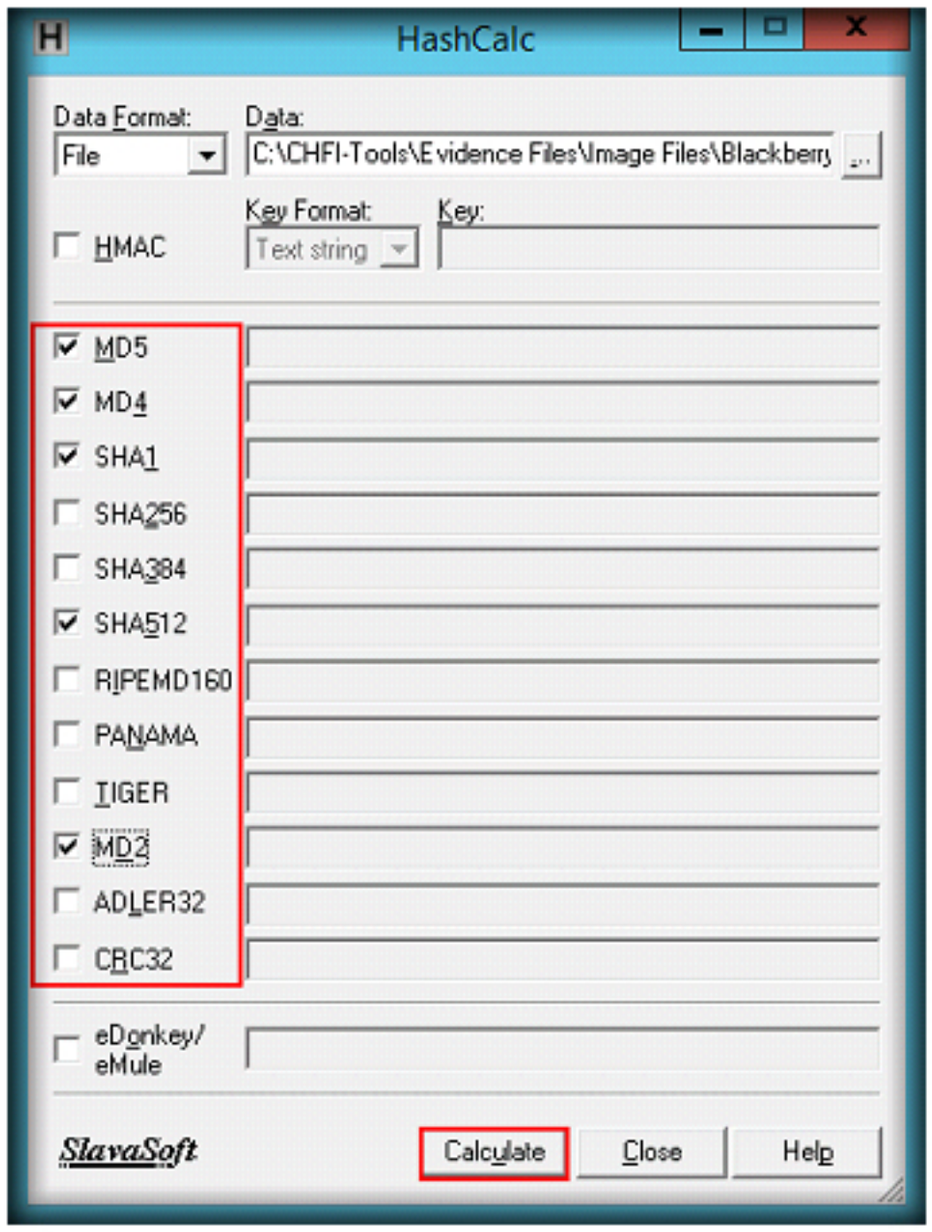

FIGURE 2.8: Calculation of hash values

10. Hash values will be displayed for the selected file as shown in the following screenshot:

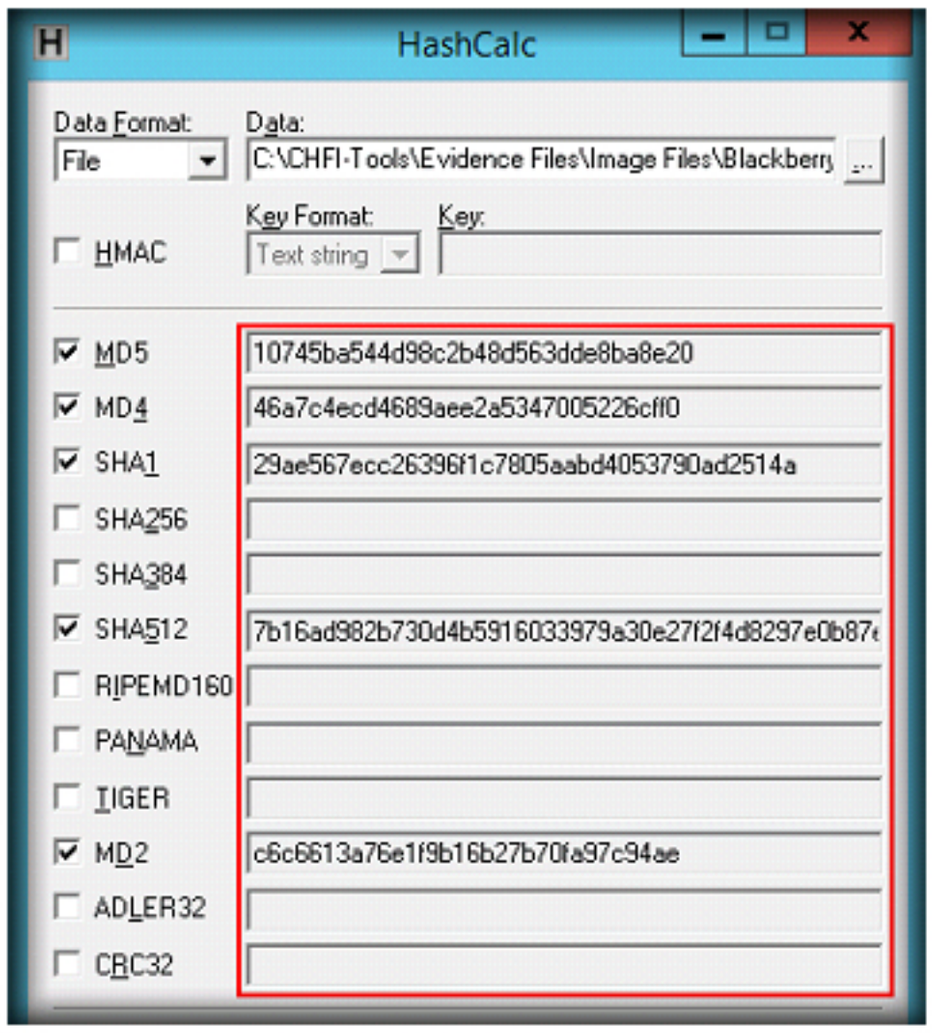

FIGURE 2.9: Window displaying hash values

Support of two modes of calculations: HASH/CHECKSUM and HMAC.

TASK 4

Calculating HMAC for the Data

11. To calculate the Keyed - Hash Message Authentication Code(HMAC) for the data:
    - Check the **HMAC** box.
    - In the **Key Format** combo box, select the type of the key you want to use for calculations. HashCalc allows you to perform calculations using text keys or hex keys.
    - In the **Key** box, enter the key for HMAC calculations (for example, here **test** is entered as key)
    - Select the algorithms you want to use for calculations by checking the required.algorithms, and then click **Calculate**

HashCalc supports a custom hash algorithm (MD4-based) used in eDonkey and eMule applications.

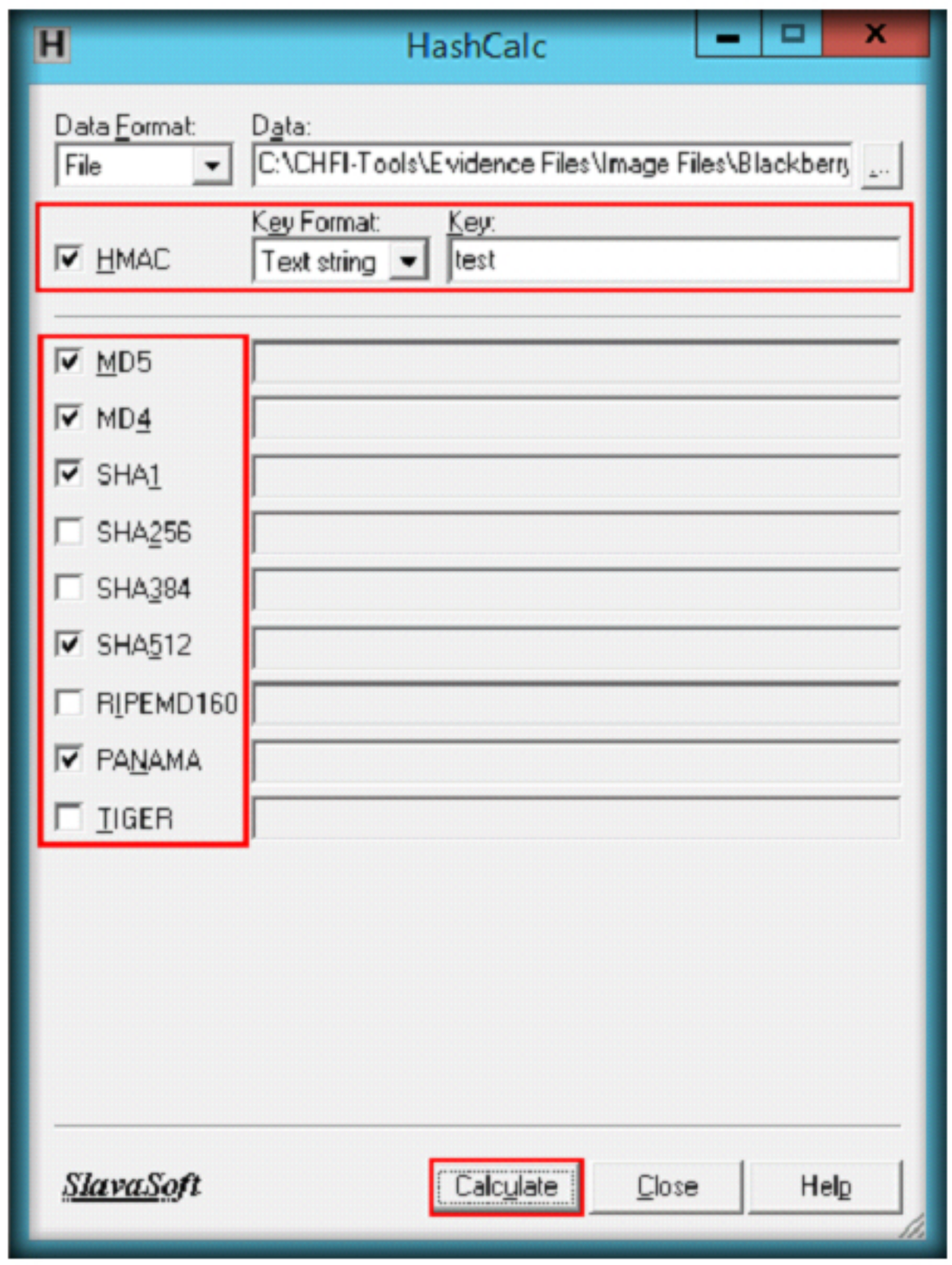

FIGURE 2.10: Calculating HMAC with key

12. HashCalc calculates the hashes of the specified file and displays them as shown in the following screenshot:

HashCalcoffers a choice of 13 of the most popular hash and checksum algorithms for calculations.

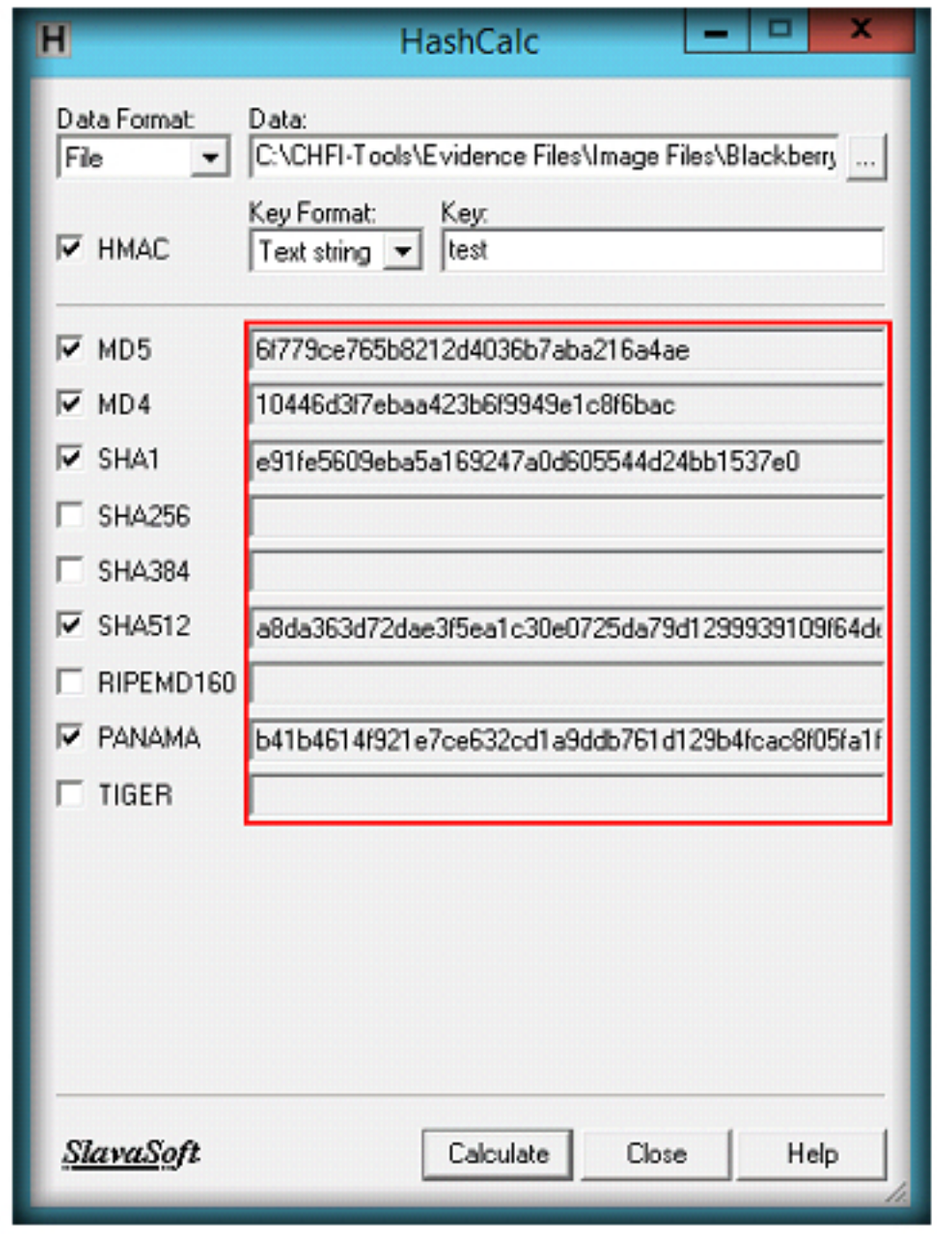

FIGURE 2.11: Window displaying hash values

13. Both the windows containing MD5 hash values (with key and without key) are shown below for students' understanding:

Supports the MD4-based hash algorithm used in many P2P applications (eDonkey, eMule, etc.).

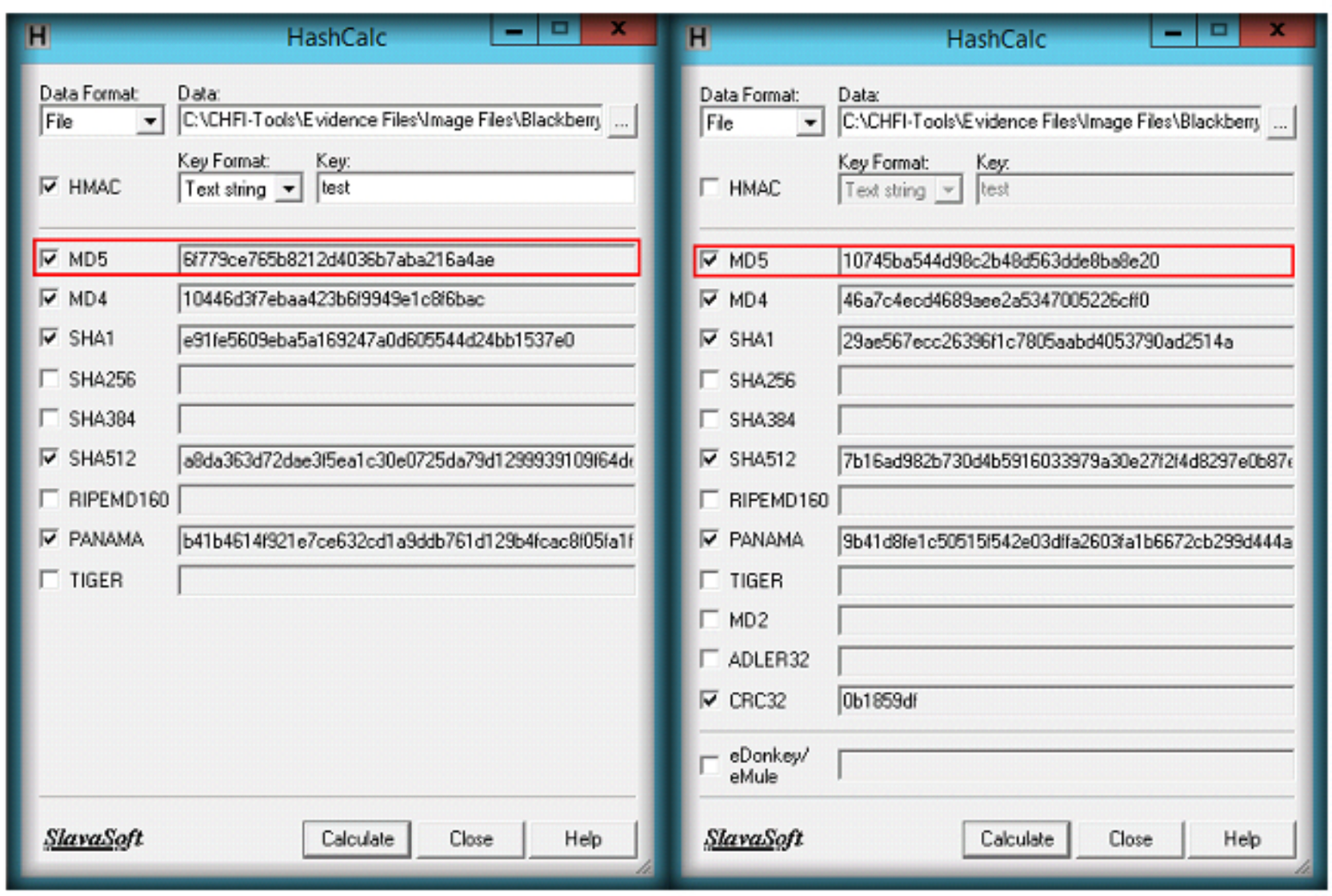

FIGURE 2.12: Windows displaying hash values with and without key

TASK 5

Calculating Hex Value of Text String

14. If you want to perform a calculation for a text string, first select **Text string** from the **Data Format** drop-down list and then enter the text in the **Data** field.
15. Select the algorithms you want to use for calculations by checking the required algorithms and then click the **Calculate** button.

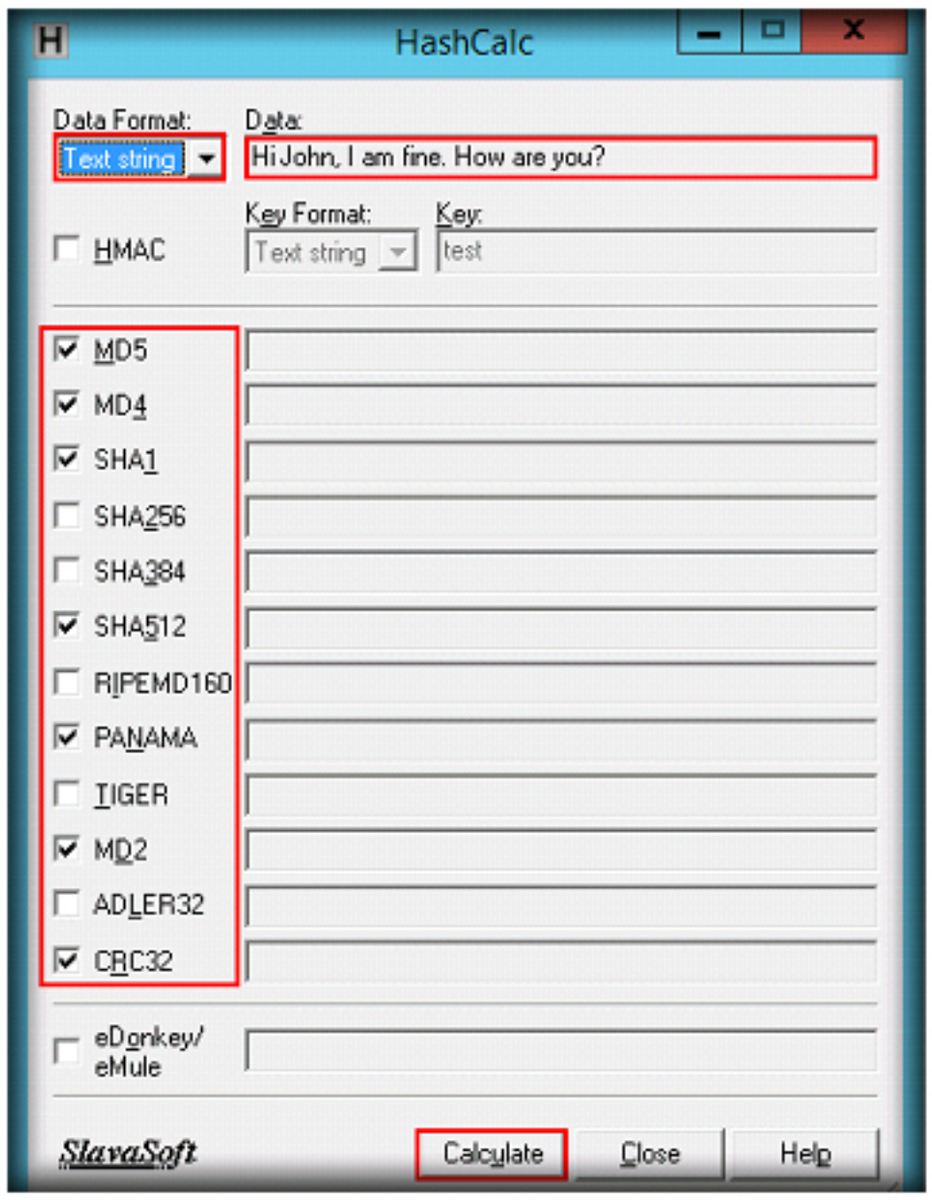

FIGURE 2.13: Calculating hash values for given text

16. Hash values will be displayed for the selected algorithms as shown in the following screenshot:

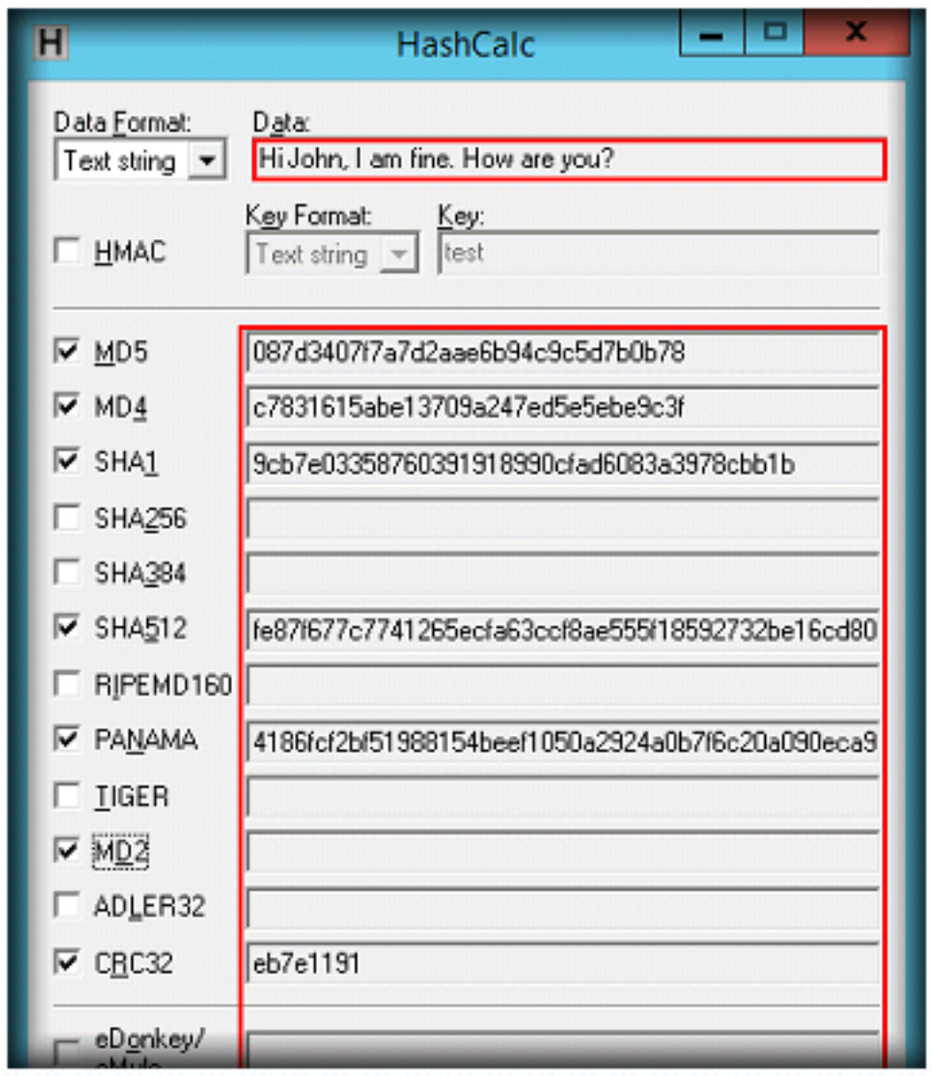

FIGURE 2.14: Display of encoded data in HashCalc

Lab Analysis

Document all Hash, MD5, and CRC values for further reference.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐Yes	☑No
Platform Supported	
☑ Classroom	☑iLabs

Lab

3

Generating MD5 Hashes Using MD5 Calculator

MD5 Calculator is a simple application that calculates the MD5 hash of a given file. It can be used with big files with sizes measured in GBs. It features a progress counter and a text field from which the final MD5 hash can be copied easily to the clipboard.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

During an investigative process, a forensics examiner was successful in extracting some programs from a target computer. The examiner uses MD5 hash values to check the presence of similar file across a malware database and finds the malicious file.

To be an expert computer forensic investigator,one must have sound knowledge of tools used for computing hashes and checking the checksums.

Lab Objectives

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

- Use encrypting commands.
- Calculate the MD5 value of selected files.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

Lab Environment

This lab requires:

- MD5 Calculator, which is located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\MD5 Calculator**.
- A computer running **Windows Server 2012 virtual machine**.
- Administrative privileges to run tools.

- You can also download the latest version of **MD5 Calculator** from http://www.bullzip.com/download.php.
- Kindly note that, if you decide to download the latest version, then screenshots shown in the lab might differ.

Lab Duration

Time: 10 Minutes

Overview of MD5 Calculator

MD5 Calculator is a bare-bones program for calculating and comparing MD5 files. While its layout leaves something to be desired, its results are fast and simple.

Lab Tasks

TASK 1

Selecting an Evidence Image

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\MD5 Calculator**.
2. Double-click **md5calc(1.0.0.0).msi** to launch the setup, and then follow the wizard-driven installation steps to install the application.

   Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

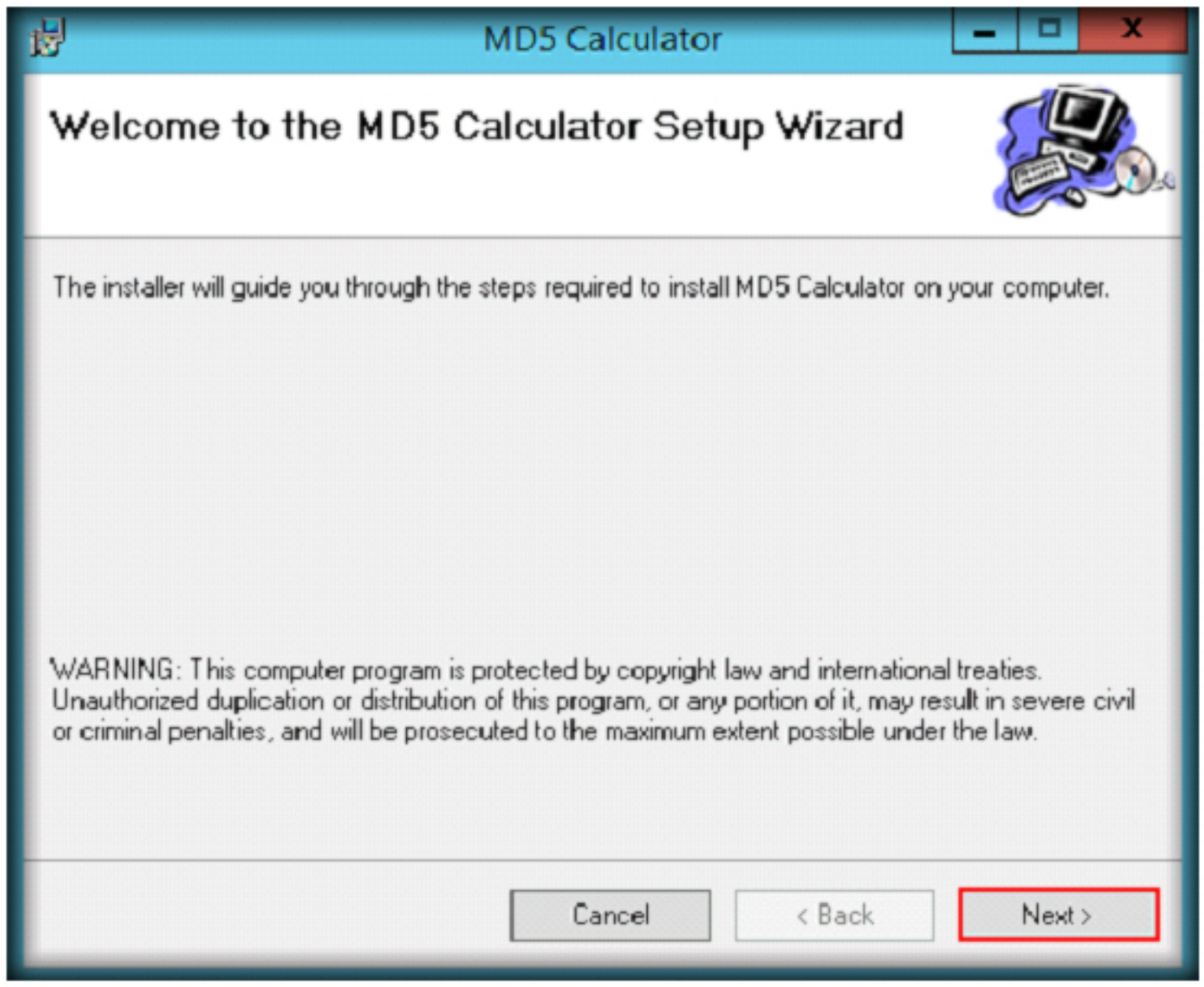

FIGURE 3.1: MD5 Calculator Setup Wizard

3. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** for the evidence file for this lab.

The Message-Digest algorithm 5 (MD5) was created by a professor named Ronald L. Rivest of MIT. Using this algorithm, you are able to calculate a hash value or digest of any message. A digest works as a fingerprint for the text on which you apply the algorithm. A fingerprint has a 128-bit length and is often written as a characterstring of 32 hex digits.

