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 until 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 in incidents of cyber-crime 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 complies with local laws and established precedents and any deviation from the standard process may jeopardize the whole 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 cross examination.

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 files from the evidence
- Generating hashes and checksum files
- Calculating the MD5 value of the selected file
- Viewing files of various formats
- Analyzing an evidence file and generating investigative report
- Creating a disk image file of a hard disk partition

Lab Environment

This lab requires:

- A system running a **Windows Server 2016** virtual machine
- A system running a **Windows 10** virtual machine

- A web browser with Internet access
- Administrative privileges to run tools

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process

Lab Duration

Time: 90 minutes

Overview of the Computer Forensics Investigation Process

A computer forensics expert should be well-versed with the 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 compare the checksums 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 can 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 have built 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 corporation.

Lab Tasks

Recommended labs to assist in computer forensic investigation process:

- Recovering Data from a Windows Hard Disk
- Performing Hash or HMAC Calculations
- Comparing Hash Values of Files to Check their Integrity
- Viewing Files of Various Formats
- Handling Evidence Data
- Creating a Disk Image File of a Hard Disk Partition

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 from a Windows Hard Disk

A hard disk is a non-volatile data storage device used to store data or install programs on your computer.

ICON KEY

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

Lab Scenario

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 investigator to investigate the issue. What tool(s) should the investigator use to recover the deleted files?

To be an expert computer forensic investigator, one must have sound knowledge of the tools that can be used to recover deleted files/data.

Lab Objectives

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

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process

This lab requires:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute the commands
- A web browser with internet access
- **EaseUS Data Recovery Wizard** installer located at **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Data Recovery Tools\EaseUS Data Recovery Wizard**

Note: You can download the latest version of **EaseUS Data Recovery Wizard** from the link https://www.easeus.com/datarecoverywizard/free-data-recovery-software.htm

If you are using the latest version of software for this lab, then the steps and screenshots demonstrated in the lab might differ.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 15 minutes

Overview of the Lab

This lab familiarizes you with the tool EaseUS Data Recovery Wizard and helps you understand how to recover files that have been deleted from a Windows system.

Lab Tasks

1. Log on to the **Windows 10** virtual machine.
2. Make sure that the **Windows Server 2016** virtual machine is also turned **on**.
3. Before beginning this lab, navigate to **Documents** directory and create a folder named **Recovered Files**.

TASK 1

Install and Launch EaseUS Data Recovery Wizard

4. Navigate to **Z:\CHFIv10 Module 02 Computer Forensics Investigation Process\Data Recovery Tools\EaseUS Data Recovery Wizard** and double-click **DRW13.5_Free.exe**. A **Select Setup Language** window will appear; ensure to select **English** language and click **OK**.

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

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

Note: If a **Windows Security** dialog box appears, enter the credentials of the **Windows Server 2016** virtual machine and then click **OK**.

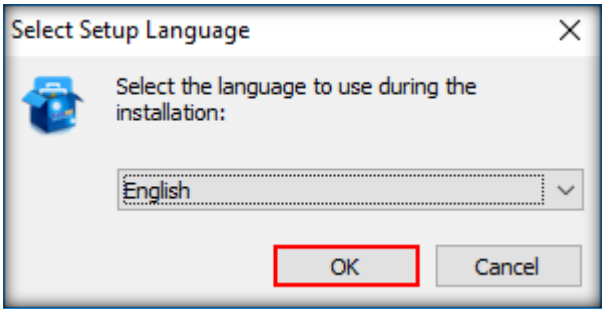

FIGURE 1.1: EaseUS Data Recovery Language Setup Wizard

5. **Setup - EaseUS Data Recovery Wizard** will appear; follow the wizard-driven installation steps to install the application.

FIGURE 1.2: EaseUS Data Recovery Installation Wizard

6. In the final step of the installation, uncheck **Participate in the Customer Experience Improvement Program** and click **Finish**.

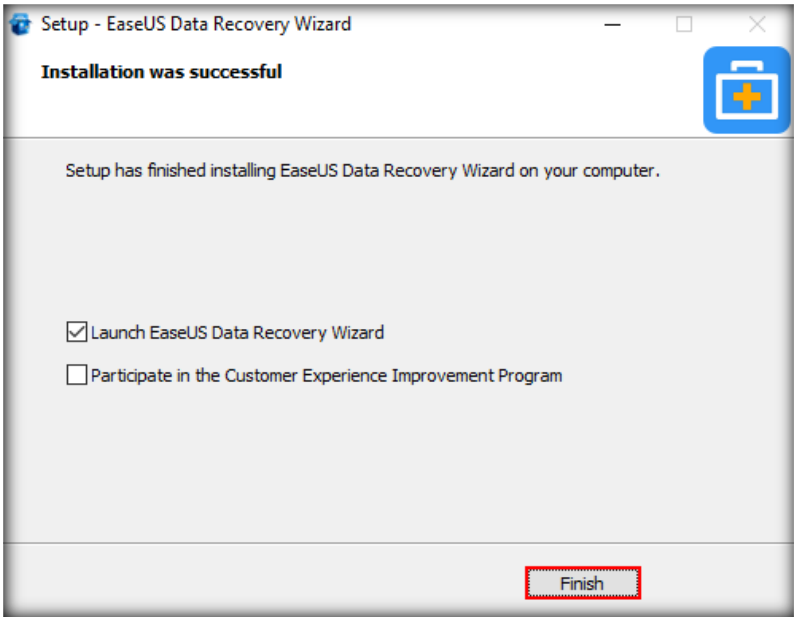

FIGURE 1.3: EaseUS Data Recovery Installation Completed

Note: If a pop-up appears stating **This app can't open**, click **Close**.

Note: An EaseUS Installation Successful webpage appears in a web browser. Close the browser.

7. If a **Check Update** pop-up appears and the application begins to look for updates, click **Cancel** to cancel the updates.

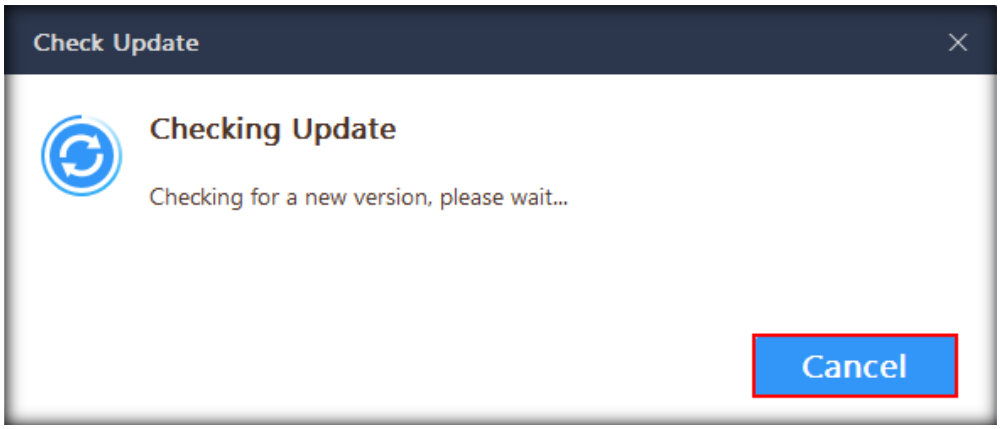

FIGURE 1.4: Update Checker

8. **EaseUS Data Recovery Wizard** opens along with an **EaseUS Data Recovery Wizard** pop-up at the lower-right side corner of the screen. **Close** the pop-up.

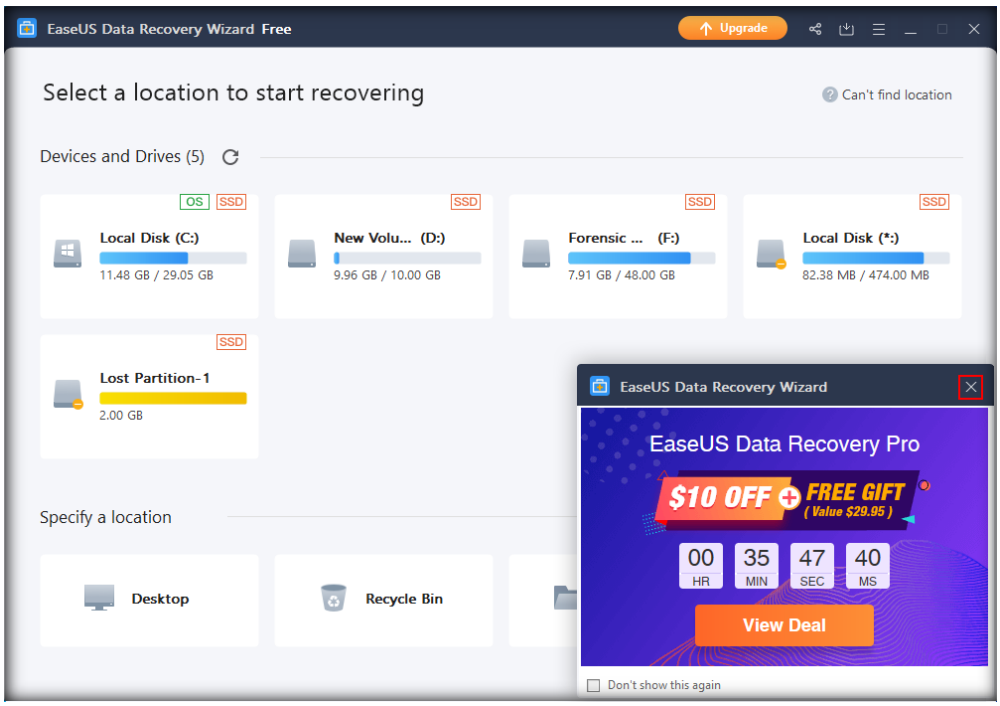

FIGURE 1.5: EaseUS Data Recovery Wizard Main Window

9. **EaseUS Data Recovery Wizard** displays the **Hard Disk Drives** under the **Devices and Drivers** section. Hover the mouse cursor over the drive/location you want to scan so that the **Scan** button appears below the location. In this lab, we will be scanning **D Drive** (**D:**); therefore, hover the cursor over the **New Volume (D:)** to see the **Scan** button, then click on **Scan**.

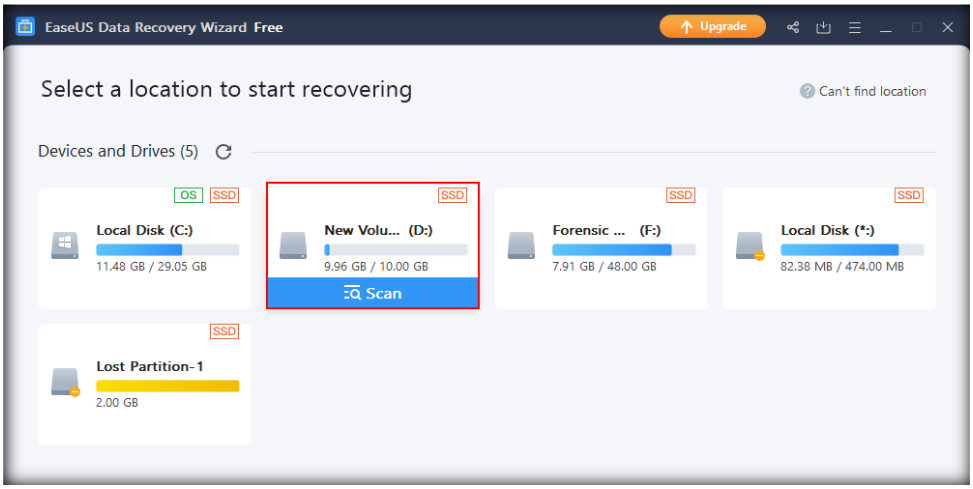

FIGURE 1.6: Scanning a Drive for Deleted Files/Folders

EaseUS Data Recovery is a professional data recovery software for:

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

TASK 2

Recover Deleted Files

10. The application runs two types of scans: **Quick Scan** and **Advanced Scan**. Upon completion of the scan, it displays the scan results under three folders: **Deleted Files**, **Lost Files,** and **Existing Files**.

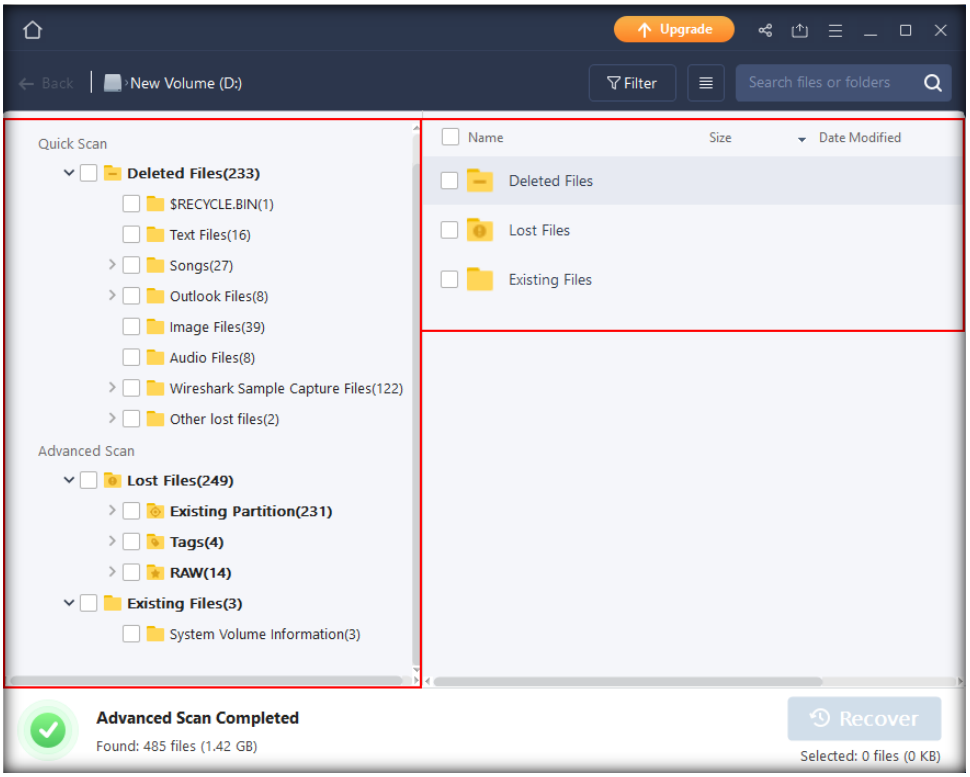

FIGURE 1.7: Files Recovered by the Application

11. The deleted files are contained within the **Deleted Files** directory under the **Quick Scan** section. You can choose either to preview these files or recover them depending on your requirement.

12. In this lab, we will be previewing a text file named **1.txt**. To do that, expand **Deleted Files** and then select **Text Files** folder. A list of files associated with this folder appears in the right pane, right-click on **1.txt** and select **Preview**.

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

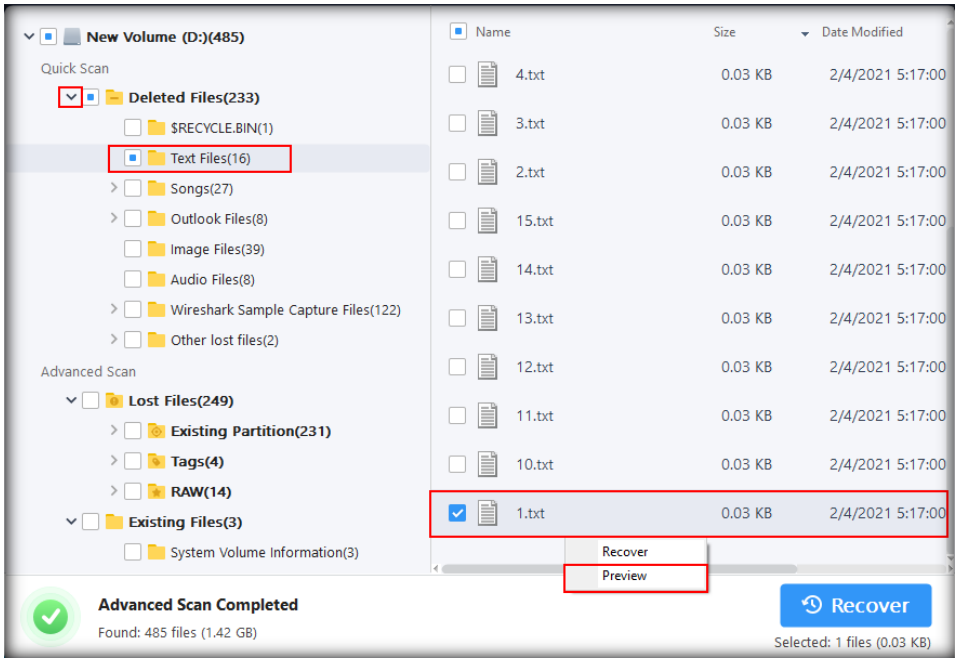

FIGURE 1.8: Previewing File to be Recovered

13. The preview of the selected file will appear as shown in the screenshot below:

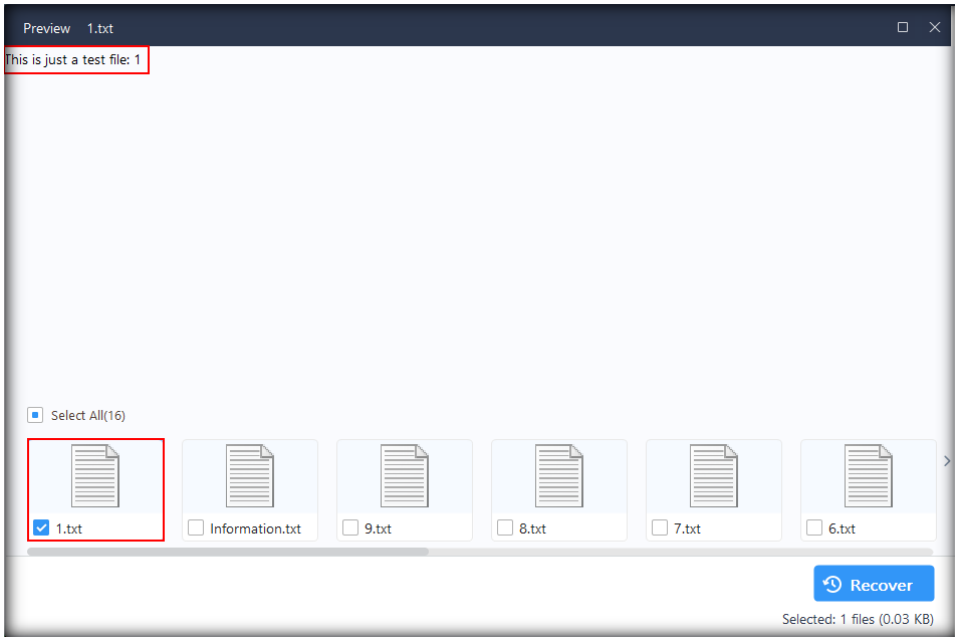

FIGURE 1.9: Image File Preview

14. If you wish to recover this text file, click on **Recover**.

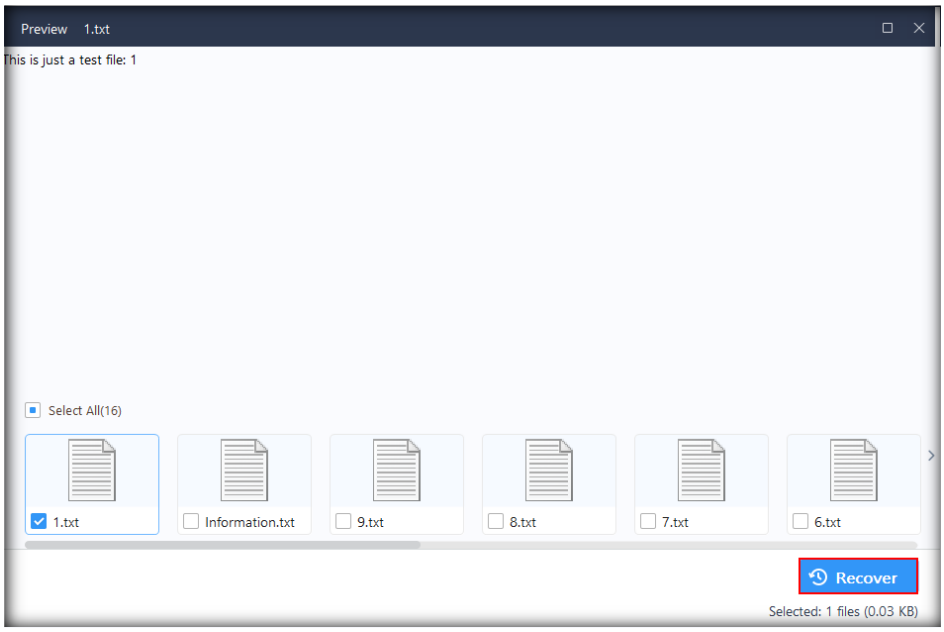

FIGURE 1.10: Recovering Previewed Image File

15. A **Browse for Folder** window appears where you need to choose the location for saving of the file. We will be saving the file to the **Recovered Files** directory that we created in the beginning of the lab.

16. Therefore, under **This PC** section, expand **Documents**, select **Recovered Files** folder, and click **OK**. The file being recovered then gets saved to this **Recovered Files** folder.

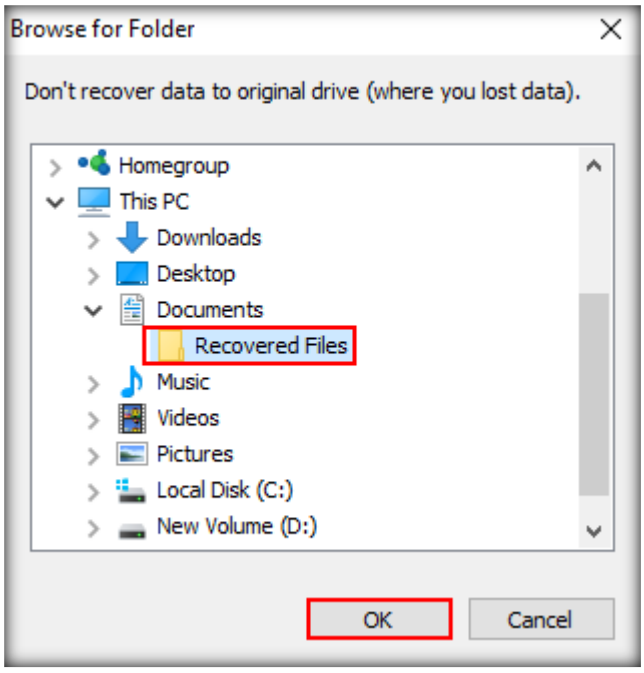

FIGURE 1.11: Browse for Folder Window

17. On completing the recovery, a **Recover Complete** window will appear, and the application automatically directs you to the **Recovered Files** folder.
18. Close the **Recover Complete** window and the **Preview** window.

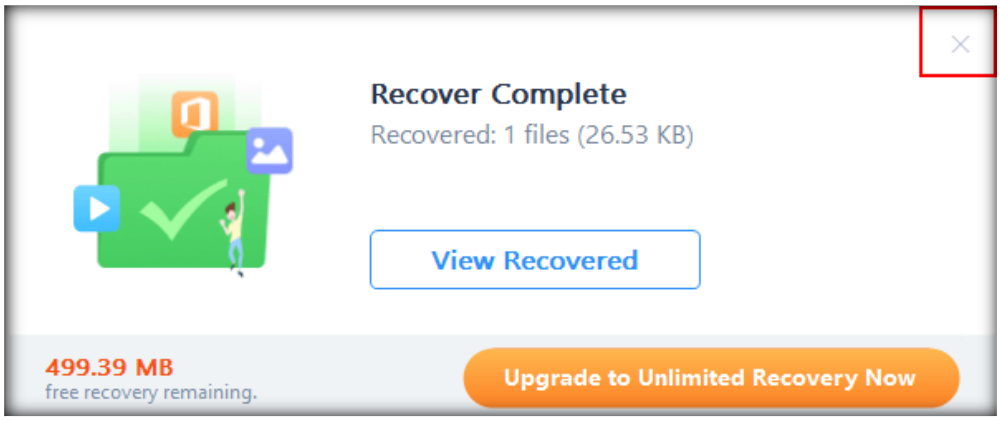

FIGURE 1.12: Recovery Complete Screen

19. EaseUS auto-creates a sub-folder named **Preview** inside yet another auto-created sub-folder named **Easeus [DD HH_MM]** under the **Recovered Files** folder, where **DD** denotes the **date**, **HH** denotes the **hours,** and **MM** denotes the **minutes**.

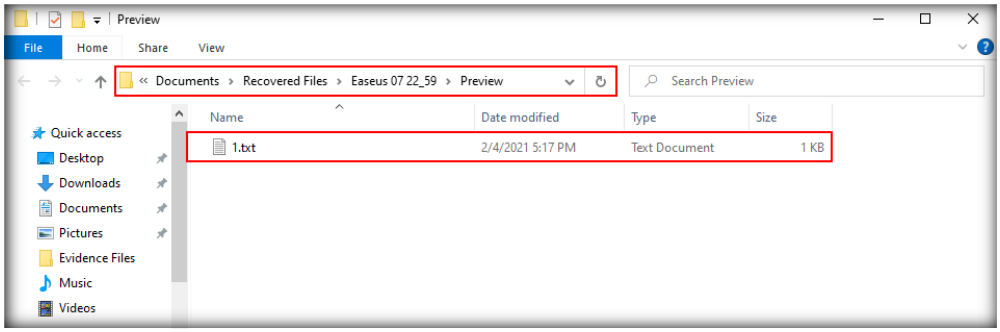

FIGURE 1.13: User Auto-directed to Location Where Recovered File is Saved

20. You can also manually view this recovered file by navigating to the location **Documents\Recovered Files\Easeus [DD HH_MM] \Preview** (or **C:\Users\Admin\Documents\Recovered Files\Easeus [DD HH_MM] \Preview**) .

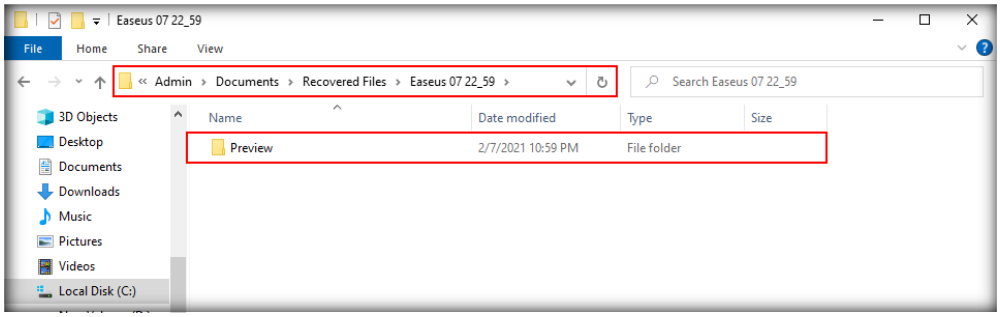

FIGURE 1.14: Navigating to the "Preview" Sub-Folder

21. To recover multiple files, select the files you want to recover, then click **Recover**. In this lab, we are going to recover **2.txt**, **3.txt**, **4.txt**, **5.txt**, **Information.txt**. Therefore, select these files and click **Recover**.

