Defeating Anti-forensics Techniques

Module 05

Defeating Anti-forensics Techniques

Perpetrators of cybercrimes use anti-forensic techniques to avert detection through forensics investigation processes. These techniques hinder proper forensics investigation by reducing the quantity and quality of digital evidence.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

In order to investigate cybercrimes, as a **forensic investigator**, you must be able to collect and analyze evidence from victims' or attackers' systems. The attackers attempt to avert detection through the forensics processes by applying some anti-forensics techniques that damage evidence, hide the pathways used, and delete the data exfiltrated from the victims' systems. You must be aware of such techniques and their impact on the evidence and systems.

Lab Objectives

The objective of this lab is to provide expert knowledge about the following:

- Solid-state drive (SSD) file carving on Windows and Linux file systems
- Recovering lost/deleted partitions and their contents
- Cracking passwords of various applications
- Detecting steganography
- Detecting hidden data streams
- Detecting file-extension mismatch
- Unpacking program packers

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques

Lab Environment

You need the following for this lab:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- A web browser with an internet connection
- Administrative privileges to install and run tools

Lab Duration

Time: 170 minutes

Overview of Defeating Anti-forensics Techniques

There are different types of anti-forensics techniques such as data/file deletion, wiping/overwriting of data and metadata, corruption/degaussing, cryptographic file systems, password protection, etc.

Forensic investigators need to overcome/defeat anti-forensics techniques so that an investigator yields concrete and accurate evidence that helps identify and prosecute the perpetrators.

Lab Tasks

The following are the recommended labs that will assist you in defeating anti-forensics techniques:

- SSD File Carving on a Windows File System
- SSD File Carving on a Linux File System
- Recovering Data from Lost/Deleted Disk Partition
- Recovering Data from a Partition that is Deleted and Merged into another Partition
- Cracking Application Passwords
- Detecting Steganography
- Detecting Alternate Data Streams
- Detecting File Extension Mismatch
- Unpacking Program Packers

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

SSD File Carving on a Windows File System

File carving is a technique to recover files and fragments of files from unallocated hard disk space in the absence of file metadata.

ICON KEY

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

Lab Scenario

Sam, a forensic investigator, is supposed to perform file carving on a forensic image file of an SSD acquired from a Windows file system. Law enforcement agents acquired the image from the machine of a suspect who is accused in performing nefarious activities. Now, the forensic investigator should use file carving techniques to recover more data related to the case. To do so, the investigator should possess knowledge of the file system structure to identify and recover files and fragments of files from unallocated space of the SSD in the absence of file metadata.

As a forensic investigator, you should know how to perform SSD file carving on a Windows file system.

Lab Objectives

The objective of this lab is to help you understand how to perform SSD file carving on a Windows file system.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques

This lab requires the following:

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

Note: You can download the latest Windows based version of **Autopsy** from https://www.autopsy.com/download/

If you use the latest software version 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: 20 minutes

Overview of the Lab

This lab familiarizes you with the Autopsy tool for Windows and helps you understand how the TRIM functionality influences the possibility of data recovery on an SSD. It also helps you learn how to recover data from a Windows file system on an SSD when the TRIM functionality is disabled. In other words, we will perform SSD file carving on a Windows file system in this lab.

Lab Tasks

TASK 1

Perform File Carving on Windows File System (Trim Enabled)

1. Login to **Windows Server 2016** virtual machine.
2. In this lab, we will be using Autopsy to examine TRIM-enabled and TRIM-disabled SSD images of Windows-based evidence.

Note: Autopsy tool for Windows is already installed on Windows Server 2016 virtual machine (**In Module 03, Lab 01 Analyzing File System of a Linux Image)**.

3. To launch Autopsy, double-click the **Autopsy 4.14.0** shortcut icon on the Desktop.
4. Autopsy **Welcome** window appears along with Autopsy main window in the background. In the **Welcome** window, click **New Case**.