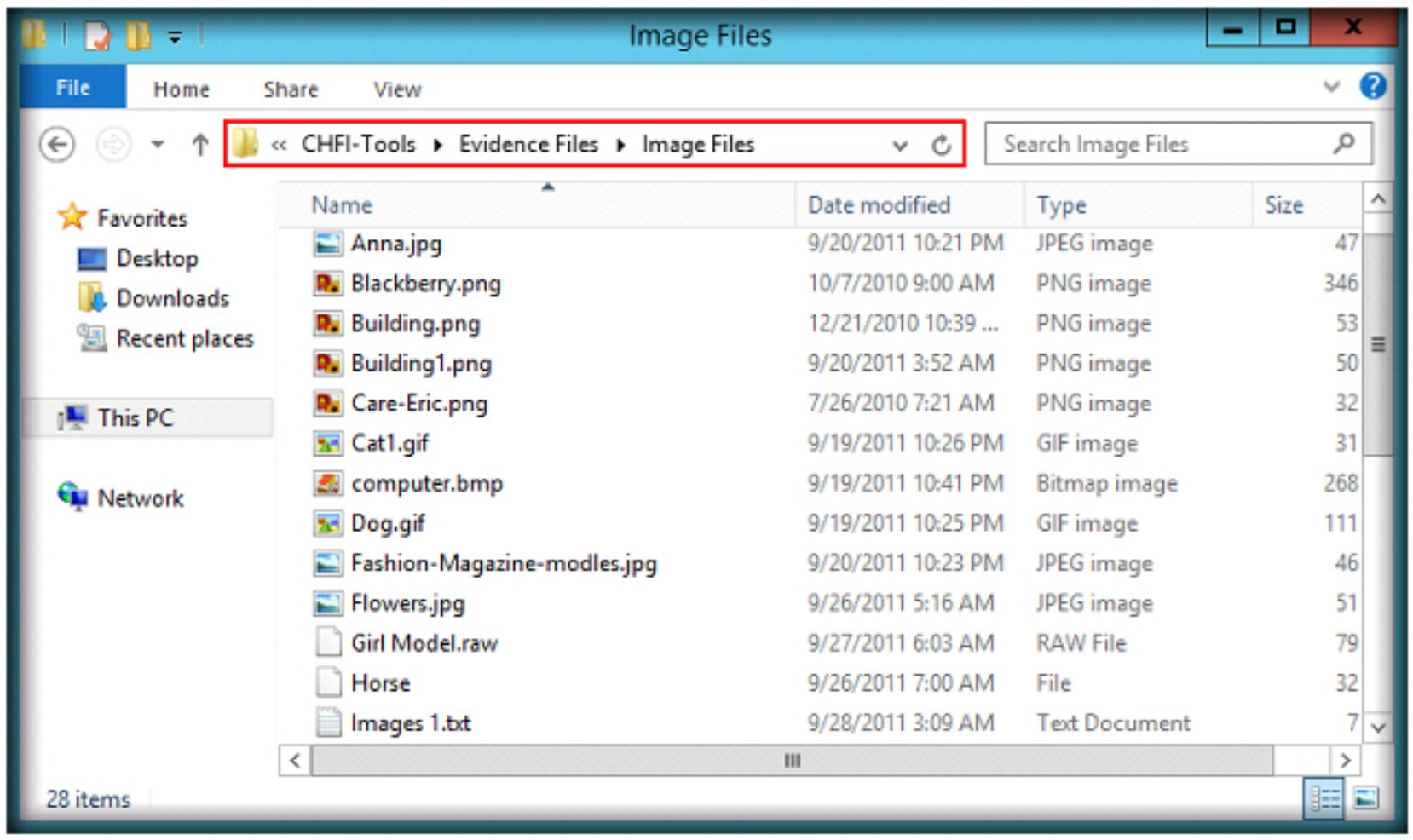

FIGURE 3.2 Evidence file

4. To calculate the MD5 hash of a file, first select a particular file, right-click on it and then select MD5 Calculator from the context menu.

You can compare the calculated value to a value given to you by another person or from a website.

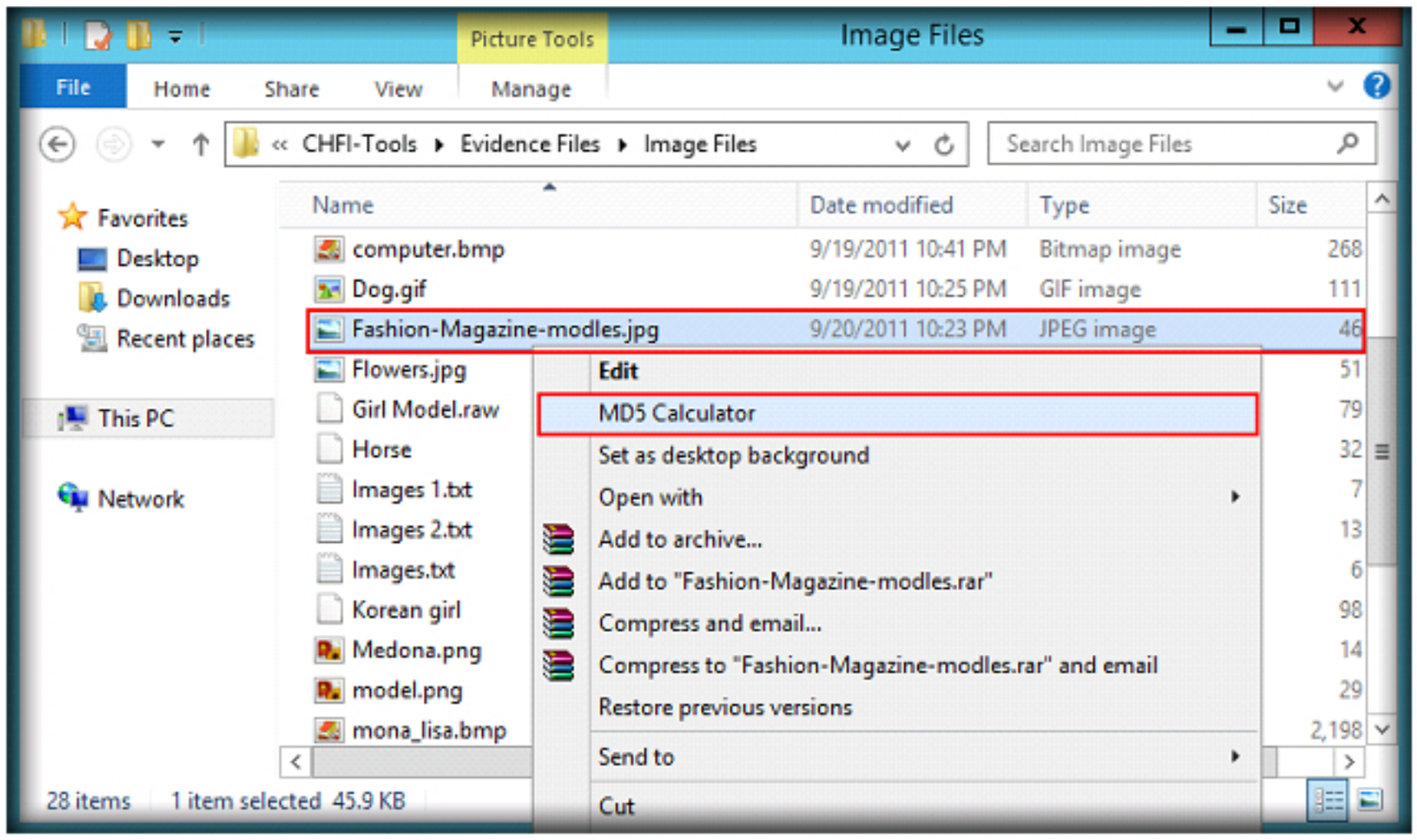

FIGURE 3.3 MD5 Calculator

TASK 2

Calculating MD5 Hash Value

5. The **MD5 Calculator** window will subsequently appear, displaying the MD5hash value for the selected file as shown in the following screenshot:

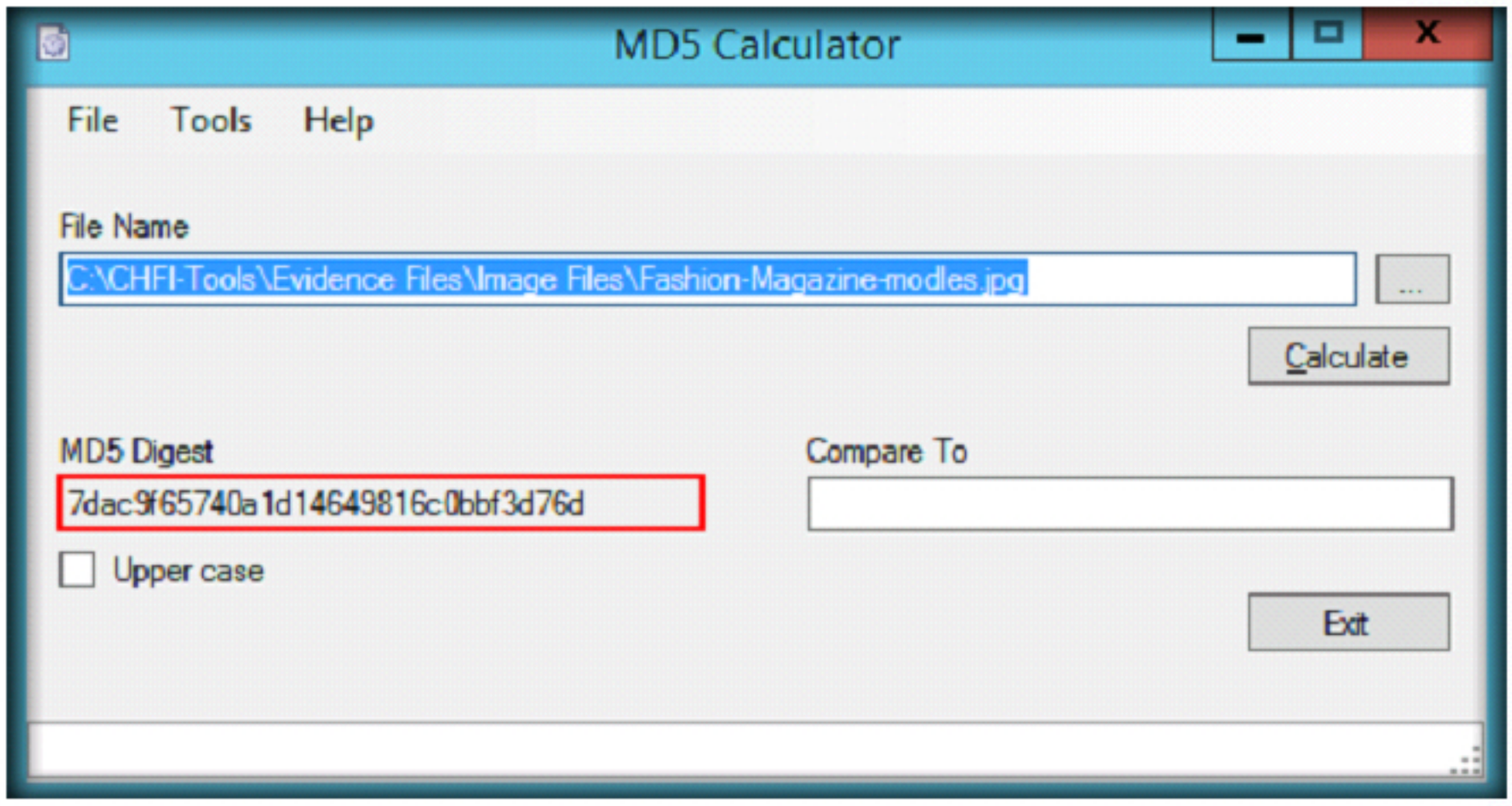

FIGURE 3.4: Displayed hash value in MD5 calculator

Note: When the tool is used for the first time, it displays the result of the selected file directly under the **MD5 Digest** column and there is no need to click the **Calculate** button.

6. If you want to calculate the hash value of another file, click the **ellipsis** button corresponding to the **File Name** field.

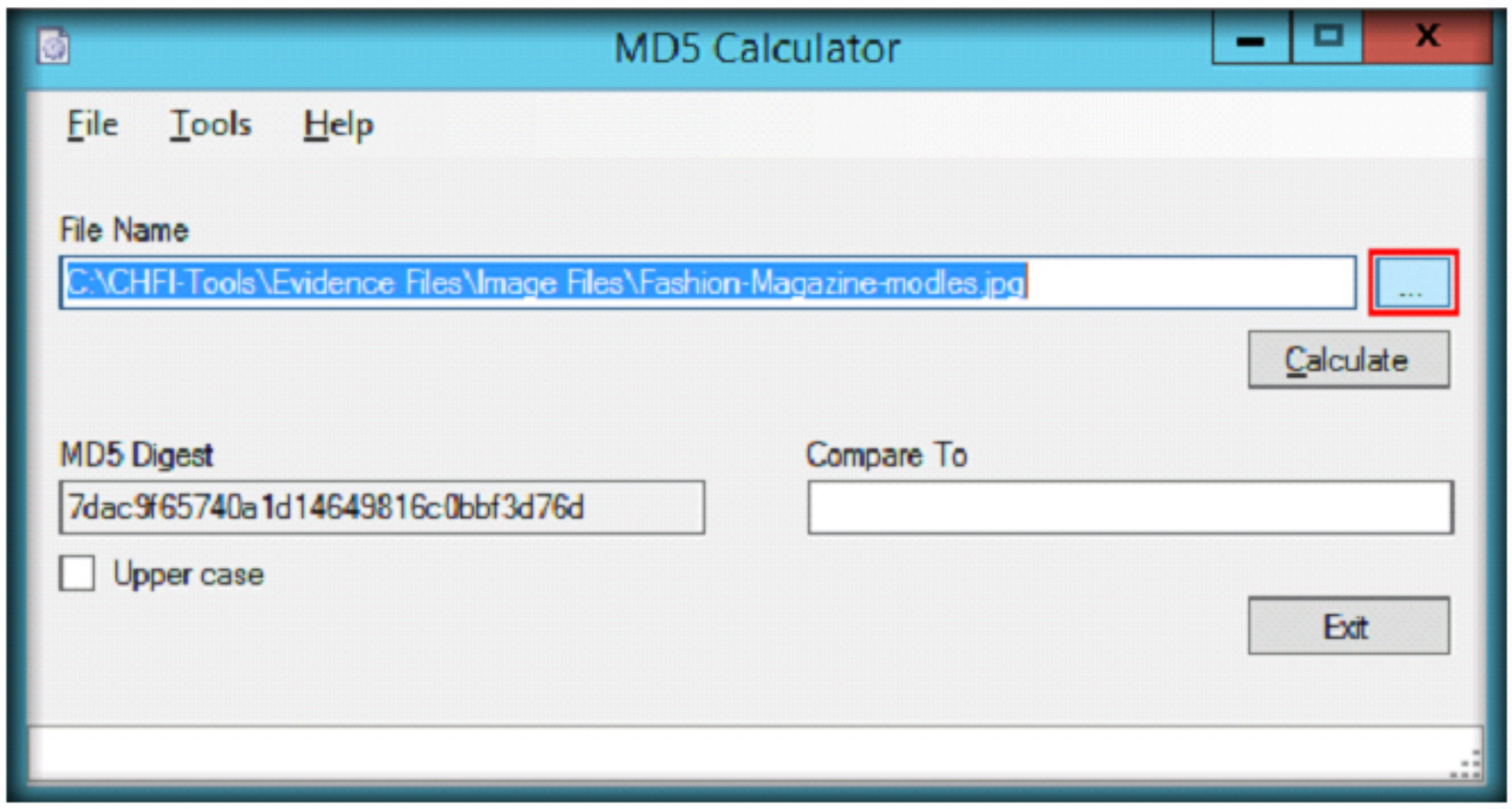

FIGURE 3.5: MD5 calculators browse option

The MD5 algorithm was created by a professor named Ronald L. Rivest of MIT.

7. The **Select file to calculate MD5 hash** window will pop up. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files**, select a file other than the previously selected file, (here we are selecting**Building.png** file) and then click **Open**.

The **MD5 Digest** field contains the calculated value. If you want to compare this MD5 digest to another, you can paste the other value into the **Compare To** field. An **=** sign will appear between the two values if they are equal. Otherwise, the <> sign will tell you that the values are different. Analyze and document the results related to the lab exercise.

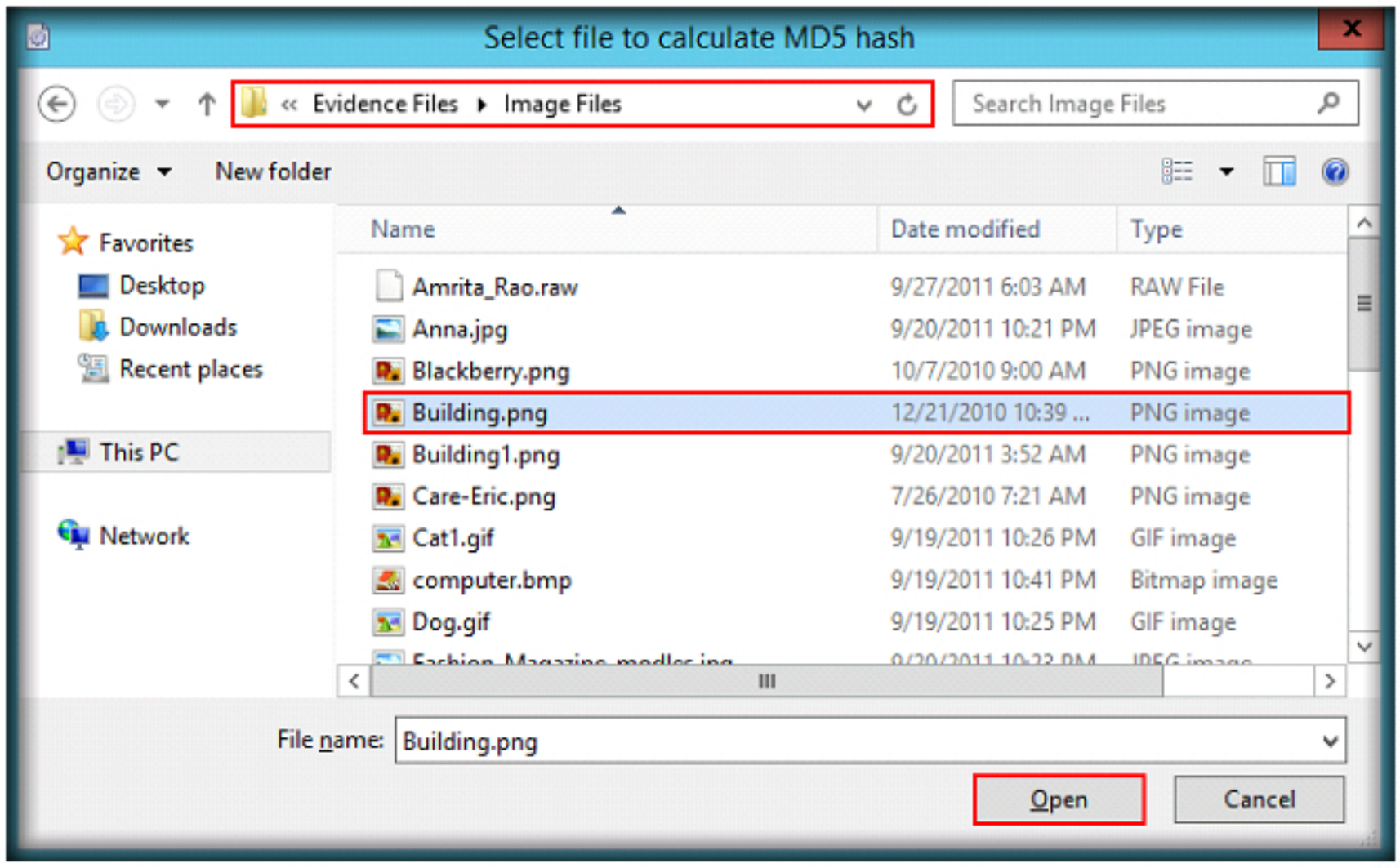

FIGURE 3.6: MD5 calculators file selection window

8. The selected file will be displayed in the **File Name** field, click the **Calculate** button to calculate the MD5 hash of the file.

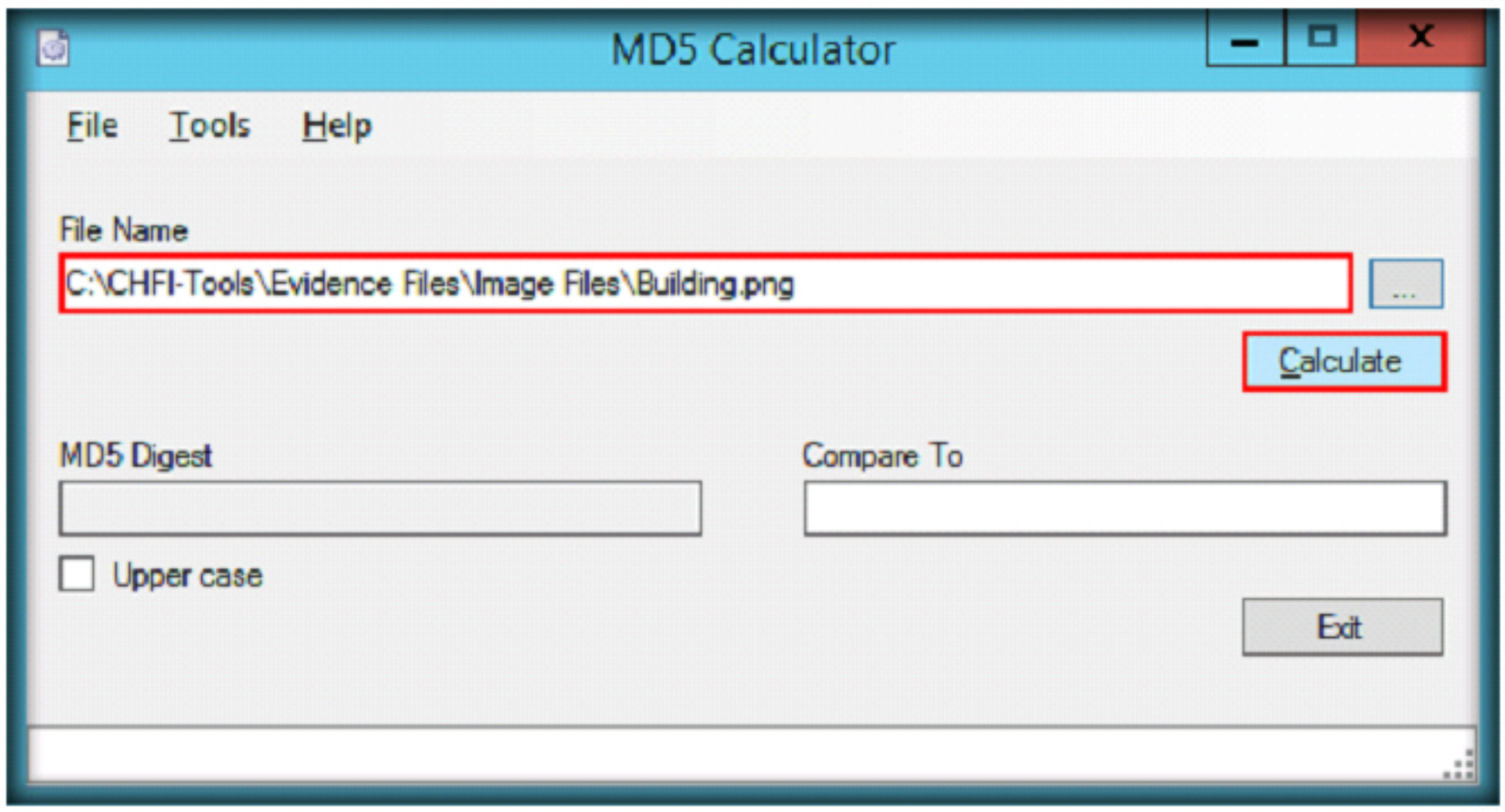

FIGURE 3.7: MD5 calculators calculating MD5 hash

9. **MD5 Calculator** displays the**MD5 Digest** (hash value) for the selected file as shown in the following screenshot:

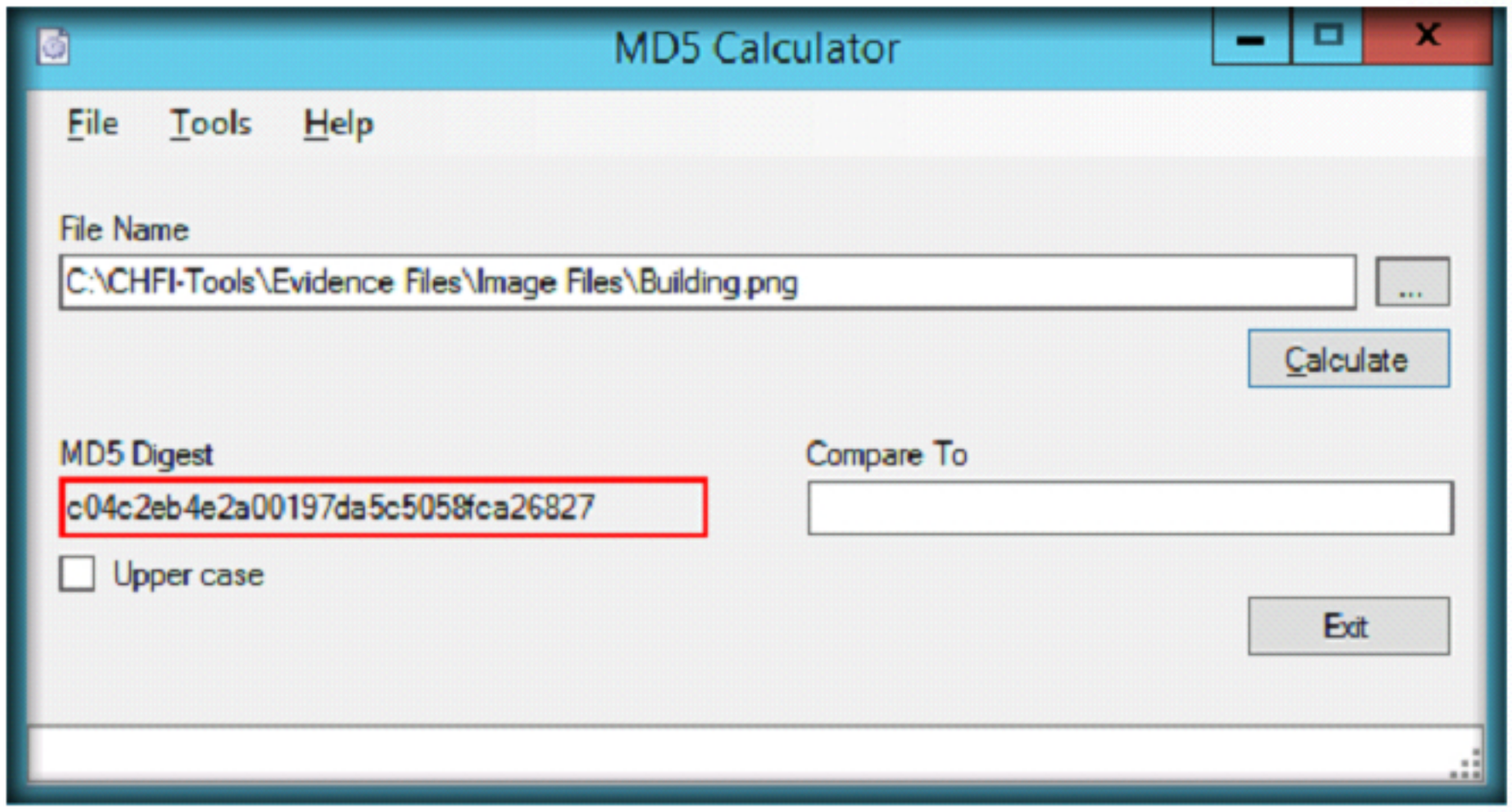

FIGURE 3.8: Displayed hash value in MD5 calculator

Lab Analysis

Analyze and document all the calculated hash values related to this lab exercise by using MD5 calculator.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐Yes	☑No
Platform Supported	
☑ Classroom	☑iLabs

Lab

4

Viewing Files of Various Formats Using the File Viewer

File Viewer is a Disk/File Utility that helps you quickly locate, view, print, organize, and exchange files.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A network administrator has reported transmission of some unknown files across the company's network after a security breach incident. Upon investigation, the investigators found that the attacker had hidden the file format to confuse the network administrator. The investigators used File Viewer tool to recognize the format and extract its contents that led to the attack.

To be a computer forensic expert, you must have sound knowledge of various file viewing tools used for forensic investigations. This knowledge includes how to locate files quickly, view files of different formats, etc.

Lab Objectives

The objective of this lab is to help students 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
- Saving files of various file types

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

Lab Environment

This lab requires:

- File Viewer tool, located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\File Viewer**.
- You can also download the latest version of **File Viewer** from http://www.accessoryware.com/fileview.htm
- Kindly note that if you decide to download the latest version, then the screenshots shown in this lab might differ slightly.
- A computer running **Windows Server 2012 virtual machine**.
- Administrative privileges to install and run tools.

Lab Duration

Time: 10 Minutes

Overview of File Viewer

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.

Lab Tasks

TASK 1

Launching File Viewer

1. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** to view the evidence files. You will be selecting a file from this location in the subsequent steps.

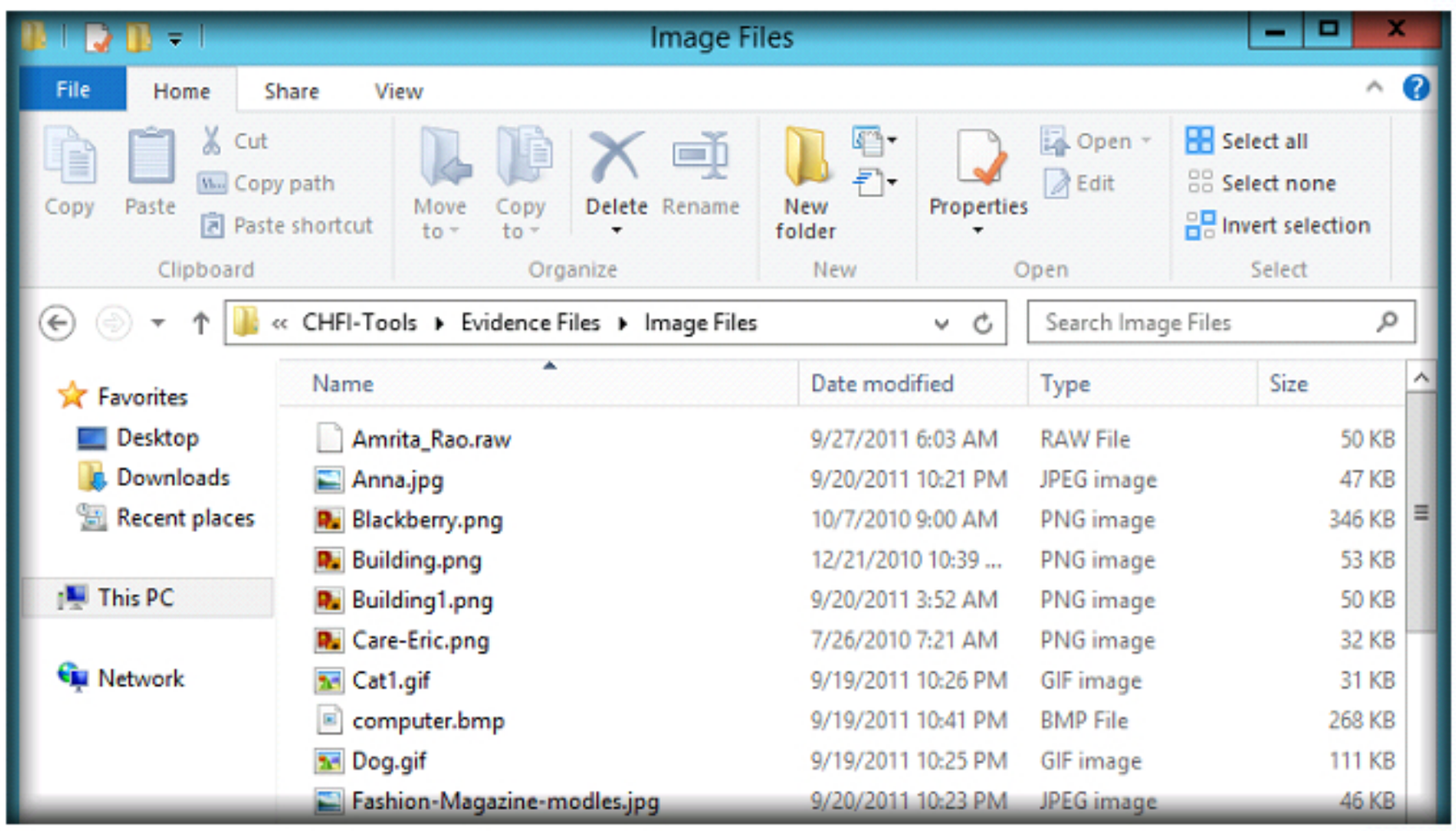

FIGURE 4.1: Image Files Folder

Files can be rated by priority, and up to three search words or phrases can be included per file for extra search capability. This is useful if you are on a network, and frequently need files on other computers

2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\File Viewer**, double click **FileView.exe** to launch the setup and follow the wizard-driven installation steps to install the application.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

File viewer supports different Picture File Types such as JPG, CMP, GIF, uncompressed TIF, TIFF, BMP, ICO, CUR, PCX, DCX, PCD, FPX, WMF, EMF, FAX, RAW, AWD, XPB, XPM, IFF, PBM, CUT, PSD, PNG, TGA, EPS, RAS, WPG, PCT, PCX, CLP, XWD, FLC, ANI, SGI, XBM, MAC, IMG, MSP, CAL, ICA, SCT, SFF, SMP, etc.