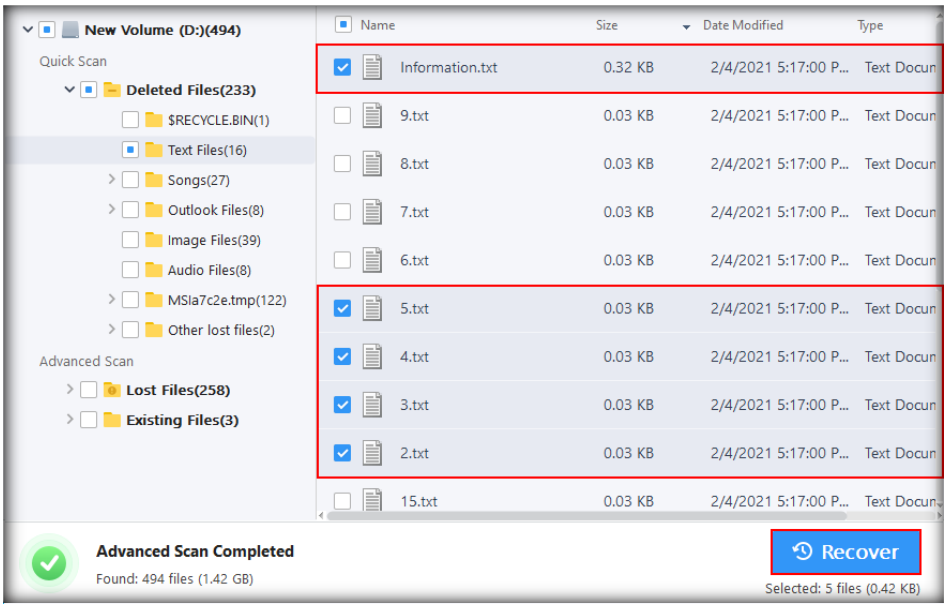

FIGURE 1.15: Recovering Multiple Image Files

22. On clicking **Recover**, the **Browse for Folder** window appears where you need to choose the location for saving of the file, like the previous case where a single file was recovered. You may either choose the **Recovered Files** folder created earlier to save the files or choose another location. In this lab, we will be saving the files to the same folder (**Recover Files**).

23. Following the same method as in the previous case, from the **Browse for Folder** window, expand **Documents**, select **Recovered Files** folder, and click **OK**. The file being recovered then gets saved to this **Recovered Files** folder.

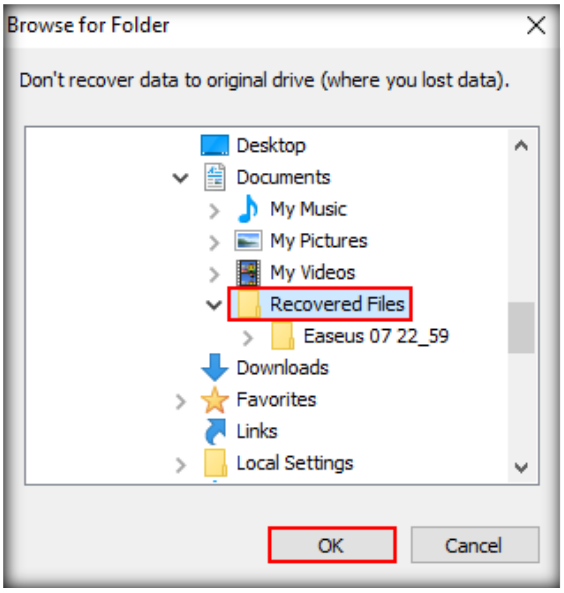

FIGURE 1.16: Browse for Folder Window

24. On completing the recovery, a **Recover Complete** window appears as previously seen, and the application automatically directs you to the location where the recovered files are saved.

25. Close the **Recover Complete** window.

26. EaseUS auto-creates a series of sub-folders inside **Recovered Files** folder in this order: **Easeus [DD HH_MM] → New Volume(D) → Deleted Files**, where **DD** denotes the **date**, **HH** denotes the **hours**, and **MM** denotes the **minutes**.

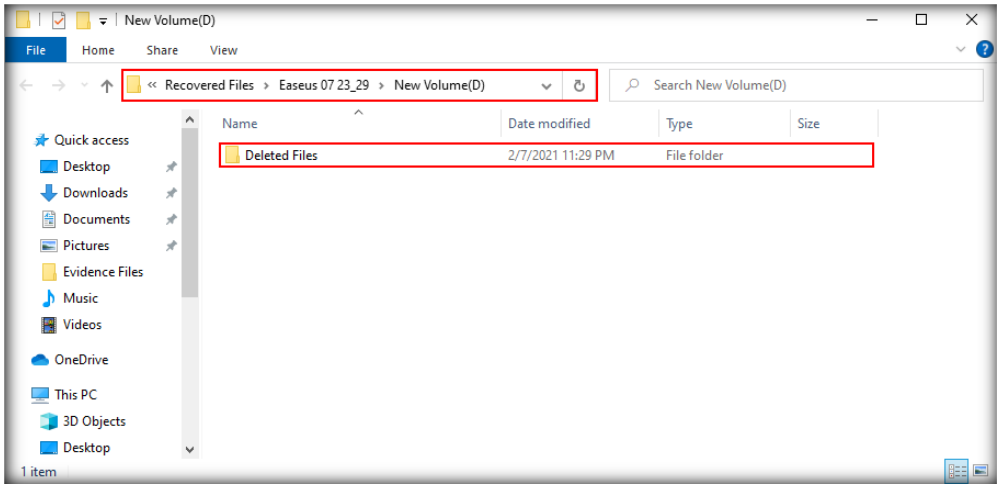

FIGURE 1.17: Recovered Files Saved to 'Deleted Files' Sub-folder

27. To view the recovered files, open **Deleted Files → Text Files**. The recovered files appear in this location, as shown in the following screenshot:

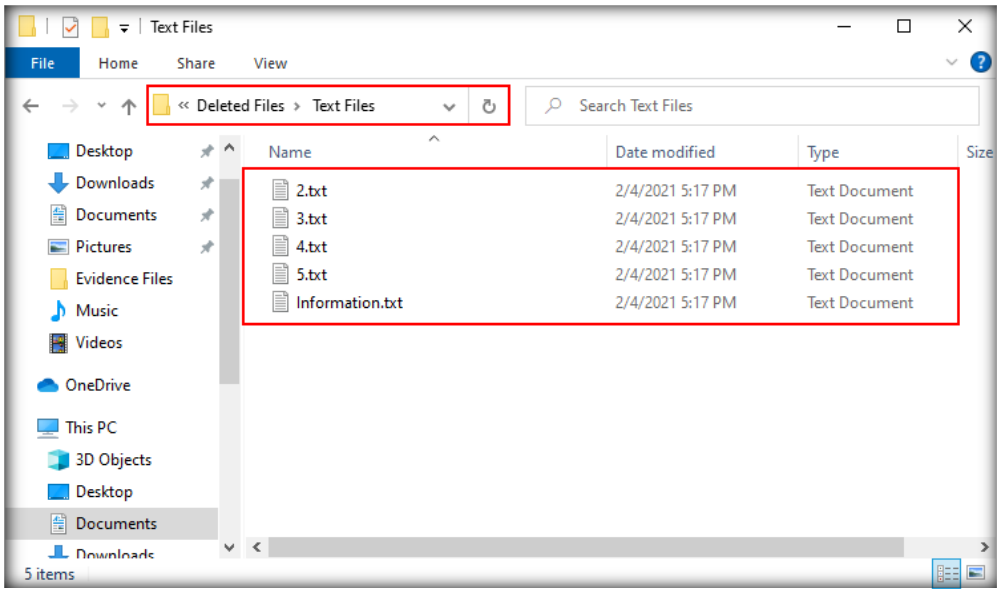

FIGURE 1.18: Multiple Image Files Recovered

28. In the same way, you may recover single or multiple folders, sub-folders, or even the entire **Deleted Files** folder by following the above steps.

Note: If the space required for saving the files/folders is insufficient, then consider saving the data to another location such as an external hard disk with

adequate space and create a backup. The recovered data may also be saved to cloud.

Note: Since we are using the trial version of **EaseUS Data Recovery Wizard**, the tool may have the limitation of not supporting the preview/recovery of files of certain formats.

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.

Lab

2

Performing Hash or HMAC Calculations

Hashing is performed on data such as files or text to generate unique fixed-length string called hashes or checksum. The generated hashes are helpful in determining whether the given data has maintained integrity.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

A multi-national company has undergone a network attack and has called a forensics investigator to investigate the issue. The investigator found some codes that appear to be familiar and needs to cross-check for their availability across a malware database. The major problem here is that the codes are huge and require a large amount of storage space, making it difficult for search and indexing purposes. 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 hashing and the tools used to compute hashes.

Lab Objectives

The objective of this lab is to demonstrate how to:

- Compute hashes of files and text string
- Check the hashes on VirusTotal to see if the file(s) are malicious

Note: Hashes or **hash values** may also be referred to as **checksums**.

Lab Environment

This lab requires:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute the commands
- A web browser with internet access

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process.

- **HashCalc** installer located at **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\HashCalc**

Note: You can download the latest version of **HashCalc** from the link https://www.slavasoft.com/hashcalc/

If you are using the latest version of software for this lab, then the steps and screenshots demonstrated in the lab might differ.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 10 minutes

Overview of the Lab

This lab familiarizes you with HashCalc, a tool that helps you determine the hash values of various files. Determining the hash values of files enables an investigator to establish their integrity.

Lab Tasks

TASK 1

Launching HashCalc Tool

1. Login to **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** to find the evidence files for this lab.

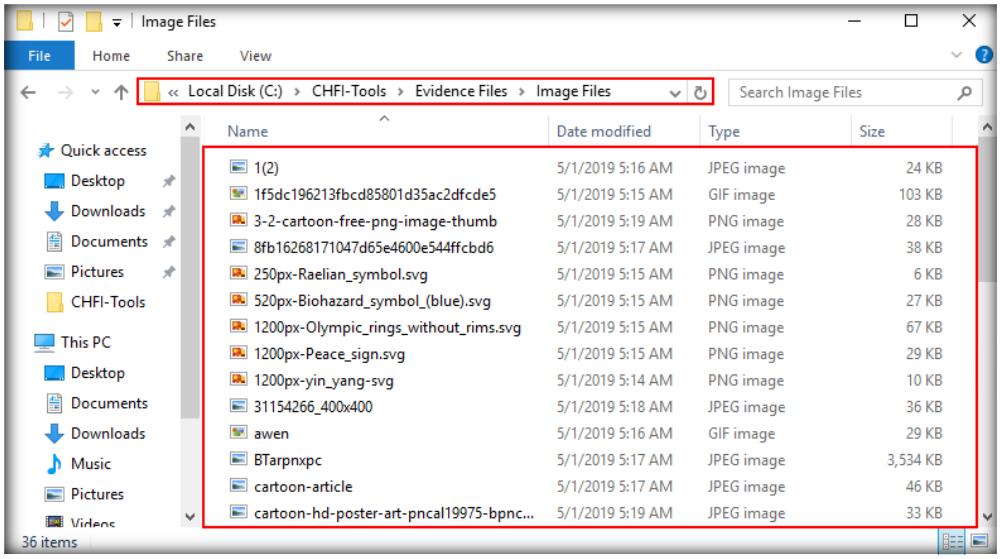

FIGURE 2.1: Evidence File

3. Navigate to **C:\CHFI-Tools\CHFIv10 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**.

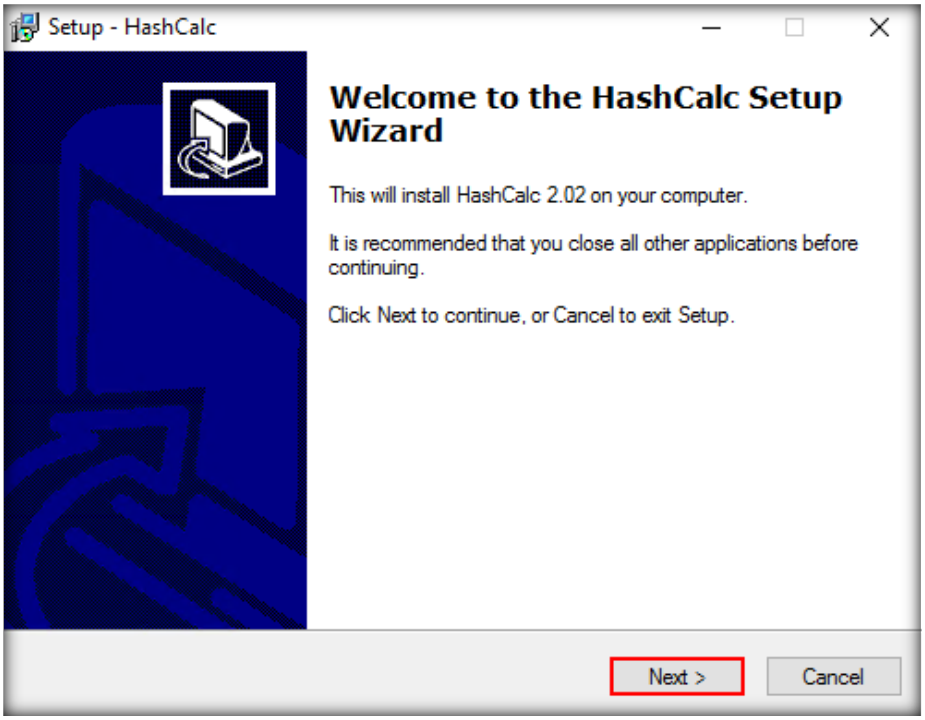

FIGURE 2.2: HashCalc Setup Wizard

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

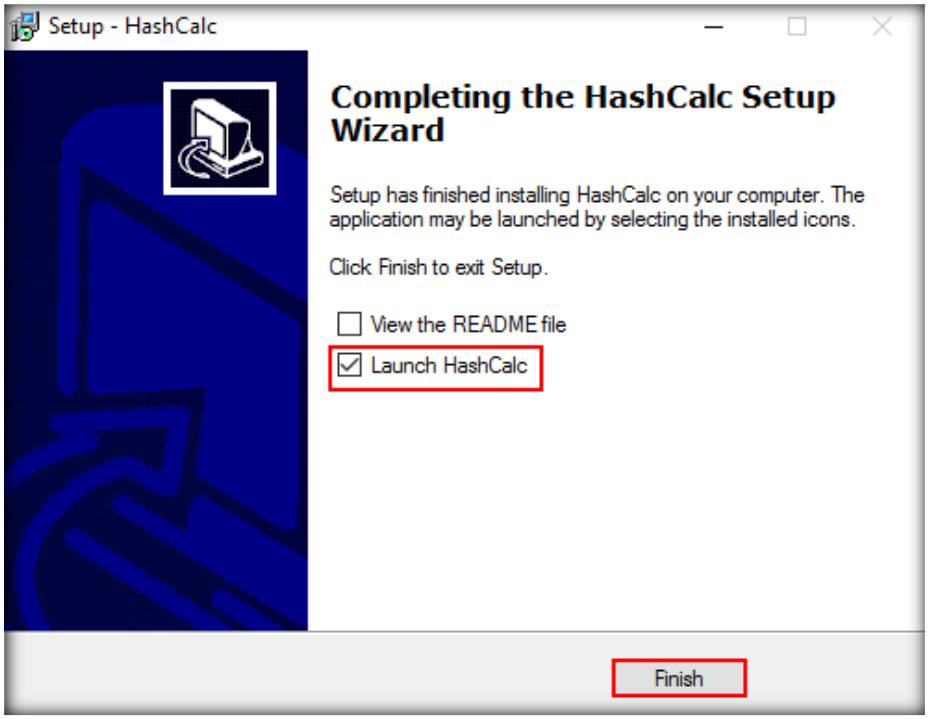

FIGURE 2.3: HashCalc Setup Wizard

HashCalc supports 13 well-known and documented hash and checksum algorithms: MD2, MD4, MD5, SHA-1, SHA-2 (256, 384, 512), RIPEMD-160, PANAMA, TIGER, ADLER32, and CRC32.

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

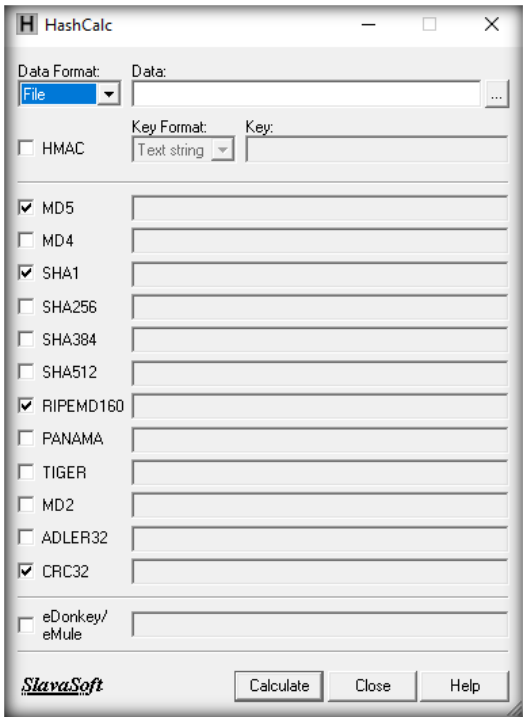

FIGURE 2.4: HashCalc Main Window

HashCalc works with large file sizes as well. 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 data format as **File** and click the **ellipsis** button associated with the **Data** field to select the file.

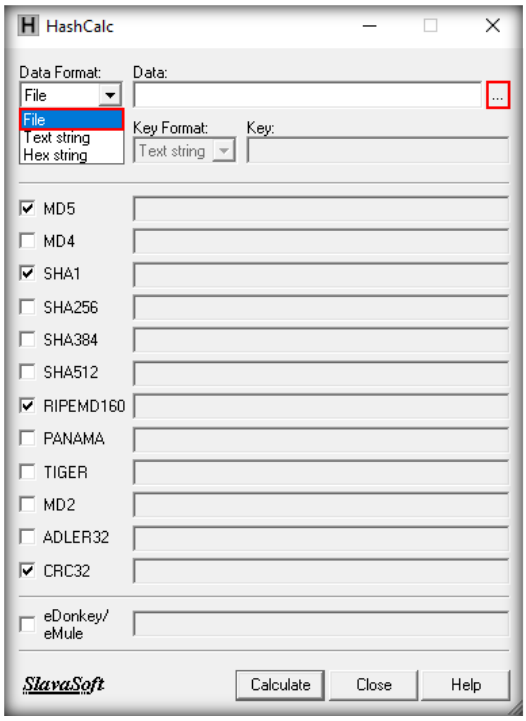

FIGURE 2.5: HashCalc Data Format Options

7. Subsequently, **Find** window will appear; 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 **Fan-oven.png**. Once you select the file, click **Open**.

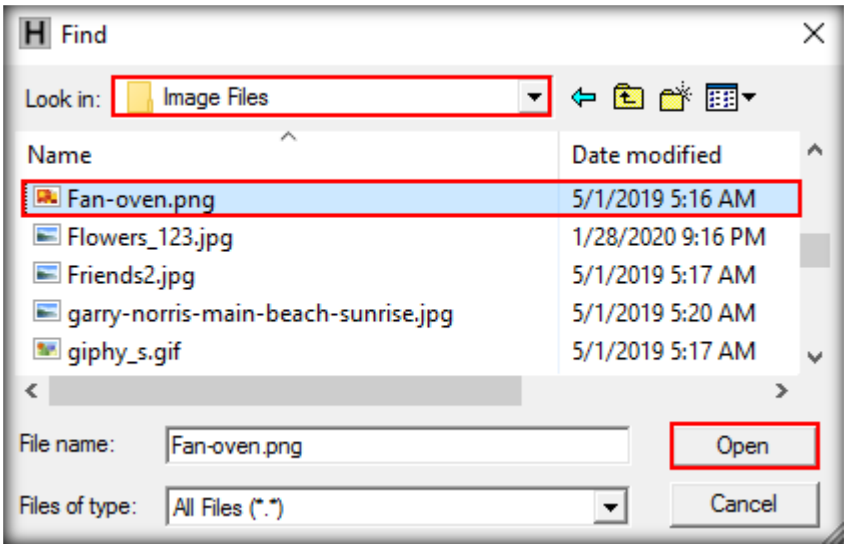

FIGURE 2.6: Selecting Evidence File in D Drive

HashCalc supports two modes of calculations: HASH/CHECKSUM and HMAC.

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

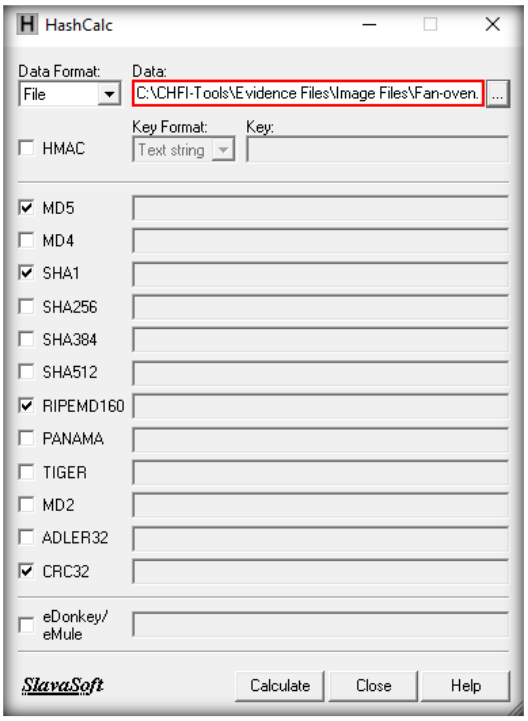

FIGURE 2.7: HashCalc Window

HashCalc calculates hash/checksum and HMAC for files of any type, including music, audio, video, image, icon, text, compression, etc., with the following 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.

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.

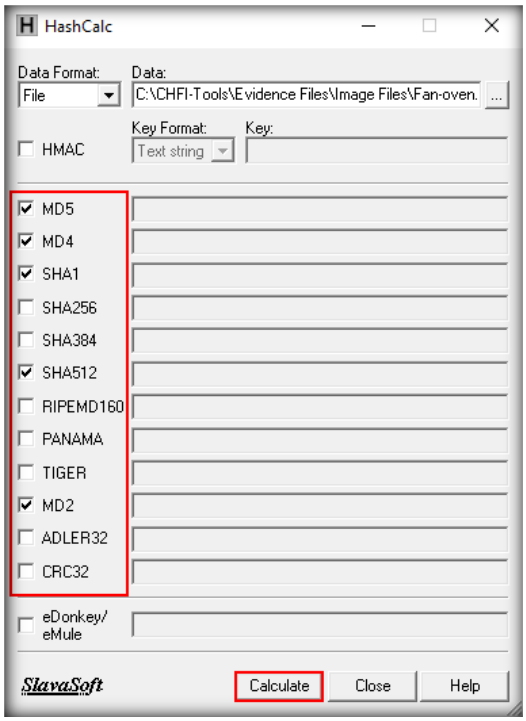

FIGURE 2.8: Calculation of Hash Values

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

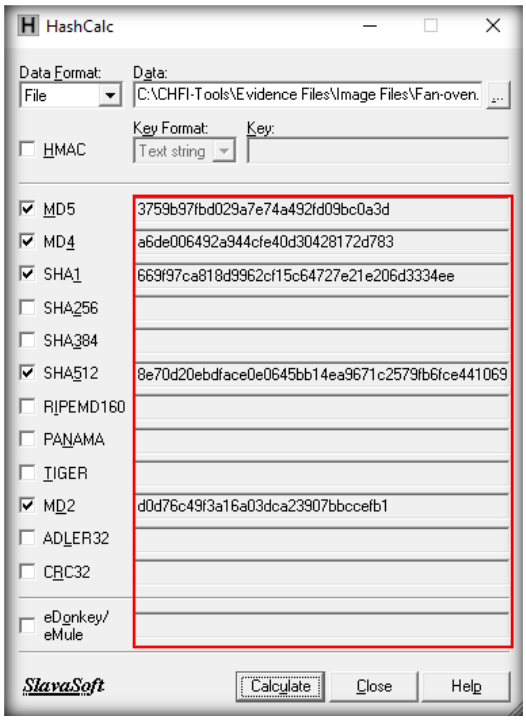

FIGURE 2.9: Window Displaying Hash Values

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 (Here, we have selected **Text String** in the **Key Format** combo box).
    - In the **Key** box, enter the key for **HMAC** calculations (for example, **test** is entered as key here).
    - Select the algorithms you want to use for calculations by checking the required algorithms, and then click **Calculate**.

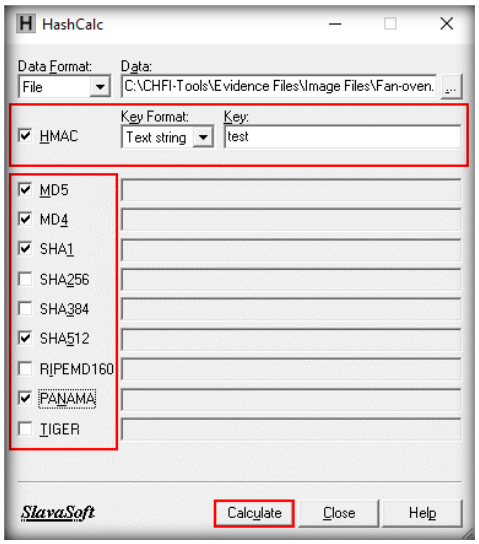

FIGURE 2.10: Calculating HMAC with Key

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.

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

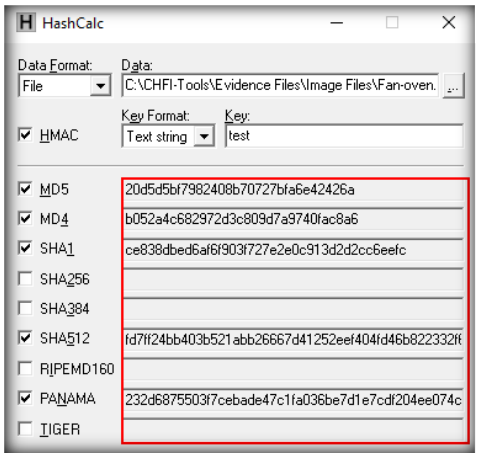

FIGURE 2.11: Window Displaying Hash Values

13. Both the windows, containing MD5 hash values - one generated using **HMAC** and the other **without** using **HMAC**, respectively are shown below for students' understanding:

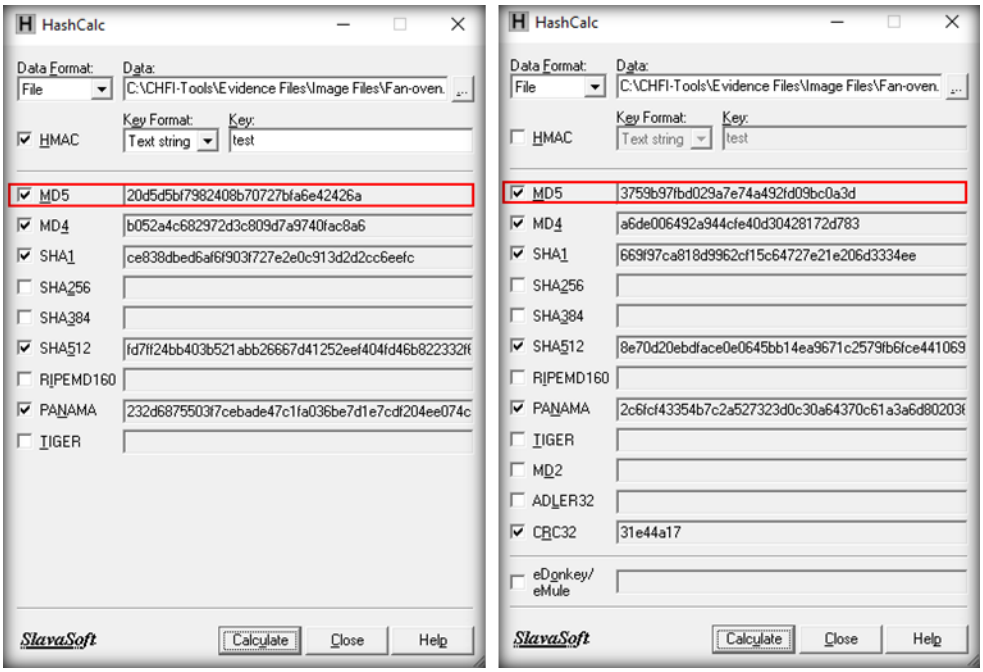

FIGURE 2.12: Windows Displaying MD5 Hash Value Using HMAC and Without HMAC

14. If you want to perform a calculation for a text string, first select **Text string** from the **Data Format** drop-down list, uncheck **HMAC** box and then enter the text in the **Data** field.

TASK 5

Calculating Hex Value of Text String

15. Select the algorithms you want to use for calculations by checking the required algorithms and then click the **Calculate** button.