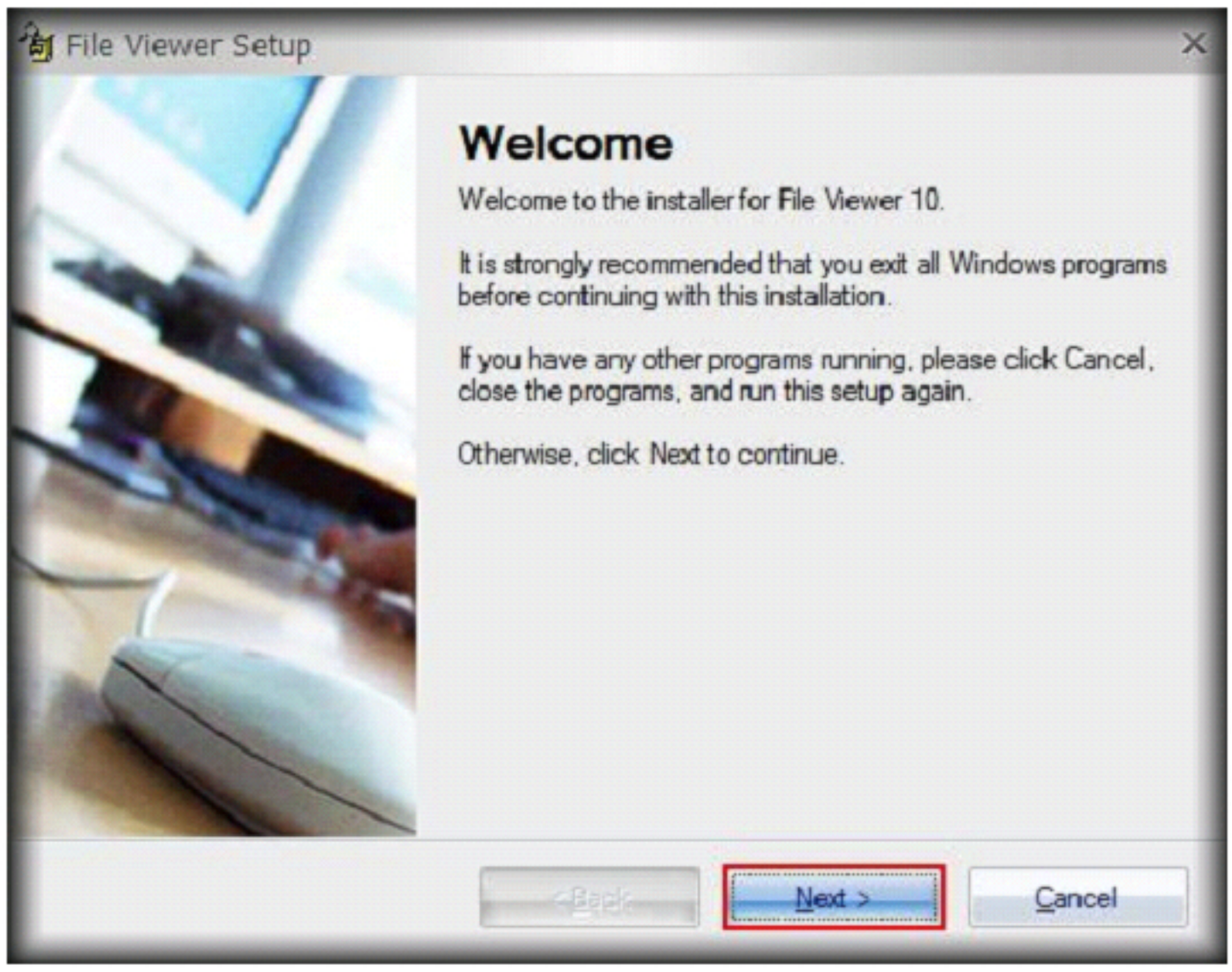

FIGURE 4.2: File Viewer Installer

3. Double-click **File Viewer 9.5** icon on the **Desktop** to launch the application.

Note: Alternatively, you may launch the application from the Apps screen.

4. The **File Viewer Registration** pop-up appears. Click the **Close** button to open the **File Viewer** window.

File viewer is supported by Windows 2000/XP/Vista/7/Server 2008/Server 2012.

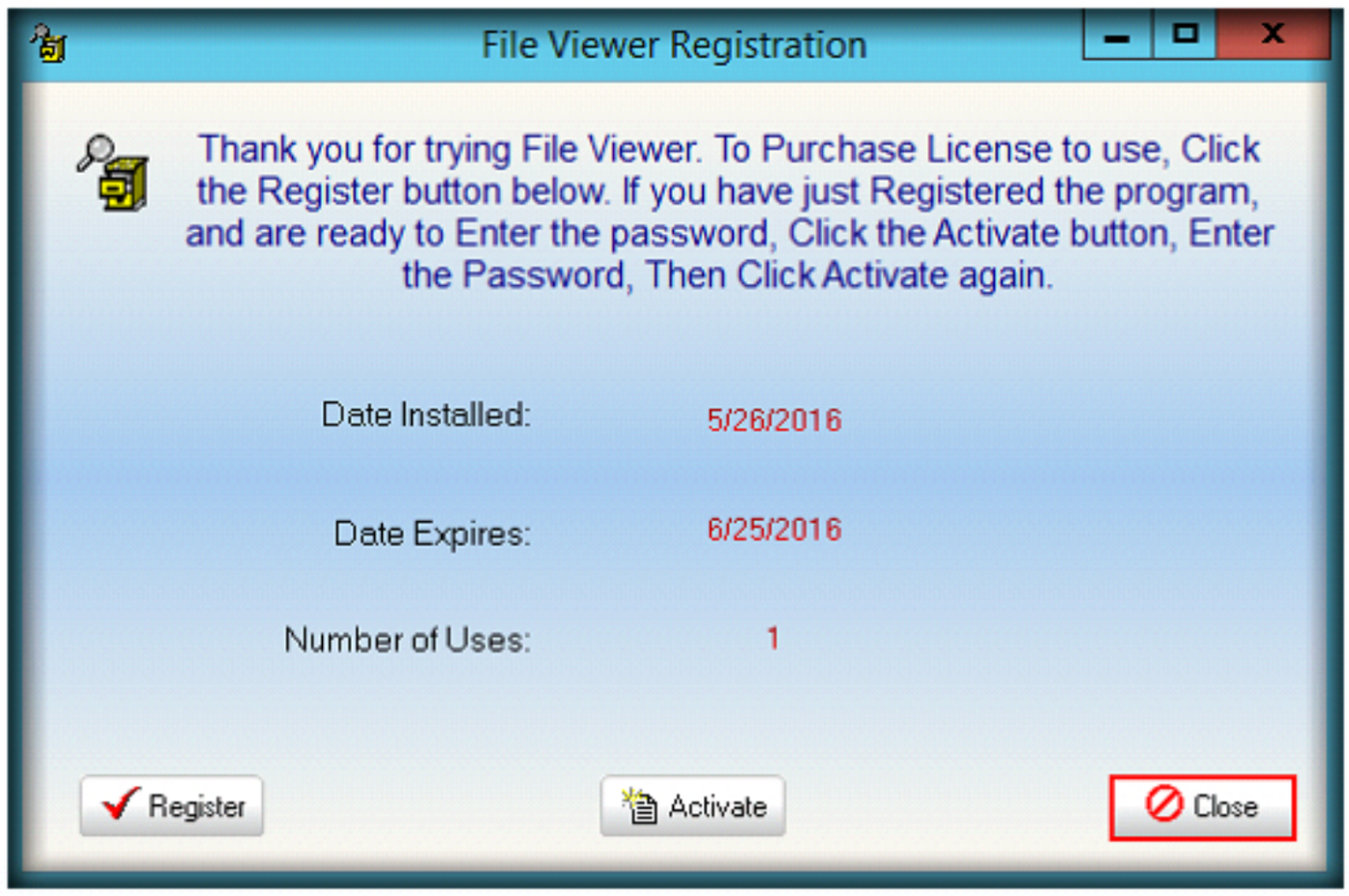

FIGURE 4.3: File Viewer registration

5. The **File Viewer** main window appears, along with a **Getting Started with File Viewer** dialog-box. Check on the **Do Not Show on Start Up** option and click **Cancel**.
6. If the pop-up does not appear, skip to the next step.

You must have at least 128 MB of RAM for the program to run. If you have 256 MB or greater, memory problems using File Viewer should be minimal. Loading too many pictures can cause you to stay on one window, not being able to access the viewing window.

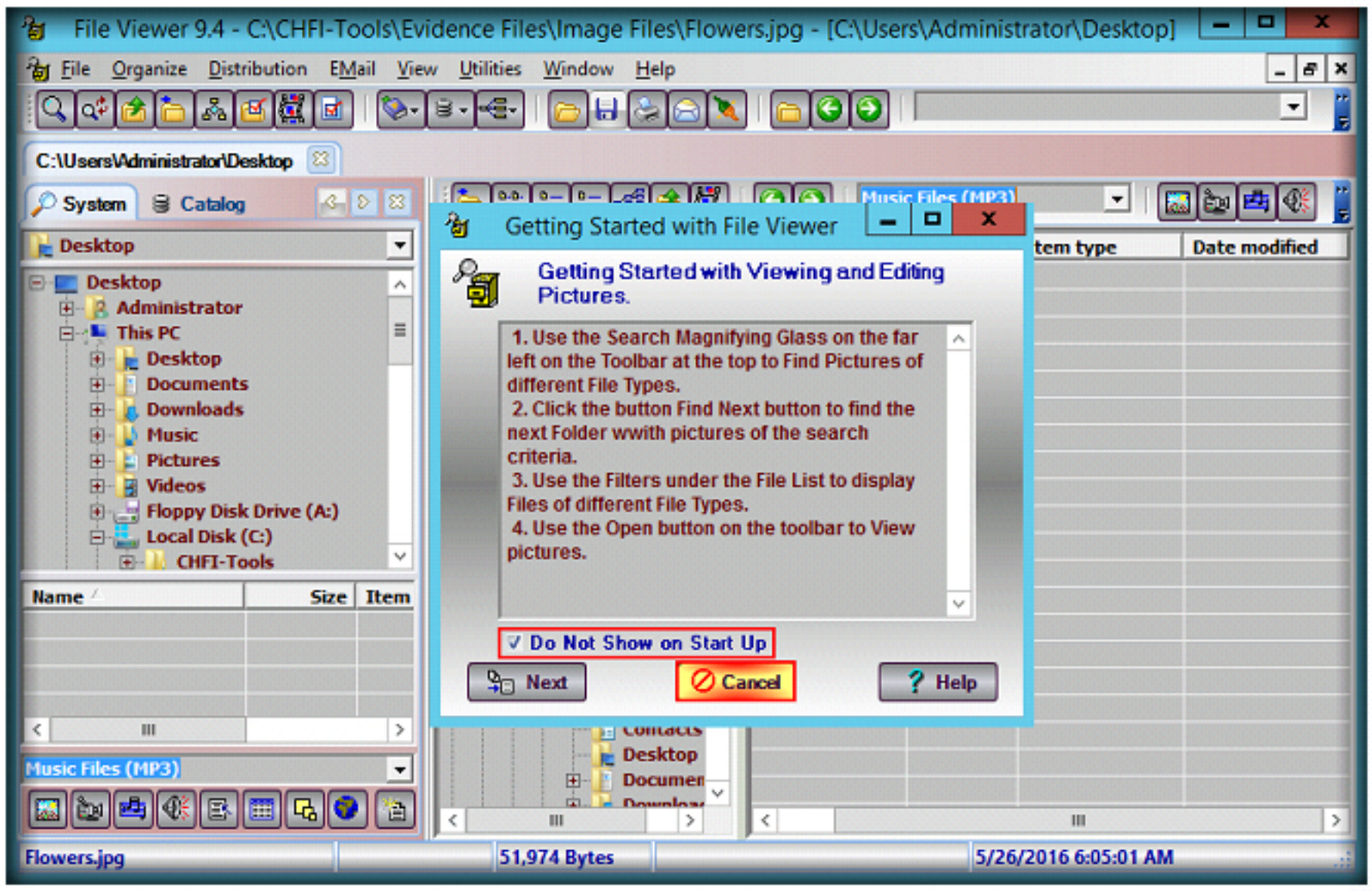

FIGURE 4.4: Getting Started with File Viewer dialog-box

TASK 2

Selecting the Evidence File

7. Go to **File** menu and click **Open**.

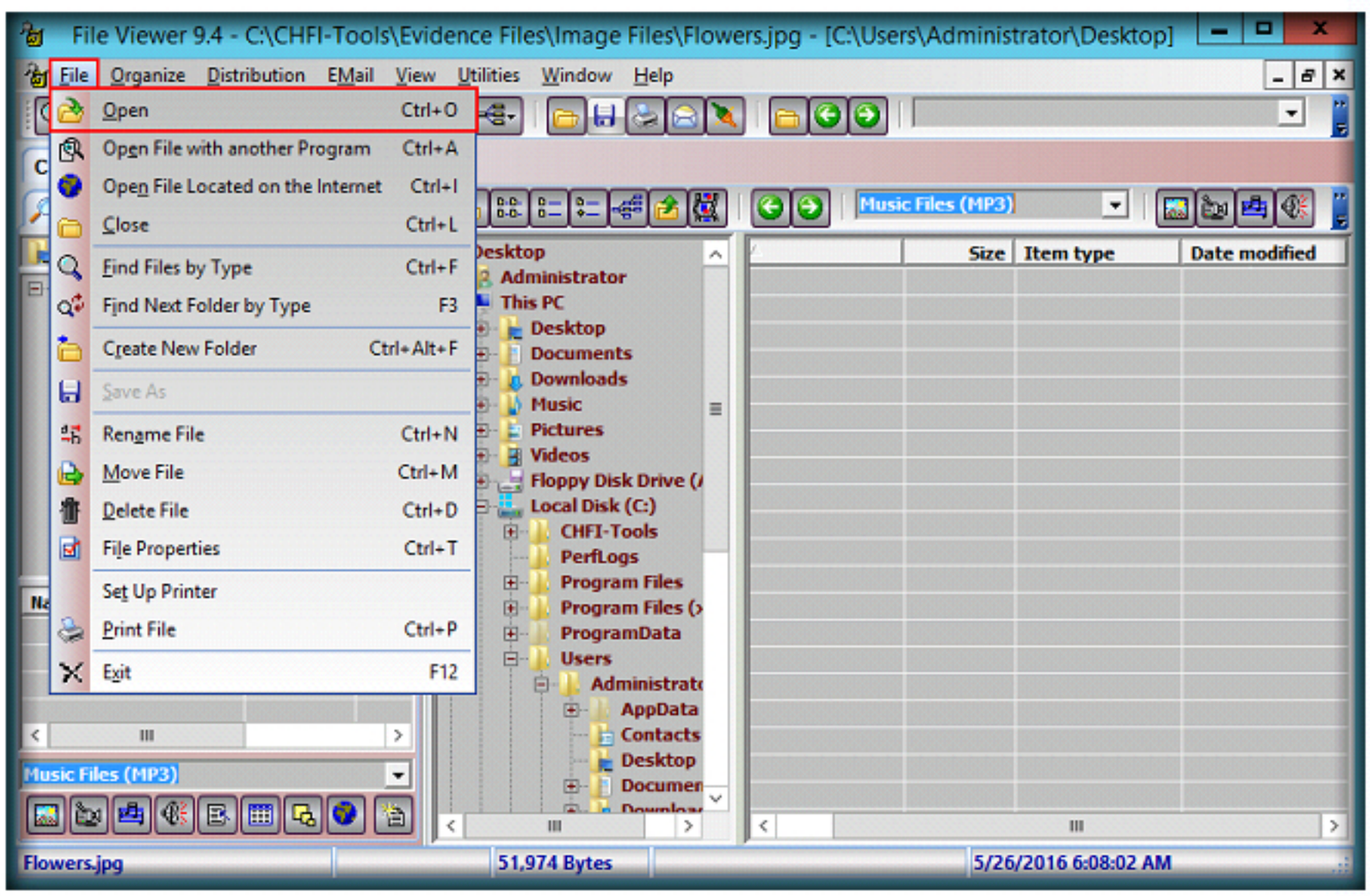

FIGURE 4.5: File Viewer File Menu

8. In the **Open** dialog box:
   - Locate the evidence file path (**C:\CHFI-Tools\Evidence Files\Image Files**).
   - Select **All files (*.*)** in the **File type** drop-down list.
   - Select the file (**Flowers.jpg**), and then click **Open**.

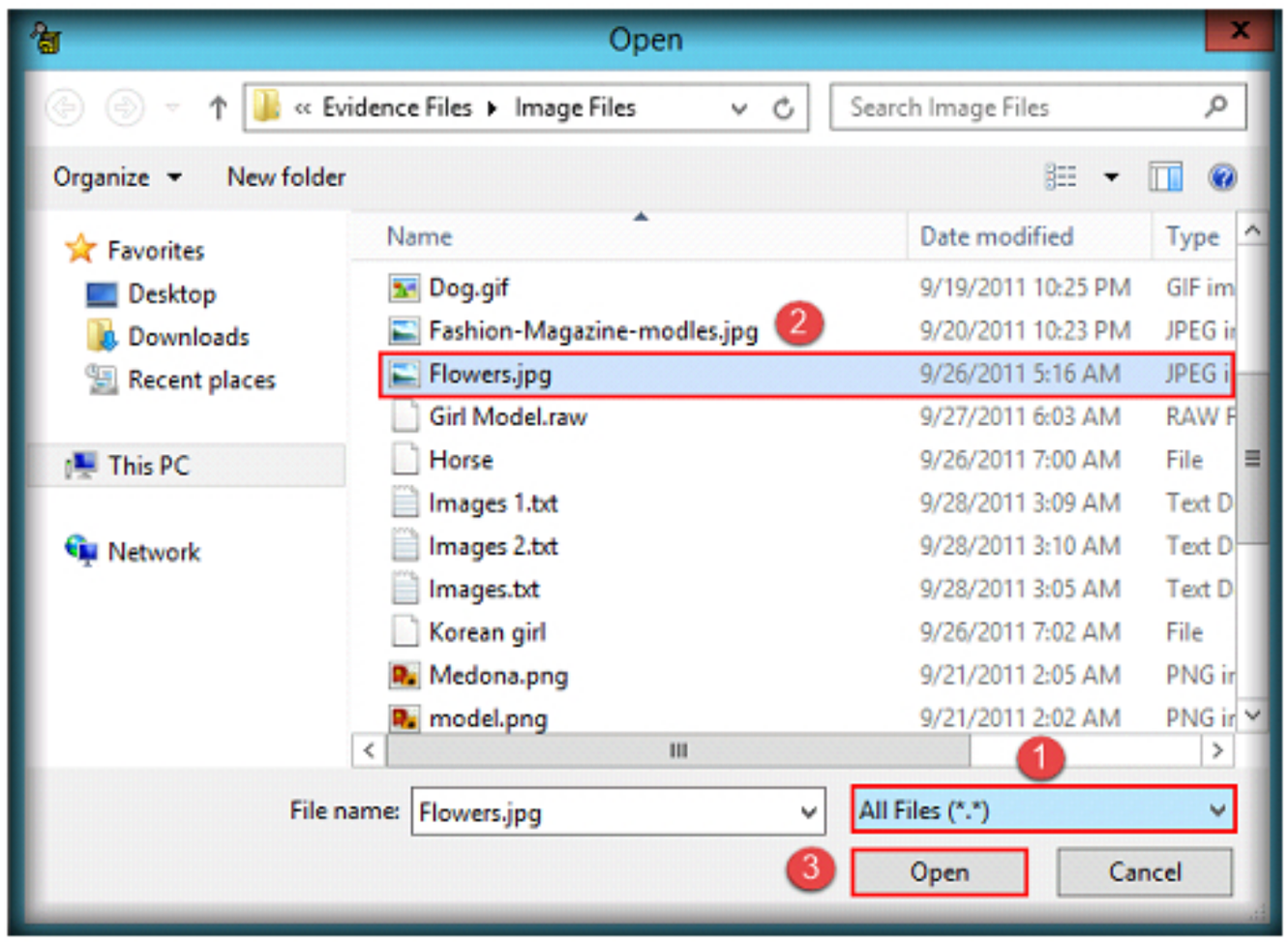

FIGURE 4.6: Opening of evidence files

9. If a **Getting Started with File Viewer** pop up appears, click **Cancel**.
10. The image **Flowers.jpg** opens in the file viewer screen as shown in the following screenshot:

The File Viewer contains the Microsoft Multimedia player component, so you can play Video Files (AVI, MPG, MOV) and music files (MP3, MIDI, and M3U). Separate playlists are included for video and audio files.

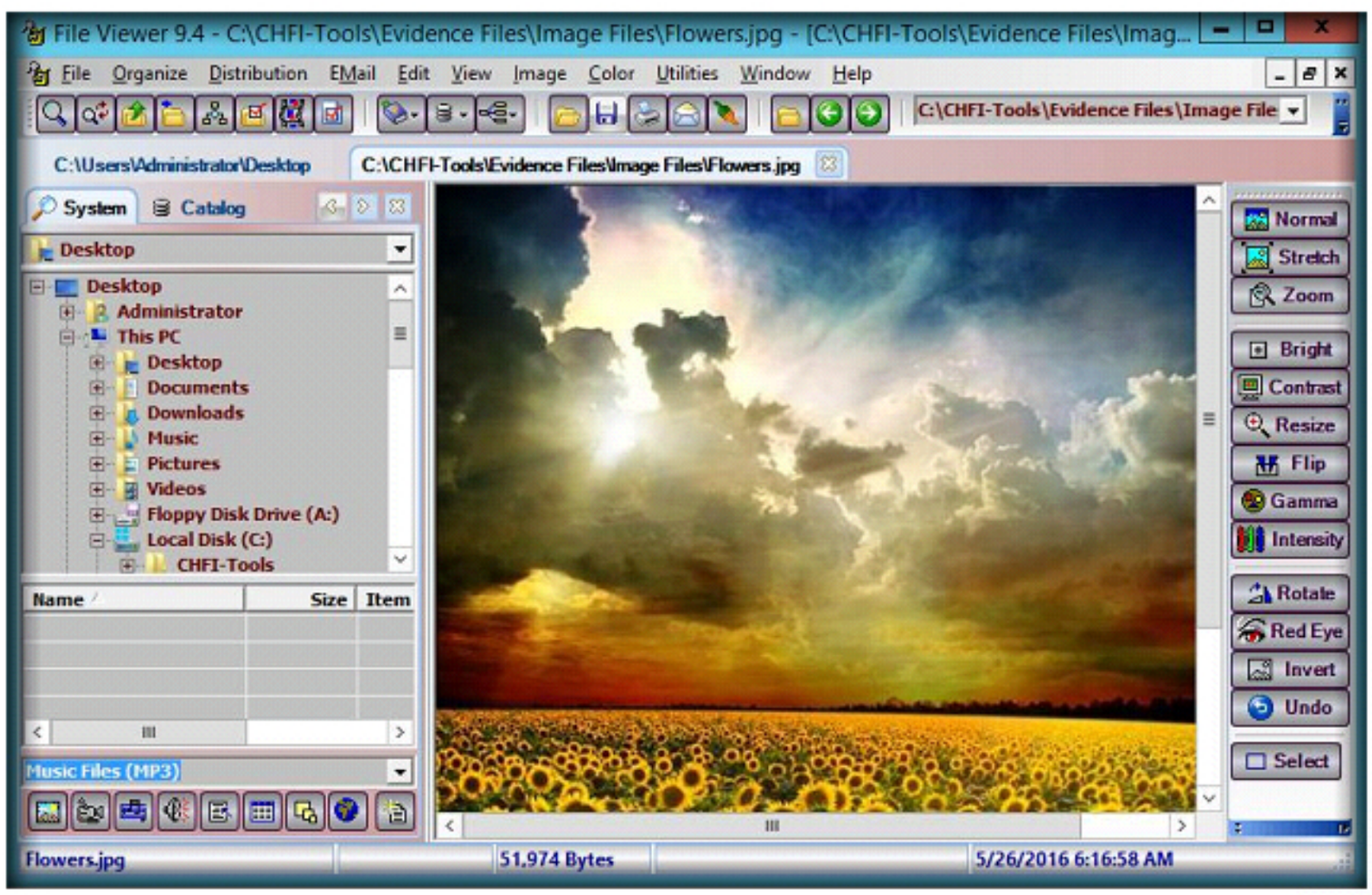

FIGURE 4.7: Opening of image file

TASK 3

Viewing the File Properties

11. Navigate to **File→File Properties** to view various properties of the selected image.

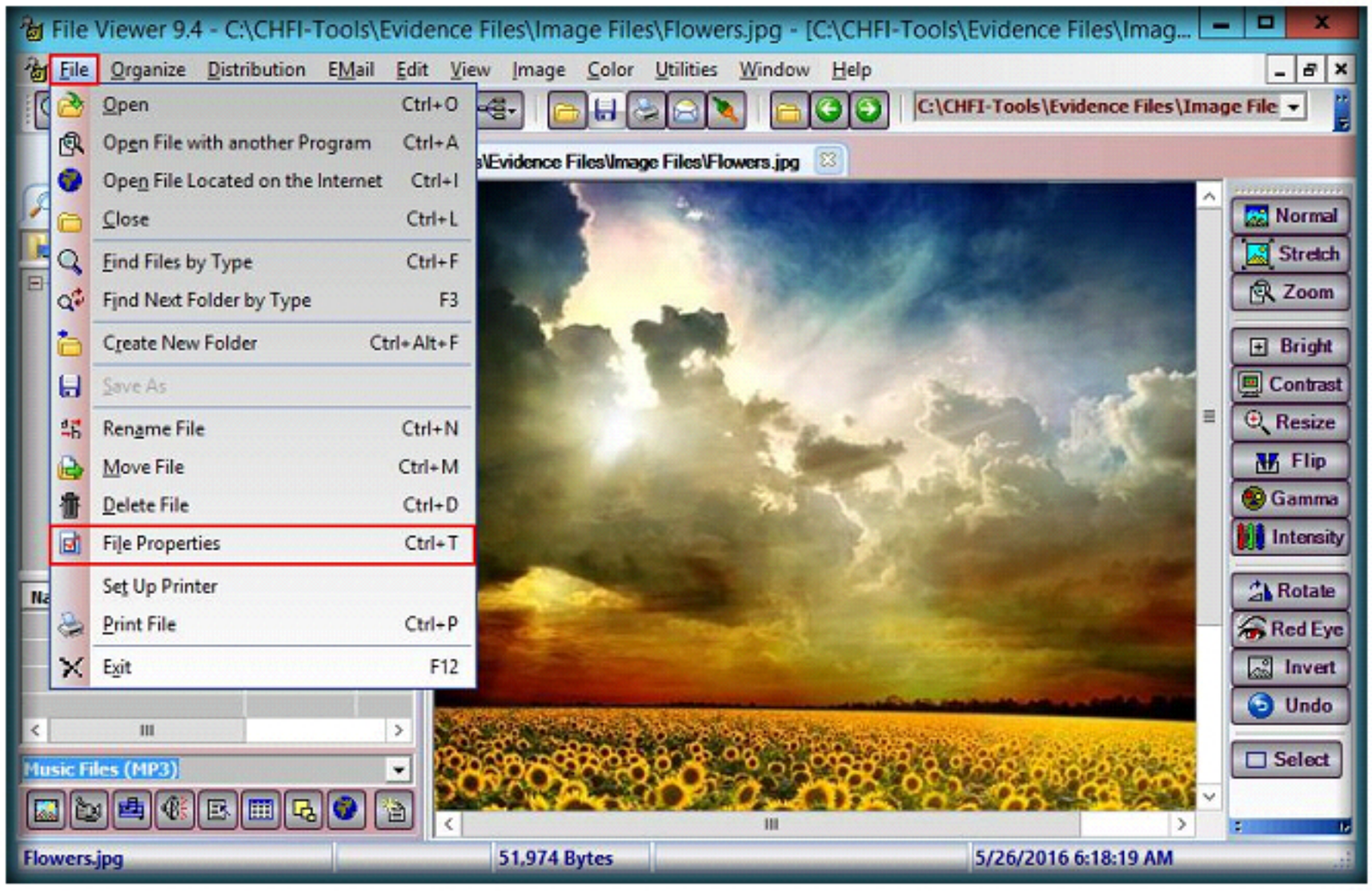

FIGURE 4.8: File Viewer File Properties option

File Viewer provides many functions such as viewing, printing, email, playing multimedia files, organizing, and batch file functions. The Multifile Selection window allows you to select any number of files to be used for performing these functions.

12. The **File Properties** window will pop up showing various properties of the selected file. Click **OK** to close the window.

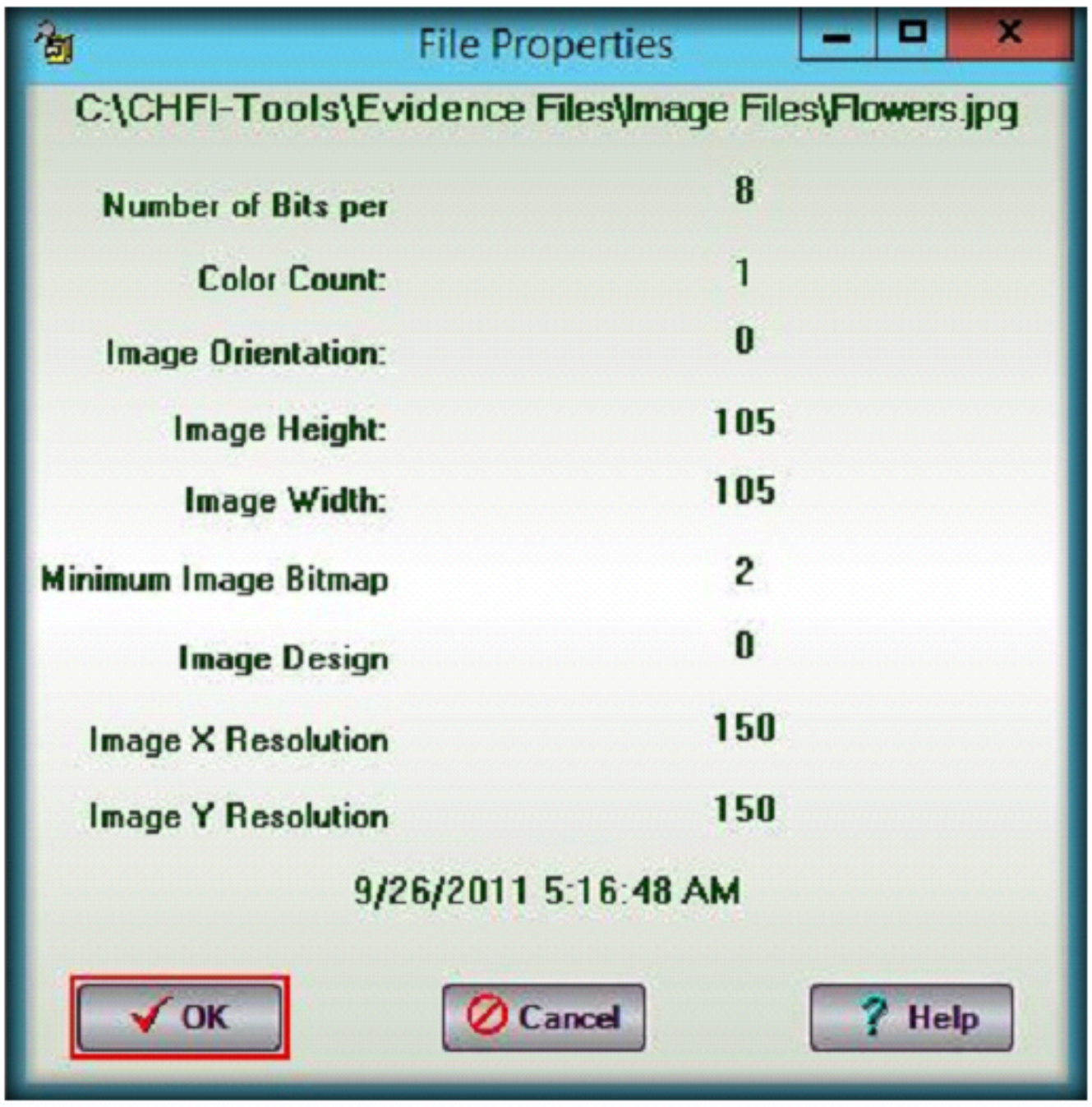

FIGURE 4.9: File Viewer File Properties window

File Viewer provides you with a Thumbnail window showing all the pictures in a selected folder.