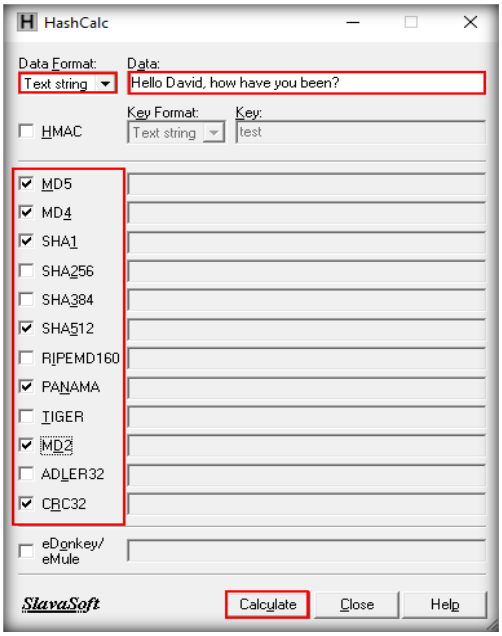

FIGURE 2.13: Calculating Hash Values for Given Text

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

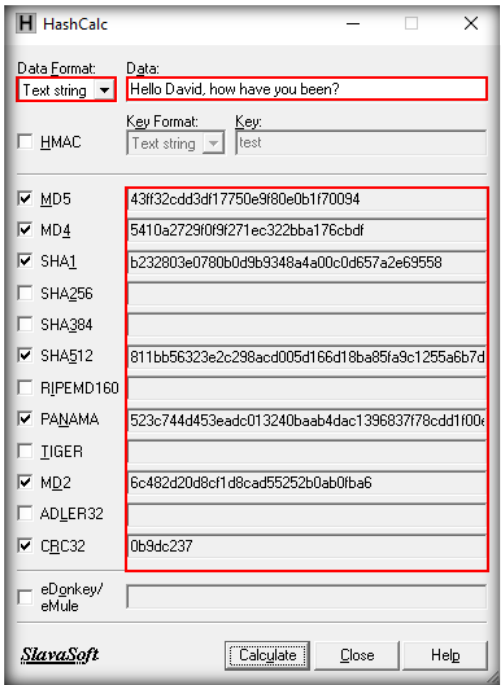

FIGURE 2.14: Display of Encoded Data in HashCalc

TASK 6

Search a File's Hash Value on VirusTotal

17. Next, we shall calculate the MD5 hash value of an infected/malicious pdf and search this hash value in the **VirusTotal** database to see whether the file is safe to access or malicious.
18. In this lab, we shall be testing a file named **Infected.pdf** located in the **Evidence Files** folder.
19. 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.

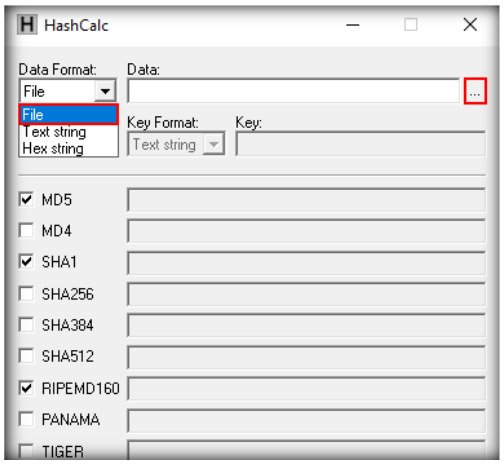

FIGURE 2.15: HashCalc Data Format Options

20. **Find** window will appear; navigate to **C:\CHFI-Tools\Evidence Files**, select **Infected.pdf** and click **Open**.

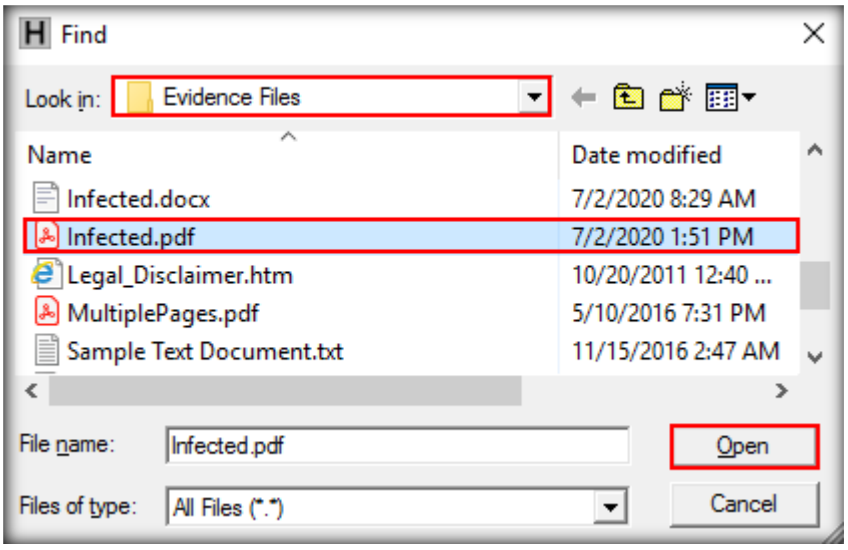

FIGURE 2.16: Selecting Evidence File in D Drive

21. The selected file will be displayed in the **Data** field; click **Calculate** to calculate the hash value of the file.

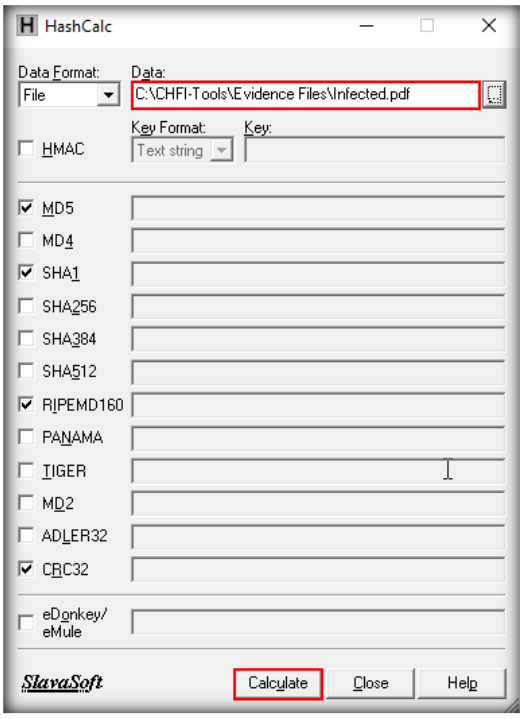

FIGURE 2.17: HashCalc Window

TASK 7

Selecting Algorithms

22. Since **MD5 algorithm** is already selected, HashCalc calculates the MD5 value followed by the other hashes (that were selected) of the file. **Copy** the MD5 hash value as shown in the following screenshot:

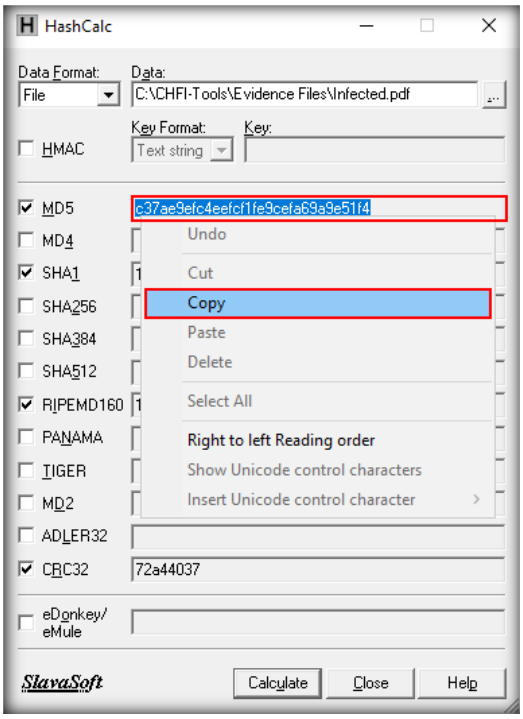

FIGURE 2.18: Calculation of Hash Values

23. Now, launch **Firefox** web browser and browse the URL https://www.VirusTotal.com/gui/home/search. The **VirusTotal** Search page will appear as shown in the screenshot below:

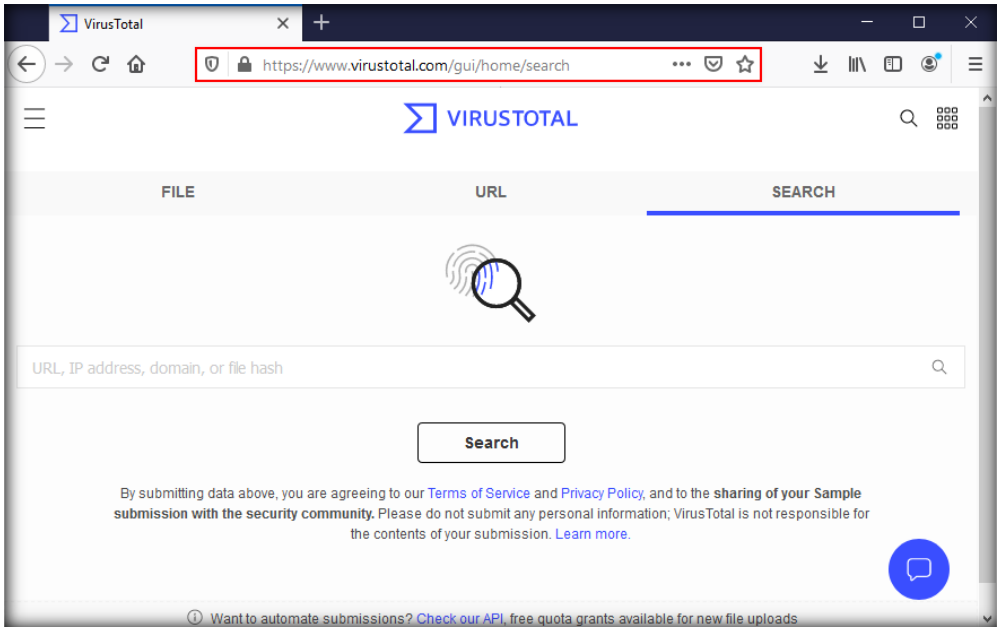

FIGURE 2.19: Browse VirusTotal Search Page

24. Paste the **MD5** hash in the **Search** field and click **Search**.

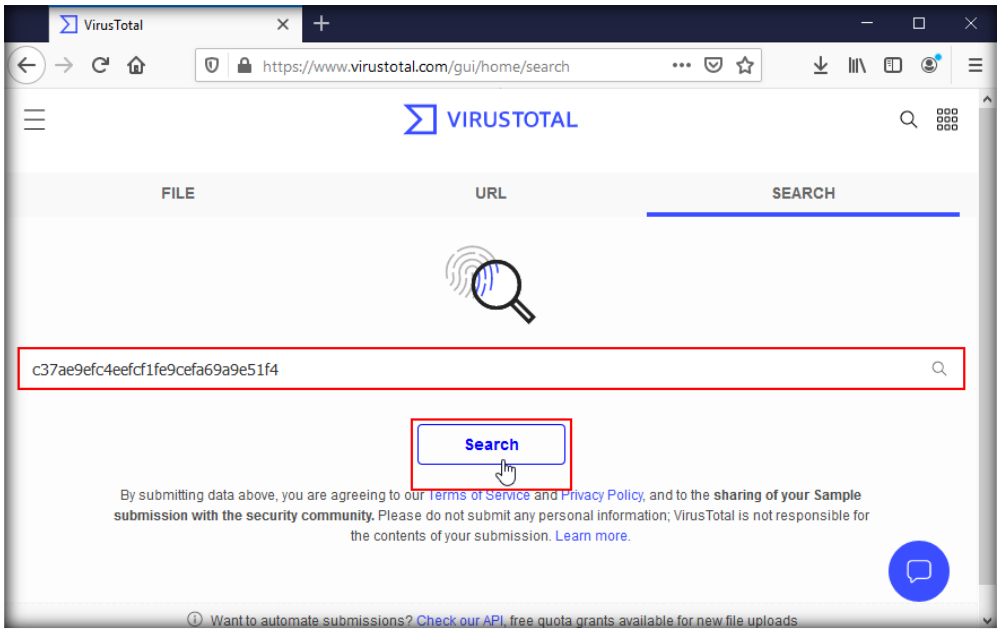

FIGURE 2.20: Paste the MD5 hash in the Search Bar

25. **VirusTotal** searches this value in its database and returns the result as shown in the following screenshot:

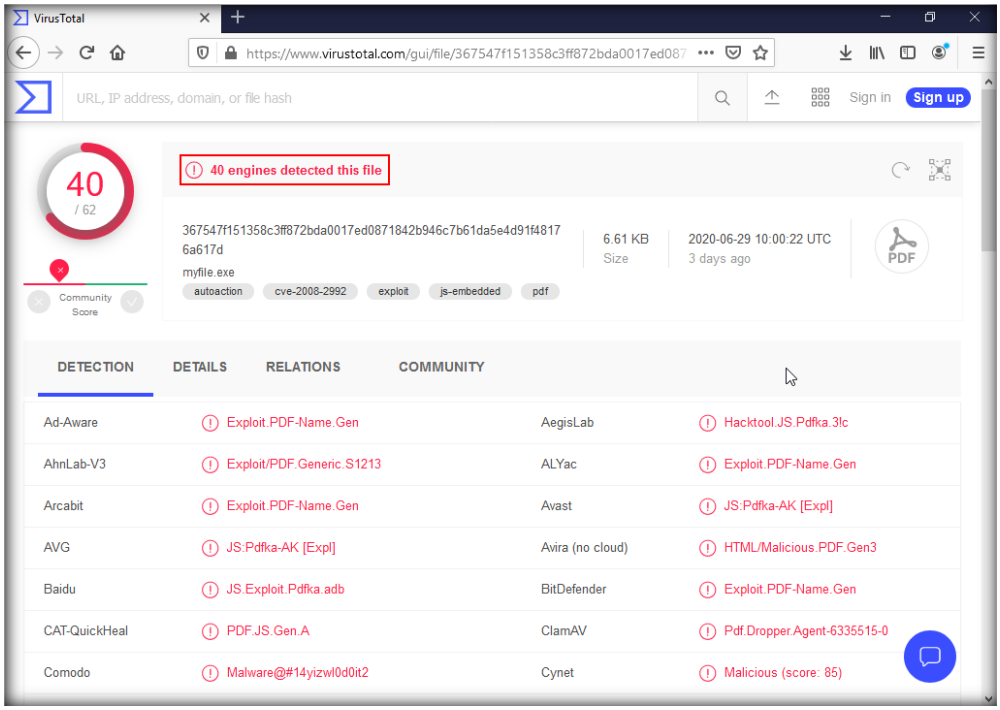

FIGURE 2.21: Suspicious Files are Detected by VirusTotal

Note: The number of anti-virus engines and detection rate might vary in your lab environment.

26. The result indicates that many anti-virus engines detected the file as malicious. In real-time, when a file appears to be suspicious, you may upload the file or its hash value in malware scanning applications like VirusTotal to know if the file is malicious. We will be covering malicious pdf analysis in detail in **CHFIv10 Module 14 Malware Forensics**.
27. This way, you can calculate the MD5 hashes of files and text strings and look up for the hash values of suspicious files in online malware scanners.

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.

Lab

3

Comparing Hash Values of Files to Check their Integrity

Hashing is performed on data such as files or text to generate unique fixed-length strings called hashes or checksum. Using hashes, one can determine the integrity of the given data.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

During an investigative process, a forensics examiner has to check the integrity of copies of several files that contained sensitive data of an organization. For this, he/she must calculate the hash values of the copies that are suspected to have been modified and compare them with the hash values of the original files that store the organization's confidential data. Essentially, the investigator needs to compare the hashes of the suspect files with their pre-existing hashes to check whether the integrity of files is preserved. What tool should the investigator use to compute and compare the hashes?

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

Lab Objectives

This objective of this lab is help you learn how to:

- Generate the MD5 hash value of selected files using MD5 Calculator
- Compare the generated hash values of files with their pre-existing hash values to determine the integrity of files

Lab Environment

This lab requires:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute the commands
- A web browser with internet access

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process.

- **MD5 Calculator** installer located at **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\MD5 Calculator**

Note: You can download the latest version of **MD5 Calculator** from the link https://www.bullzip.com/download.php

If you are using the latest version of software for this lab, then the steps and screenshots demonstrated in the lab might differ.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 10 minutes

Overview of the Lab

In this lab, you will be calculating the hashes of the files and comparing them with the hashes stored in the repository (i.e., Evidence Files\Image Files\Hashes.txt).

Lab Tasks

TASK 1

Calculating Hash Values

1. Log in to **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Hash Value Calculator Tools\MD5 Calculator**.
3. Double-click **md5calc(1.0.0.0).msi** to launch the setup, and follow the wizard-driven instructions to install the application.

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

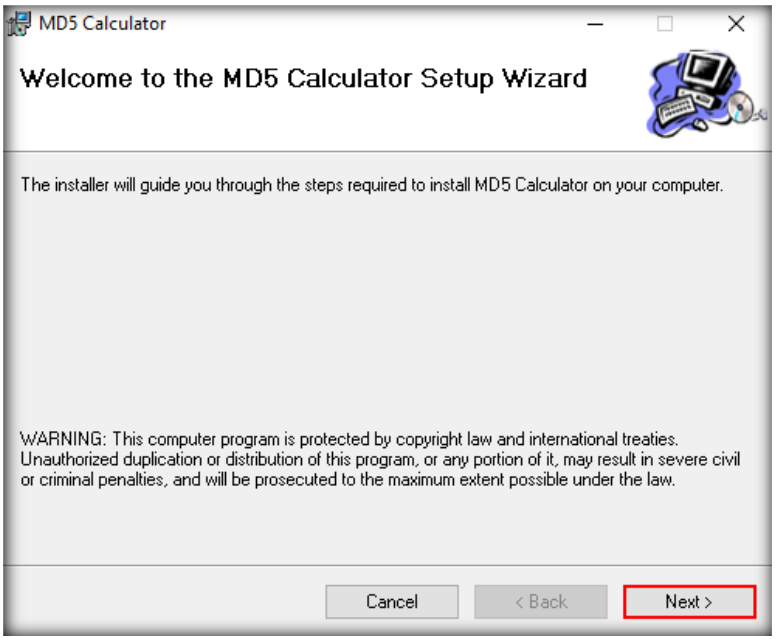

FIGURE 3.1: MD5 Calculator Setup Wizard

The Message-Digest Algorithm 5 (MD5) was created by a professor named Ronald L. Rivets of MIT. Using this algorithm, you can 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 character string of 32 hex digits.

4. Upon completing the installation, click **Close** to exit the installation wizard.

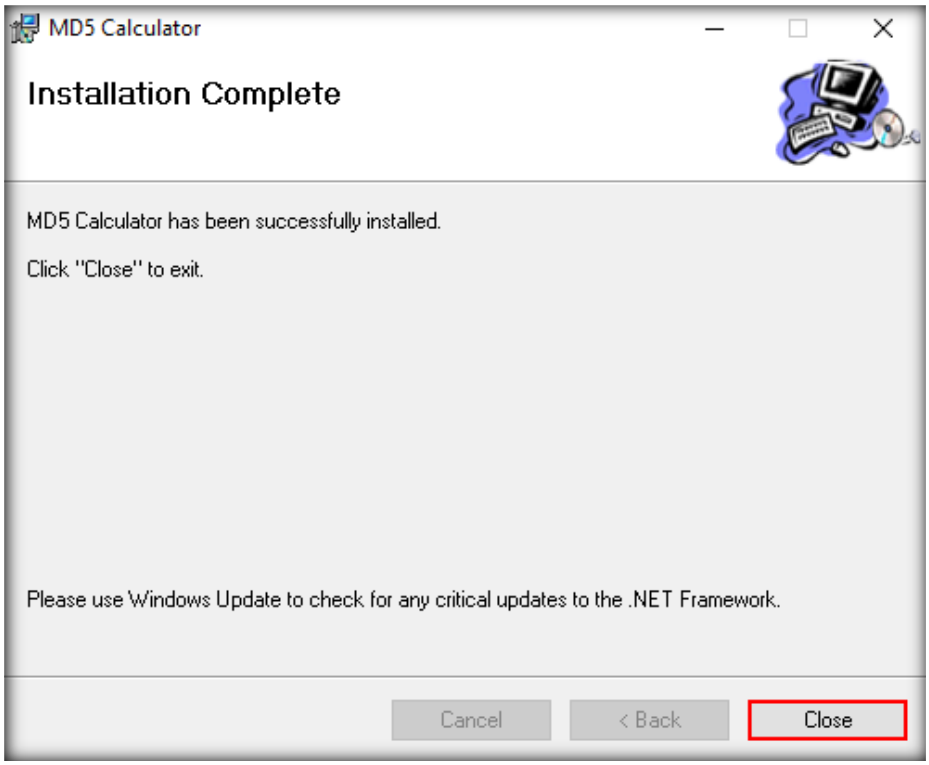

FIGURE 3.2: Installation Complete; Click Close to Exit

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

You can compare the calculated MD5 value to a value given to you by another person or from a website.

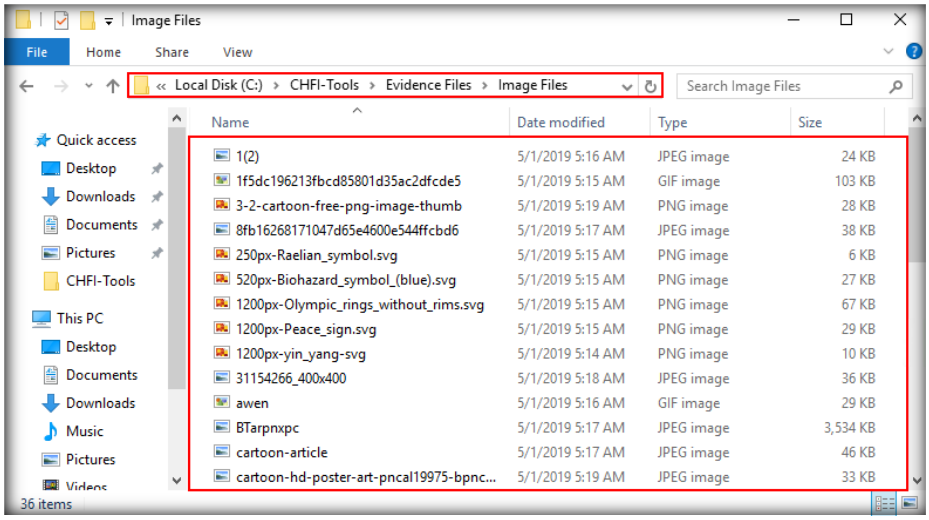

FIGURE 3.3: Evidence File

6. To calculate the MD5 hash of a file, first select a file, right-click on it and then select **MD5 Calculator** from the context menu. Here, we are selecting the image file **cartoon-article.jpg** for calculation of its MD5 hash value:

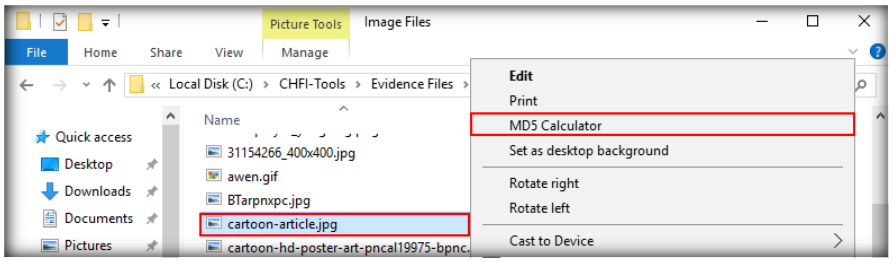

FIGURE 3.4: MD5 Calculator

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

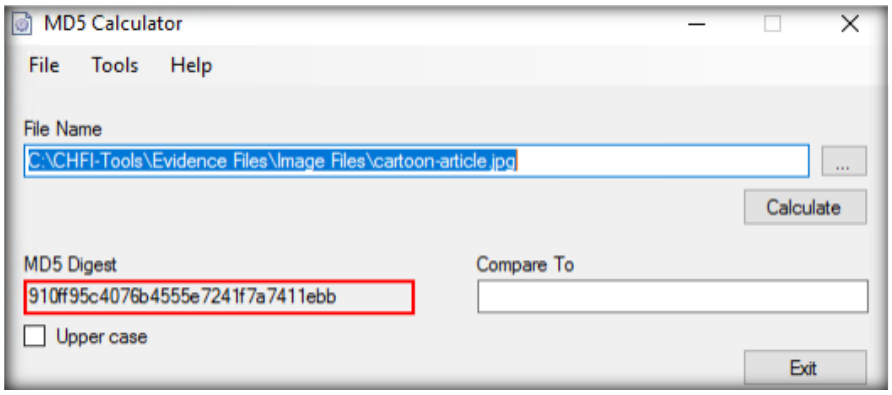

FIGURE 3.5: Displayed Hash Value in MD5 Calculator

8. On checking the MD5 digest, close the tool.

TASK 2

Comparing Hash Values

9. If you want to compare the hash value of a file, enter the pre-existing hash value of that file under the **Compare To** section and calculate the file's hash. In this lab, we shall compare hash values of multiple files to see if their generated hash values match with the pre-existing hash values.

10. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** and open **Hashes.txt**. This file contains hashes of some of the image files located in **C:\CHFI-Tools\Evidence Files\Image Files**.

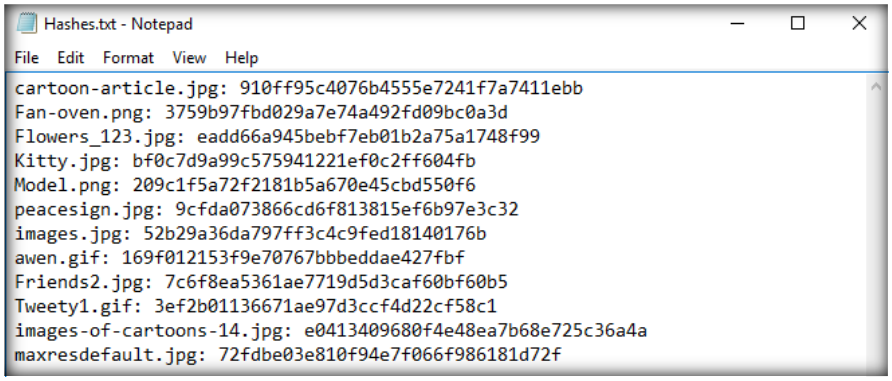

FIGURE 3.6: Hashes.txt File

11. In this lab, we will be comparing hashes of two files, **Kitty.jpg** and **Model.png**.
12. To compare the hashes of **Kitty.jpg**, copy the hashes corresponding to the file.

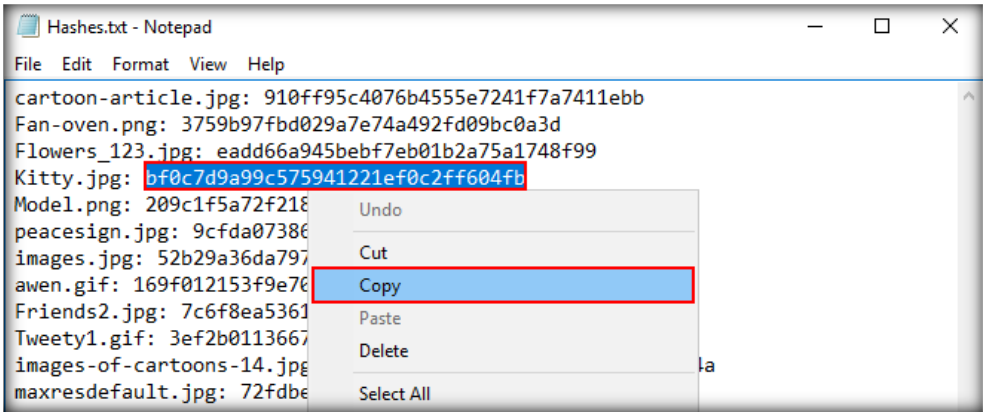

FIGURE 3.7: Copy the Hash Value of Specified File

13. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files**, right-click on **Kitty.jpg** and then select **MD5 Calculator** from the context menu.

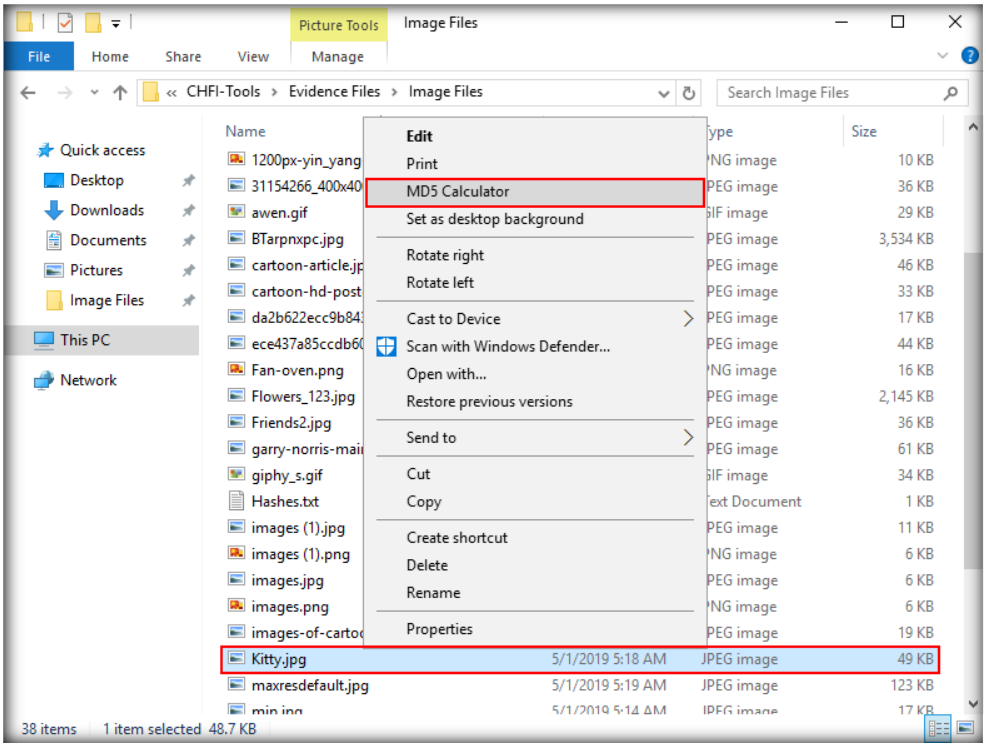

FIGURE 3.8: Select MD5 Calculator

14. **MD5 Calculator** displays the **MD5 Digest** (hash value) for the selected file. Now paste the hash value that you copied in **Step 12** into the **Compare To** section.

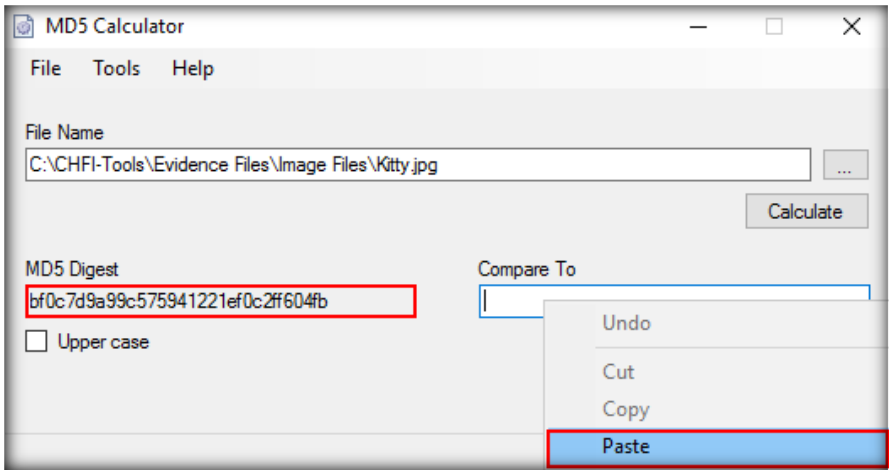

FIGURE 3.9: Paste the Hash Value

15. MD5 Calculator instantly compares both the hashes. If the hashes are equal, as shown in the following screenshot, the file's integrity is intact.

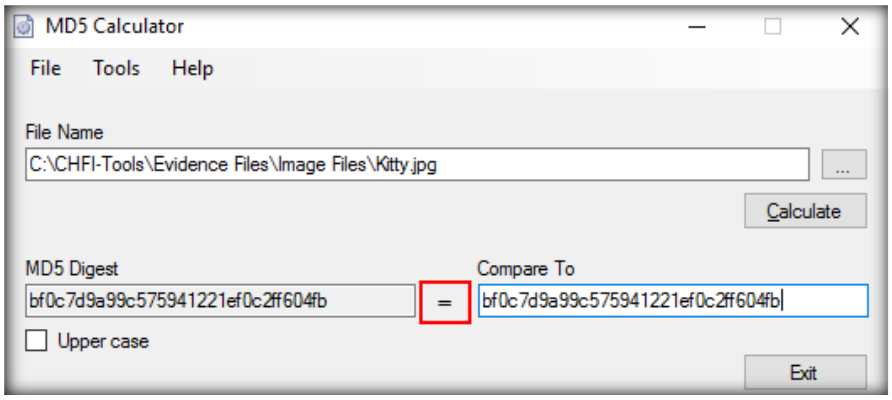

FIGURE 3.10: Compare the Hashes

16. Our next task would be to compare the hashes of the file **Model.png**.

17. To compare the hashes of **Model.png**, copy the hashes corresponding to the file from **C:\CHFI-Tools\Evidence Files\Image Files\Hashes.txt**.

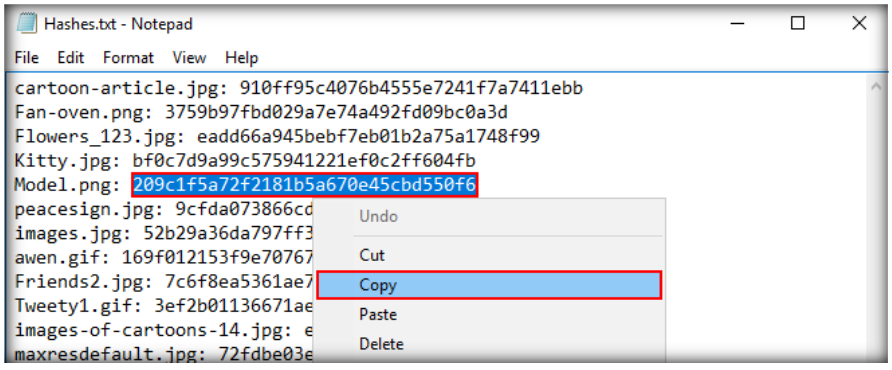

FIGURE 3.11: Copy Hash Value of Specified File

18. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files**, right-click on **Model.png** and then select **MD5 Calculator** from the context menu.

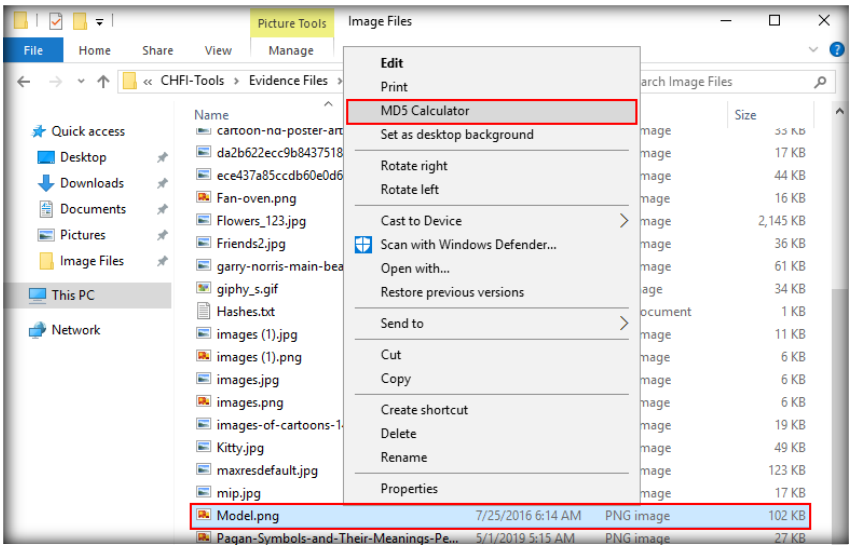

FIGURE 3.12: Select MD5 Calculator

19. **MD5 Calculator** displays the **MD5 Digest** (hash value) for the selected file. Now paste the hash value that you copied in **Step 17** into the **Compare To** section.

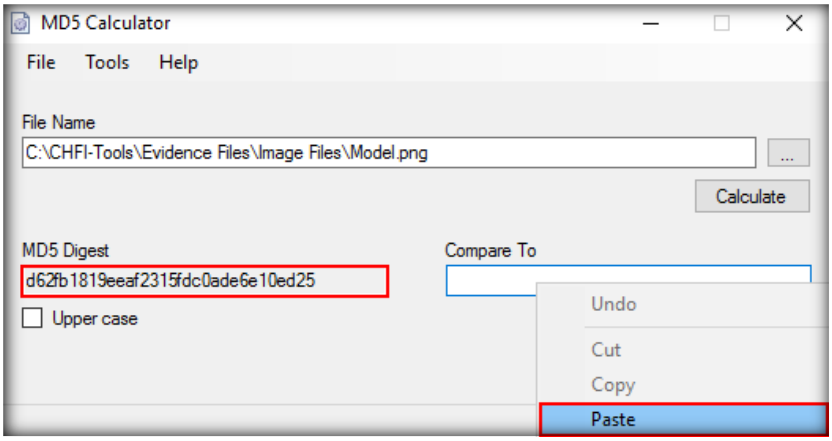

FIGURE 3.13: Paste the Hash Value

20. MD5 Calculator instantly compares both the hashes and shows that the hashes do not match, as shown in the following screenshot:

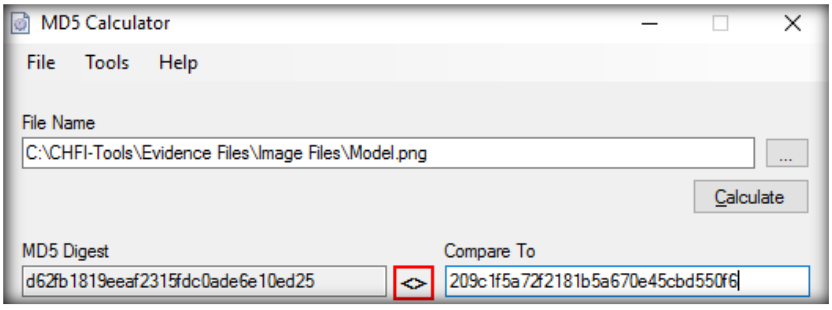

FIGURE 3.14: Compare the Hash Value

21. If the hashes do not match, the file's integrity is under question and it needs to be further investigated. The file might have possibly been modified to act as a payload for an attack (or) to hide data inside it, etc.
22. Investigation of this file Model.png is covered in **CHFIv10 Module 05 Defeating Anti-forensics Techniques** labs.
23. This way, you can check the file hashes using MD5 Calculator, and compare the hashes to verify the file/files' integrity.

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.

Lab

4

Viewing Files of Various Formats

A file format is a layout of a file that tells a program how to display its contents. Some of the common file formats are .doc, .gif, .jpg, .png, .mp3, .pdf, .txt, etc.

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 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.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process

This lab requires:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to install and run tools
- **File Viewer** installer located at **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\File Viewer**

Note: 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.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 15 minutes

Overview of the Lab

In this lab, you will learn how to examine files of various formats using File Viewer and understand if they need further investigation.

Lab Tasks

TASK 1

Launching File Viewer

1. Log in to **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv10 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**.

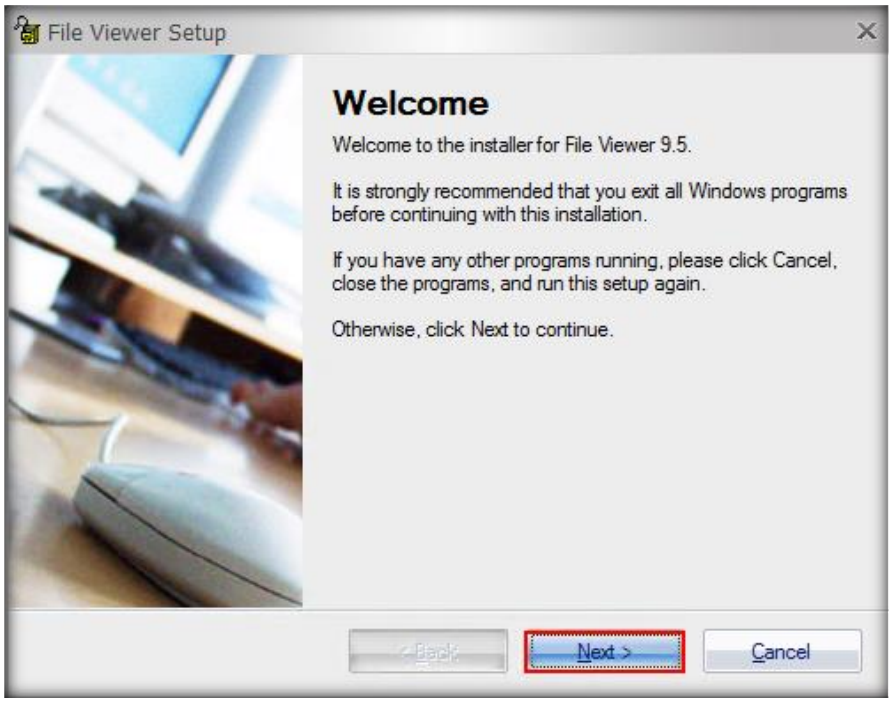

FIGURE 4.1: File Viewer Installer

Note: If a **User Information** section appears, provide details in the **Name** and **Company** fields and click **Next** to continue.

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

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.

3. On completing the installation, click **Finish**.

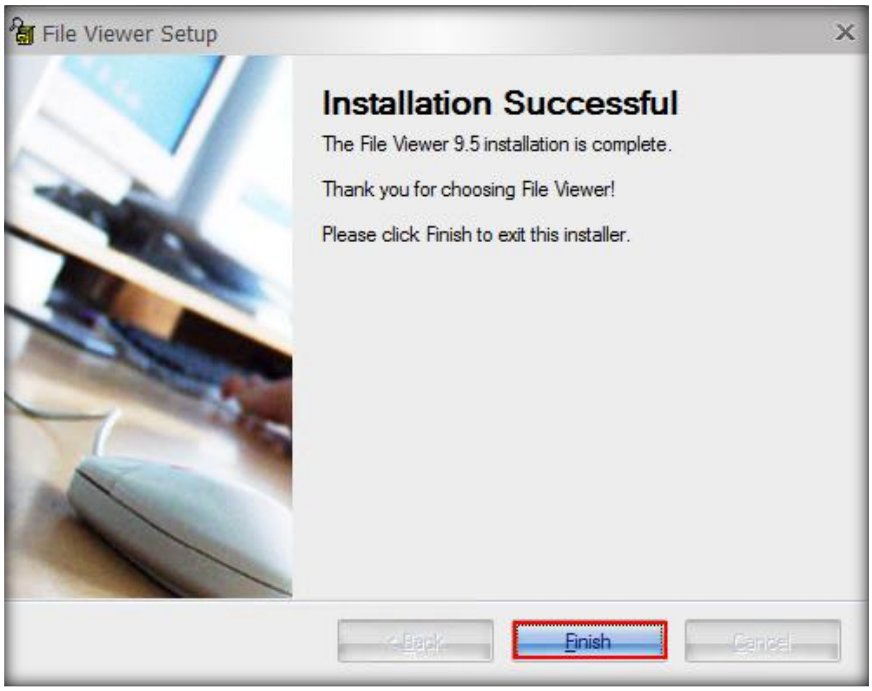

FIGURE 4.2: Installation Successful

4. Double-click **File Viewer 9.5** icon on the **Desktop** to launch the application.
5. The **File Viewer Registration** pop-up appears. Click the **Close** button to open the **File Viewer** window.

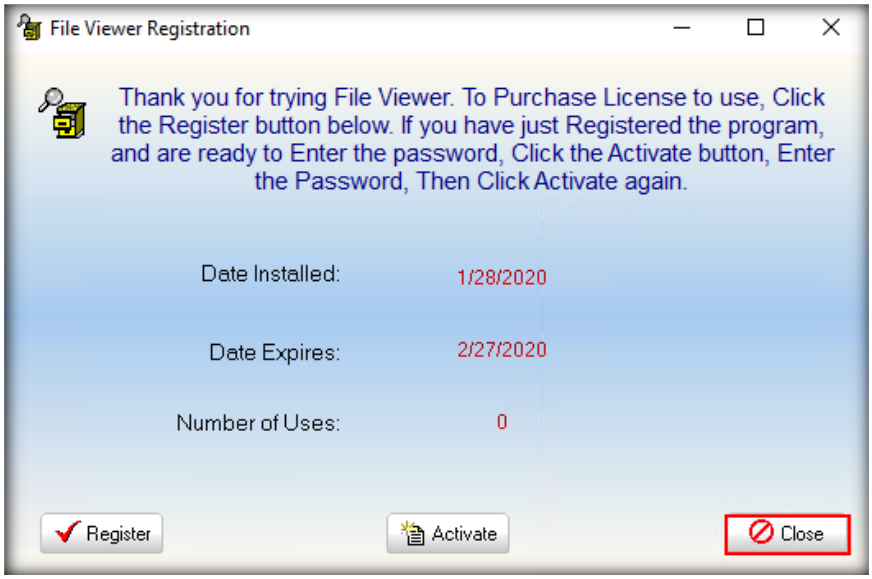

FIGURE 4.3: File Viewer Registration

6. The **File Viewer** main window will appear, along with a **Getting Started with File Viewer** dialog box. Check the **Do Not Show on Start Up** option and click **Cancel**.

7. If the dialog box does not appear, skip to the next step.

FIGURE 4.4: Getting Started with File Viewer Dialog Box

You must have at least 128 MB of free 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.

TASK 2

Selecting the Evidence File

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

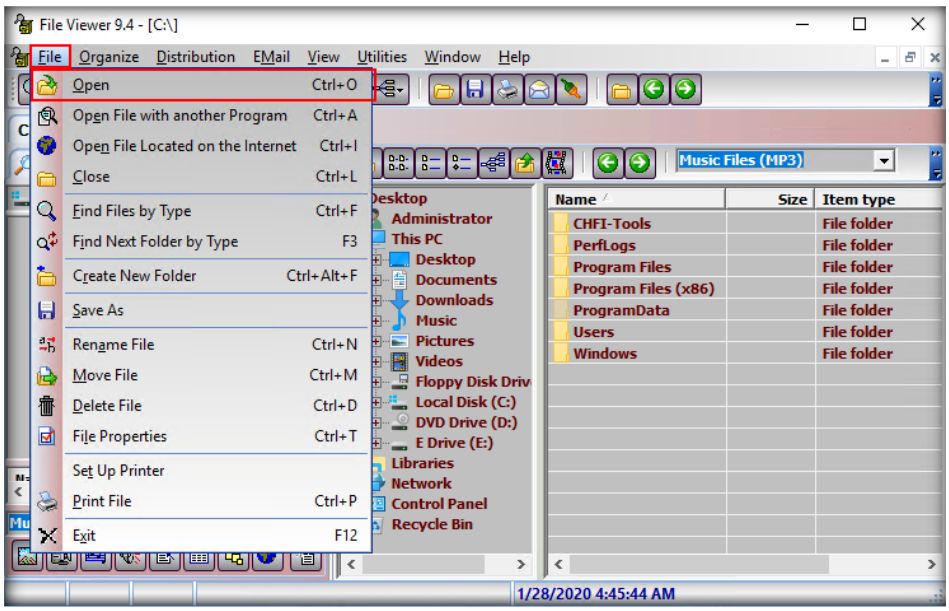

FIGURE 4.5: File Viewer File Menu

9. In the **Open** dialog box:
   a. Locate the evidence file path (**C:\CHFI-Tools\Evidence Files\Image Files**).
   b. Select **All files (*.*)** in the **File type** drop-down list.

c. Select the file **Friends2.jpg** and then click **Open**.

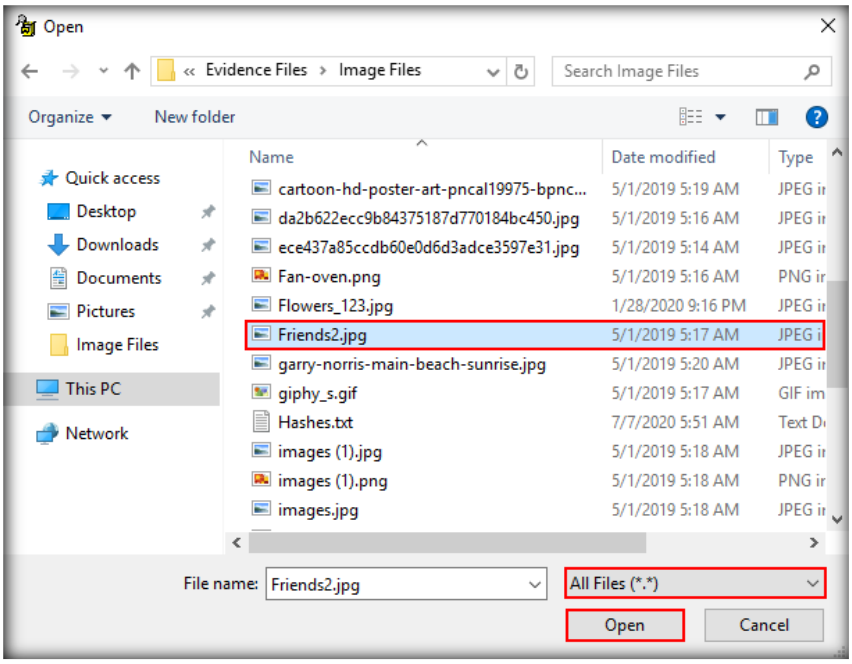

FIGURE 4.6: Opening of Evidence Files

10. If a **Getting Started with File Viewer** dialog box appears, click **Cancel**.
11. The image **Friends2.jpg** opens in the file viewer screen, as shown in the following screenshot:

FIGURE 4.7: Opening of Image File

📖 File viewer contains Microsoft's Multimedia player component, which can play video files (AVI, MPG, MOV) and music files (MP3, MIDI, and M3U). Separate playlists are included for the video and audio files.

TASK 3

Viewing the File Properties

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

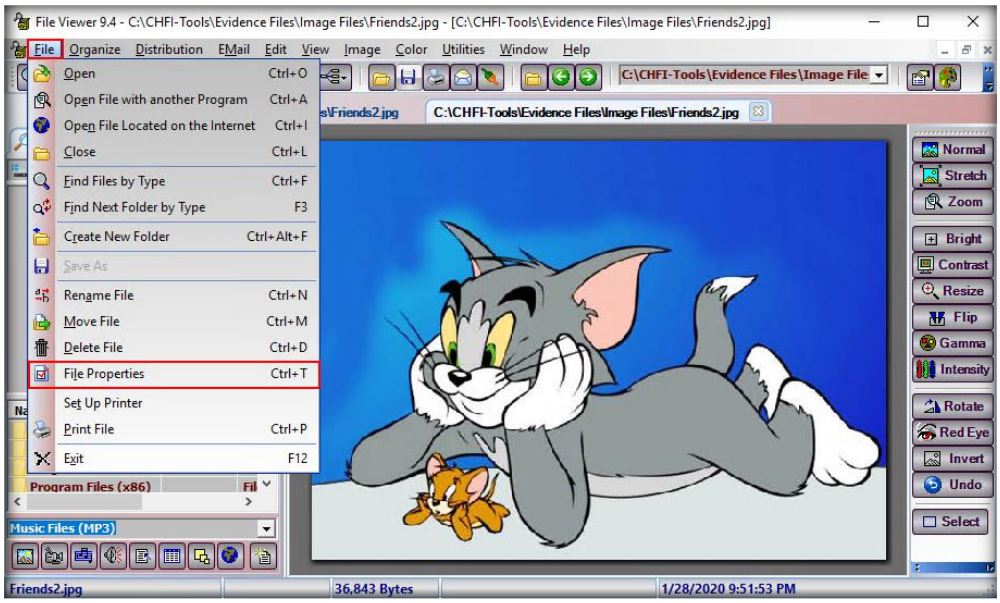

FIGURE 4.8: File Viewer File Properties Option

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

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

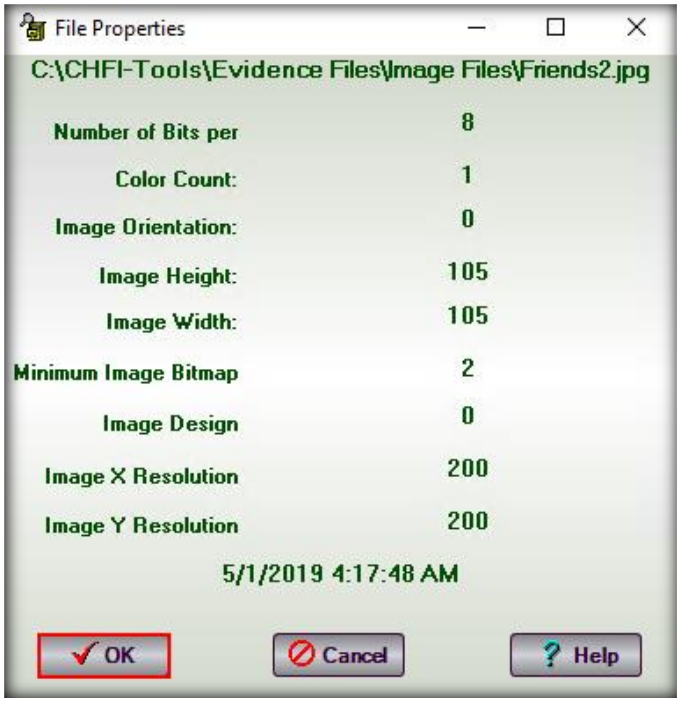

FIGURE 4.9: File Viewer File Properties Window

File Viewer provides a thumbnail window showing all the pictures in a selected folder.

14. Now, we shall open an mp4 (**520px-Biohazard_symbol_(blue).mp4**) file in the application.

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

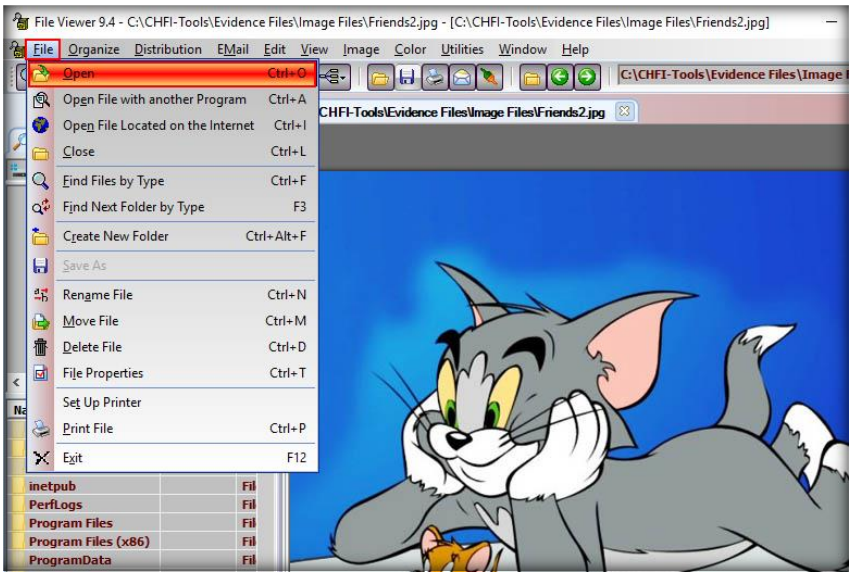

FIGURE 4.10: File Viewer File Menu

16. In the **Open** dialog box:
    a. Locate the evidence file path (**C:\CHFI-Tools\Evidence Files\Image Files**).
    b. Select **All files (*.*)** in the **File type** drop-down list.
    c. Select the file **520px-Biohazard_symbol_(blue).mp4** and then click **Open**.