13. You may save the image for further reference, and you have an option to save the image in a different file format. However, this feature is available only for the licensed version of File Viewer.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐Yes	☑No
Platform Supported	
☑ Classroom	☑iLabs

Lab

5

Handling Evidence Data Using the P2 Commander

P2 Commander is a comprehensive digital forensic tool designed to handle more data, more efficiently while keeping a specialized focus on the entire forensic examination process.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

After concluding the investigation process, a junior investigator had submitted the evidence files to the court for trial. The judge dismissed the case citing submission of poorly handled evidence or improperly presented data. This incident shows the importance of properly handling the evidence and presenting the data in a viable manner.

To be a computer forensic expert, you must have sound knowledge of handling forensic data more efficiently by using different tools such as P2 Commander.

Lab Objectives

The objective of this lab is to help students learn and use P2 commander for handling evidence data.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

This lab requires:

- The P2 Commander tool, which is located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\P2 Commander**.
- You can also download the latest version of **P2 Commander** from http://www.paraben.com/p2-commander.html.
- Please note that, if you decide to download the latest version, then the screenshots shown in this lab might differ slightly
- A computer running **Windows Server 2012 virtual machine**.
- Administrative privileges to install and run tools.

Lab Duration

Time: 20 Minutes

Overview of Handling Evidence Data Using the P2 Commander Tool

P2 Commander is a comprehensive digital forensic tool designed to handle more data, more efficiently while keeping a specialized focus on the entire forensic examination process. P2 Commander utilizes an advanced plug-in architecture to create specialized engines that focus on things such as email, network email, chat logs, file sorting, internet file analysis, and many more, while increasing the amount of data that can be processed and utilizing resources through multi-threading and task scheduling.

Lab Tasks

TASK 1

Launching P2 Commander

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\P2 Commander**.
2. Double-click **p2c-demo.exe** to launch the setup, and follow the wizard-driven installation steps to install the application.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

FIGURE 5.1: Paraben's P2C Installer

3. On completing the installation, Paraben's Dongle Manager installation wizard appears, follow the wizard driven installation steps to install Paraben's Dongle Manager.

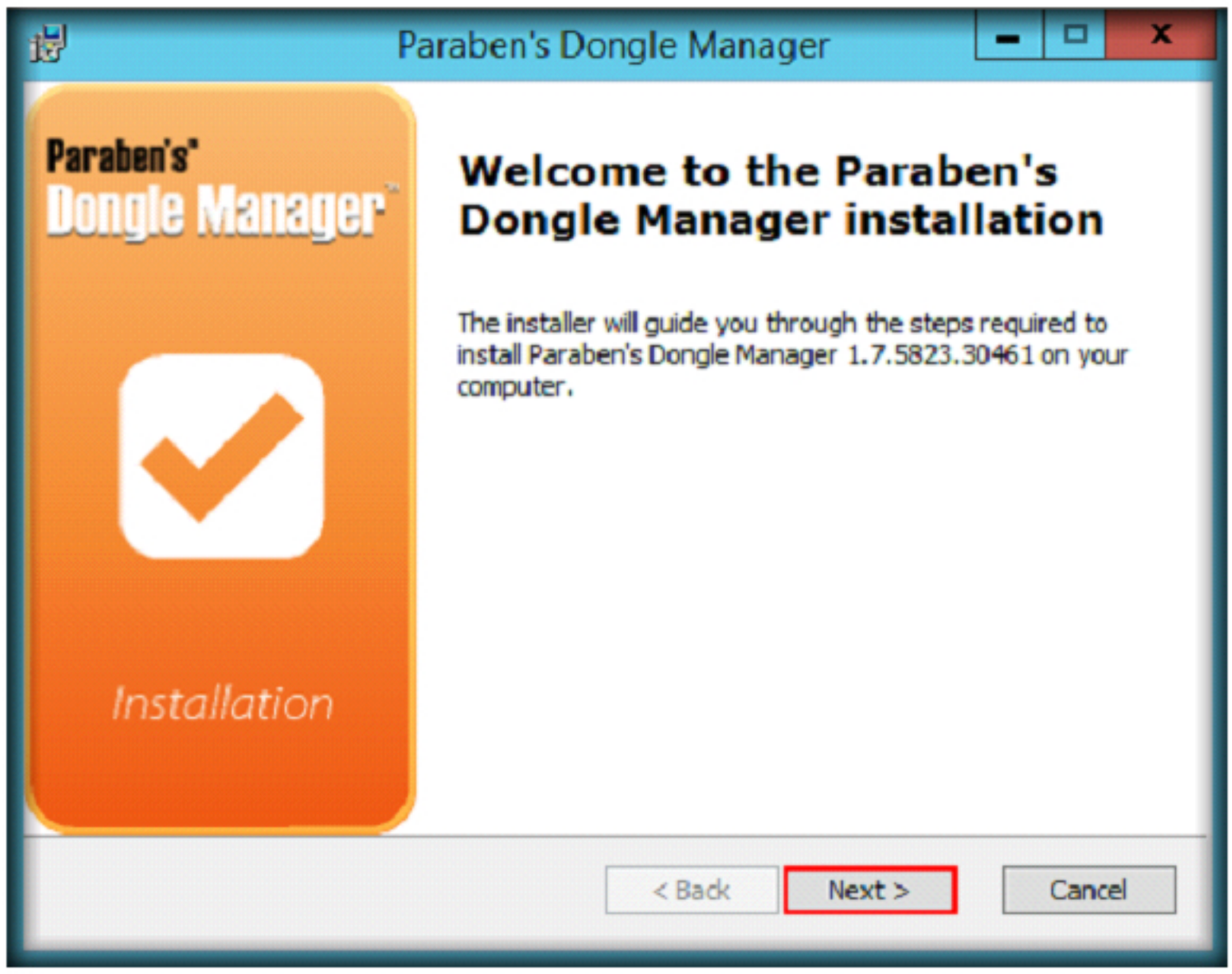

FIGURE 5.2: Paraben'sDongle Manager Installer

4. Once the installation is completed, a Paraben's P2C dialog box appears asking you to restart your computer. Click **Yes**, to restart the machine, for the configuration changes to take effect.

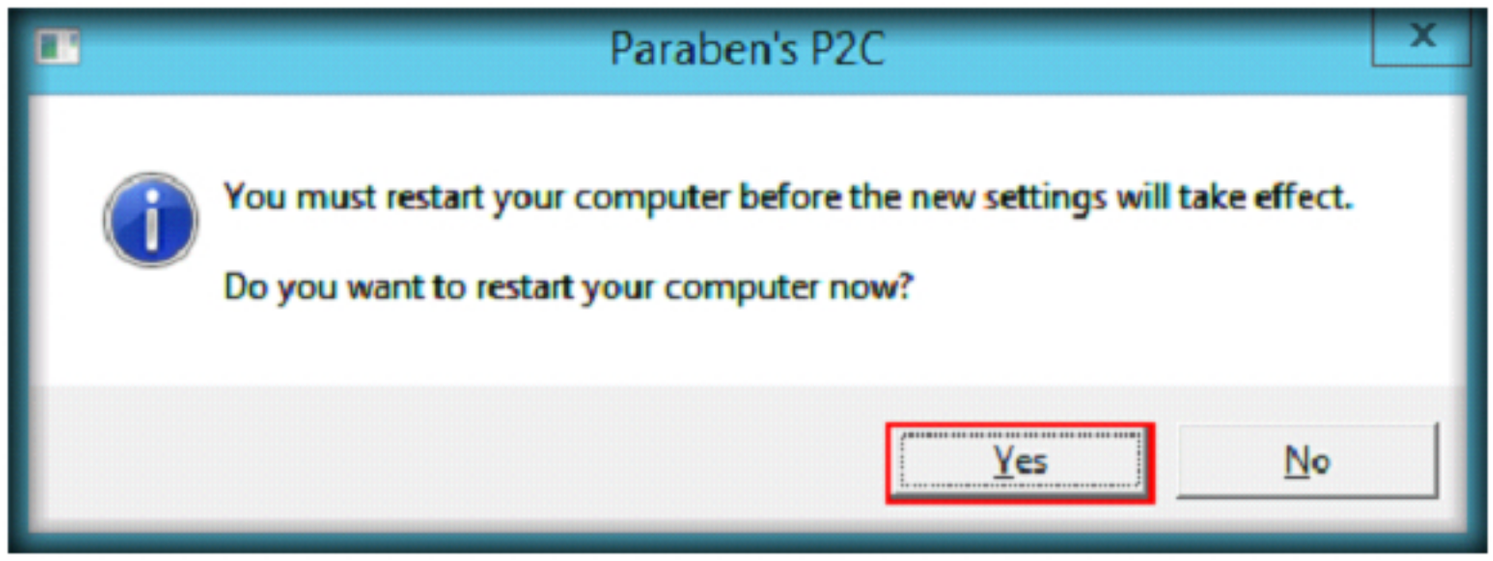

FIGURE 5.3: Paraben's P2C Restart Computer Dialog Box

5. Double-click on the **P2C** icon located on Desktop, to launch the application.

Note: Alternatively, you may launch the application from the Apps screen.

6. An Activation pop-up subsequently appears, click **Later**.

P2 Commander examines logical and physical disks as well as individual files and folders with FAT12, FAT16, FAT 32, and NTFS filesystems.

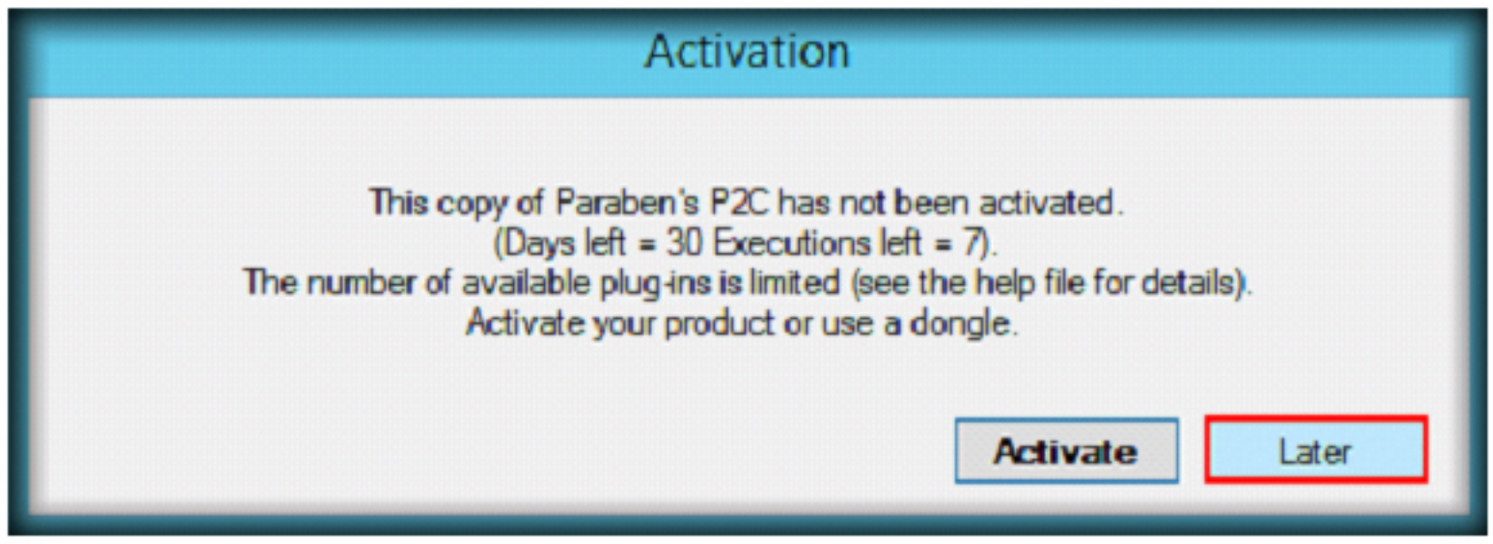

FIGURE 5.4: Pop-up window of P2 Commander

Note: TheP2 Commander Trial version can be used for only 30 days with limited number (7) of executions.

7. The**P2 Commander** GUI appears, along with a **Paraben's P2C** pop-up as shown in the following screenshot:

To view and define P2 Commander options, select **Tools - Options** or dick **Options** on the **P2 Commander** welcome page.The **Options** window will open. It consists of two panes. In the left pane, the groups of options will be displayed. In the right pane, the corresponding

FIGURE 5.5: Main window of P2 Commander

TASK 2

Creating a New Case

8. Click **Create New Case** icon in the **Paraben's P2C** pop-up.

FIGURE 5.6: P2 Commander creating a new case

The **Properties** paneallows the user to view the properties of the selected case item.

9. A **New Case** window appears, displaying the **Welcome** section. Click **Next**

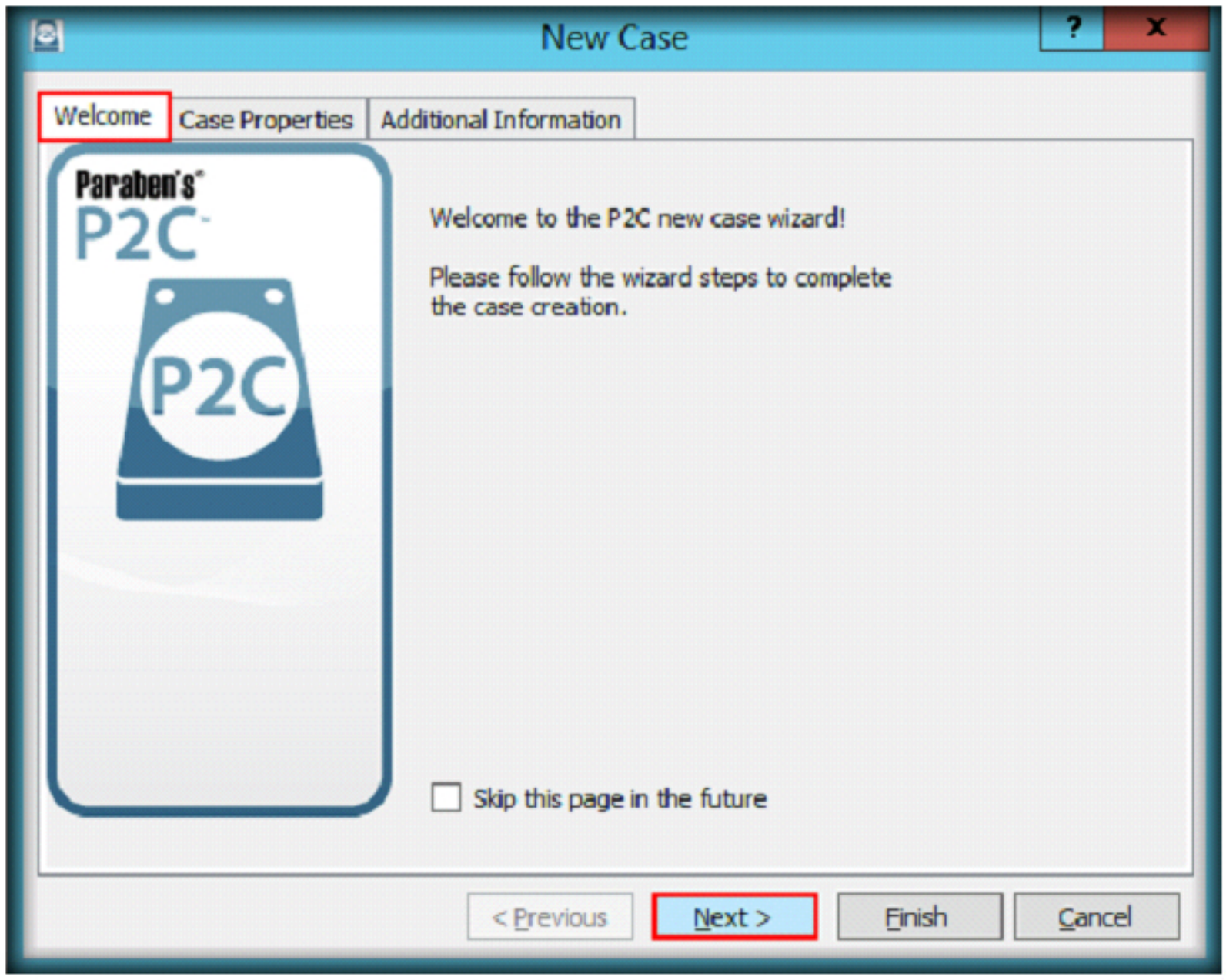

FIGURE 5.7: Welcome Wizard of P2 Commander

The Sorted Files pane includes a main node type, 13 types of sub-nodes, in which files are sorted, and two additional sub-nodes. The type sub-nodes are:

- Documents
- Emails
- Chats
- Spreadsheets
- Graphics
- Databases
- Executable
- Compressed
- Multimedia
- XML
- Text
- Encrypted
- Others

10. In the **Case Properties** section; provide a **Case name**, write a case **Description** information in the respective fields, and then click **Next**.

The Properties pane is a grid with the left column being the property's name and the right column being the property's value.

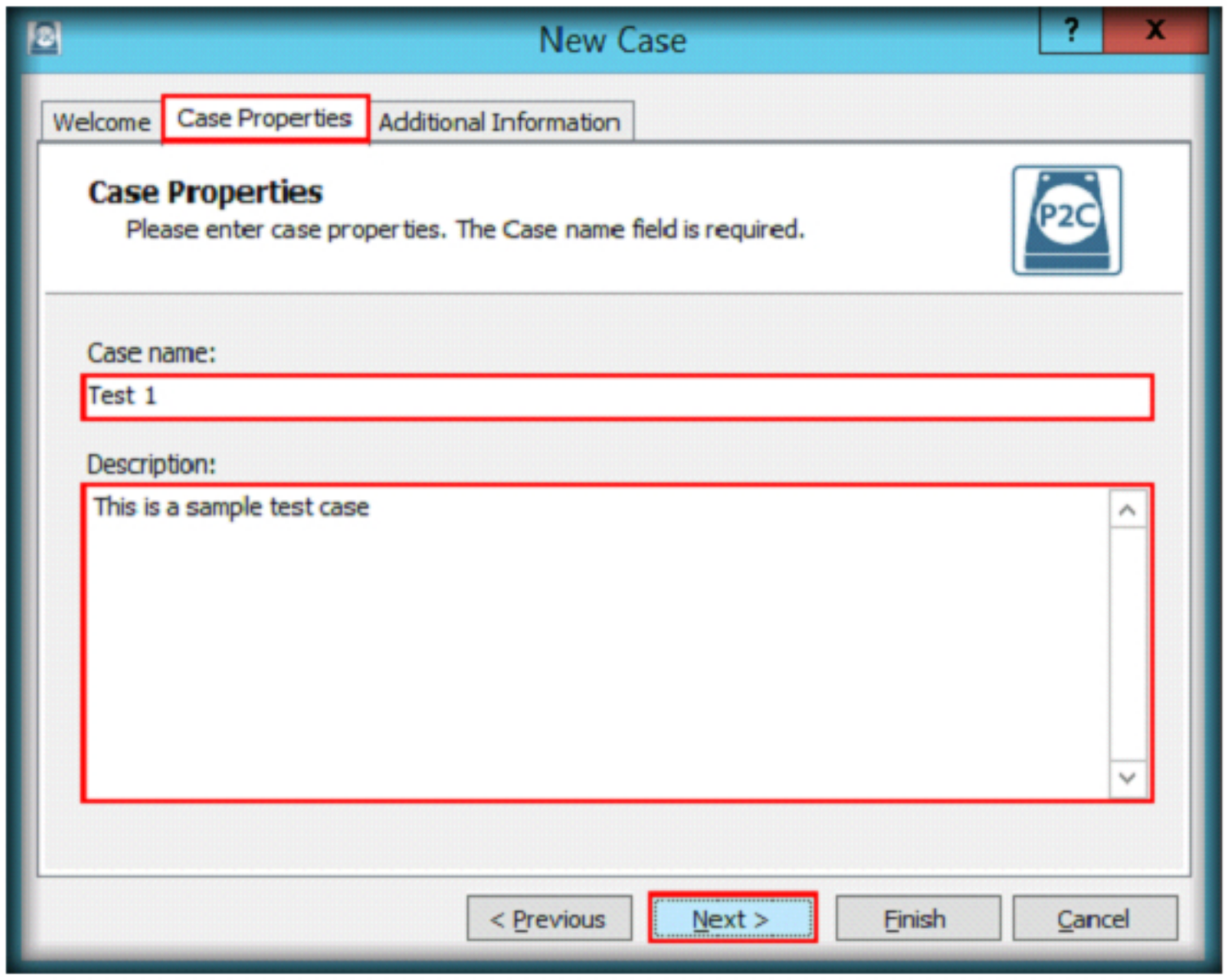

FIGURE 5.8: New case properties

11. In the **Additional Information** section, fill in additional information and click the **Finish** button.

Note: Additional information is not mandatory and can be completed any time.

The Properties pane is a grid with the left column being the property's name and the right column being the property's value.

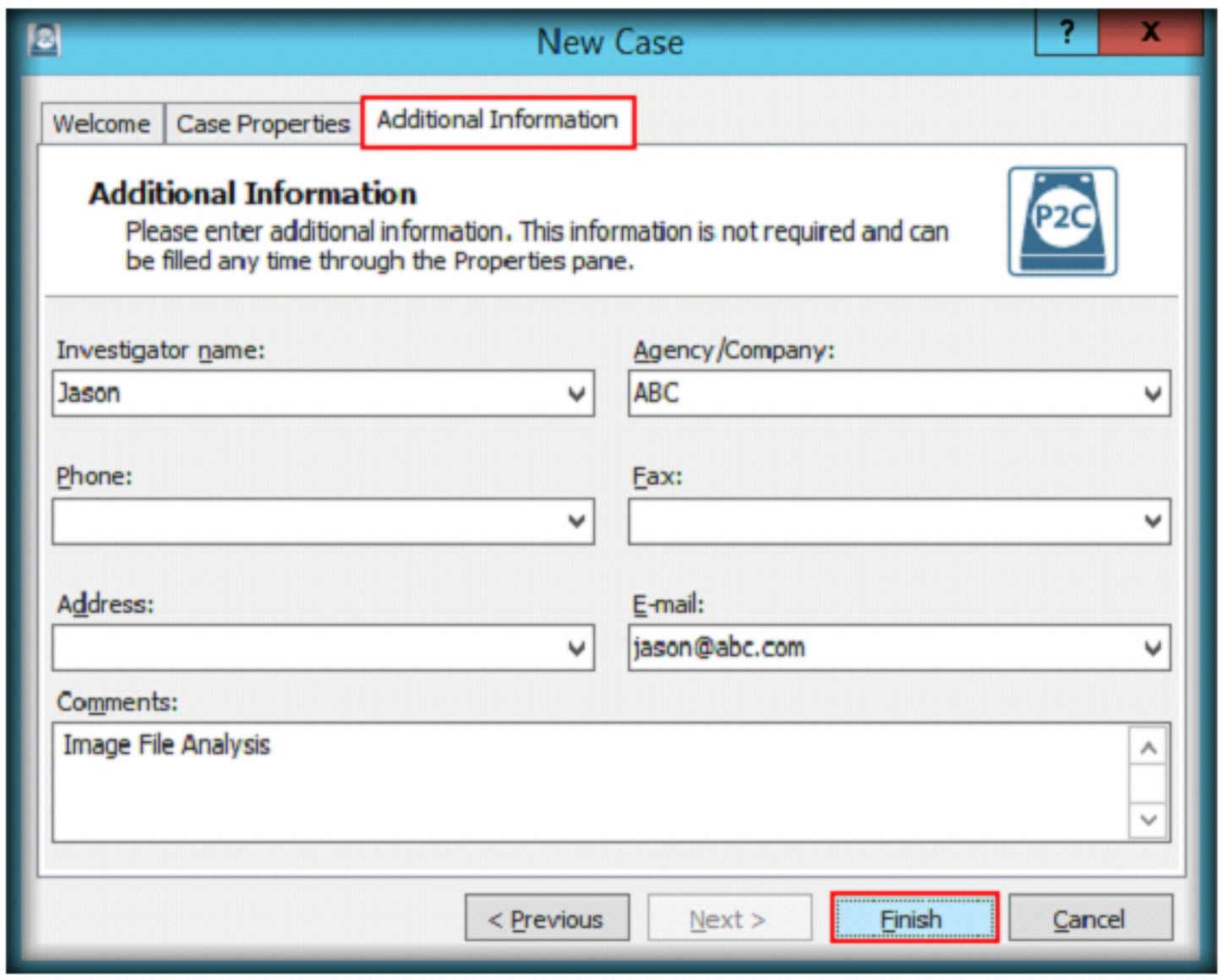

FIGURE 5.9: New case window

12. A **New case creation** window appears, navigate to Desktop, create a folder named Reports, navigate to the **Reports** folder, specify a file name (here, **Test 1.p2c**) in the **File Name** field, and click **Save**.

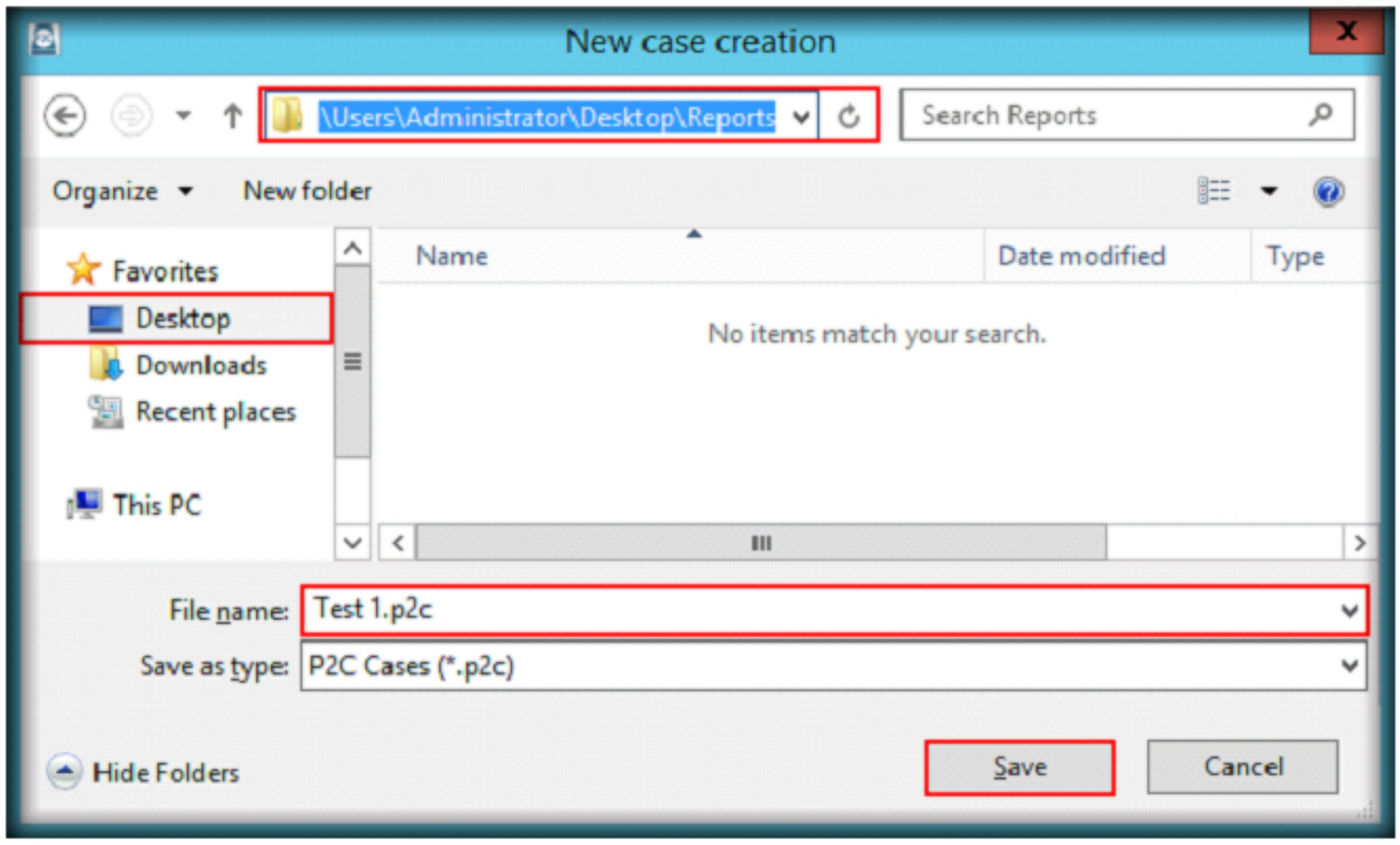

FIGURE 5.10: New case creation window

TASK 3

Adding Evidence

13. In the **Add New Evidence** window, select **Image File** under the **Category** section in the left pane, then select **Auto-detect image** under the **Source type** section and click **OK**.

The **File Menu** contains basic file options for creating, opening, and saving Paraben's **P2 Commander** files. In addition, the **File Menu** also contains options for exporting and generating reports.