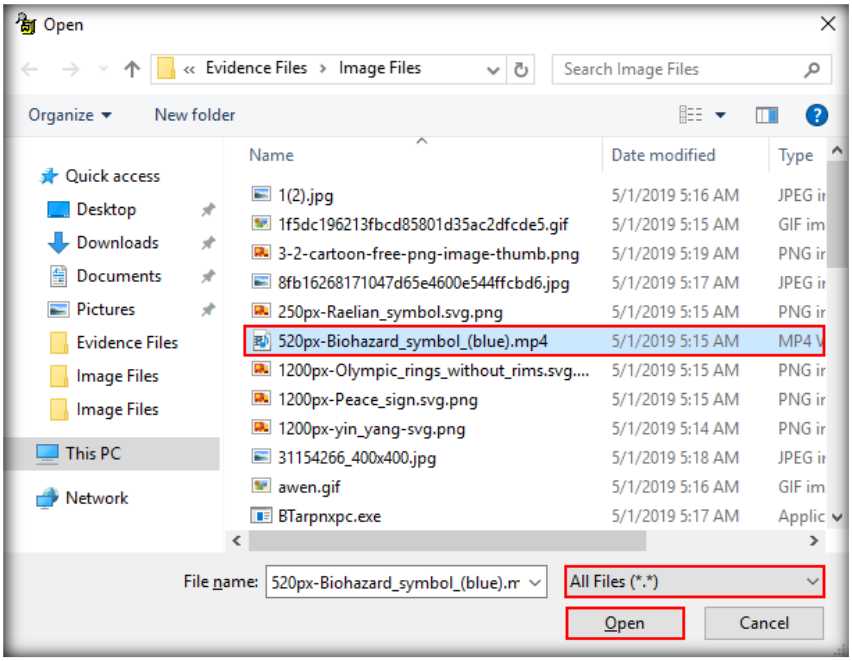

FIGURE 4.11: Opening of Evidence Files

17. If a **Getting Started with File Viewer** dialog box appears, click **Cancel**.

18. If a **File Viewer** pop-up appears stating **LTMM Error**, click **OK** to close the pop-up.
19. File Viewer will try to run the mp4 file but will fail to do so, as shown in the following screenshot:

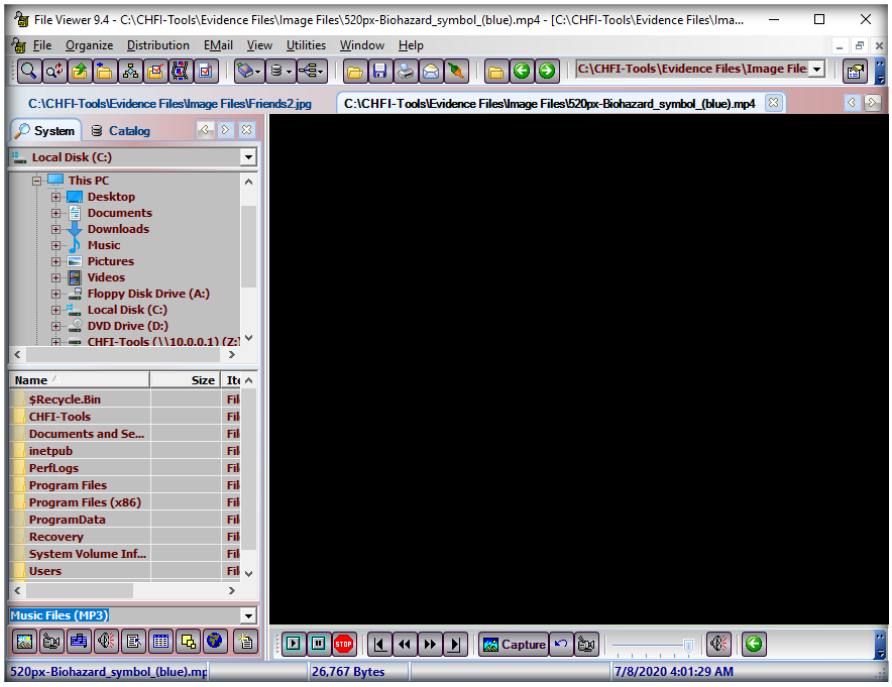

FIGURE 4.12: Opening of Image File

20. This happens when a file is either corrupt or its file extension is forcefully changed, resulting in a blank screen. Such files need to be further investigated.
21. Before investigating, you need to identify such files that are suspicious. Identification of such files and their original file formats is covered in **CHFIv10 Module 06 Windows Forensics**.

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

5

Handling Evidence Data

Forensic evidence is obtained via bit-by-bit copying of original media such as hard drive, USB drive, etc., found at the crime scene. It contains information such as files/folders, deleted data, etc., that can serve as a potential source of evidence during investigation.

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 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 Paraben's E3.

Lab Objectives

The objective of this lab is to help students learn and use Paraben's E3 Forensic Platform for handling evidence data.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process

This lab requires:

- A computer running a **Windows Server 2016 virtual machine**
- Administrative privileges to install and run tools
- A web browser with internet access

Note: You can download the latest version of **Paraben's E3: Universal** from the link https://paraben.com/dfir-tools-trial/

Explore the page https://paraben.com/e3-trial-sample-files/ on Paraben's official website for options and instructions on signing up for the Paraben's E3 trial setup.

If you download the latest version of Paraben's E3 and use it for examination, then the screenshots shown in this lab might differ.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 30 minutes

Overview of the Lab

In this lab, you will learn how to conduct forensic examination on an evidence file using Paraben's E3 Forensic Platform.

Lab Tasks

1. Log in to the **Windows Server 2016** virtual machine.

Note: Make sure that you have **active internet** connection throughout the lab.

Note: Make sure you sign up for trial version edition of E3 platform on https://paraben.com/dfir-tools-trial/, download the tool and communicate with the Paraben team in order to obtain license for activation.

TASK 1

Launch Paraben's E3

2. Double-click on the **Paraben installer** (here, we are using **Paraben_E3-x64_2.6.13017.17333.msi** installer) 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**.

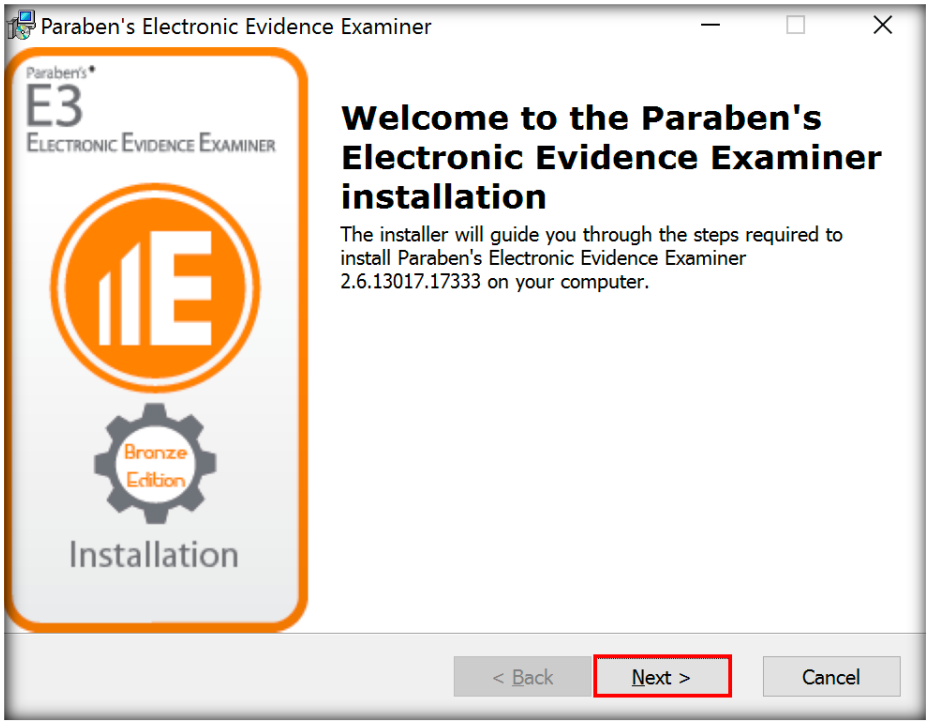

FIGURE 5.1: Paraben's E3 Welcome Window

3. At the end of the installation process, click **Finish** to exit the installation wizard.

Note: If a Paraben's Driver Pack download webpage opens in the default browser, close it.

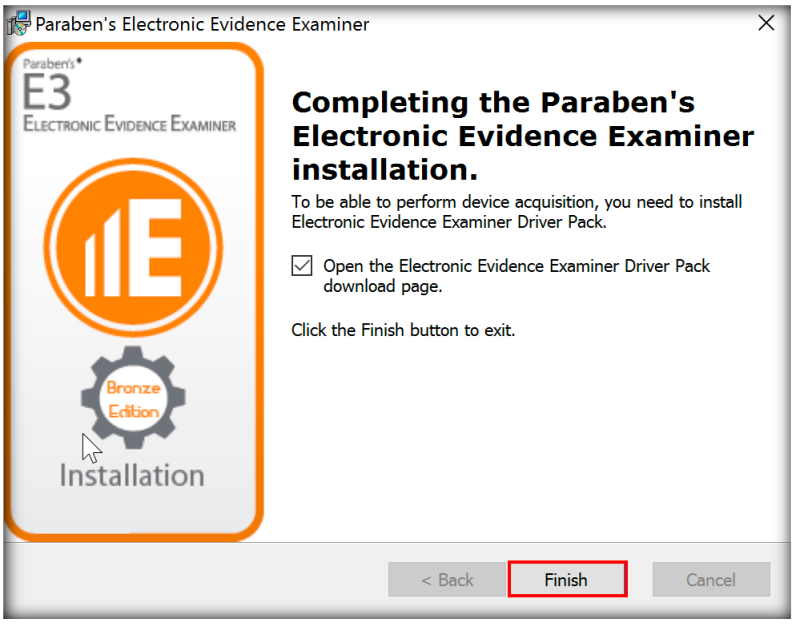

FIGURE 5.2: Paraben's Installation Finish Page

4. Double-click on the **Electronic Evidence Examiner** icon located on the desktop to launch the application. Alternatively, you can launch the application from the Apps screen.

Note: If the tool has been activated earlier, then you can skip directly to the step where we create a new case in the next task and get started with the lab exercise.

5. Upon launching the tool, the main window of **Paraben's E3** opens up along with a **Paraben's E3 pop-up**. **Close** the pop-up.

Note: If the **activation** window opens up, close it.

Note: If the tool opens up **Paraben's webpage** in the default browser, close it.

Note: If Paraben's **tutorial pop-up** appears along with the main window of E3 on launching the application, **close** the **tutorial menu pop-up**.

FIGURE 5.3: Main window of Paraben's E3

Note: Activation of the application as a **trial version** is highly recommended as the trial version offers full functionality of all the features of this tool, on par with its full, paid version. The **free version** of the tool offers only limited features and may not be suitable to run the lab.

6. To activate the trial version, go to **Case** in the menu bar and from the drop-down, **click** on **Activation.** Then **click** the option **Activate** as shown in the below screenshot.

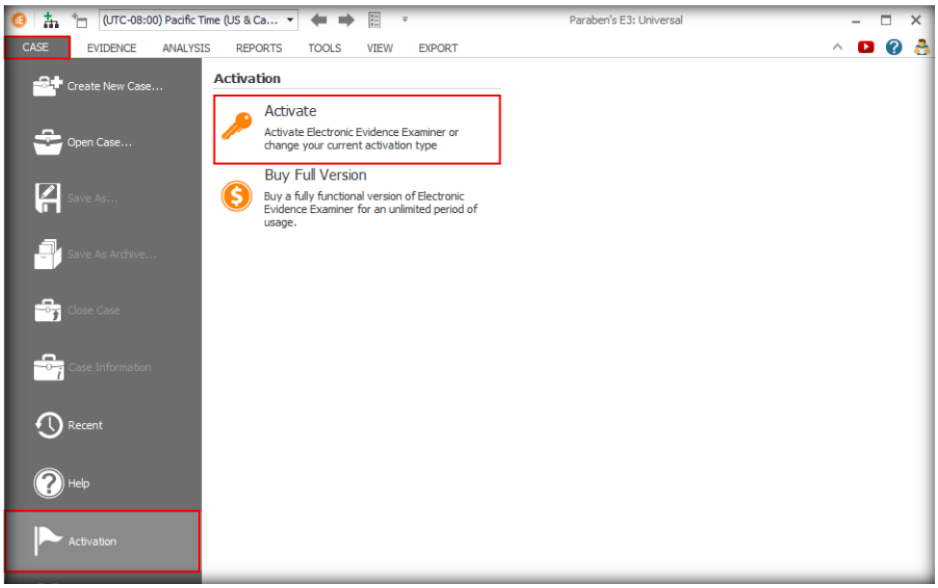

FIGURE 5.4: Paraben's E3 Activation Window

7. **Paraben's Electronic Evidence Examiner Activation** window appears listing the options for activation. Ensure that the option **Internet License** is selected and **click** on **Activate** button.

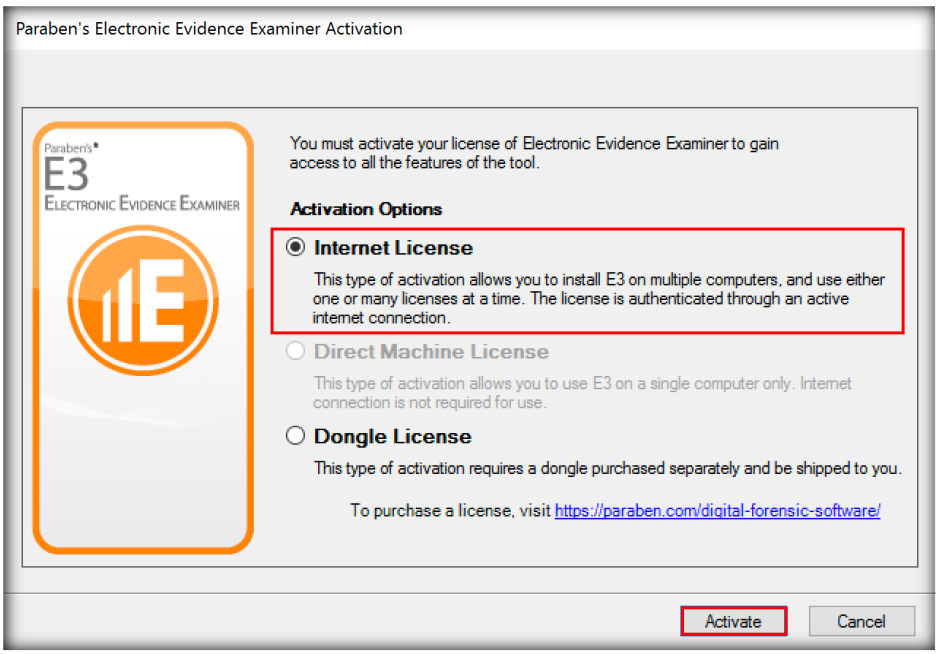

FIGURE 5.5: Paraben's E3 Activation Window

8. A **Registration** dialog box appears asking you to restart the application to finish the activation. Click **OK**. Close the application and restart it.

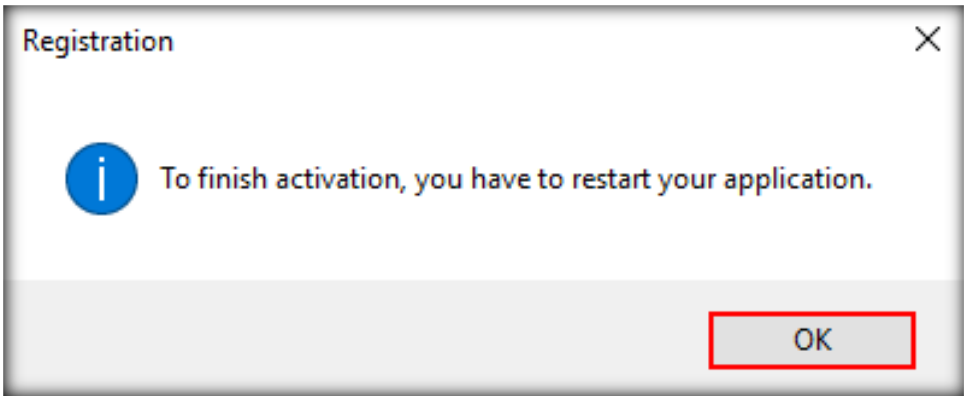

FIGURE 5.6: Registration Dialog Box

Note: The Paraben's E3 trial version is valid only for 7 days.

9. Next, **Connect to Web License Server** window opens up and asks for **user credentials** to connect to the web license server. Here, you must enter the **Login ID** (or email ID) and **Password** that has been used to **sign up/register** for the Paraben's E3 trial setup in order to access the trial version of the tool. Upon entering the credentials, click the **Connect** button.

FIGURE 5.7: Connect to Web License Server Window

10. The main window of the application opens up along with the **Paraben's E3 pop-up** that we saw upon launching the application for the very first time after completing its installation. **Close** the **pop-up**.

11. Go to **Case** on the menu bar and click **Help** to check whether the tool has been **activated**. In the right window pane, you can find information pertaining to Paraben's E3 **registration** along with **Registration key**.

Note: When the trial version of the application has been activated, you will also find that its name at the top of the window is **Paraben's E3: Universal** instead of **Paraben's E3: Free**, which will be seen only when using the free version of the tool.

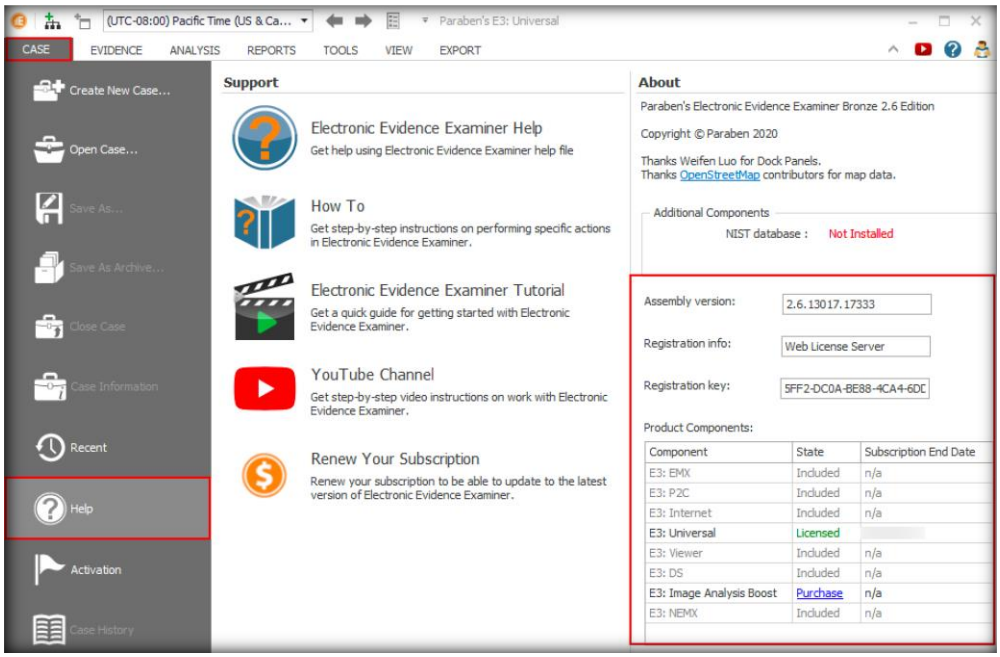

FIGURE 5.8: Registration Information of Paraben's E3

TASK 2

Create a New Case

12. Next, we will examine a forensically acquired digital evidence using the Paraben's E3 forensic platform. In order to examine a new evidence, go to **Case** on the menu bar and click **Create New Case**.

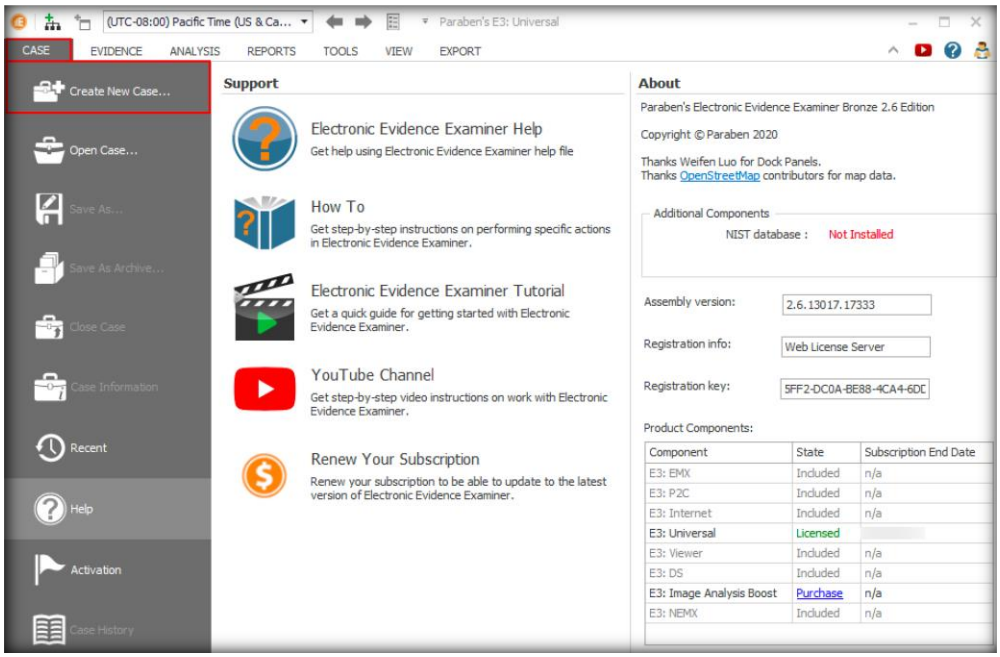

FIGURE 5.9: Creating New Case

13. A **New Case** window appears which displays the **Welcome** section. Click **Next** button.

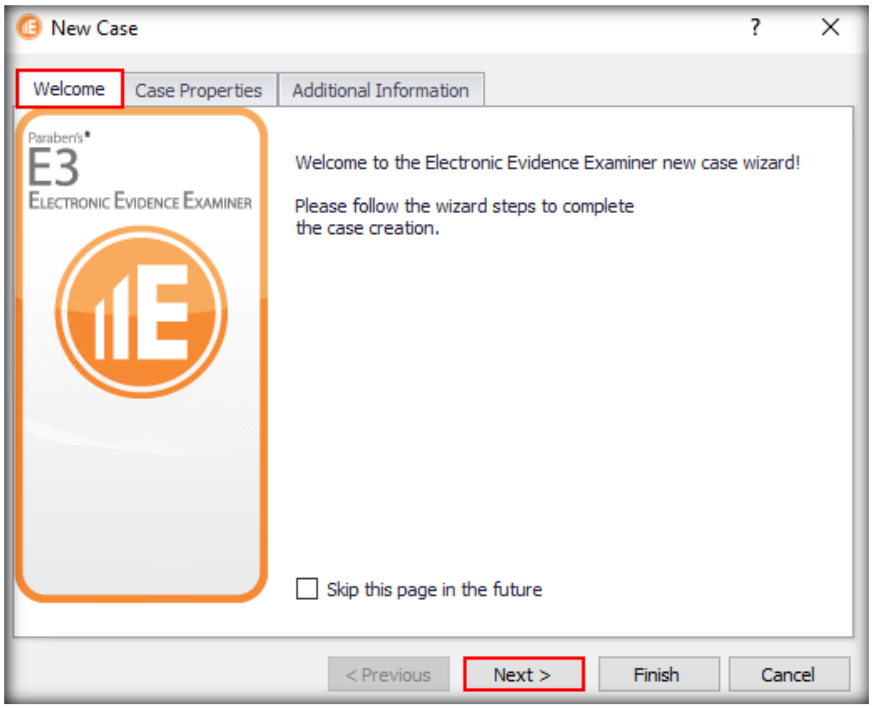

FIGURE 5.10: Welcome Section of New Case Window

14. In the **Case Properties** section, provide a **Case name** and case **Description** in the respective fields. You may enter these details according to your requirement. Click **Next**.

The Case Properties pane allows the user to view the properties of the selected case item.

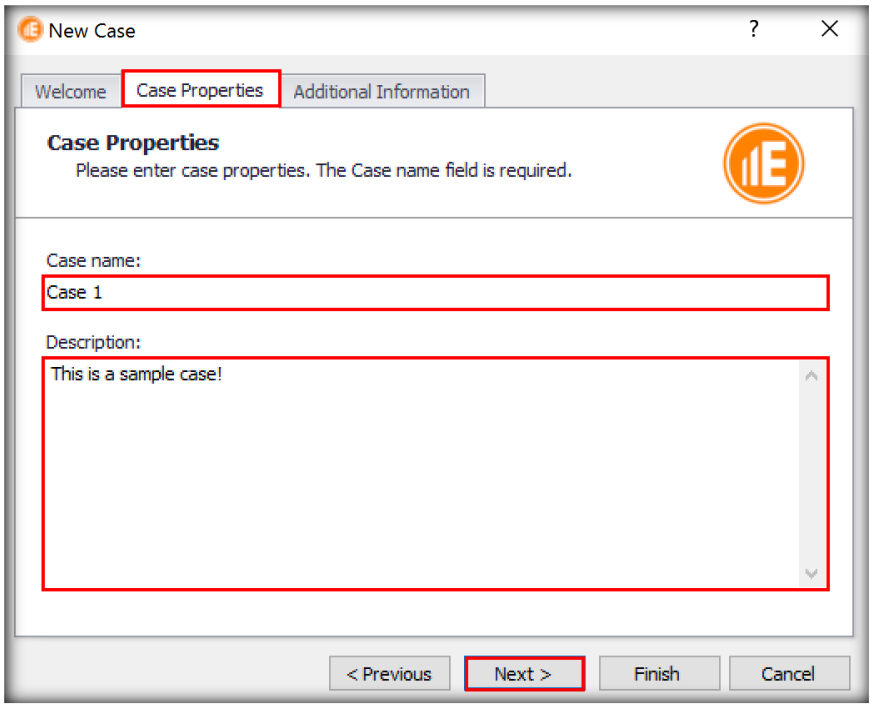

FIGURE 5.11: Case Properties Section

15. In the **Additional Information** section, enter additional information related to the investigator (you may also enter your details in this section) and click the **Finish** button.

Note: Additional information is not mandatory and can be filled any time through the **Properties** pane.

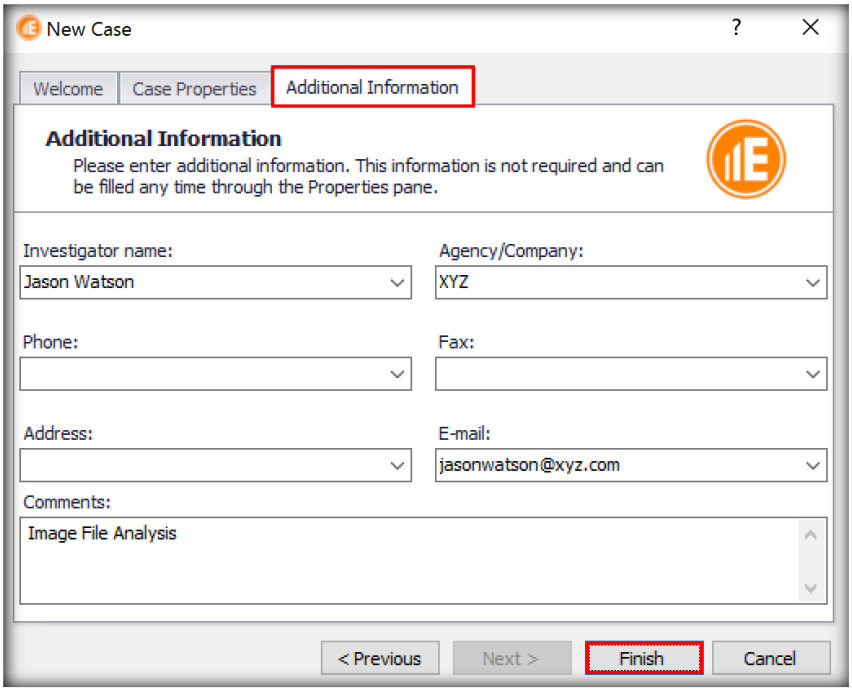

FIGURE 5.12: Additional Information Section

16. In the **New case creation** window that appears next, navigate to the **Desktop** and create a folder named **Reports**. Then, go into the **Reports** folder by ensuring that it is selected and clicking **Open**. Specify a file name for the case (here, it is **Case 1.e3**) in the **File Name** field and then click **Save**.

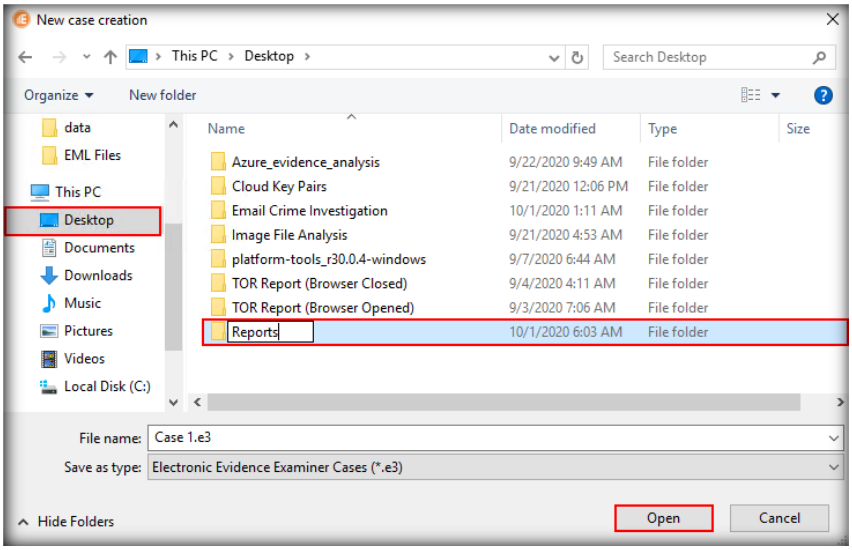

FIGURE 5.13: Create Reports Folder on Desktop and Open it

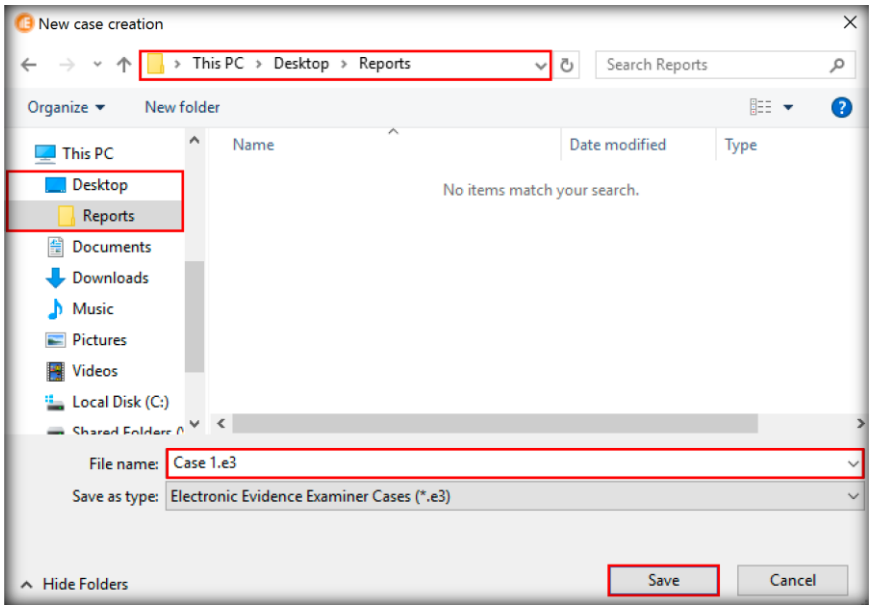

FIGURE 5.14: New Case Creation Window – Save the Case File in Reports Folder

TASK 3

Add Evidence File

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

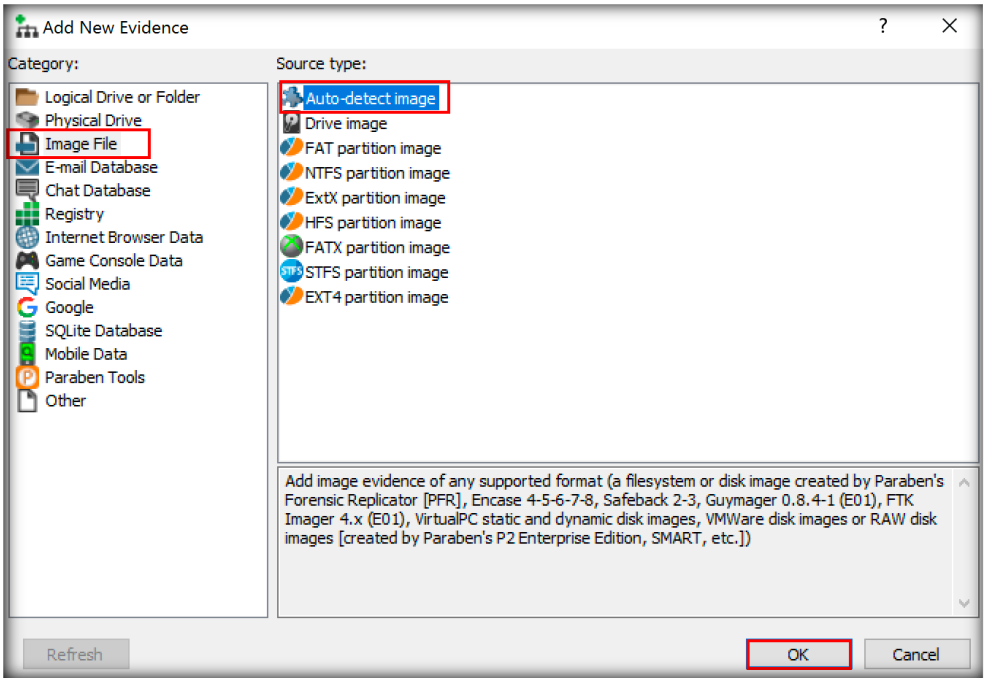

FIGURE 5.15: Add New Evidence Window

18. An **Open** window will appear; navigate to **C:\CHFI-Tools\Evidence Files\Forensic Images**, select **Windows_Evidence_001.dd** and click **Open** button.

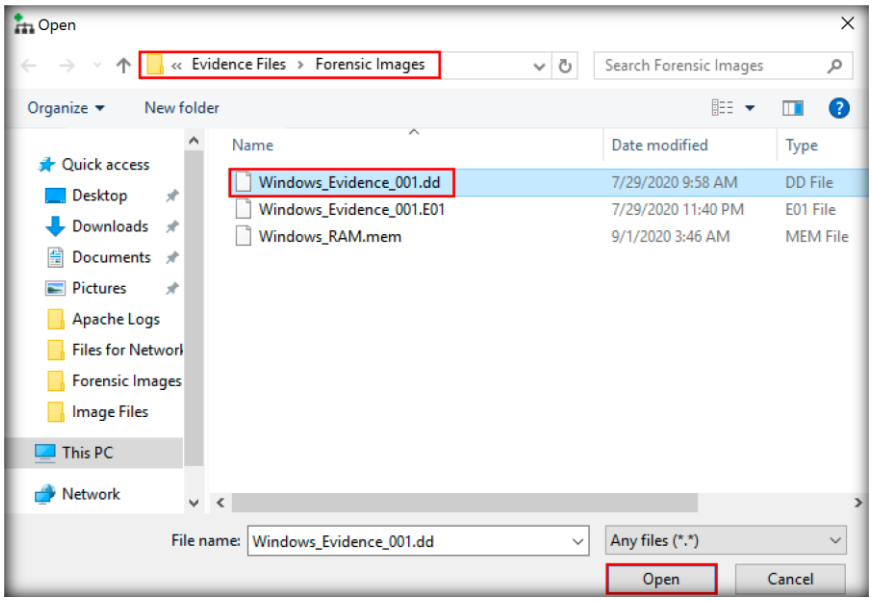

FIGURE 5.16: Selecting Image File for Examination

19. A pop-up appears where we can specify a new name for the evidence that we added. We will retain the default name (**Windows_Evidence_001**) for our evidence file. Click **OK**.

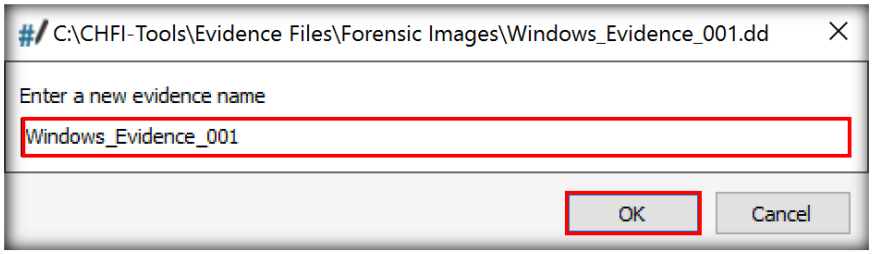

FIGURE 5.17: Specifying a Name for Evidence

20. An **NTFS Settings** window pops up. Check all the options specific to deleted data recovery and click **OK**.

Note: If the image file uses a **FAT file system**, then the below window will not pop up.

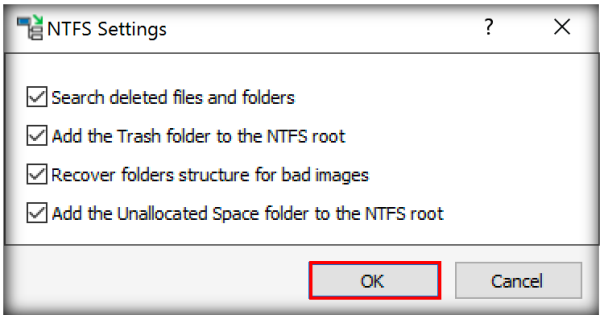

FIGURE 5.18: NTFS Settings Window

21. The selected image file is added to the case (**Case 1** file under the **Case Content** tab in the left pane of the application window).

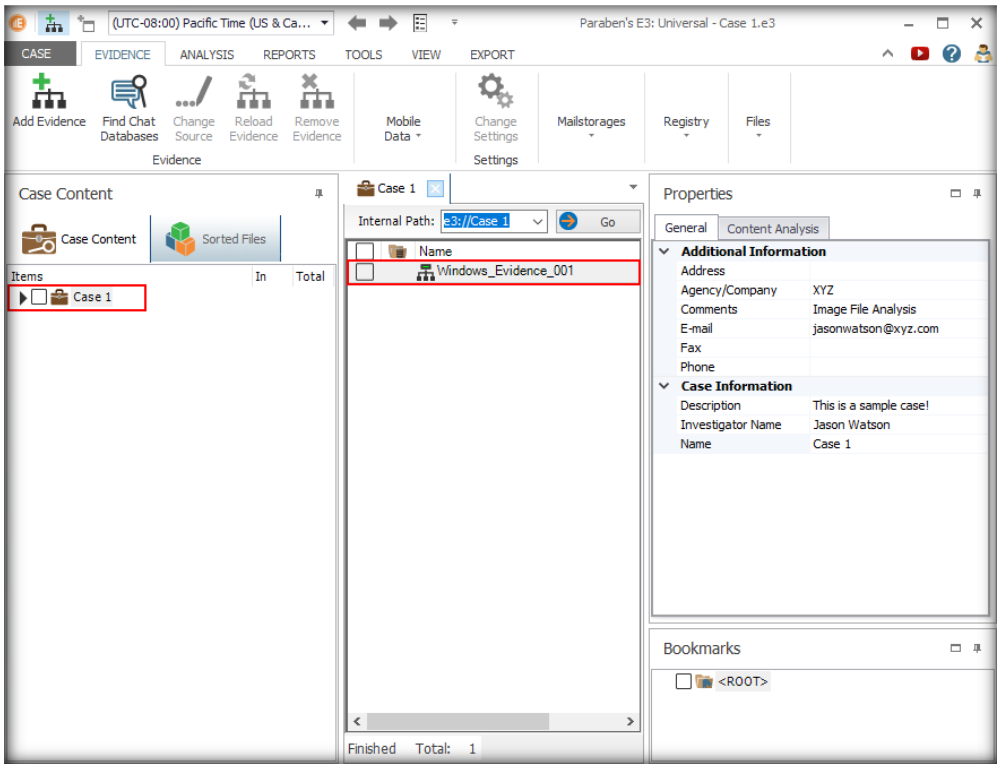

FIGURE 5.19: Image File Added to Case

22. Expand **Case 1 → Windows_Evidence_001 → NTFS → Root**. You will find the data pertaining to the evidence file.

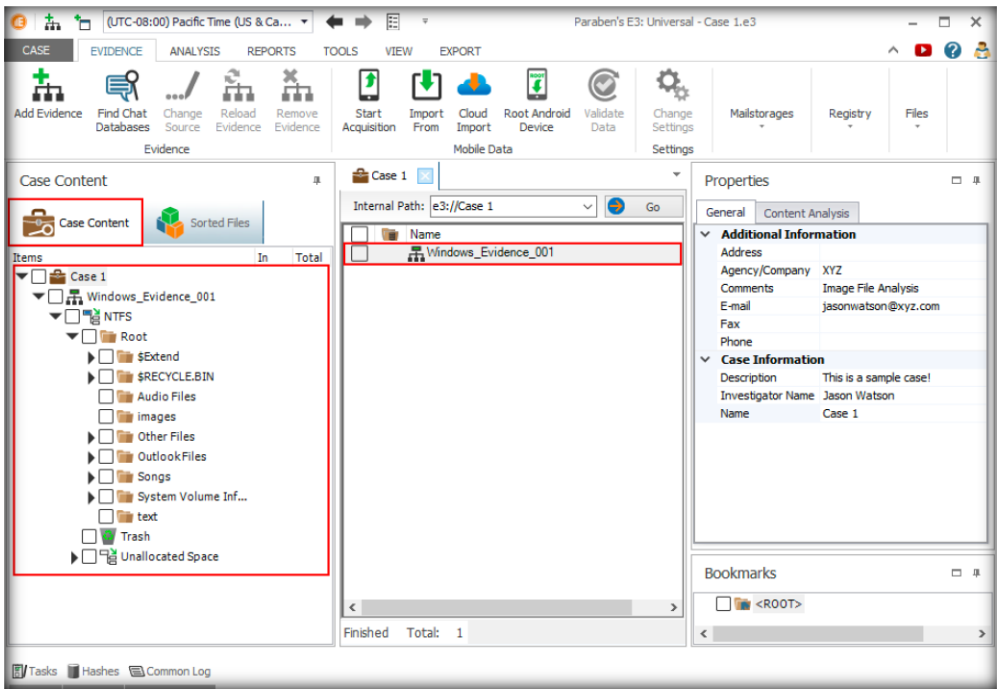

FIGURE 5.20: Evidence File Data

TASK 4

Retrieve Deleted Data from the Evidence

23. During forensic investigation, retrieving deleted data from the evidence image file is crucial. The information pertaining to the deleted data can be retrieved from the **Trash** folder. Click on the **Trash** folder to find deleted data.

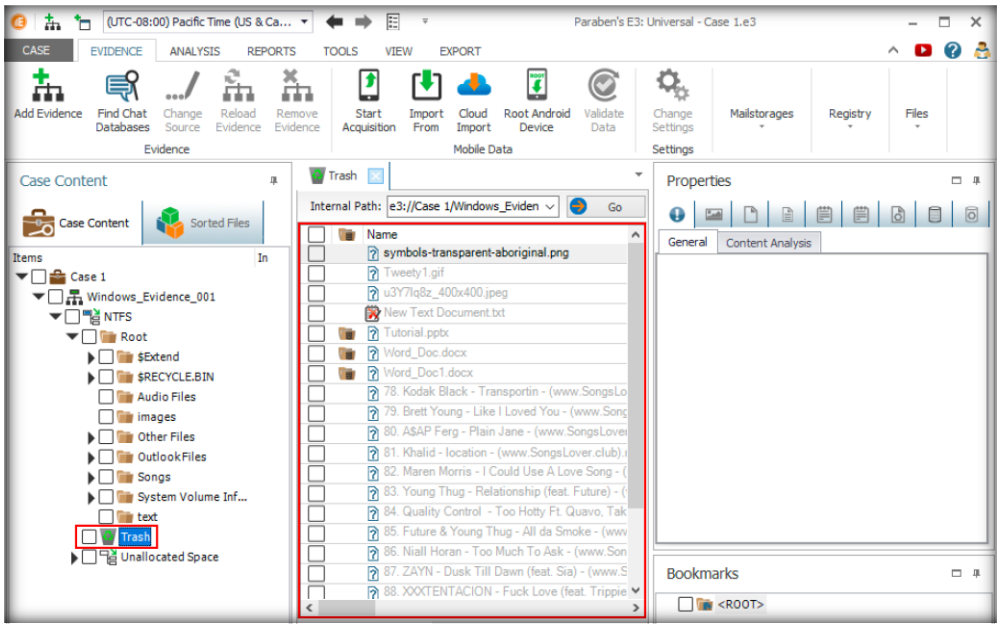

FIGURE 5.21: Deleted Files Data

24. To view the properties of a deleted file, select it. Its properties will then be displayed under the **Properties** tab in the right pane of the window as shown in the screenshot (here, we have selected the image file **Tweety1.gif**):

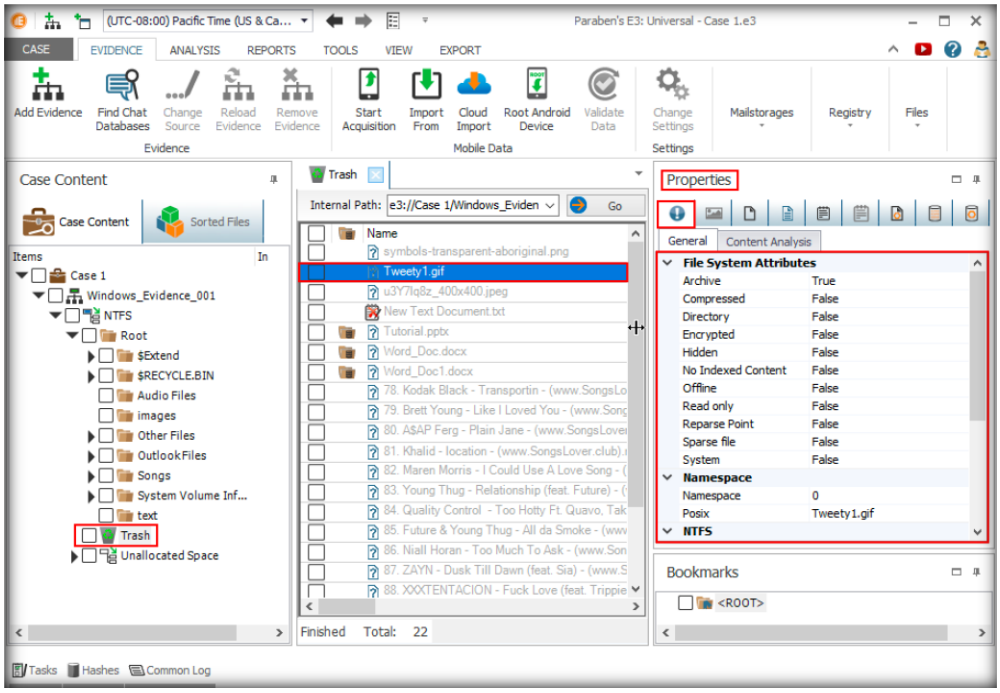

FIGURE 5.22: Viewing Properties of a Selected File

TASK 5

View the File

25. To view the actual image contained in the selected file (since the selected file is of image file format), click the **File View** tab. The image will be displayed in the right pane of the window.

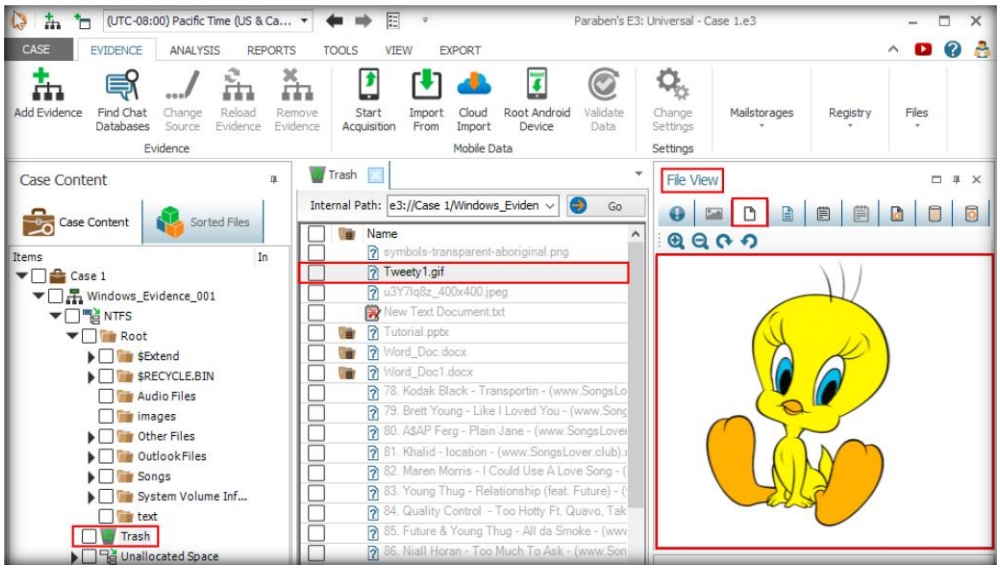

FIGURE 5.23: Viewing the Actual Image Contained in a Selected File

26. Apart from viewing the actual image contained in a selected file, **Paraben's E3** also lets you view its Hex values. Hex values help determine the raw and exact contents of a file even if it has been **deleted or overwritten**. Hex values thus help you identify and retrieve information of forensic value that normally cannot be accessed by the operating system.

27. To view the hex values of the selected file, click the **Hex View** tab. The Hex values will be displayed in the right pane of the window.

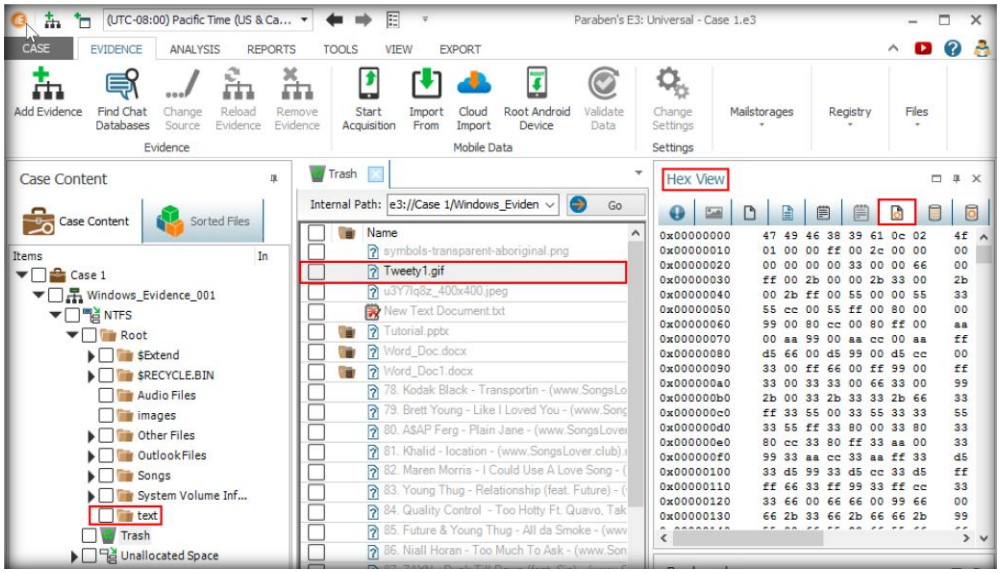

FIGURE 5.24: Viewing the Hex Values of the Selected File

28. To view the text values of a text file document, select the text file (here, we have selected the text file **New Text Document.txt**) and then click the **Text View** tab as indicated in the screenshot below:

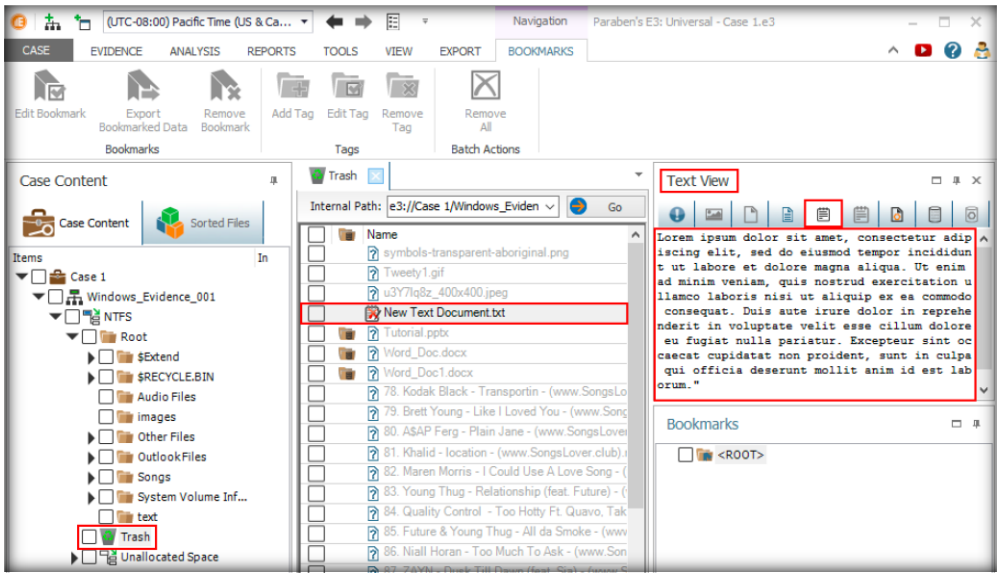

FIGURE 5.25: Text view of a Selected File

TASK 6

Generate a Report

29. To generate an investigative report, first select the desired files that must be included in the report. Then click on **Reports** on the menu bar, and then click **Generate Report** as indicated in the screenshot below:

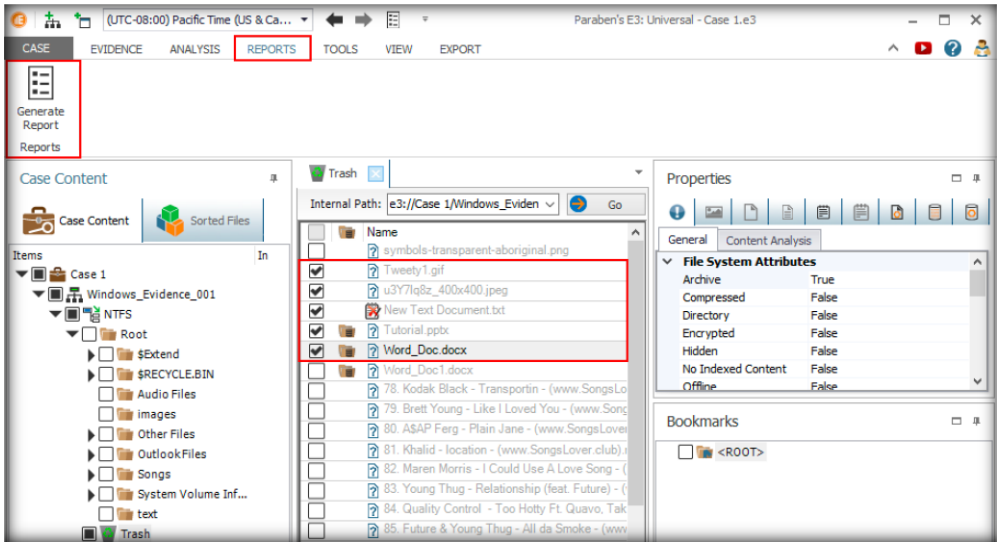

FIGURE 5.26: Generating Report

30. In the **Reports Wizard** window that appears next, we need to select the report type to be generated and also specify a **Destination folder**. In this lab, we will be selecting the **HTML Investigative Report** type option and the default destination folder location shown by the application. Ensure to **check** the options **Include Parsed Embedded Data** and **Open report on finish**. Click **Next**.