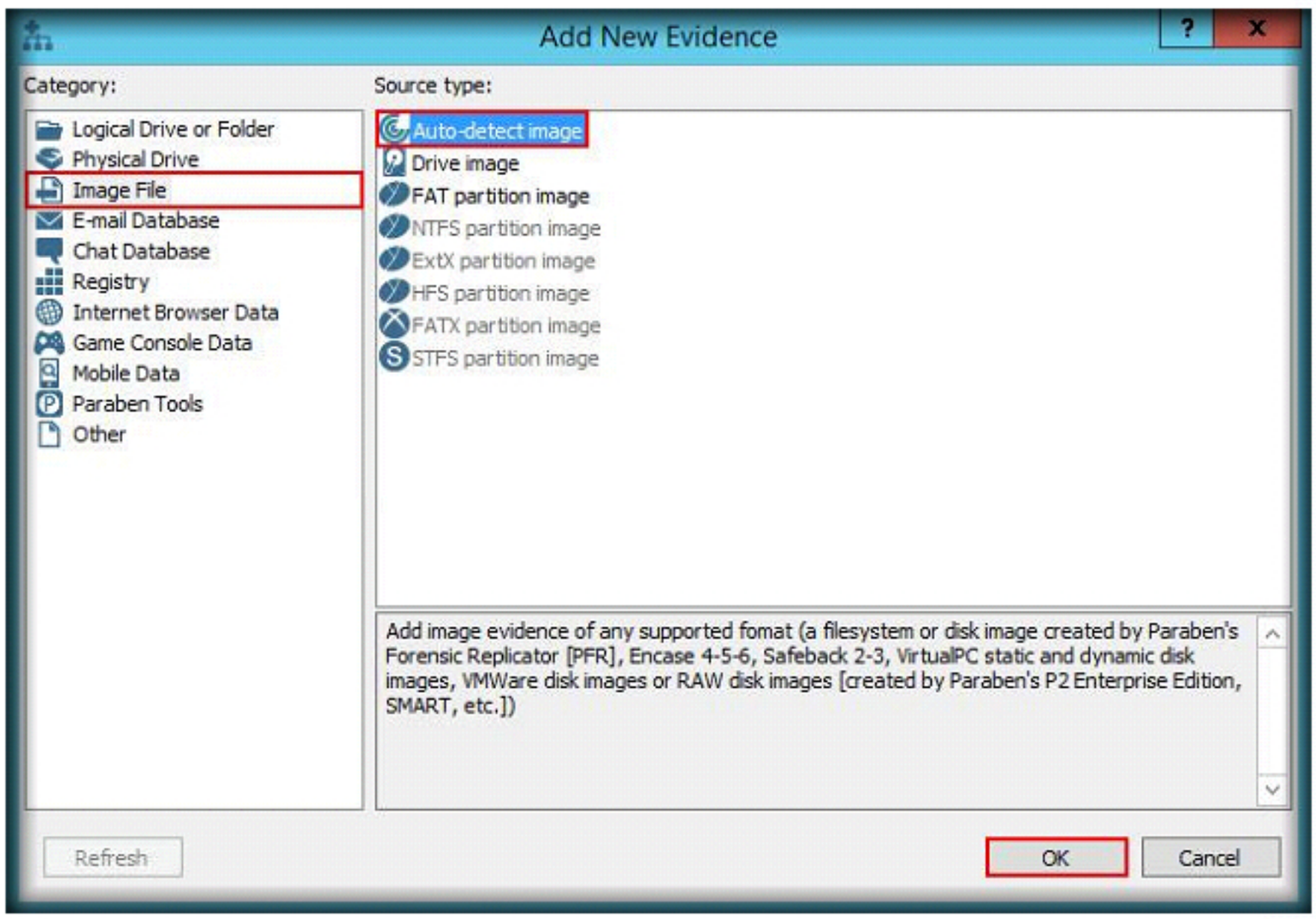

FIGURE 5.11: Add New Evidence window

14. An **Open** window appears, navigate to **C:\CHFI-Tools\Evidence Files\Raw - DD Image**, select **TestRawImage.dd** and click **Open**.

The **View** menu contains options for Paraben's **P2 Commander** layout ..

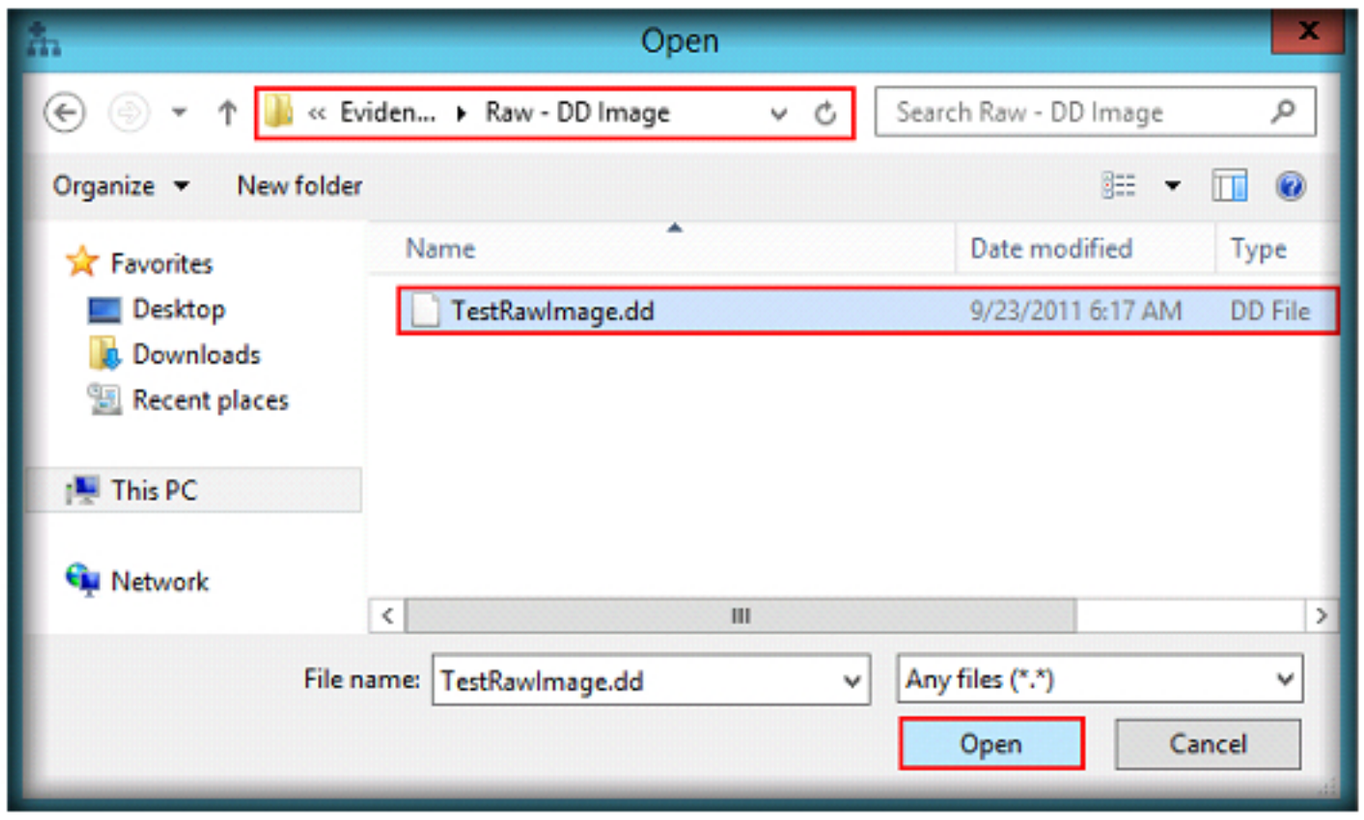

FIGURE 5.12: Raw-DD Image

15. Specify a new evidence name and click **OK**.

Navigation in the folders can be performed either in the **Case Explorer** pane or in the **Data Viewer** pane.

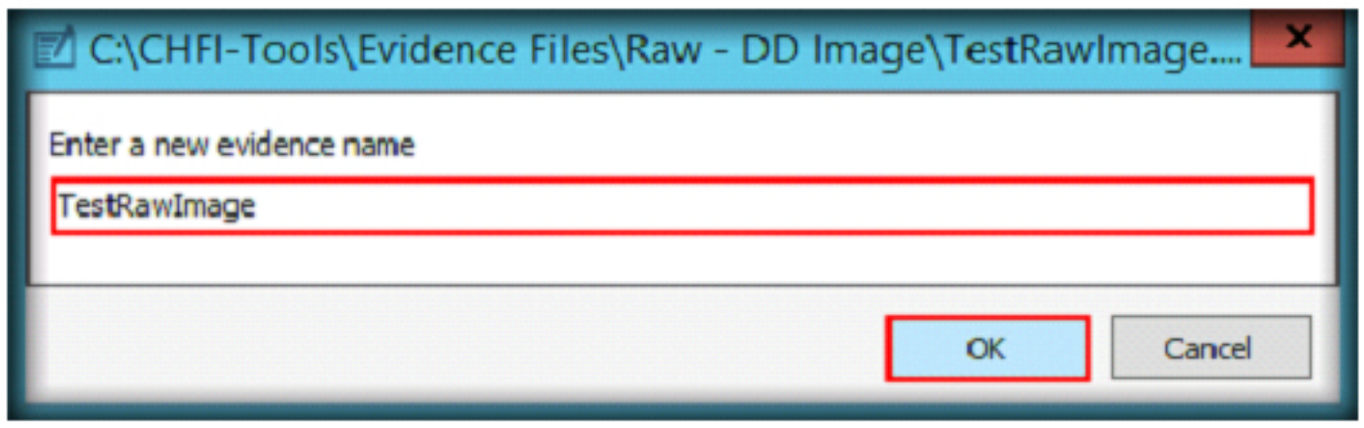

FIGURE 5.13: Pop up asking for file name

16. **P2C Content Analysis Wizard** appears displaying the **General options** section. Select the required options and click **Next**.

The **Hash Groups** pane consists of two areas:

- **Parameters** area: Here, users can set the parameters for MD5 value searches by entering the hash value, or a portion of it. The same can be done for MD5 descriptions. To begin the search, click the **Query** button.
- **Results** area: Search results for the MD5's are displayed here. It includes columns for the MD5 value and the description.

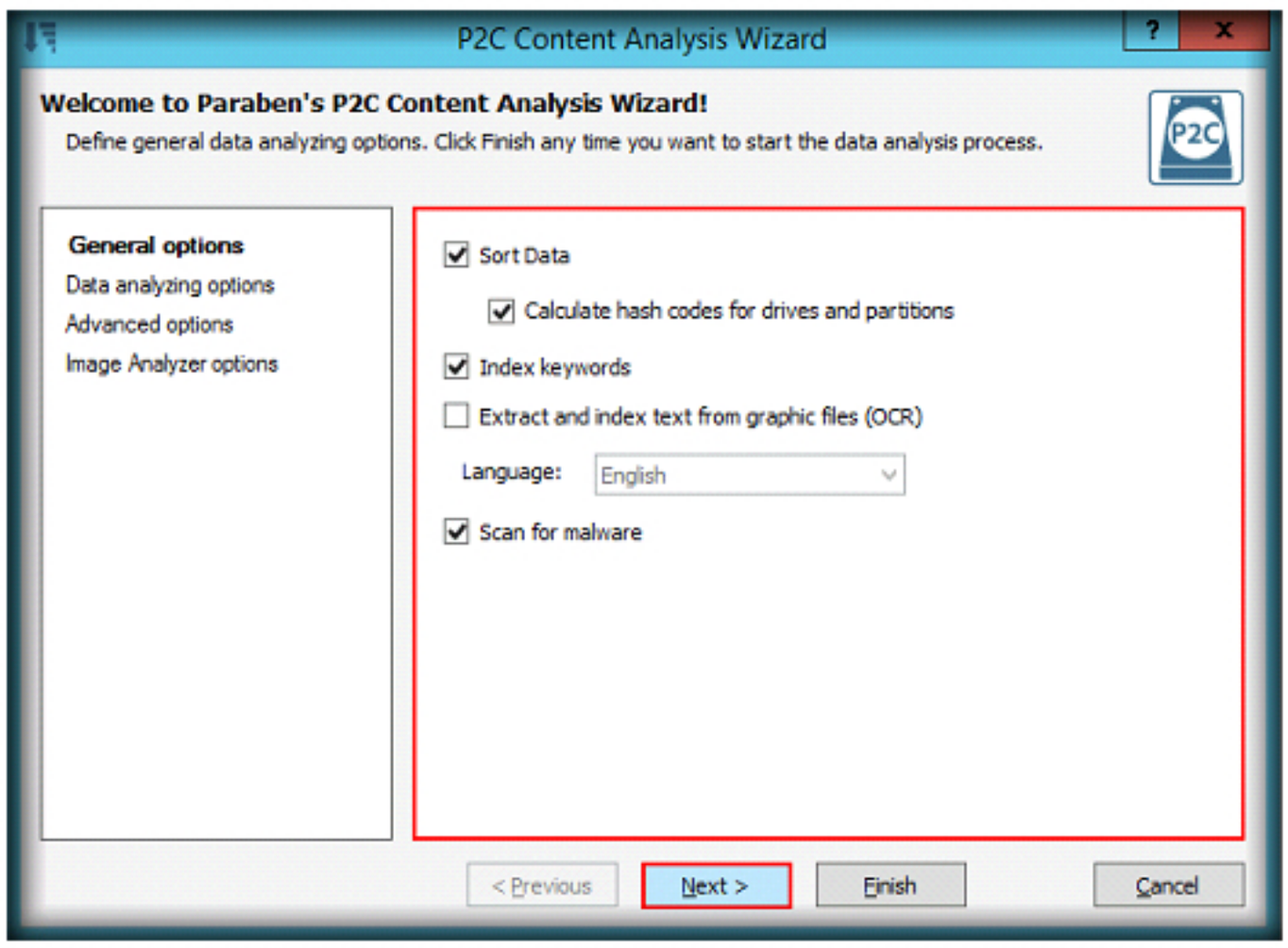

FIGURE 5.14: P2C Content Analysis Wizard

17. **Data Analyzing Options** section appears, select the required options and click **Next**.

Filesystem evidence is a link to any type of storage device containing files that allow the examiner to view and examine its structure and contents. File system evidence can recover the contents of deleted files and folders on a computer and view compressed files.

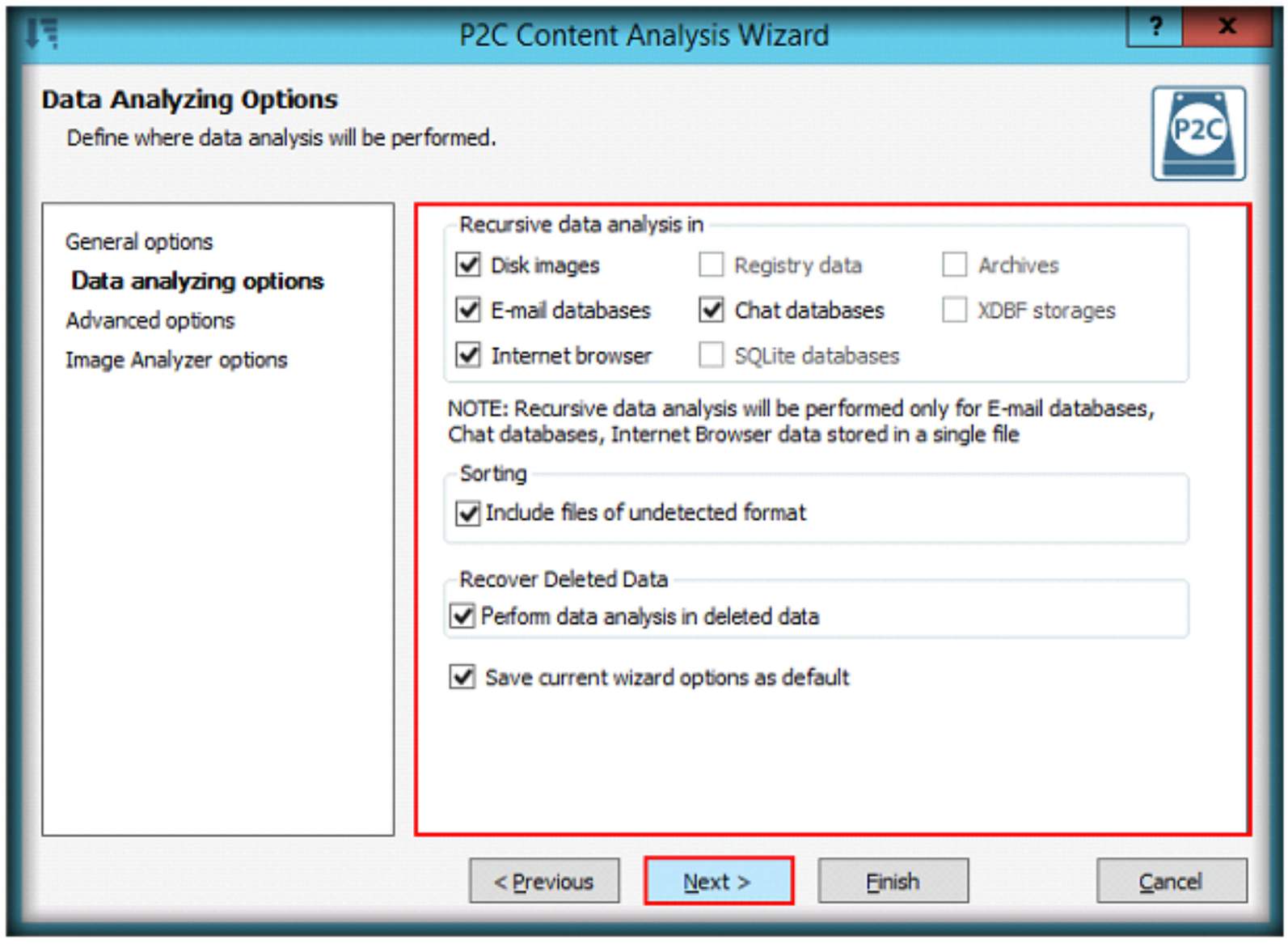

FIGURE 5.15: Data Analyzing Options section

18. Advanced Options section appears; select the options required for analyzing the image and click **Next**.

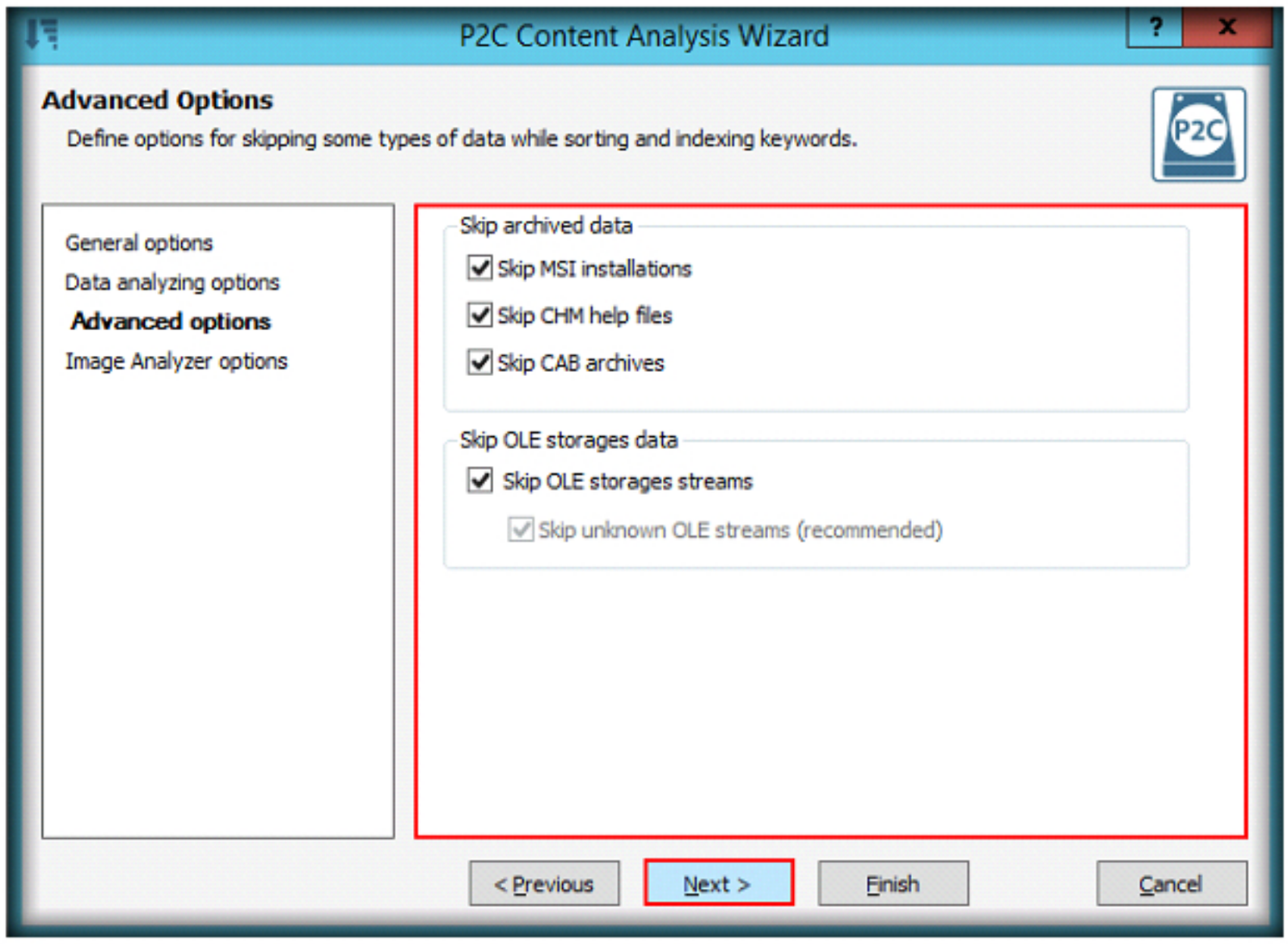

FIGURE 5.16: Advanced Options section

19. **Image Analyzer Options** section appears, leave the options set to default and click **Finish**.

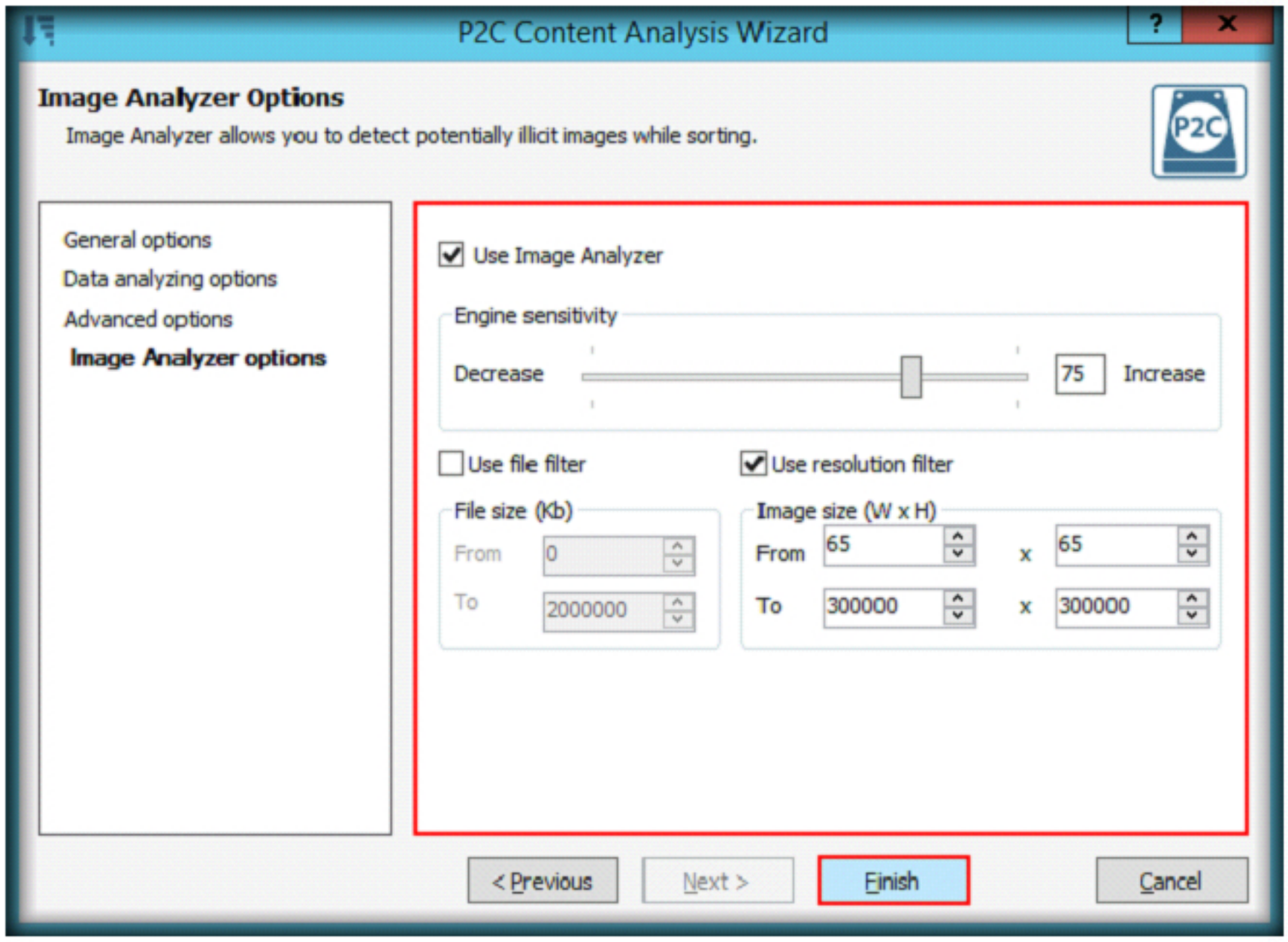

FIGURE 5.17: Image Analyzer Options section

20. The selected image file is added to the case (**Test 1** file under the Case Content).

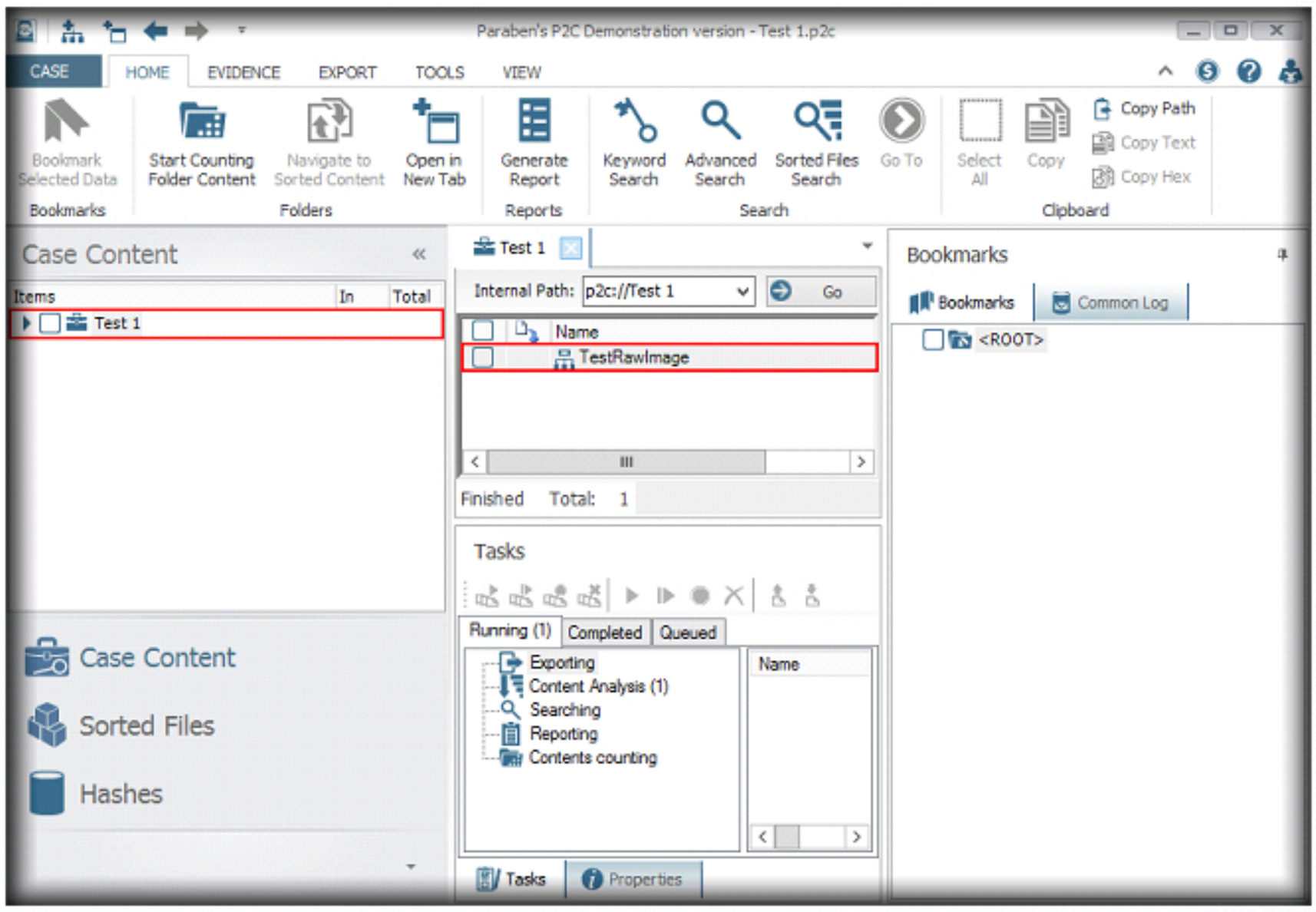

FIGURE 5.18: Case Explorer window

21. Expand **Test 1→TestRawImage→FAT→Root**. You will find that there are folders with **X** mark over the folder icons.

22. Click on the **Test1**folder and select the **More Icons** folder in the **Items** tree view. The '**X**' mark indicates that they have been deleted.

MD5 hash codes are also calculated while exporting. The calculated hash codes for exported files are stored in the file **<exported file name>.md5** that is placed in the same folder as the exported file. The calculated hash codes for a folder's contents are stored in the **summary.md5** file that is placed in the same location as the exported folder.