Note: If you want the report to be opened automatically at the end of the lab without having to manually open it by navigating to the location where it has been saved, then do ensure to check the option **Open report on finish**.

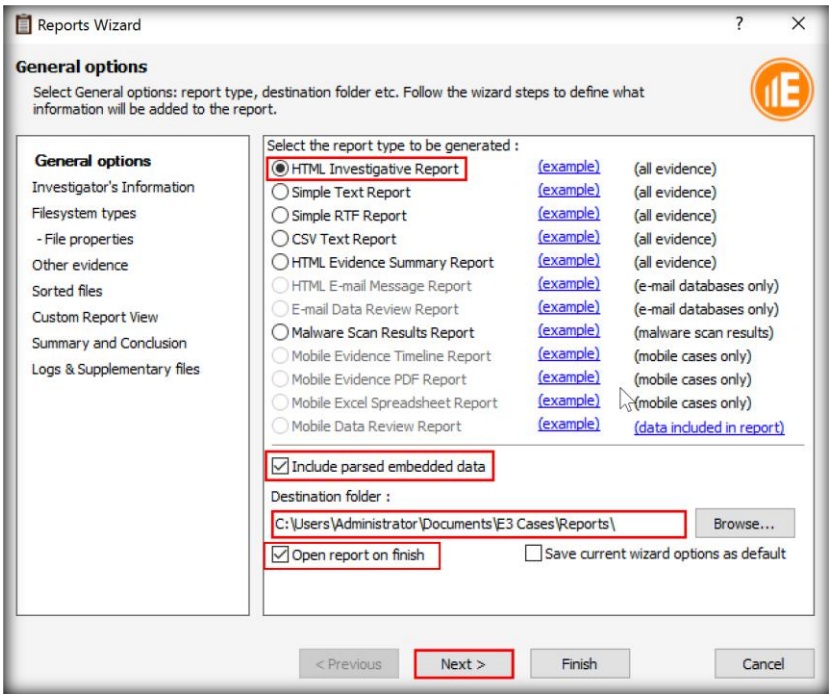

FIGURE 5.27: Reports Wizard

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

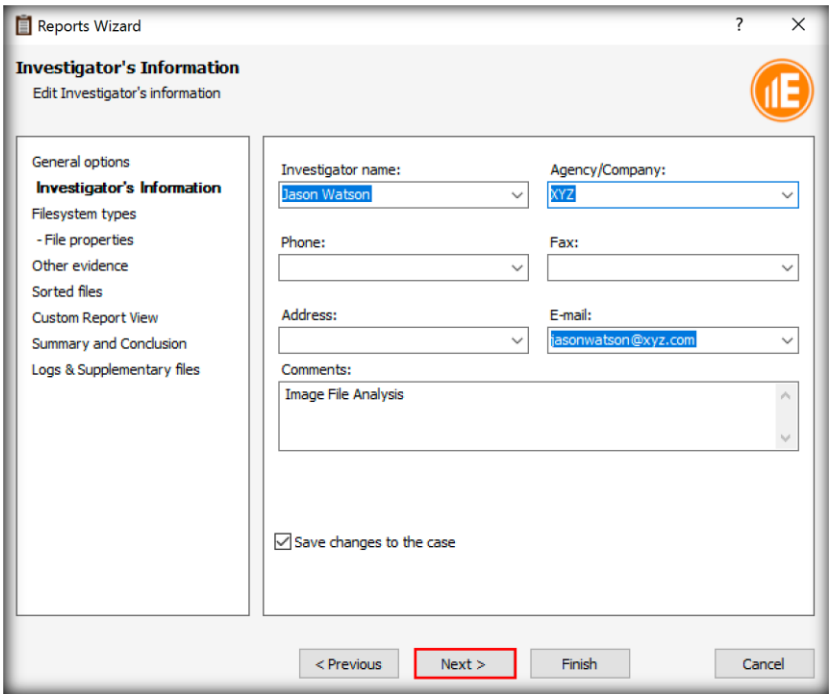

FIGURE 5.28: Investigator's Information Section

Investigator's information is 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

The filesystem type 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

32. In the **Filesystem Types** section that appears next, select the file types that you want included in the report and click **Next** button.

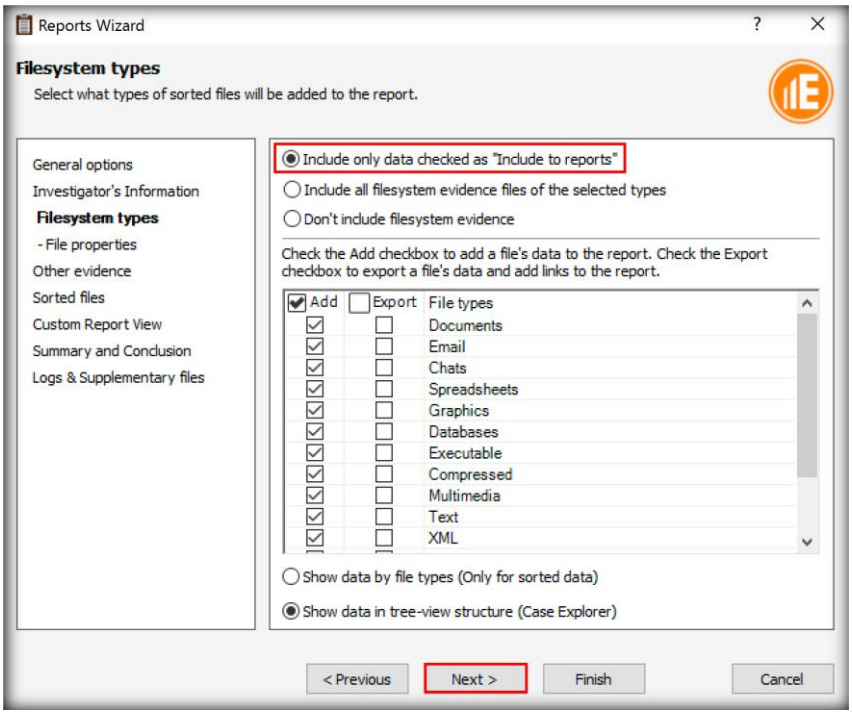

FIGURE 5.29: Filesystem Types Section

33. In the **File properties** section that appears next, select those details under properties that you want included in the report, then click **Next**.

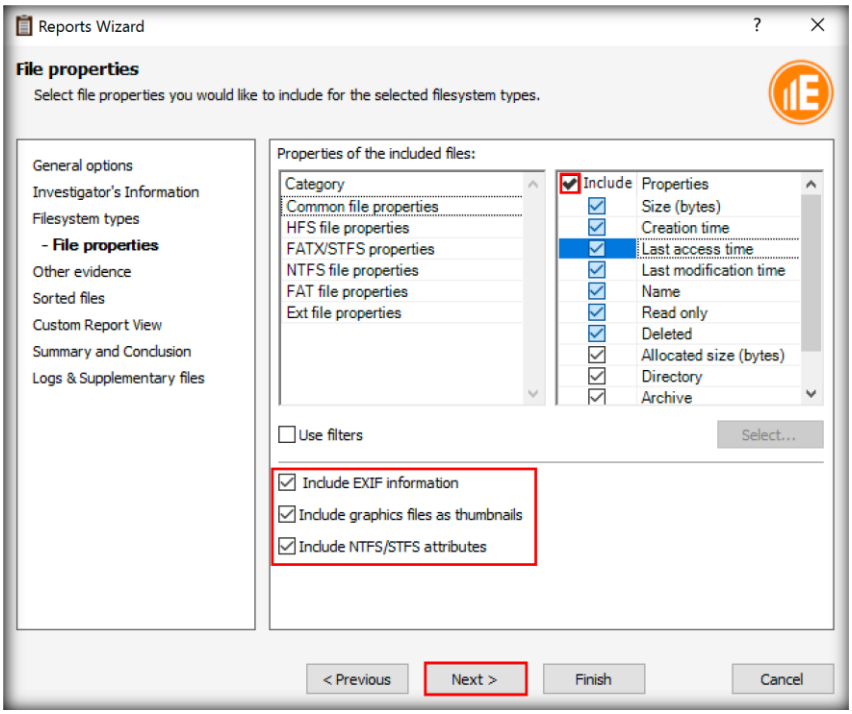

FIGURE 5.30: File Properties Section

34. In the **Other evidence** section that appears next, select the options according to your requirement (you may also leave these options set to default). Click **Next**.

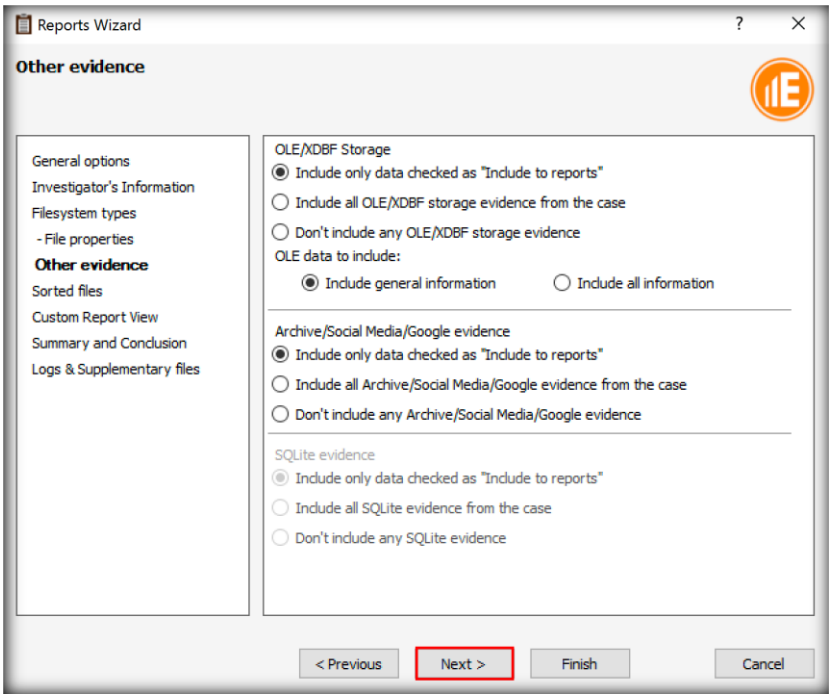

FIGURE 5.31: Other Evidence Section

35. In the **Sorted files** section that appears next, select the **Include only data checked as "Include to reports"** radio button and then click **Next**.

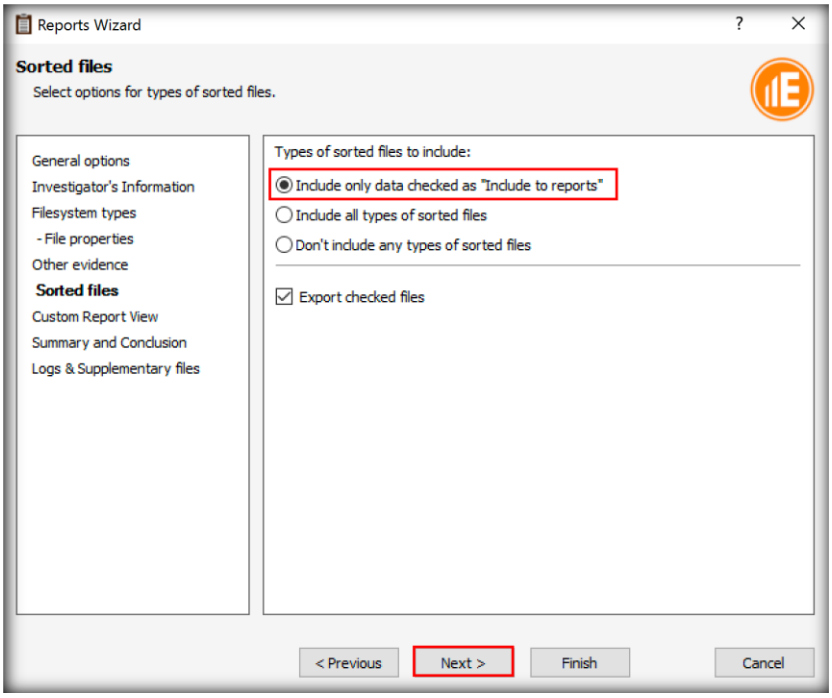

FIGURE 5.32: Sorted Files Section

36. In the **Custom Report View** section that appears next, you can customize the report view by adding your custom logo, custom header, and custom footer. Click **Next** after customizing the report view.

Note: Customizing the report view is not mandatory and can be skipped by clicking **Next**.

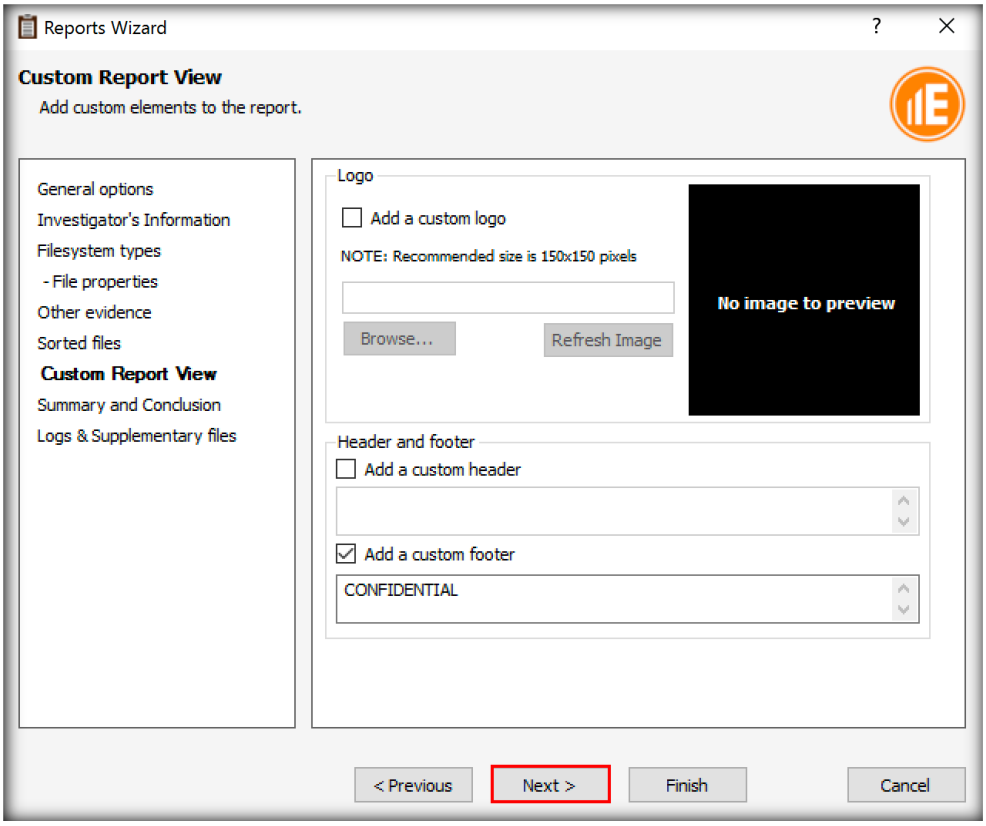

FIGURE 5.33: Custom Report View Section

37. In the **Summary and Conclusion** section that appears next, you can add the summary and conclusion pertaining to the evidence examination in the **Examination Summary** and **Examination Conclusion** sections respectively. Click on the **Edit Section** buttons below the **Examination Summary** and **Examination Conclusion** sub-sections respectively. An **Editing Section** window (which looks similar to a word document) for each of those sub-sections will open. In the **Editing Section** windows for each of those sub-sections, you can respectively write a brief summary on the evidence file examined and a conclusion describing the actions performed on it and the result generated. After adding the summary and conclusion, click **Next**.

Note: The **Summary and Conclusion** section is not mandatory to edit and can be skipped by clicking **Next**.

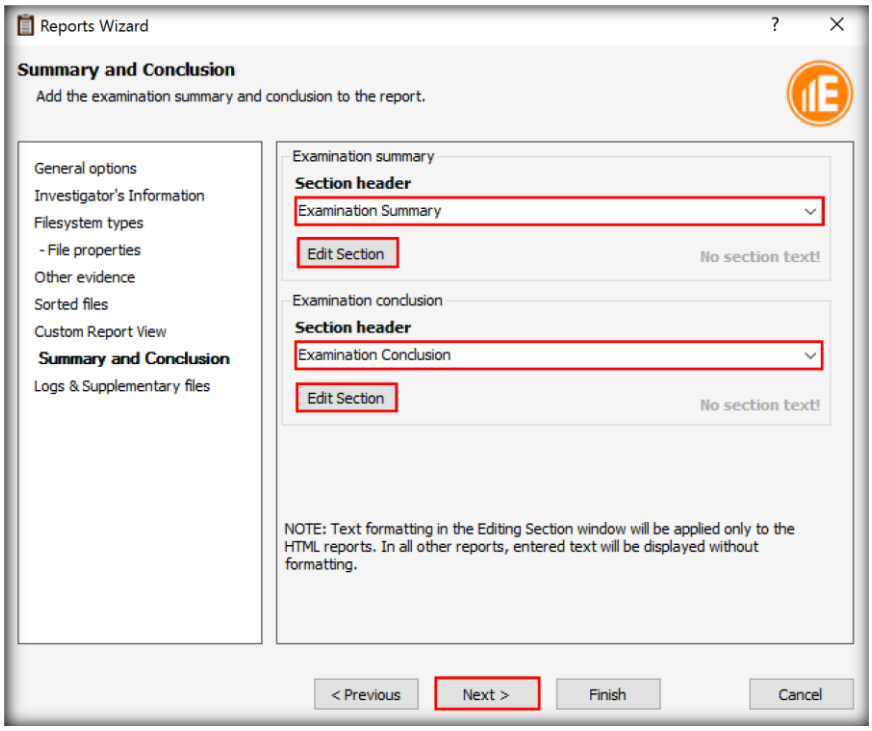

FIGURE 5.34: Summary and Conclusion Section

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

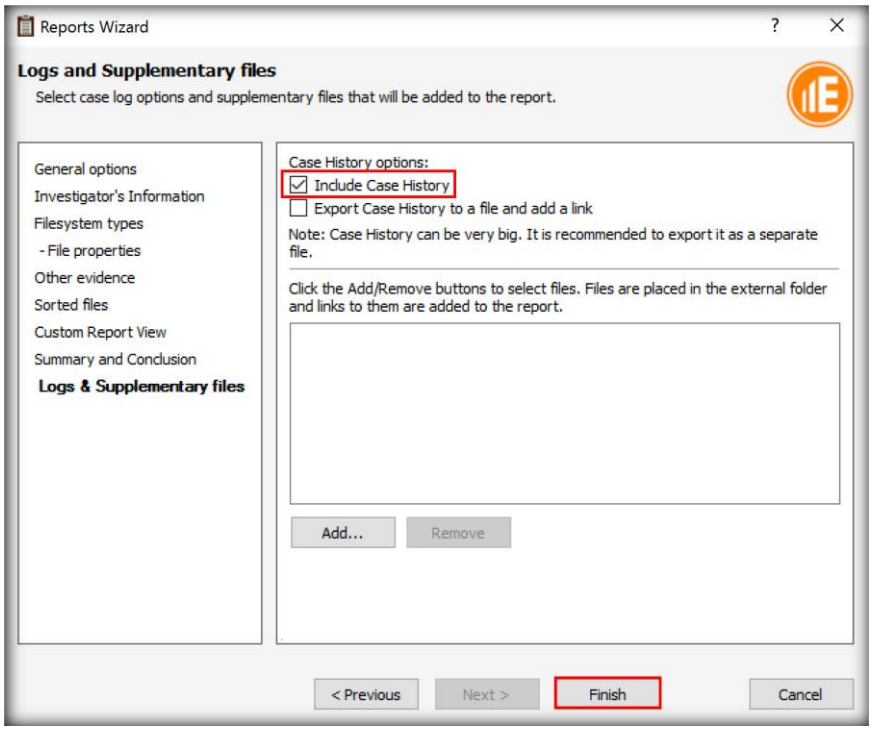

FIGURE 5.35: Logs and Supplementary Files Section

39. A **Task Status Notification** window appears indicating that report generation is finished and that the generated report has been saved to the default destination (in this case: **C:\Users\Administrator\Documents\E3 Cases\Reports\Case 1**). Click **OK** or **close** the window.

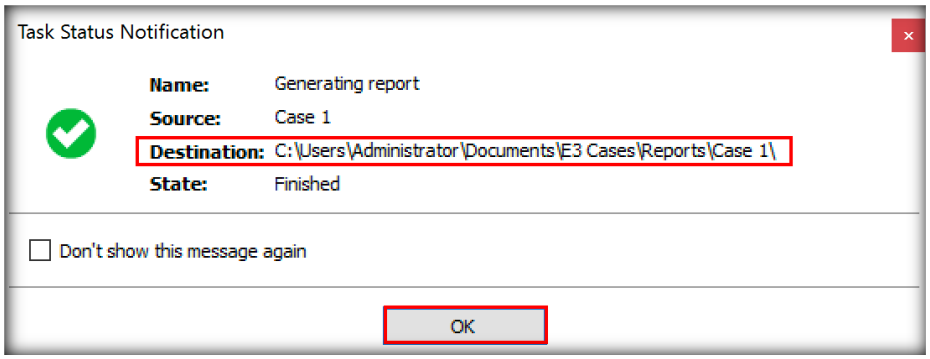

FIGURE 5.36: Task Status Notification Dialog Box

TASK 7

View the Report

Note: If asked about how you want to open the generated report, as shown in the screenshot below, then make your choice and click **OK**. The report will then be opened through the browser that you selected. After this operation, whenever you attempt to open the investigative report that you generated, it will always be opened automatically through the browser that you have chosen here.

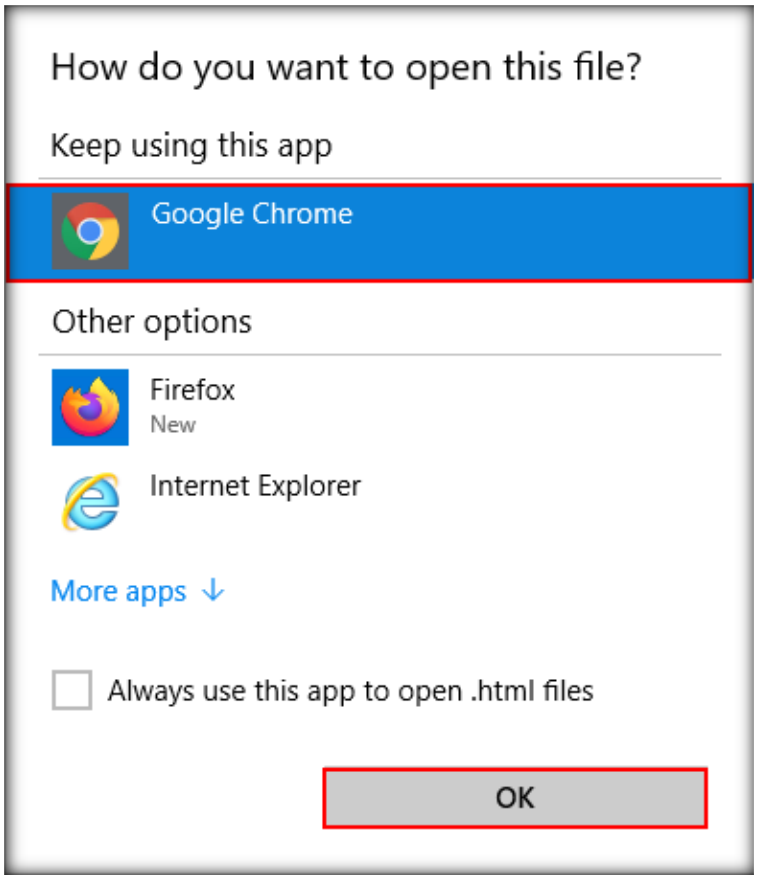

FIGURE 5.37: Opening the Investigative Report through a Browser

40. You can also manually navigate to the folder where you have saved the report file and open it from there. In this folder, you will find a sub-folder named **Case 1**. Open that sub-folder and double-click the **Case 1.html** file to open and view the report.

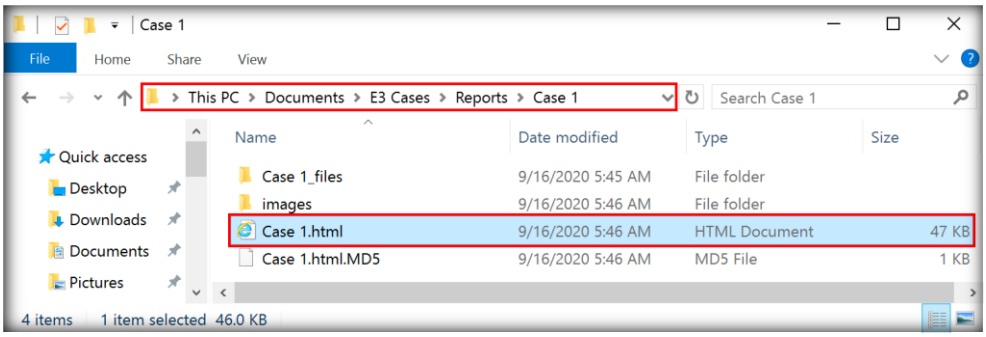

FIGURE 5.38: Opening Investigative Report from the Folder It Was Saved In

41. A detailed **Investigative Report** will open in the web browser; scroll down the browser window to examine the report in detail.

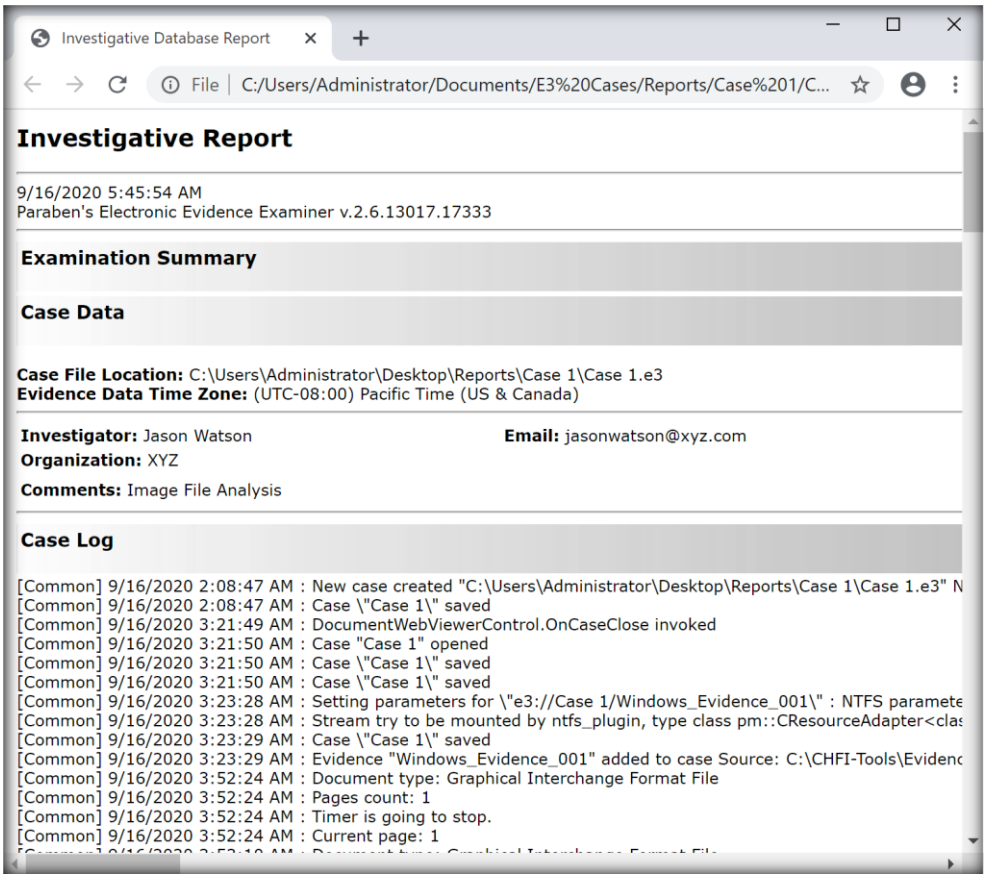

FIGURE 5.39: Detailed Investigative Report Opened in Browser

42. In this manner, you can use Paraben's E3 utility to handle evidence data.

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.