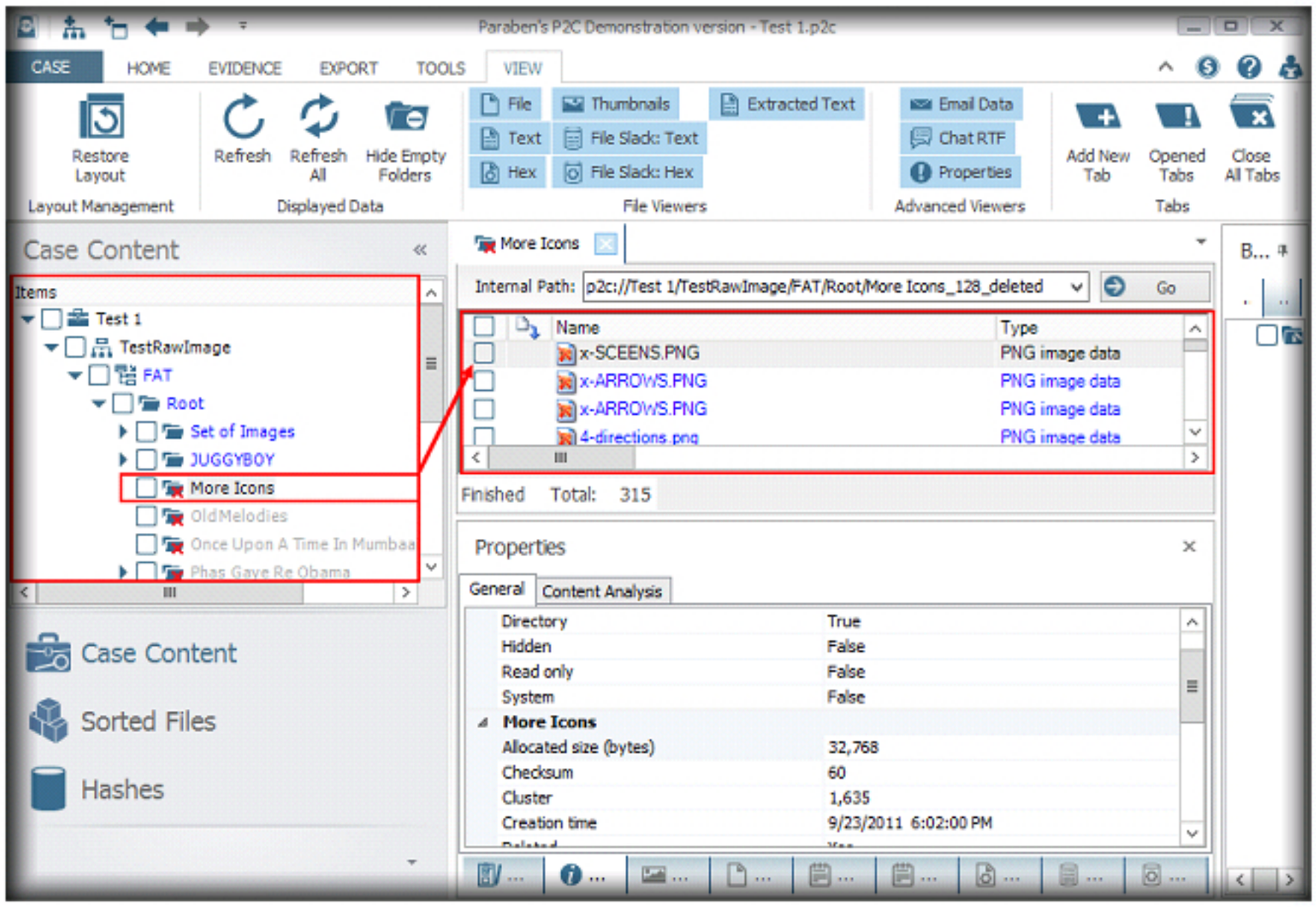

FIGURE 5.19: Test 1 file list

TASK 4

Adding the Evidence Files to the Report

23. To add a file to the report, right-click on the file and then click **Add to report/File Export**.

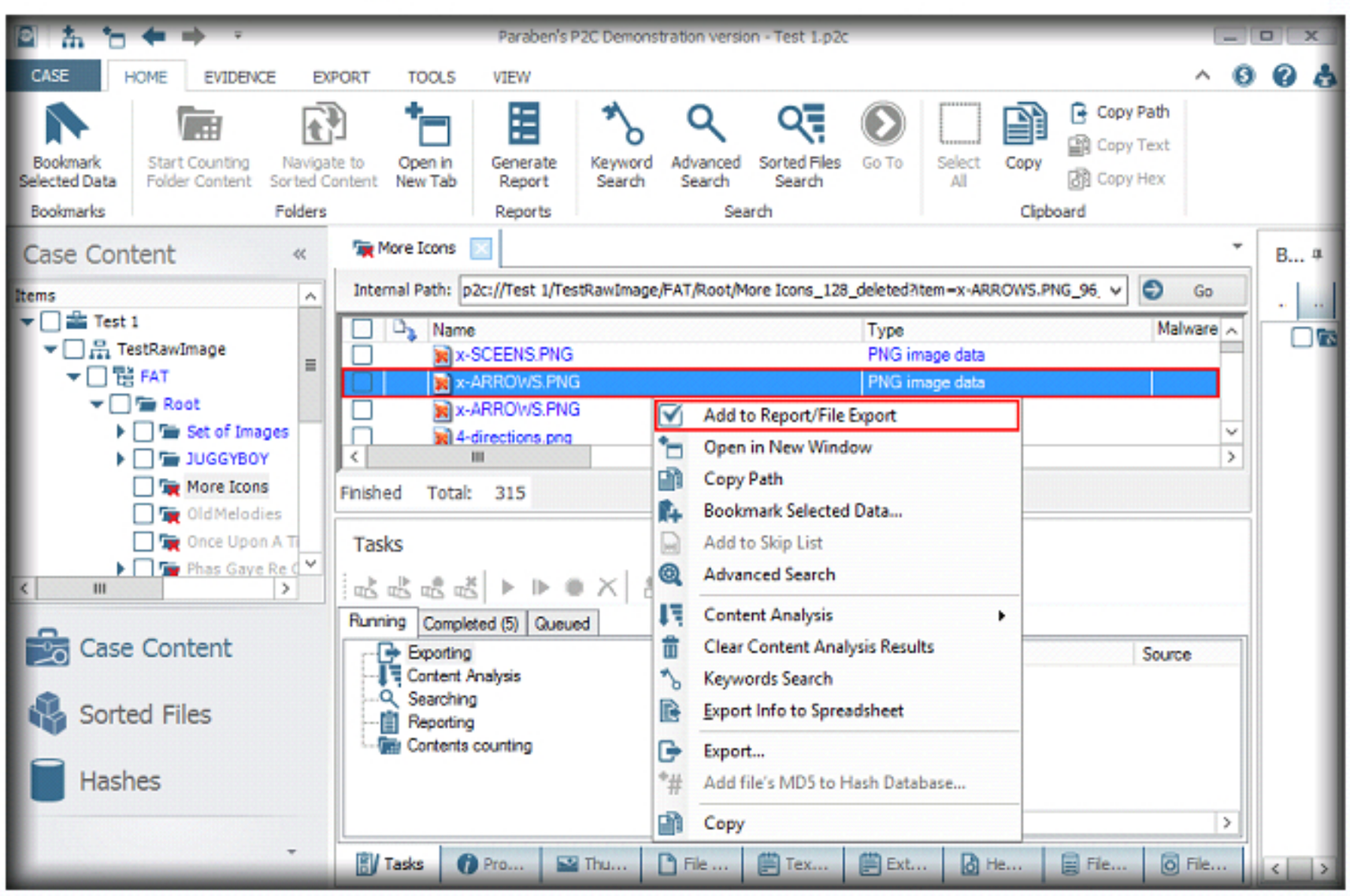

FIGURE 5.20: Adding files to the report

TASK 5

Viewing the Evidence Files in Different Formats

24. If you want to see the properties of the selected file, click the **Common Log** tab. It will display the properties of the selected file in the **Common Log** section.

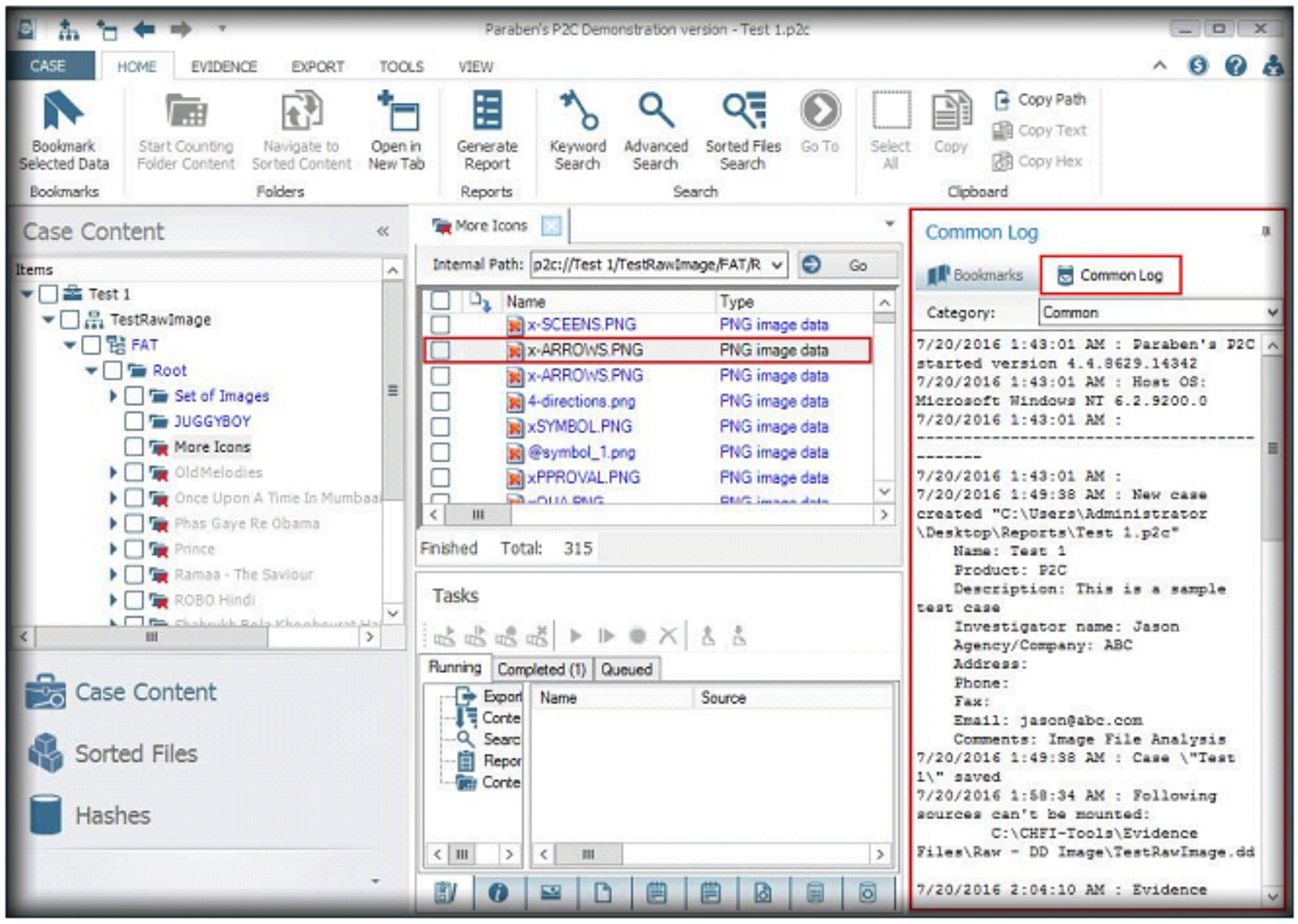

FIGURE 5.21: Adding files to the report

The Slack view panes allow the user to view a file's slack (slack space) in a NTFS filesystem evidence.

There are two slack viewers:

- **File Slack: Text View**
- **File Slack: Hex View**

25. It you want to see the actual image of the selected file, click the **File View** tab.

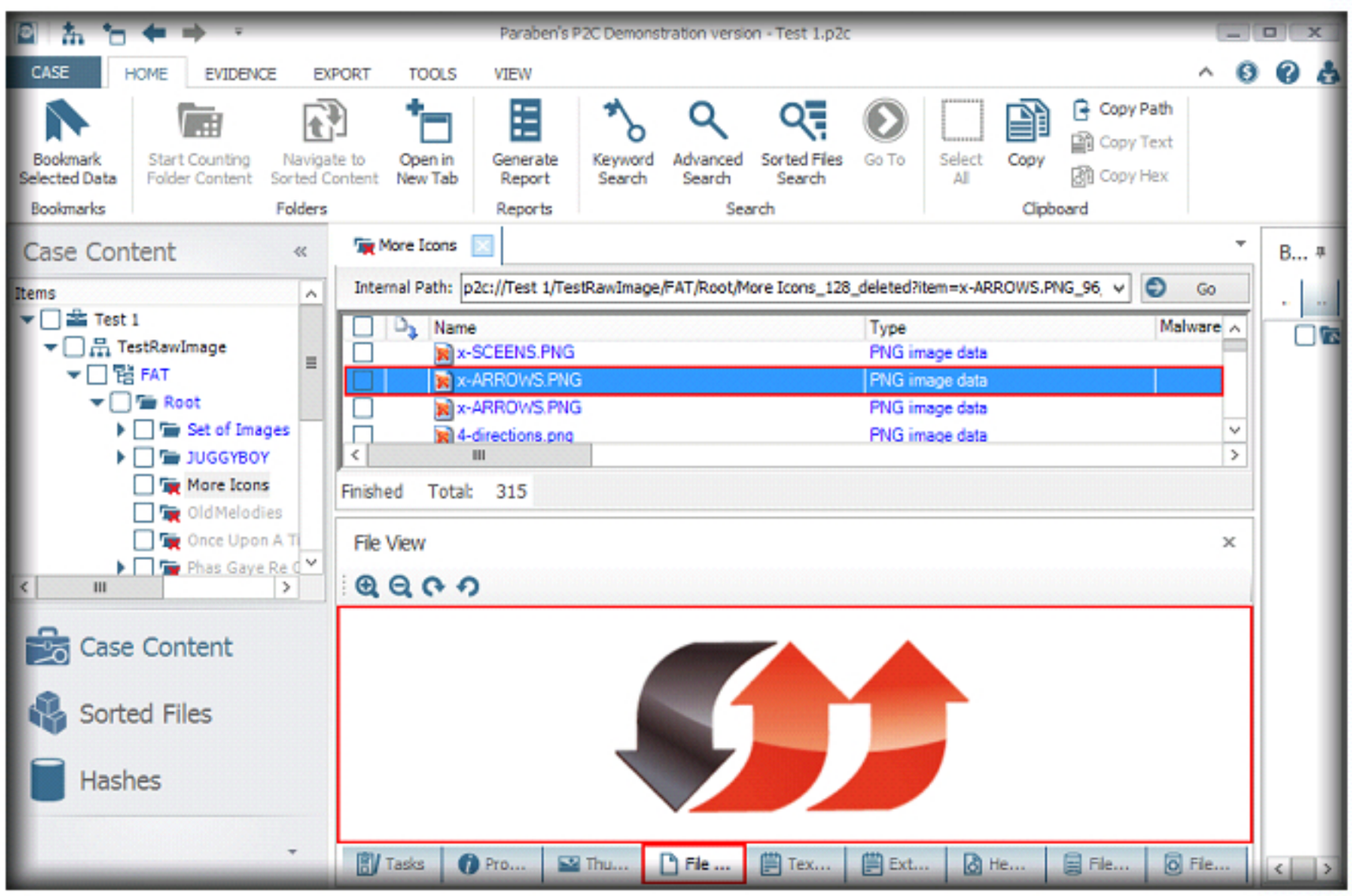

FIGURE 5.22: File view window

Evidence is a link to storage (database, disk, image file, mail storage, etc.), that allows users to view its structure and contents and to examine it.

P2 Commander supports seven types of evidence:

- Mailstorage
- Chat databases
- Filesystem evidence (disks, disk images, and individual folders)
- OLE storage
- Archive evidence
- IE cache evidence
- Registry file evidence

26. To view the hex values of the selected file, click the **Hex View** tab.

Filesystem evidence is a link to any type of storage device containing files that allow the examiner to view and examine its structure and contents. Filesystem evidence can recover the contents of deleted files and folders on a computer and view compressed files.

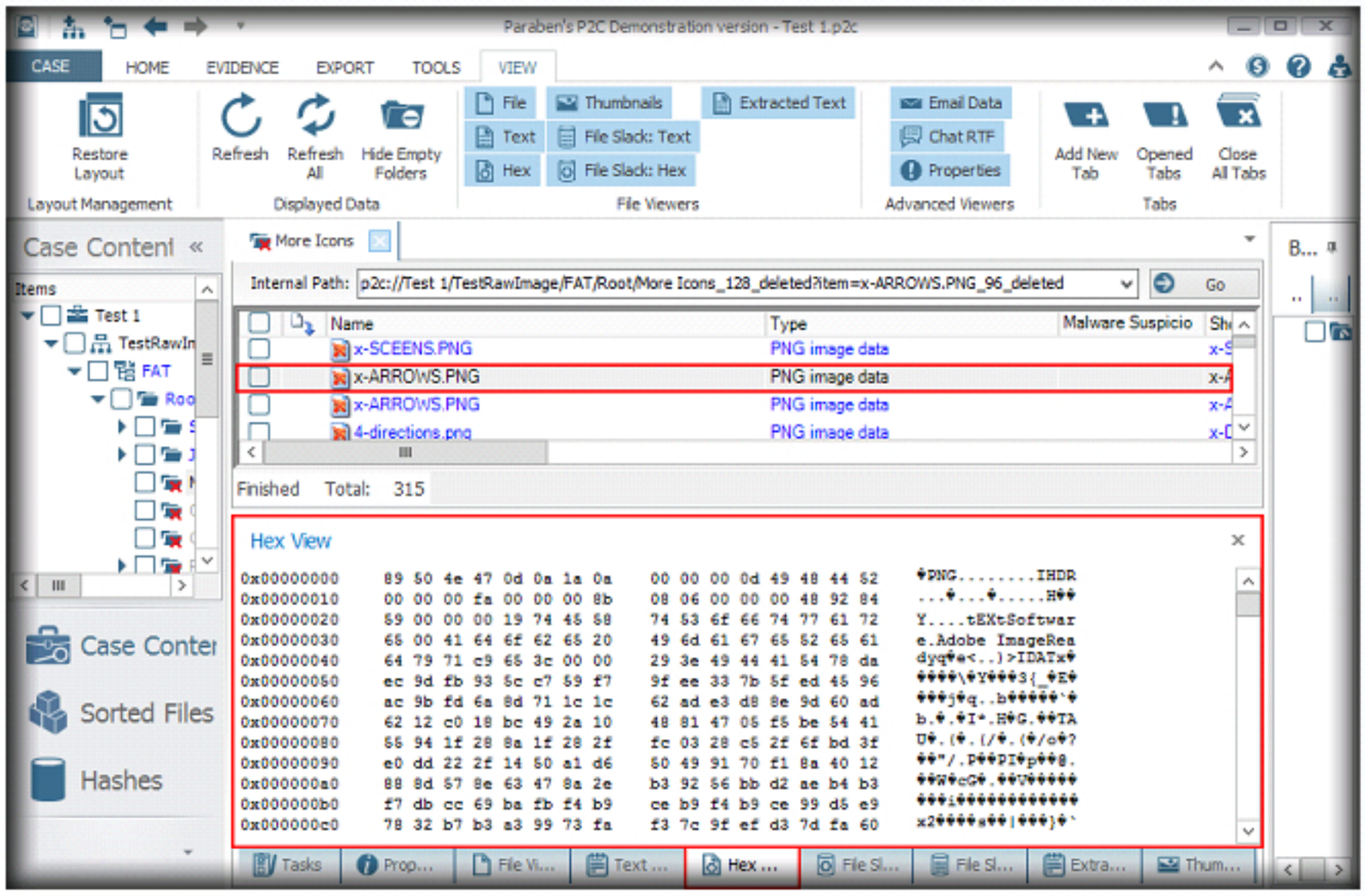

FIGURE 5.23: Hex view window

27. To view the text values of the selected file, click the **Text View** tab.

Features:

- Multiple reporting options for complete customization
- Image Analyzer for pornographic image detection
- Integrated Internet Explorer cache parser
- Hash database features can manage and Filter Out Common Hashes (FOCH)

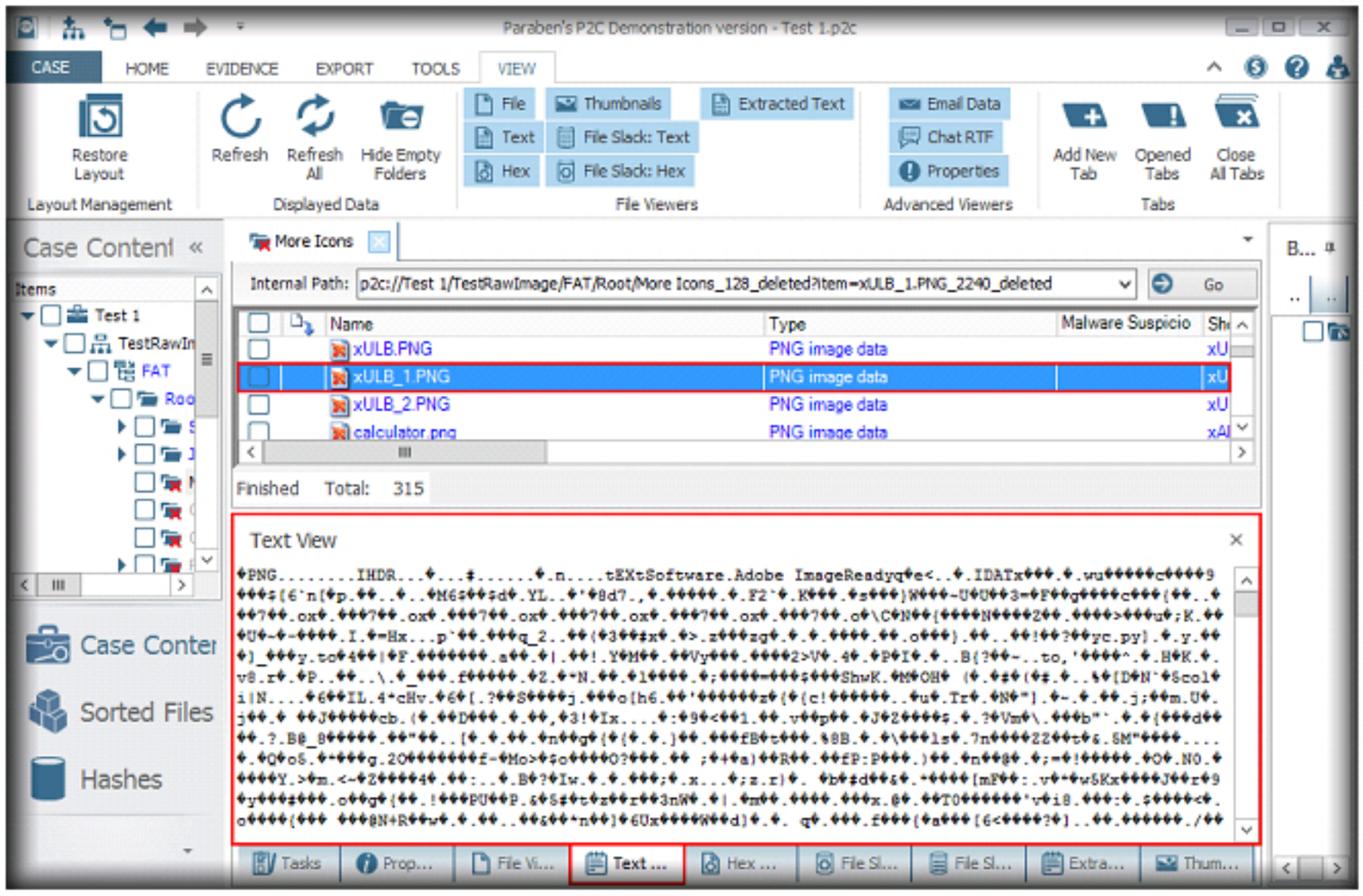

FIGURE 5.24: Text view window

TASK 6

Generating a Report

28. To generate a report, click the **Generate Report** button.

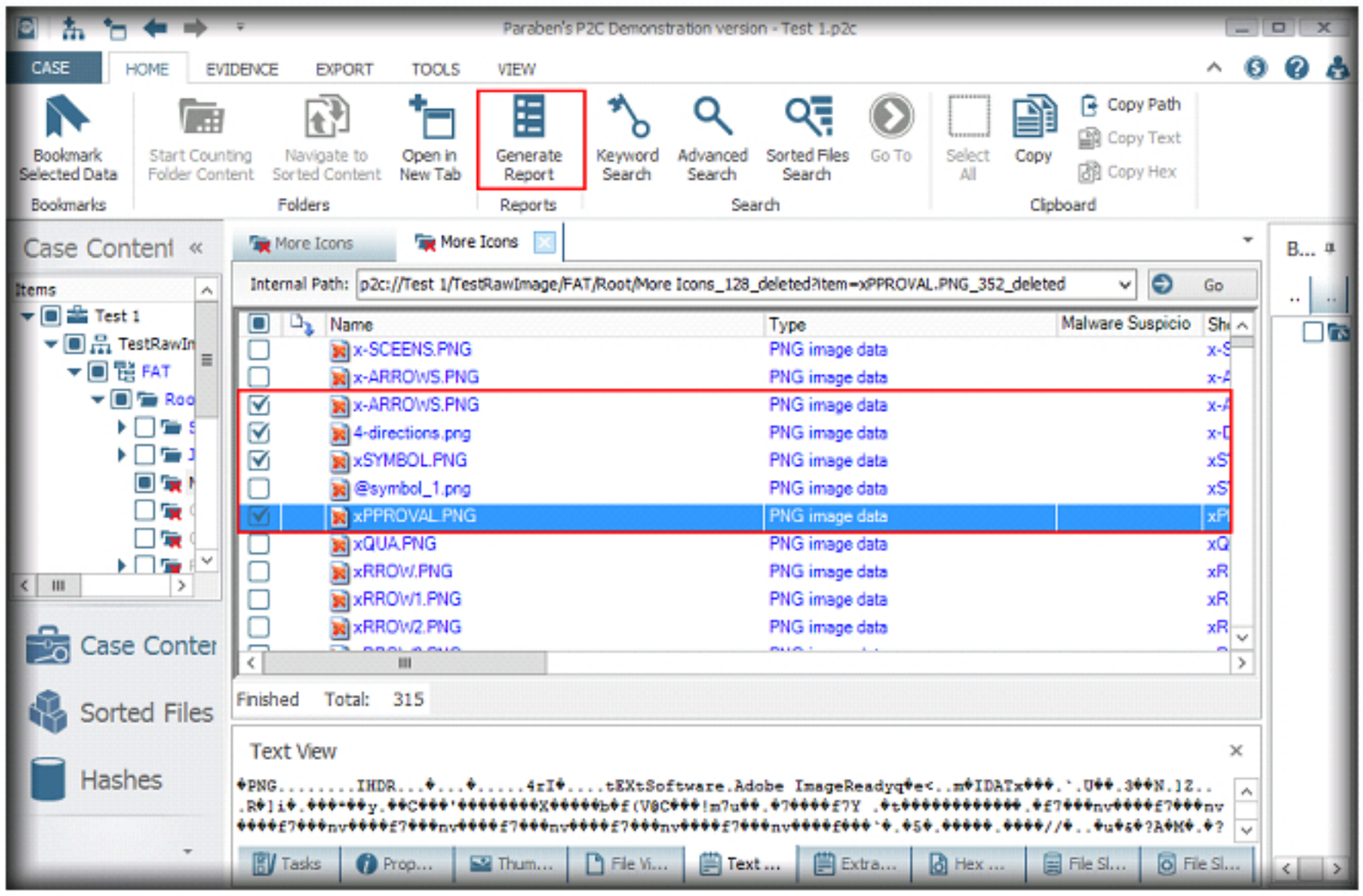

FIGURE 5.25: Generating report

29. In the **Reports Wizard** window, specify a **Destination folder**.

30. In this lab, we will be using **HTML Investigative Report** type and the default destination folder location. Click **Next**.

A bookmark is a pointer to a certain place in the case (e.g. a node in the Case Explorer, a section of data in the Text viewer, a row in the Data viewer, etc.).

Bookmarks include the following information:

- Name (bookmark's name)
- Path (the path defining where the bookmark is pointing)
- Source (a description of the place where the bookmark is pointing)
- Description (a user-defined bookmark description)
- Parent folder (the bookmark folder in which it is stored)

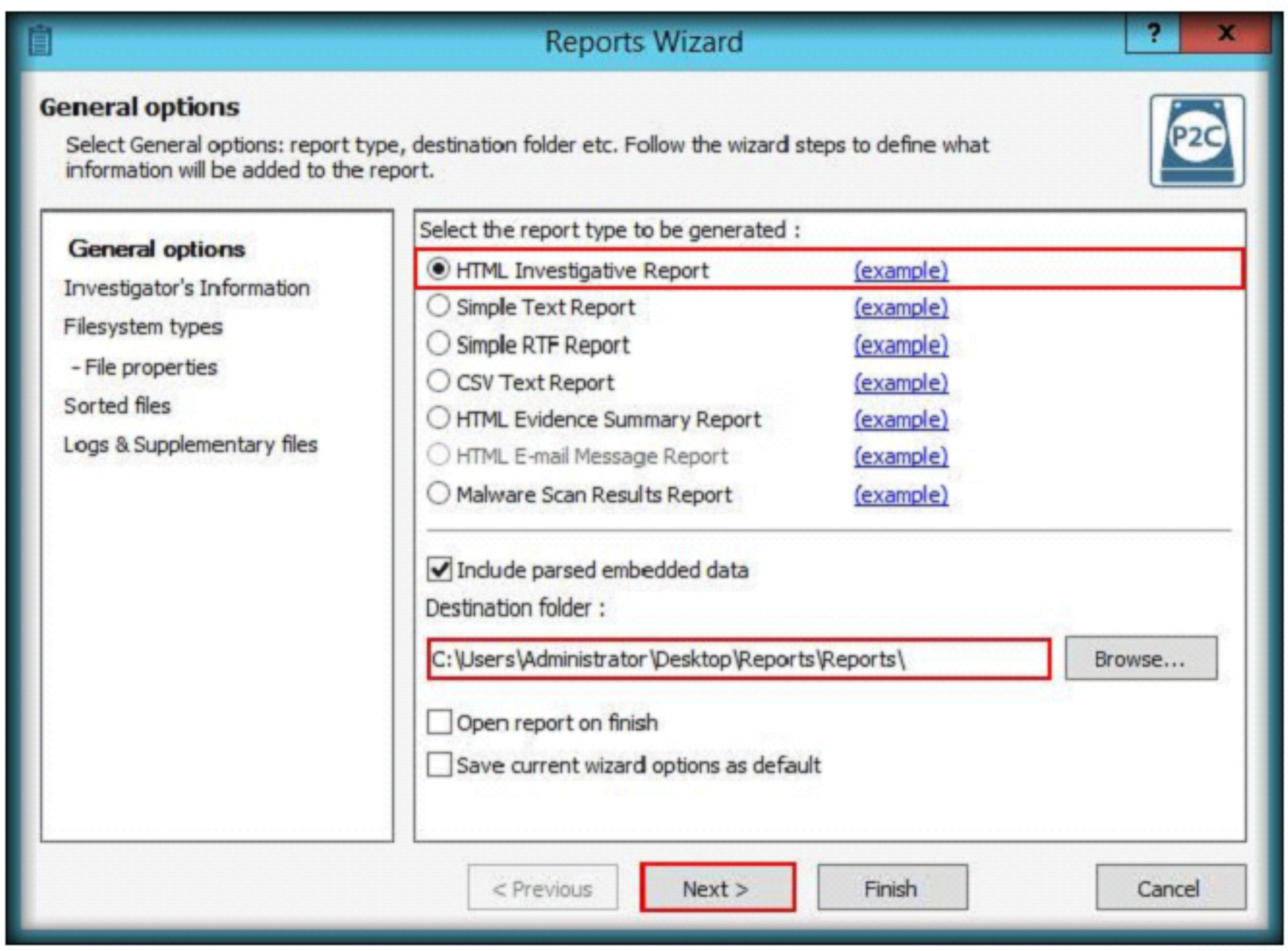

FIGURE 5.26: Reports wizard

31. You can Add or Edit any additional Investigator information, if needed in the **Investigator's Information** section and click **Next**.

P2 Commander allows you to open cases stored in shared folders on remote computers and add evidence stored in shared folders. This is done in a common way.

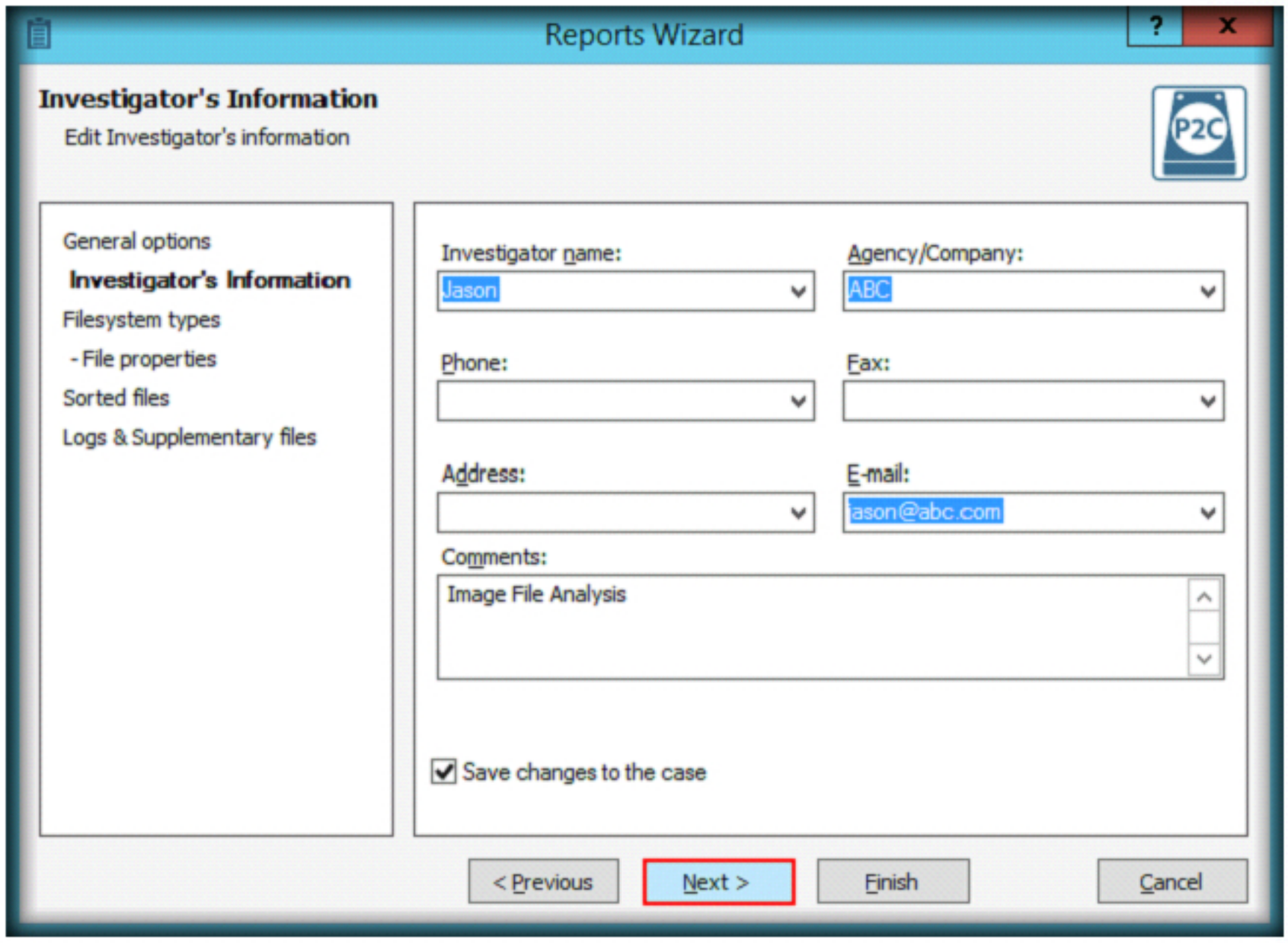

FIGURE 5.27: Investigator's Information section

32. In the **Filesystem Type** section, select the required options and click **Next**.

Investigator information is information about the examiner that created the case where the analysis was performed.

Investigator information includes the following data:

- Investigator name
- Agency/Company
- Phone
- Address
- Fax
- Email

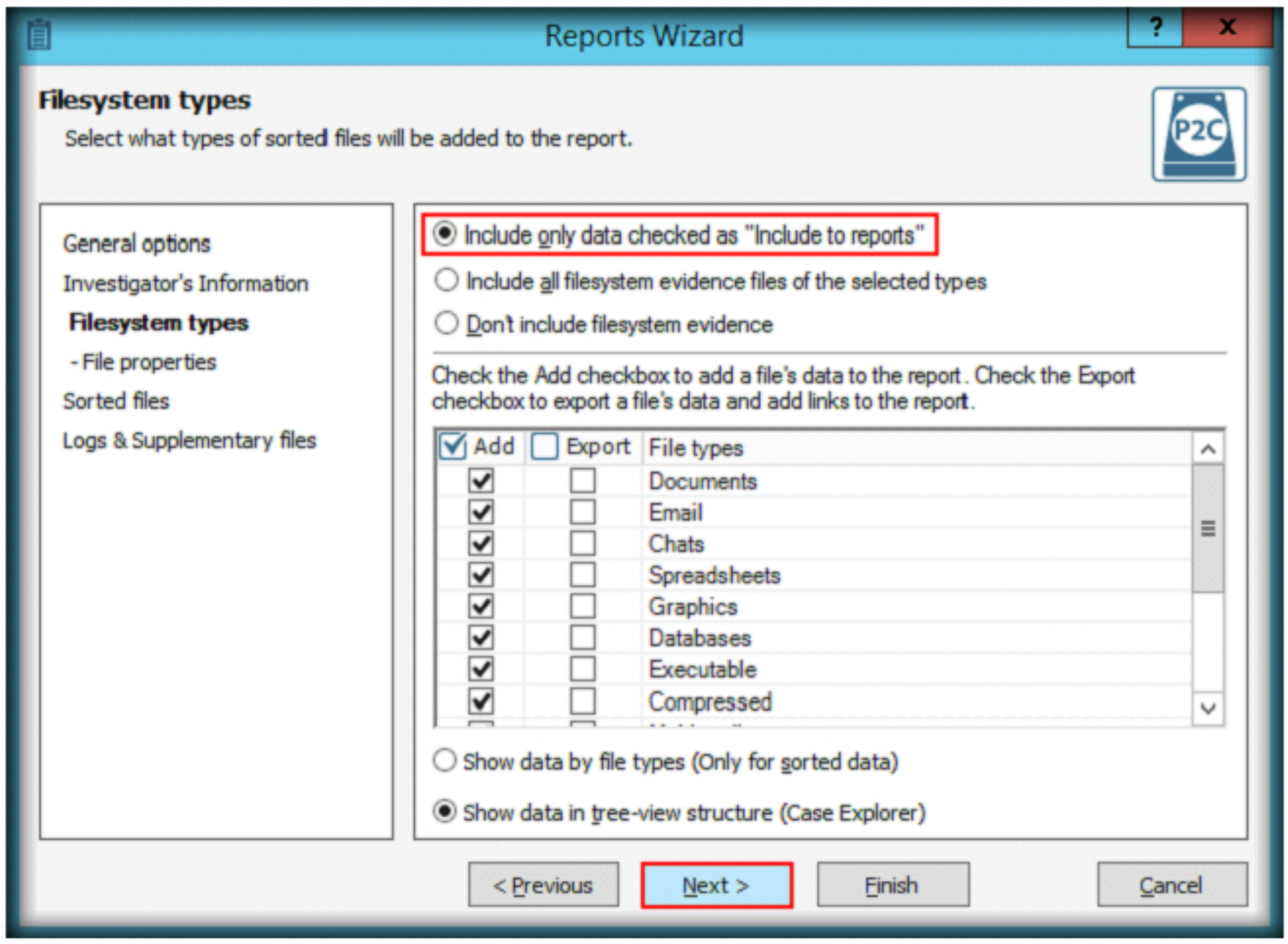

FIGURE 5.28: Filesystem Type section

33. In the **File Properties** section, leave the options set to default and click **Next**.

The case history is information about allthe events that have taken place since the creation of the case. This information includes all errors that occurred, information about evidence that was added, etc.

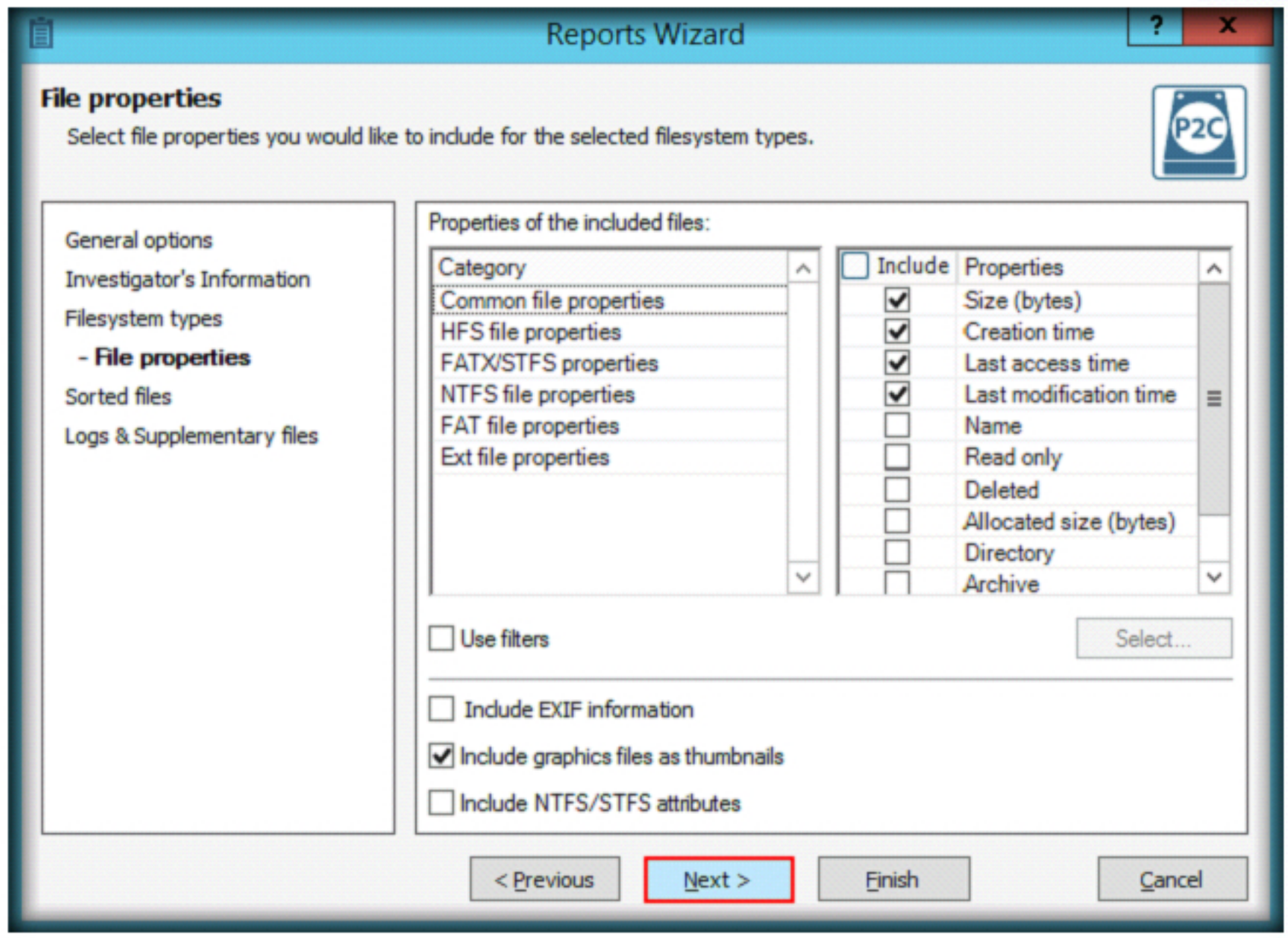

FIGURE 5.29: File Properties section

34. In the **Sorted Files** section, select the **Include only data checked as "Include to reports"** radio button and then click **Next**.

The **Case History** pane allows the user to view information about allevents that have taken place from the creation of the case. This information includes all errors that have occurred, information about evidence that was added, etc.

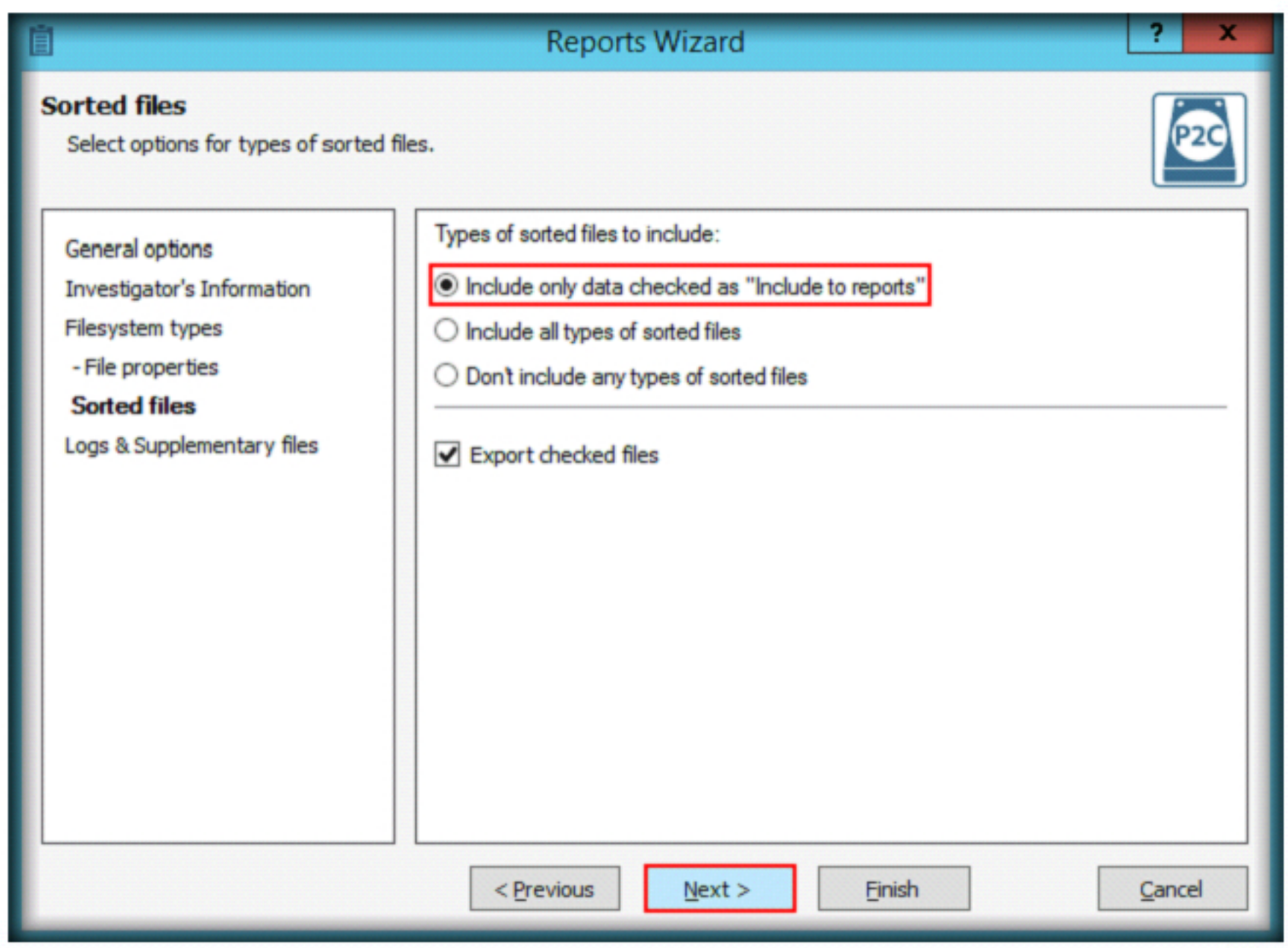

FIGURE 5.30: Sorted Files section

35. In the **Logs and Supplementary files** section, check the **Include Case History** option and click **Finish**.

The Chat RTF View paneallows users to view chat evidence contents in RTF format.

RTF Format is a kind of chat database information store where conversations are represented, message by message, in one text file and can be color-coded by the chat participant's names.

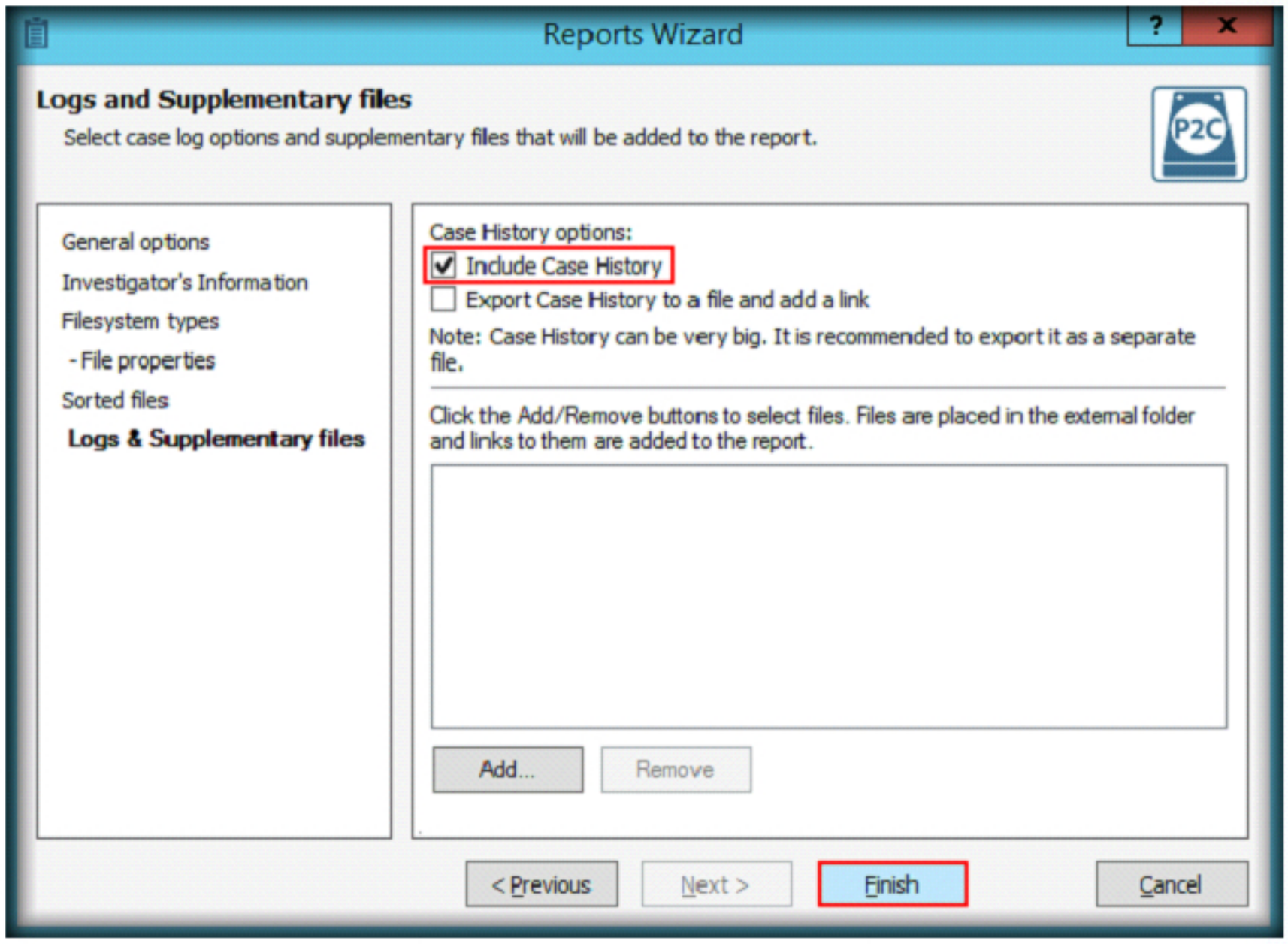

FIGURE 5.31: Logs and Supplementary files section

TASK 7

Viewing the Report

36. Navigate to the folder where you have saved the Report. In this folder, you will find a sub folder named **Test 1**.Open that folder and double-click the **Test 1.html** file to view the report.

The Common Log paneallows the user to view the common log created during one work session of P2 Commander.

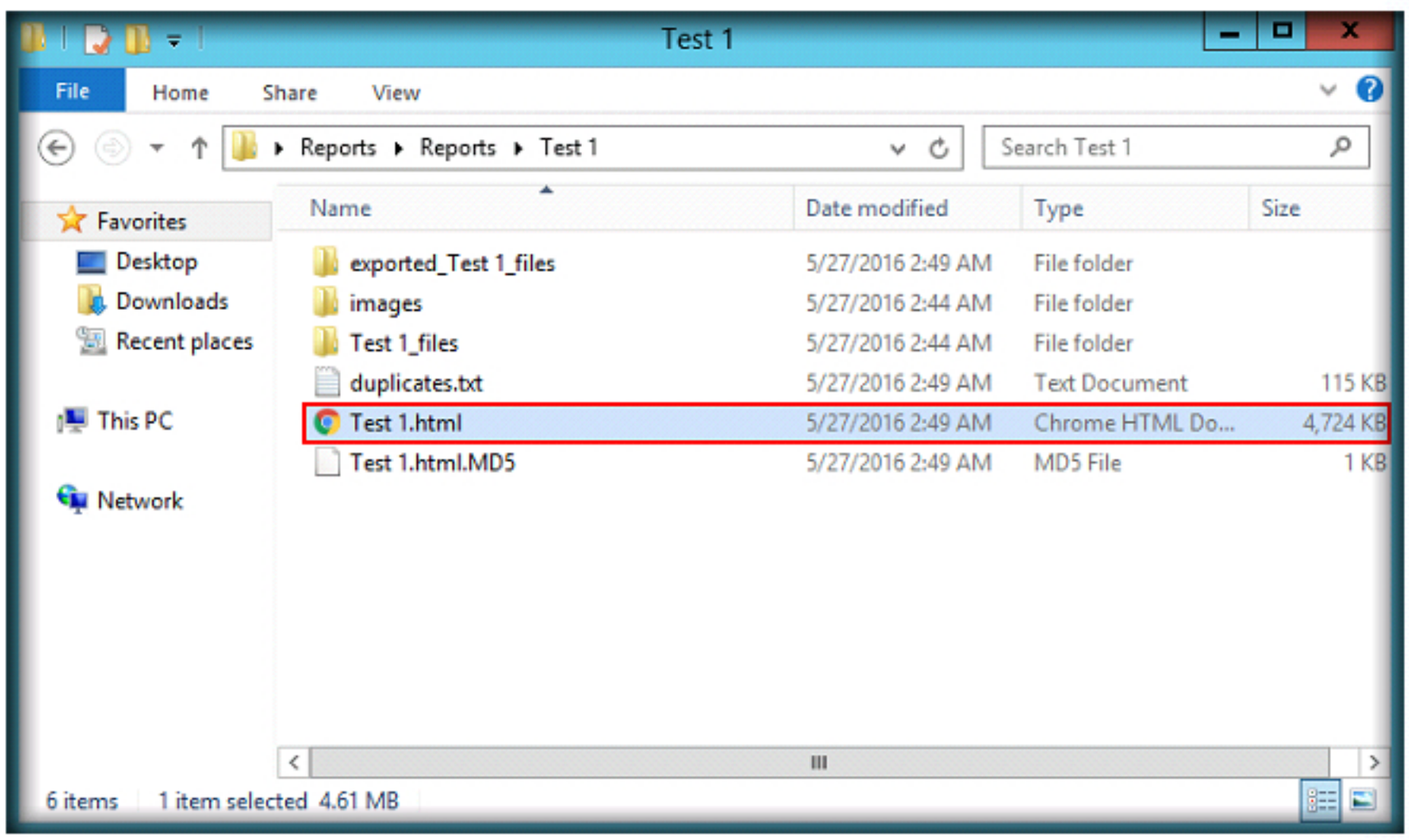

FIGURE 5.32: Output window

37. A detailed investigative report will open in the web browser, scroll down the browser window to view and examine the report.

The **Data View pane**, by default, is the large pane on the right in which the contents of the items selected in the **Case Explorer**can be viewed.

The **Data View** pane can include several tabs, each of which contains a **Data Viewer** for a separate part of the case.

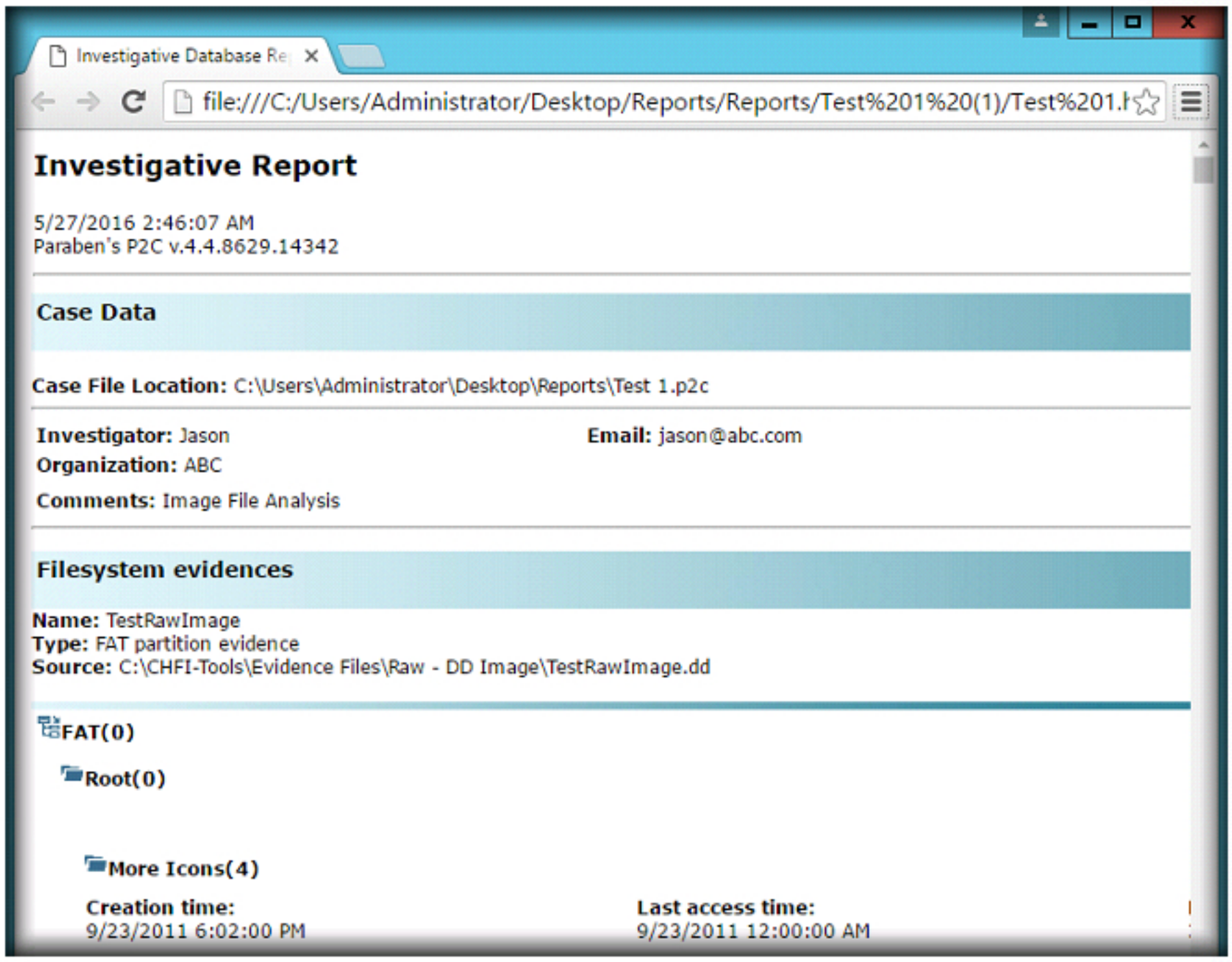

FIGURE 5.33: Final investigative report

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐Yes	☑No
Platform Supported	
☑ Classroom	☑iLabs

Lab

6

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

R-Drive Image is a potent utility providing disk image files creation for backup or duplication purposes.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process.

Lab Scenario

Investigator was performing a forensics process on a hard disk data, when he triggered a pre-loaded process that deleted the entire disk data leading to loss of the evidence. But he had already partitioned the disk into different sectors that gave him option to recover the lost data. Therefore, the investigators should always create duplicates of the hard disk and perform forensics process on the copy.

To be a **computer forensics expert**, you must have sound knowledge of various disk imaging tools used for forensics investigation.

Lab Objectives

The objective of this lab is to help students understand how to create a disk image file of hard disk partition using **R-drive image**.

Lab Environment

This lab requires:

- The R-drive Image tool, which is located at **C:\CHFI-Tools\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\R-drive Image**.
- You can also download the latest version of **R-drive Image** from the link http://www.drive-image.com/Drive_Image_Download.shtml.
- Please note that, if you decide to download the latest version, then the screenshots shown in this lab might differ slightly.

- A computer running **Windows 10** virtual machine.
- Administrative privileges to install and run tools.

Lab Duration

Time: 15 Minutes

Overview of Creating a Disk Image File of a Hard Disk Partition Using R-Drive Image Tool

R-Drive Image is a potent utility that can be used for disk image file creation, for backup or duplication purposes. A disk image file contains the exact, byte-by-byte copy of a hard drive, partition, or logical disk and can be created with various compression levels on the fly without stopping Windows OS, and therefore without interrupting your business. These drive image files can then be stored in a variety of places, including various removable media such as CD-R (W)/DVD, Iomega Zip or Jazz disks, etc.

Lab Task

TASK 1

Selecting the Hard Disk Partition

1. Navigate to **Z:\CHFIv9 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\R-drive Image**.
2. Double-click **RDriveImage6.exe** to launch the setup, select the language (here, **English**) and follow the wizard-driven installation steps to install the application.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

If a **User Account Control** pop-up appears, click **Yes**.

If a **Windows Security** dialog-box appears, enter the credentials of **Windows 10** virtual machine and then click **OK**.

FIGURE 6.1: R-Drive Image Setup

3. On completing the installation, ensure that **Launch R-Drive Image** option is checked and click **Finish**.

FIGURE 6.2: Launch R-Drive Image option

4. The **R-Drive Image** GUI appears, click **Next**.

You can also use R-Drive Image for mass system deployment when you need to set up many identical computers.

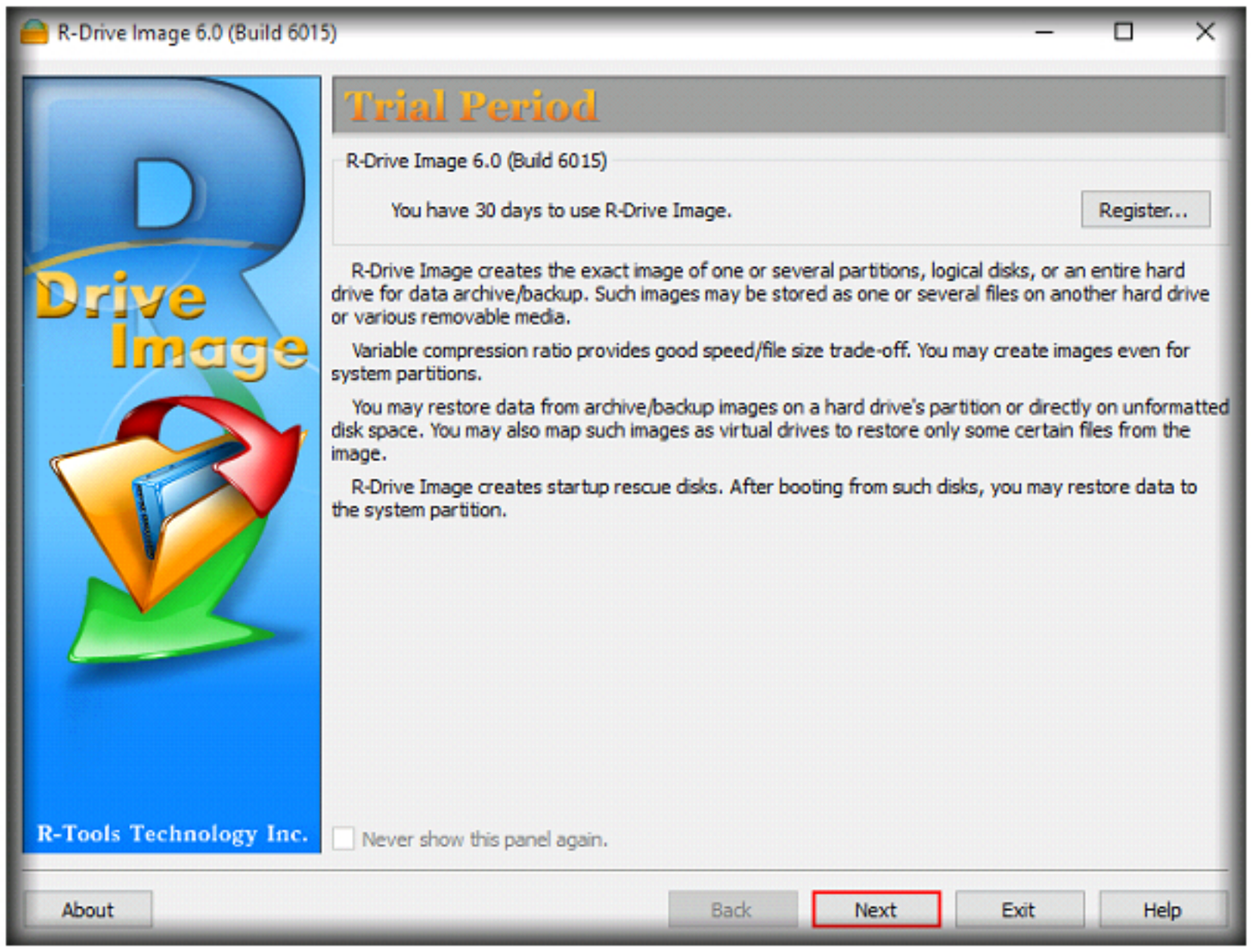

FIGURE 6.3: R-Drive Image GUI

5. In the **Action Selection** window, select the **Create an Image** option and click **Next** to continue.

R-Drive Image, can completely and rapidly restore your system after heavy data loss caused by an operating system crash, virus attack, or hardware failure.

FIGURE 6.4: Action Selection window

6. In the **Partition Selection** window, select **D drive** to create a drive image file of the D drive. Click **Next**.

In addition to FAT and NTFS, R-Drive Image now can backup only useful information for exFAT, HFS/HFS+, Little and Big Endian variants of UFS1/UFS2 and Ext2/Ext3/Ext4 FS (Linux) filesystems to reduce image file size.