Lab

6

Creating a Disk Image File of a Hard Disk Partition

A disk image is a bit-by-bit copy of a hard disk or a disk partition, which includes all the files/folders, deleted files, files left in the slack space and unallocated space, file system information, etc.

ICON KEY

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

Lab Scenario

An investigator was performing forensics on a hard disk copy when he triggered a pre-loaded process that deleted the entire disk data leading to loss of evidence. However, he had already created a forensic copy of the disk and this gave him the option to work on the same data again. Therefore, investigators should always create duplicates of the hard disk and perform the forensics process on the copy.

To be a computer forensics expert, you must have sound knowledge of the 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 a hard disk partition using **R-Drive Image**.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process.

This lab requires:

- A system running a **Windows 10** virtual machine
- A system running a **Windows Server 2016** virtual machine
- Administrative privileges to install and run tools
- **The R-drive Image** installer, which is located at **C:\CHFI-Tools\CHFIv10 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\R-drive Image**

Note: You can also download the latest version of **R-drive Image** from the link https://www.drive-image.com/Drive_Image_Download.shtml

Please note that if you use the latest version of software for this lab, then the screenshots shown in this lab might differ slightly.

Note: Make sure that **Real Time Protection** is disabled in **Windows 10** virtual machine (if it is running) before beginning this lab.

Lab Duration

Time: 10 minutes

Overview of the Lab

This lab helps you learn how to create the disk image file of a hard-disk partition. Imaging of a hard disk or a hard disk partition helps you create the forensic copy of the disk or a partition on it so that you can use the forensic copy for investigation purposes.

Lab Task

TASK 1

Selecting the Hard Disk Partition

1. Log in to **Windows 10** virtual machine.
2. Navigate to **Z:\CHFIv10 Module 02 Computer Forensics Investigation Process\Computer Forensics Software\R-drive Image**.
3. 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**.

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

Note: If a **Windows Security** dialog box appears, enter the credentials of the **Windows Server 2016** virtual machine and then click **OK**.

FIGURE 6.1: R-Drive Image Setup

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

FIGURE 6.2: Launch R-Drive Image Option

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

5. The **R-Drive Image** GUI will appear; click **Next**.

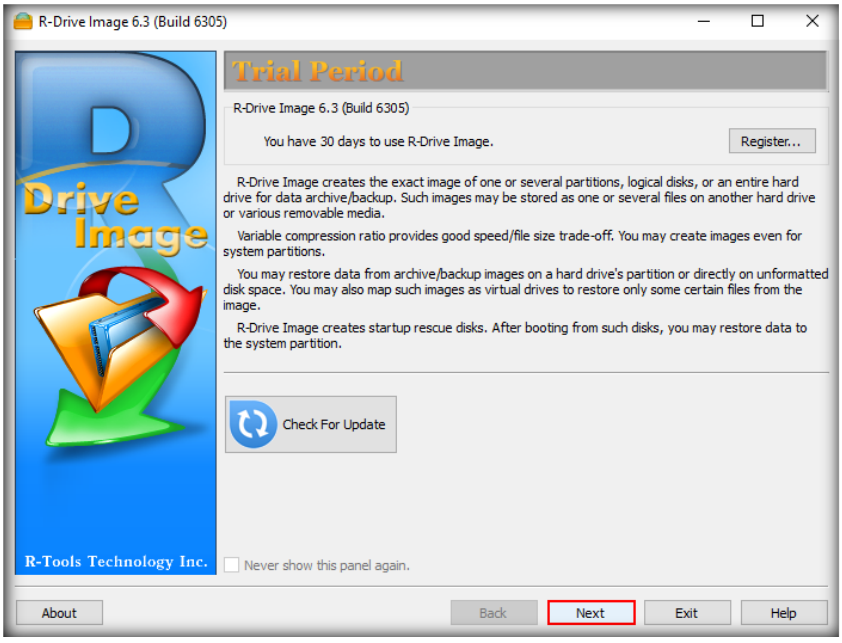

FIGURE 6.3: R-Drive Image GUI

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

6. In the **Action Selection** panel, **Create an Image** option is selected by default. Click **Next** to continue.

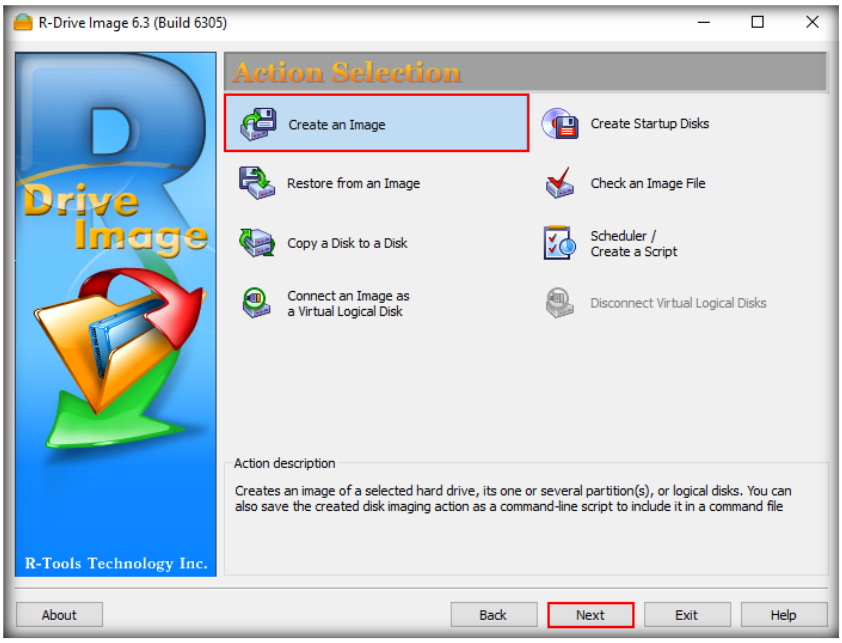

FIGURE 6.4: Action Selection Panel

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.

7. In this lab, we will be creating an image for **D:**. Therefore, in the **Partition Selection** panel, select **D drive** to create a drive image file of the drive. Click **Next**.

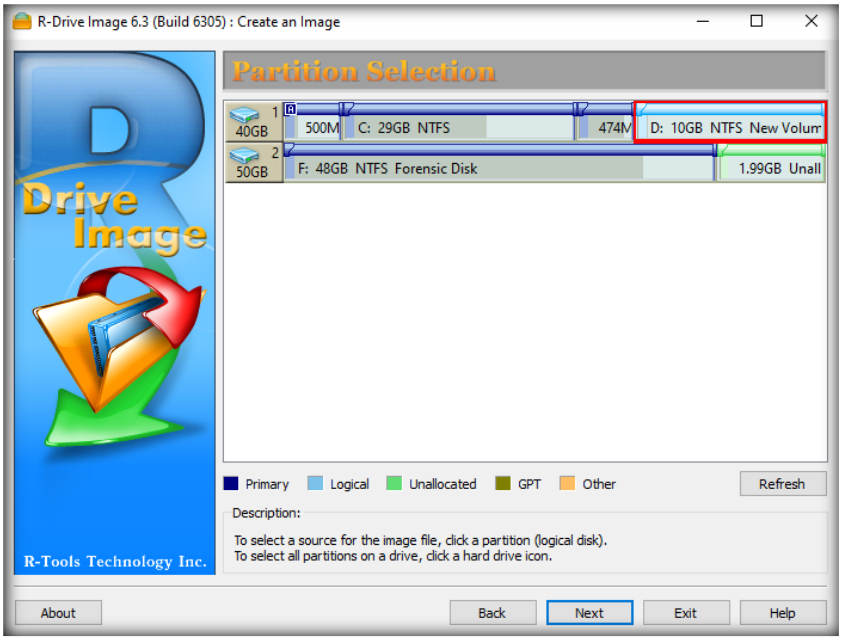

FIGURE 6.5: Partition Selection Panel

TASK 2

Selecting the Destination Folder

8. In the **Image Destination** panel:
   - Expand **This PC** and select the **Forensic Disk** (**F drive**) to save the file in this drive.
   - The filename will be automatically taken by the application.
   - Select **R-Drive Image files (*.rdr)** in the **Files of type** field and click **Next**.

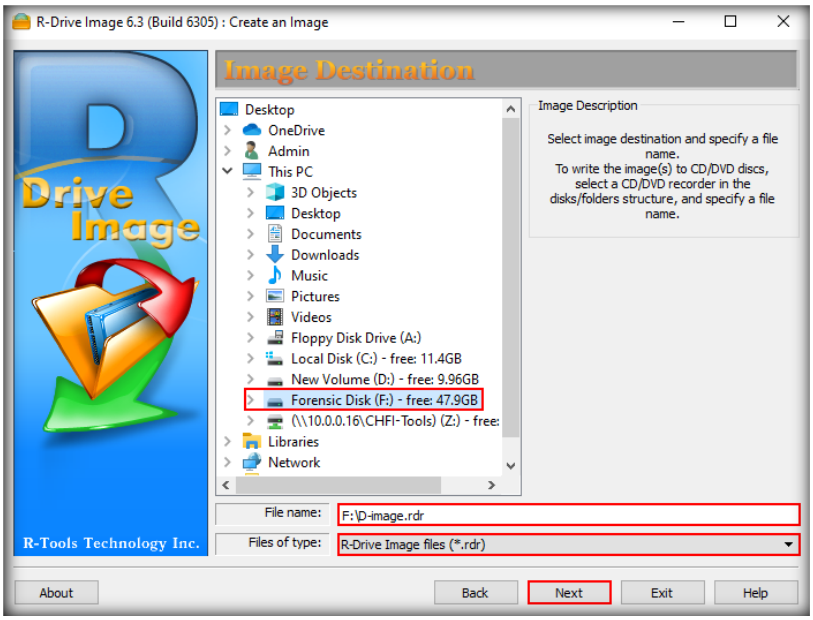

FIGURE 6.6: Image Destination Panel

9. In the **Image Options** panel, click **Next**.

Note: Providing a password is optional.

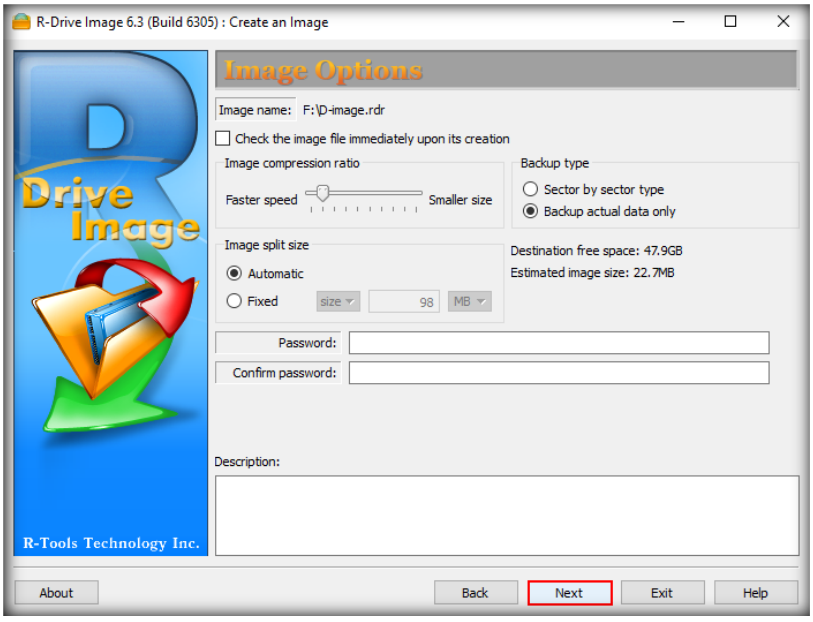

FIGURE 6.7: Image Options Panel

With R-Drive Image, 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.

10. In the **Backup Options** panel, click **Next**.

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

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

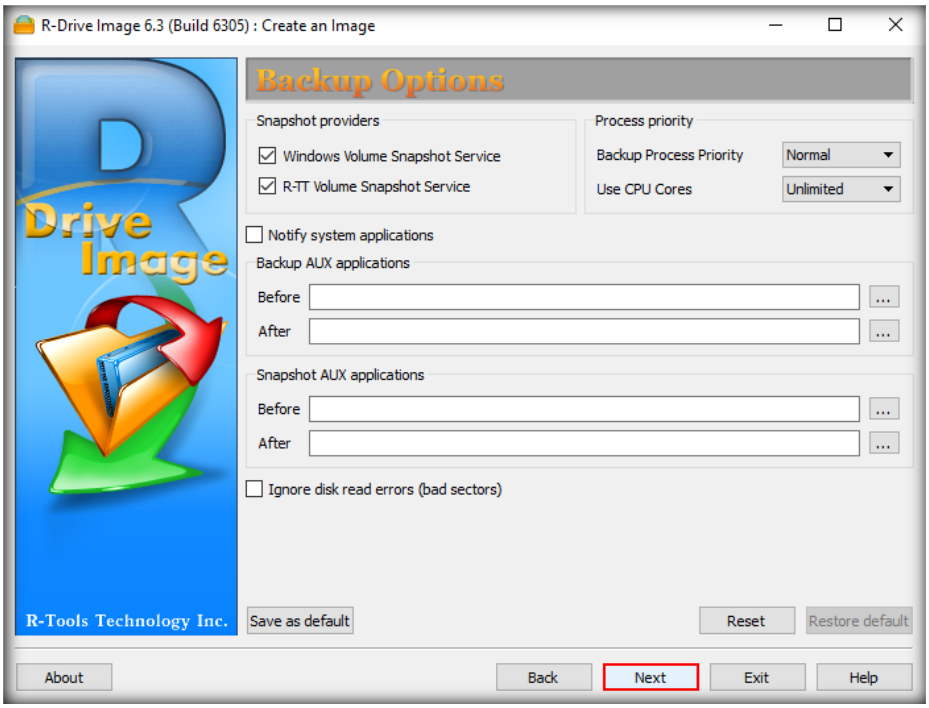

FIGURE 6.8: Backup Options Panel

TASK 3

Creating a Disk Image File

In R-Drive Image, 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. This speeds up the process of creating the incremental/differential image but also means that there is no need to change the original disks when writing the image to CD/DVD disks.

11. The **Processing** panel displays the summary of all the processes. Click **Start** to start the disk partition imaging process.

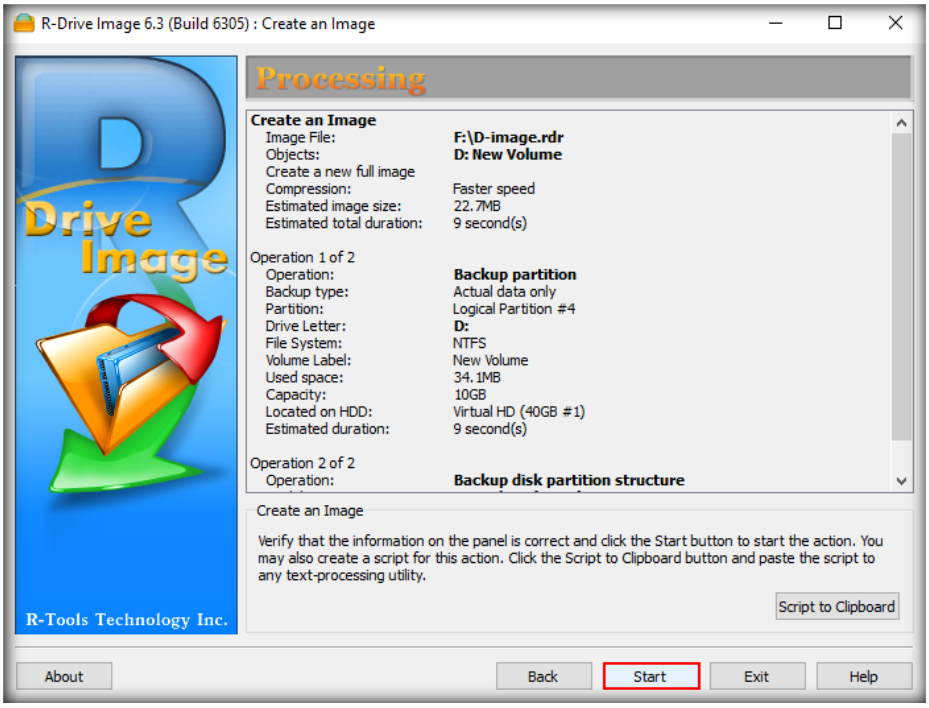

FIGURE 6.9: Processing Panel

12. The **Progress bar** in the **Processing** panel will show the percentage of task completed.

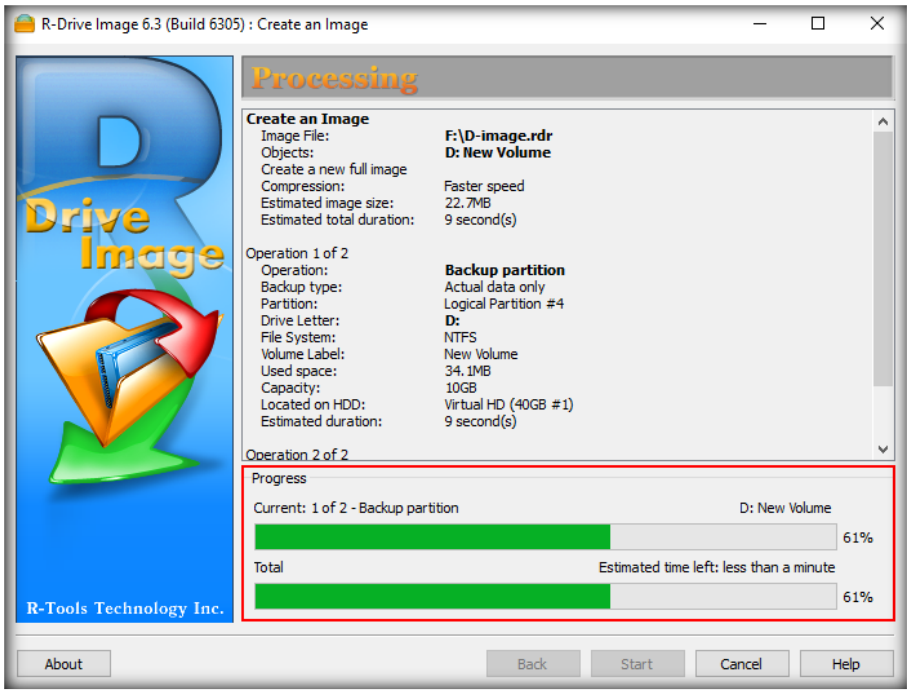

FIGURE 6.10: Processing Panel

13. Once the processing is done, a pop-up will appear displaying **Image created successfully**. Click **OK**.

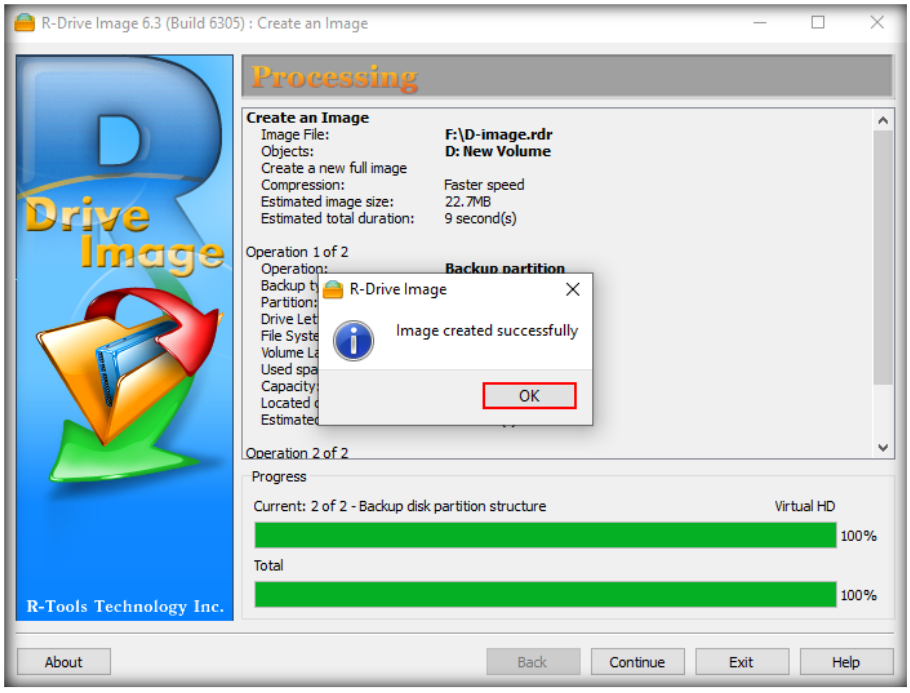

FIGURE 6.11: R-Drive Image Pop-up

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

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

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

14. In the **Processing** panel, click **Continue** to complete the process.

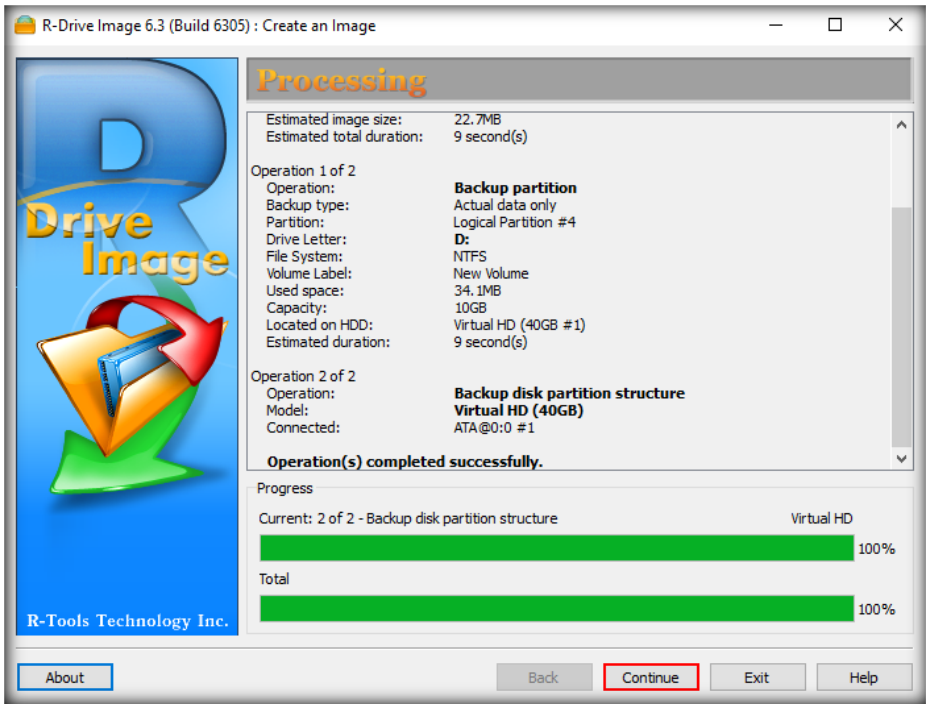

FIGURE 6.12: Processing Panel

15. In the **R-Drive Image** window that reads **Action Selection** at the top, click the **Exit** button to close the application.

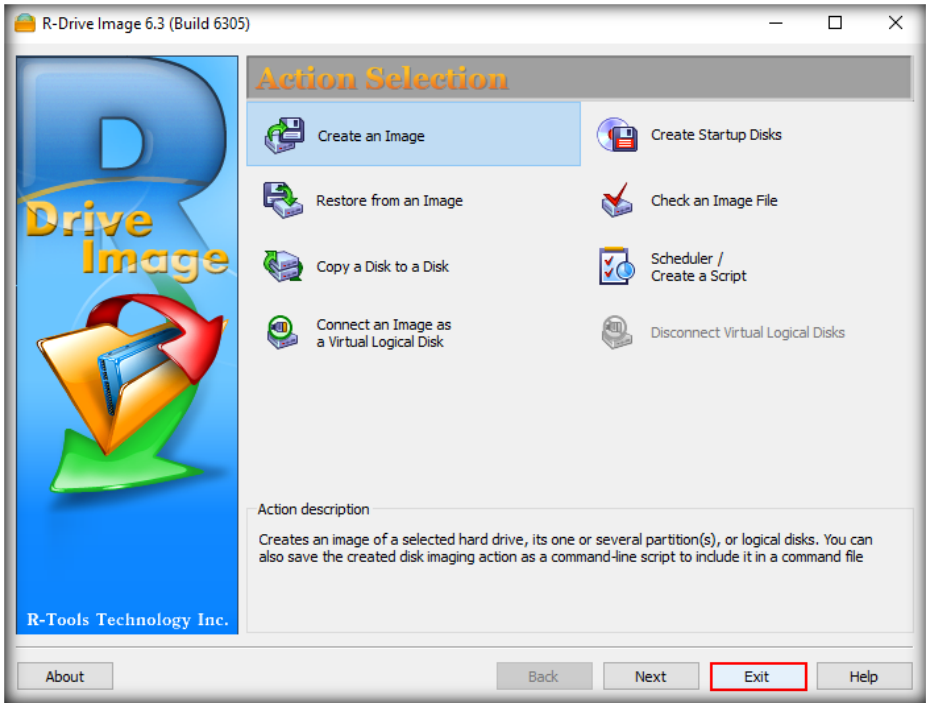

FIGURE 6.13: Exiting the Application Wizard from Action Selection Window

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.

TASK 4

Viewing a Created Disk Image File

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.

16. Now, navigate to the Forensic Disk (**F Drive**) to view the created disk partition image file.

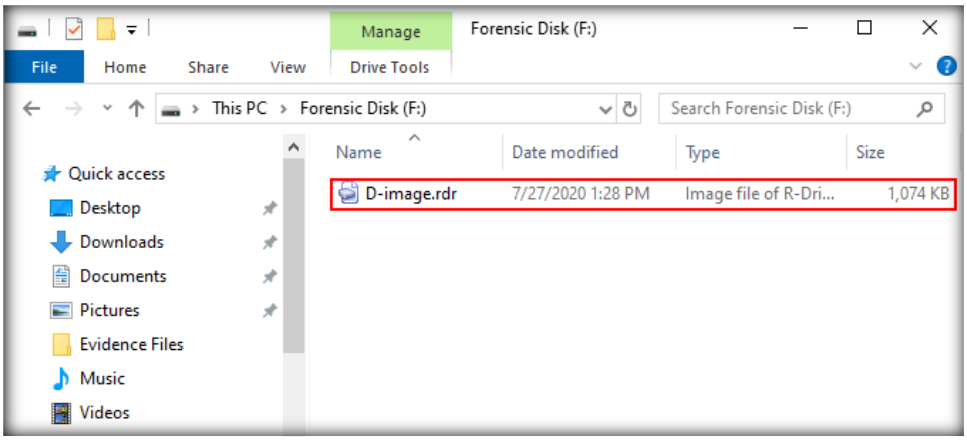

FIGURE 6.14: Disk Partition Image File in E Drive

Note: The size of the image file depends on the space filled in the drive. Since we are imaging D drive, which is currently empty, the size of the generated image file is relatively less.

17. Examination of disk image files is covered in **CHFIv10 Module 06 Windows Forensics** labs.
18. Delete the image file upon finishing this lab.

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.