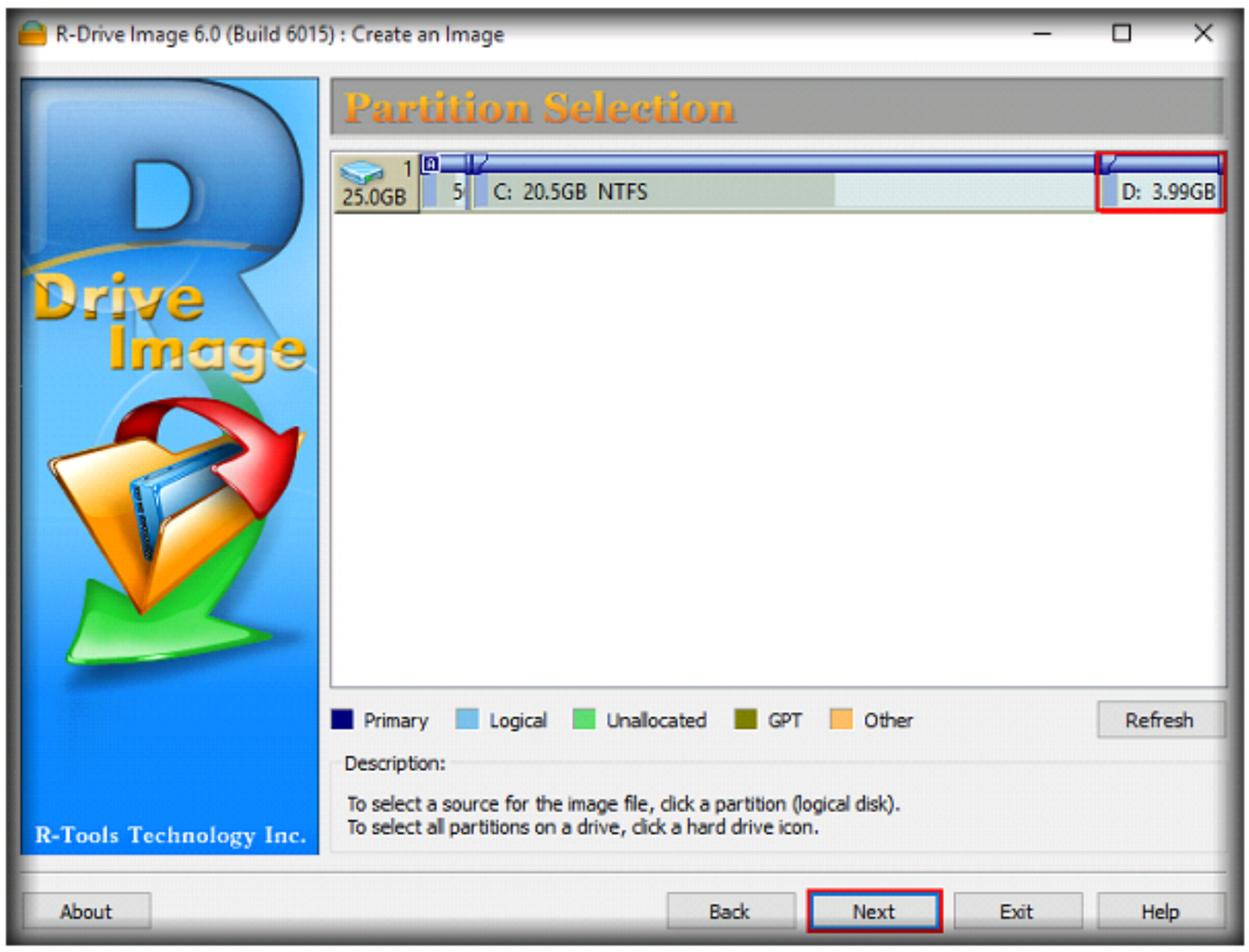

FIGURE 6.5: Partition Selection window

TASK 2

Selecting the Destination Folder

7. In the **Image Destination** window:
   - Select **D drive** in the tree pane to save the file.
   - The filename will be automatically taken by the application.
   - Select **R-Drive Image files (*.rdr)** in the **Files of type** field to save the file in **.arc** format. Click **Next**.

Image files are created on the fly; there is no need to stop and restart Windows. All other disk writes are stored in a cache until the image is created. Data from image files are restored on-the-fly as well, except on a system partition. Data to the system partition can be restored either by restarting R-Drive Image in its pseudo-graphic mode directly from Windows, or by using specially created startup disks.

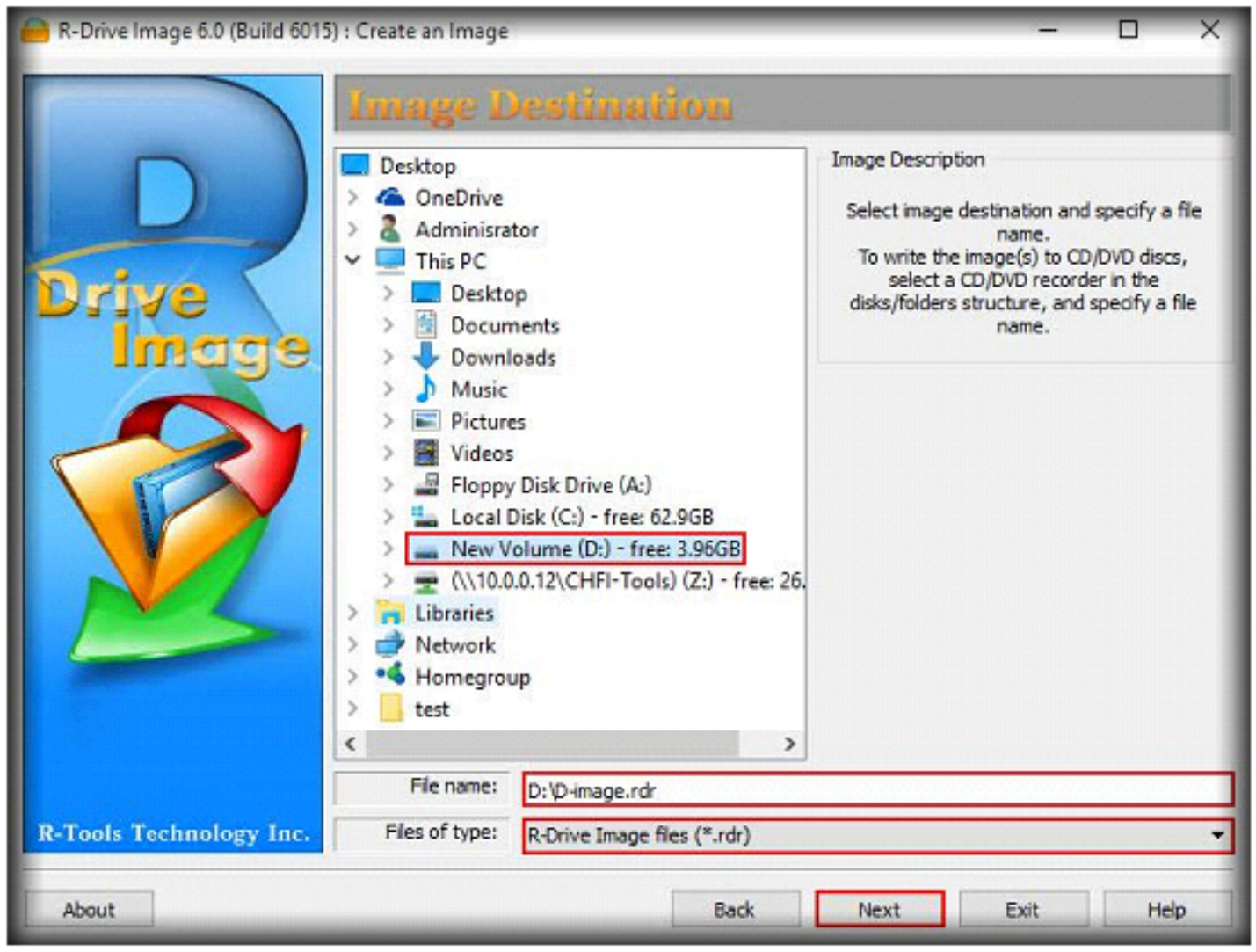

FIGURE 6.6: Image Destination window

8. In the **Image Options** window, click **Next**.

Note: Providing a password is optional.

R-Drive Image bootable version (based on the Linux kernel) supports writing to NTFS partitions as well as R-Drive Image Windows version.

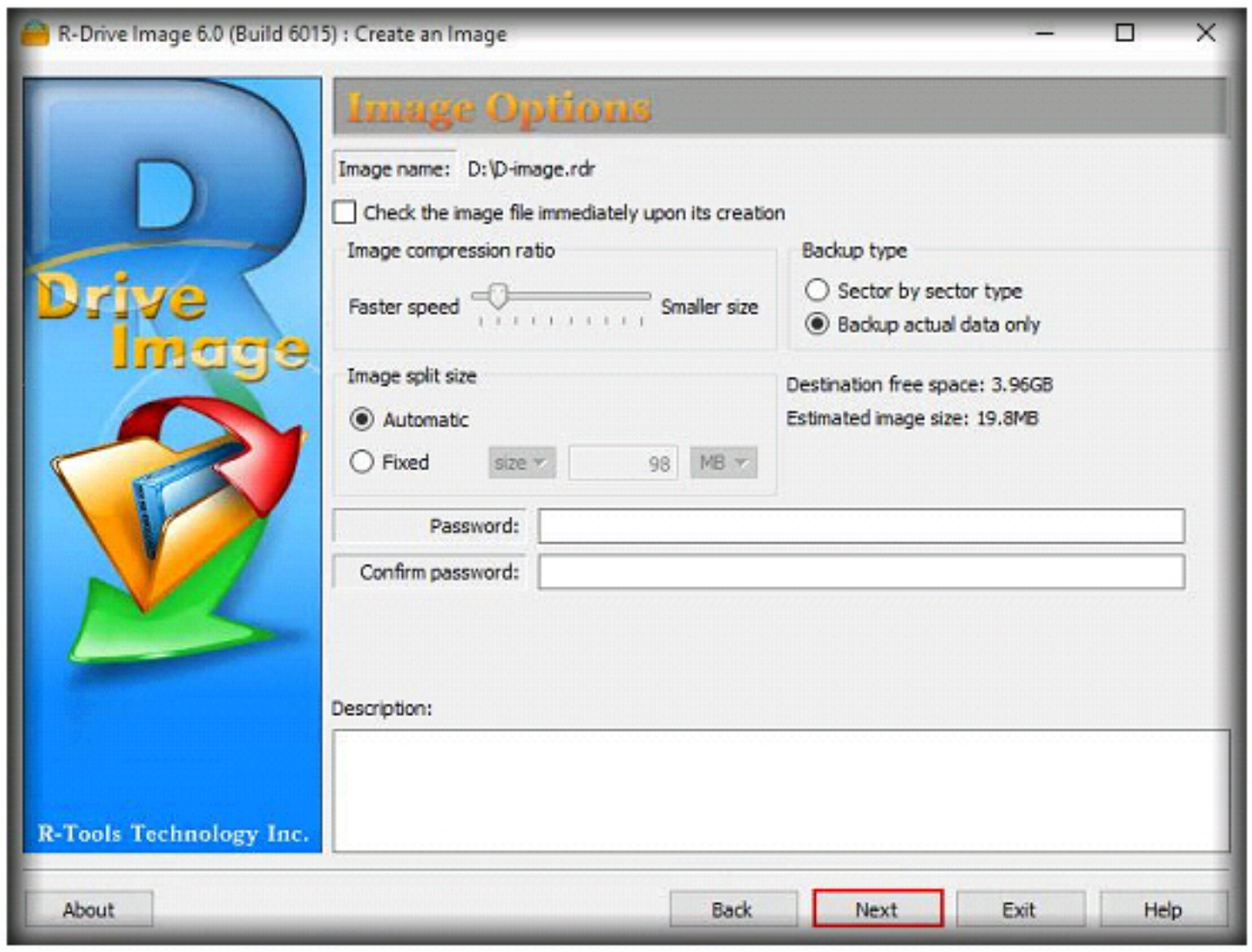

FIGURE 6.7: Image Options window

9. In the **Backup Options** window, click **Next**.

Asynchronous I/O and distributed the zlib compression library were added among different processors. As a result, users can see up to 200% speed gains in image creation and disc copy operations.

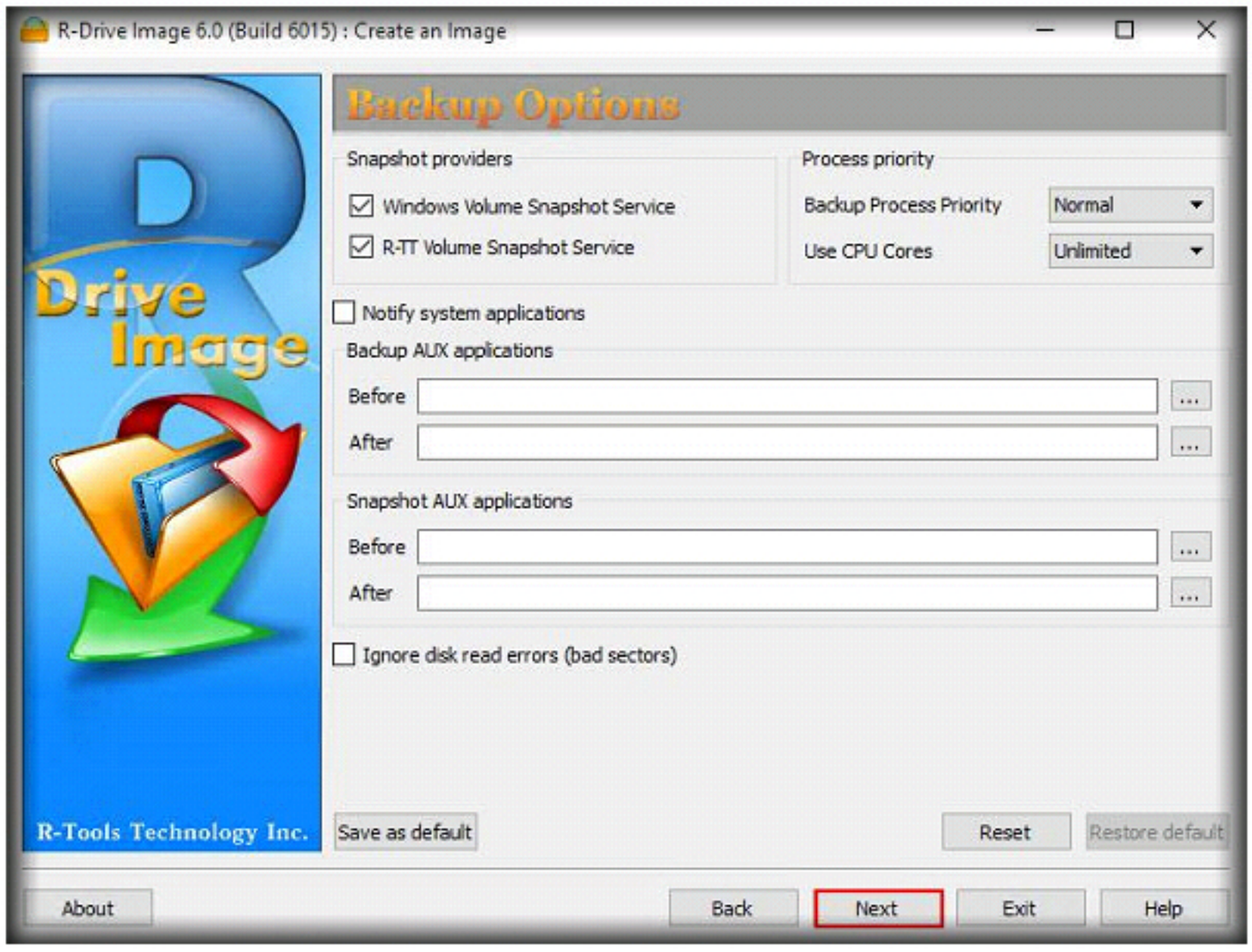

FIGURE 6.8 Backup Options window

TASK 3

Creating a Disk Image File

When the incremental/differential backup is being created, the differential image can be created by comparing the current data with the 128-bit hash of the original data without reading the main image. That speeds up the process of creating the incremental/differential image in any case, but also means there is no need to change the original discs when writing the image to

10. The **Processing** window will show the summary of all the processes. Click **Start** to start the disk partition imaging process.

FIGURE 6.9: Processing window

11. The **Progress bar** in the **Processing** window will show the completed percentage task.

R-Drive Image is switched to the pseudo-graphic mode directly from Windows, or the bootable version created by the utility is launched from CDs or diskettes.

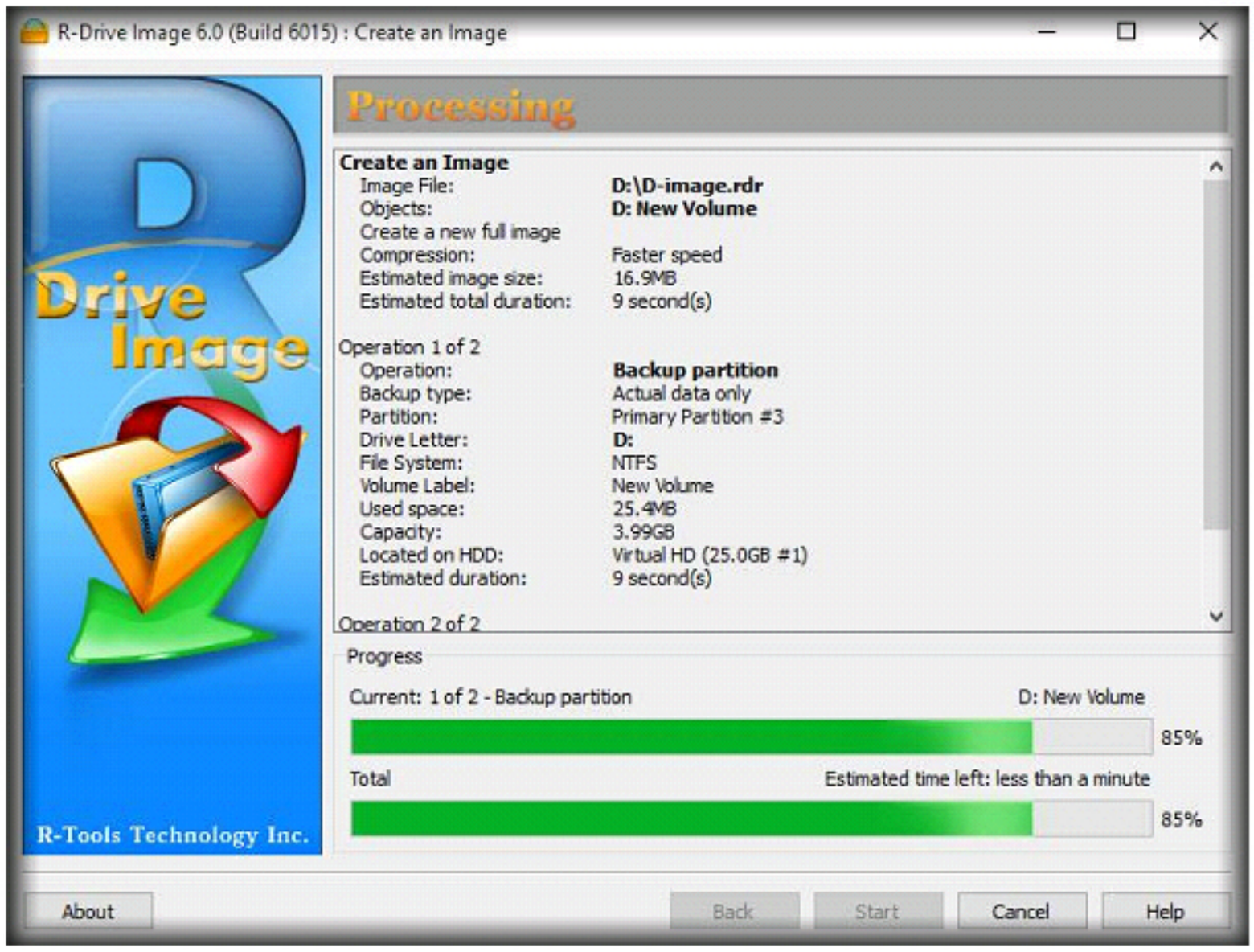

FIGURE 6.10: Processing window

12. Once the processing is done, the following pop-up window is displayed. Click **OK**

R-Drive Image is a backup and disaster recovery solutions to prevent losing your data after a fatal system failure.

R-Drive Image handles bad sectors encountered on the disk.

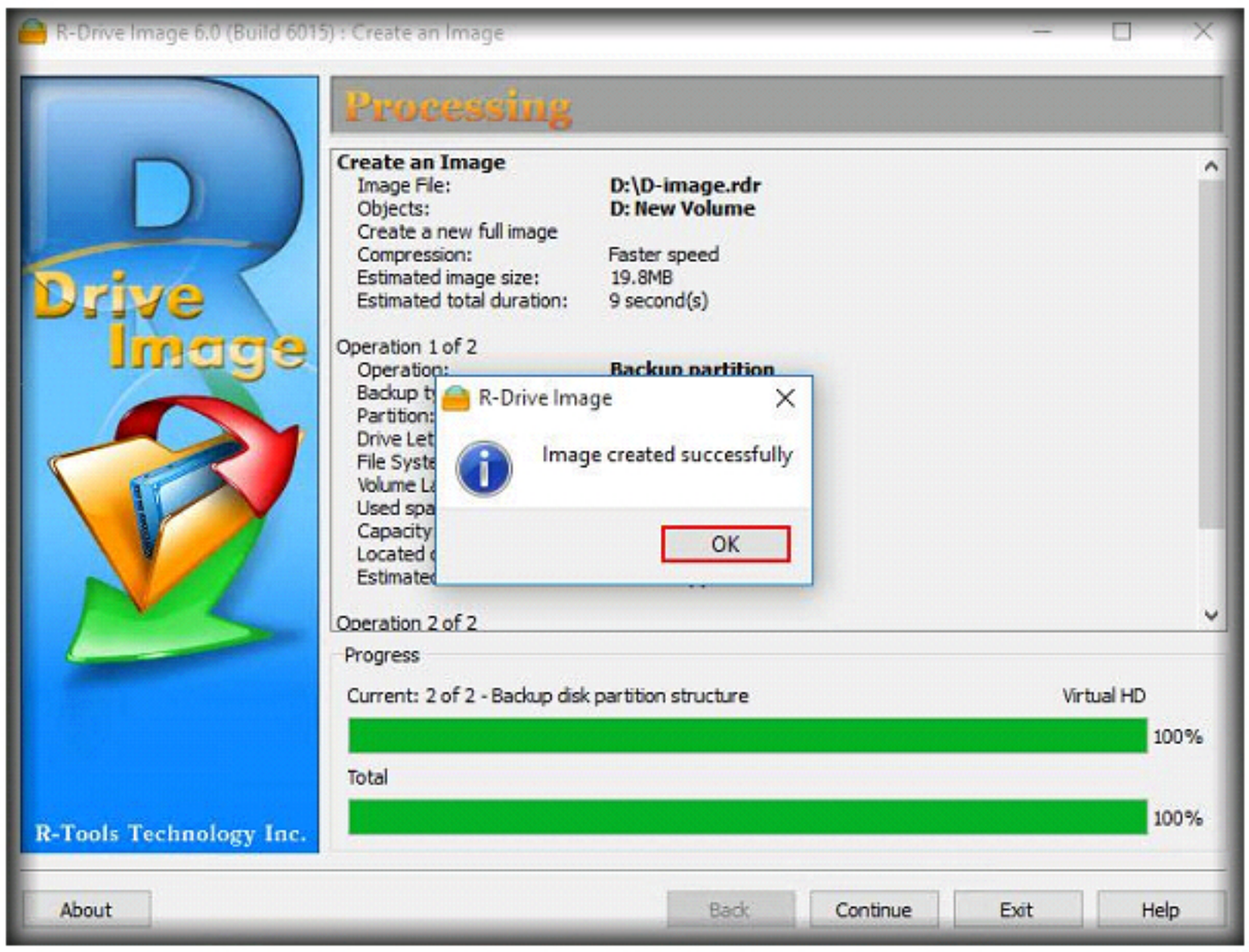

FIGURE 6.11: R-Drive Image pop-up window

13. In the **Processing** window, click **Continue** to complete the process.

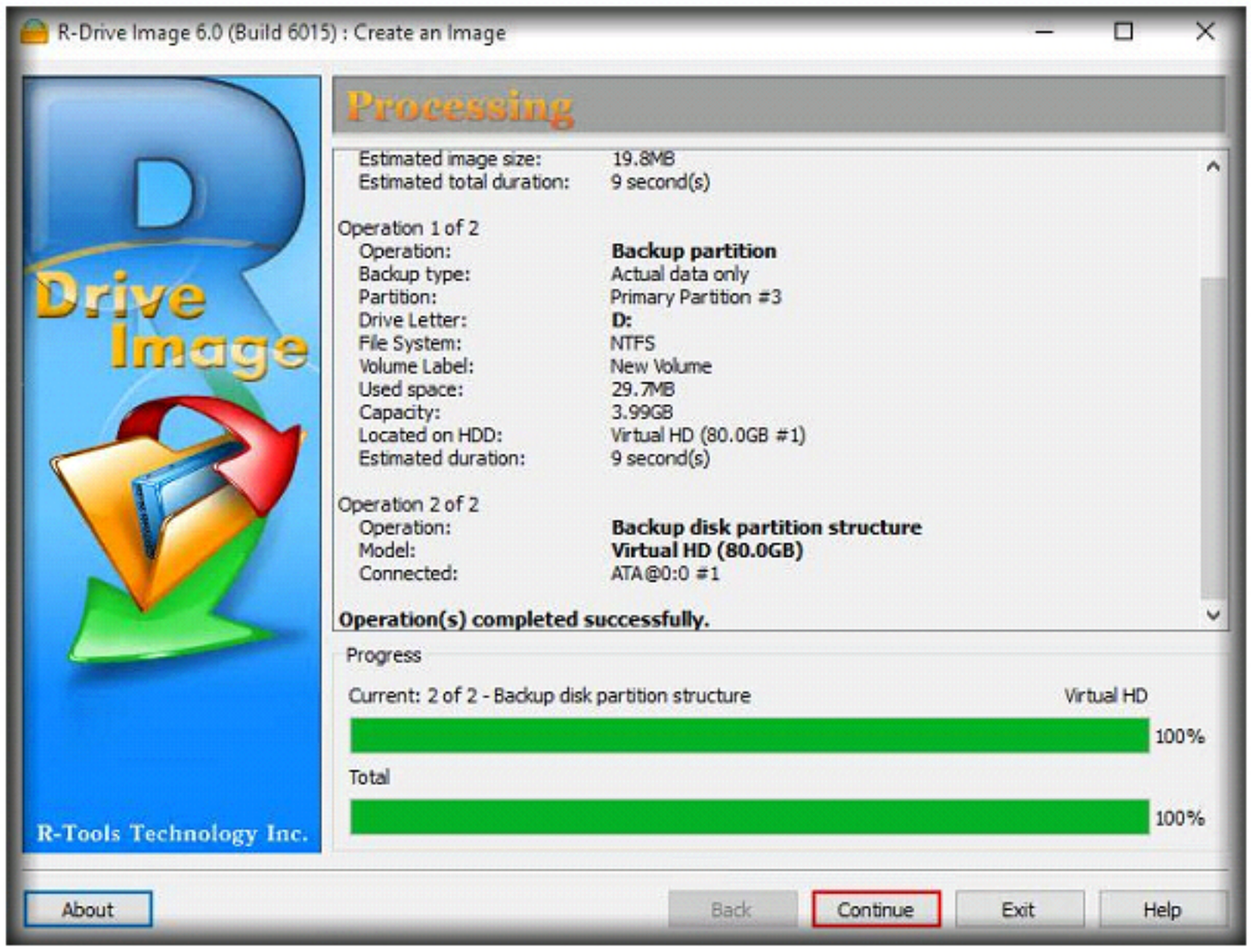

FIGURE 6.12: Processing window

R-Drive Image restores the images on the original disks, on any other partitions, or even on a hard drive's free space on the fly.

14. In the **R-Drive Image** window, click the **Exit** button to close the application.

TASK 4

Viewing a Created Disk Image File

15. Go to the **D Drive** to view the created disk partition image file.

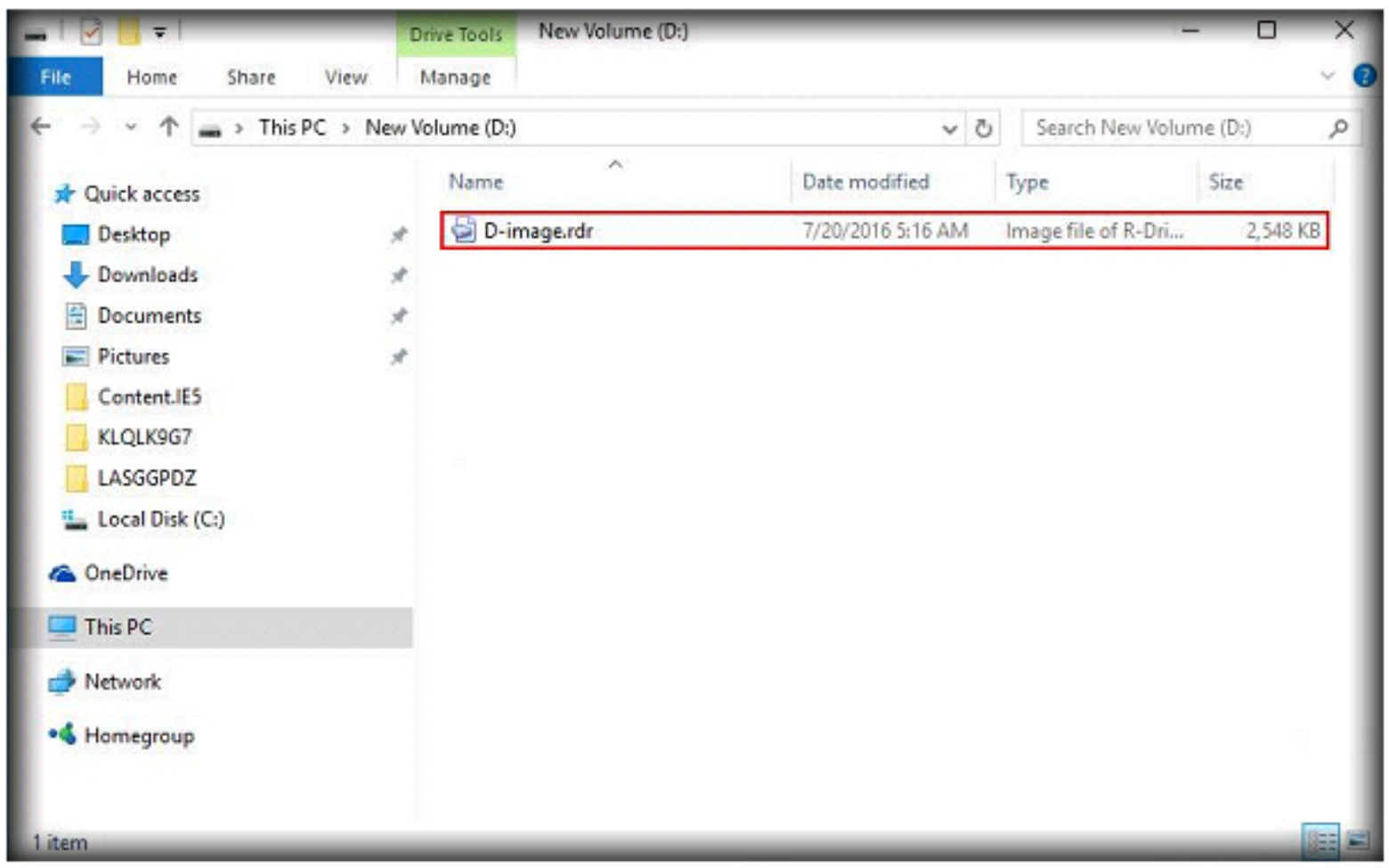

FIGURE 6.13: C Drive files

Dynamic disks and BSD slices can be backed up, restored, and copied. The feature is supported in both Windows and bootable versions of R-Drive Image.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐Yes	☑No
Platform Supported	
☑ Classroom	☑iLabs