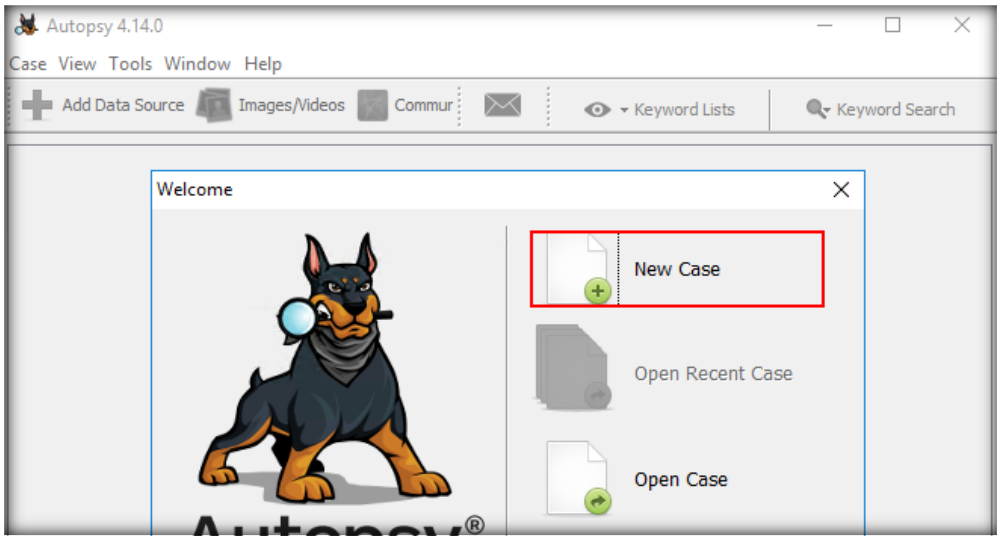

FIGURE 1.1: Autopsy Welcome Window

5. A **New Case Information** window opens, prompting you to provide the **Case Name** and **Base Directory**. The base directory is the location where the case data is to be stored. The case name may be entered according to your identification purpose. In this lab, we assign the case name as **SSD File Carving (Windows, TRIM Enabled)**.

6. We will save the case data in the **Image File Analysis** folder (created during the lab **Analyzing File System of a Linux Image using Autopsy** in **Module 03**) located on **Desktop**. So, click on **Browse** to assign this folder as the **Base Directory** and click **Next**.

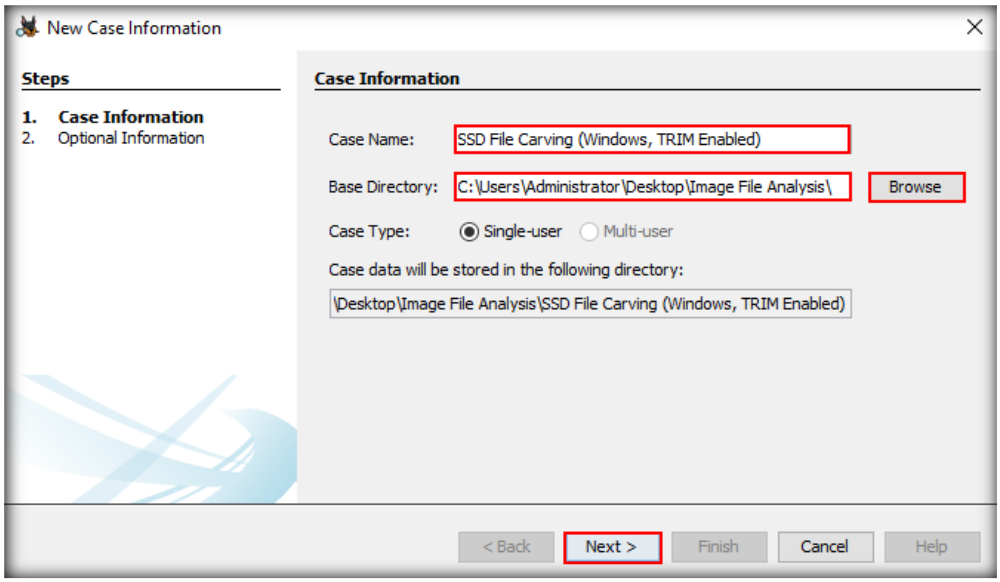

FIGURE 1.2: Autopsy New Case Information Window

7. The **Optional Information** section appears. Provide the **Case Number** and **Examiner Details** (here, we have provided the **Case Number** as **99**). You may enter your details in the **Examiner** section. Click **Finish**.

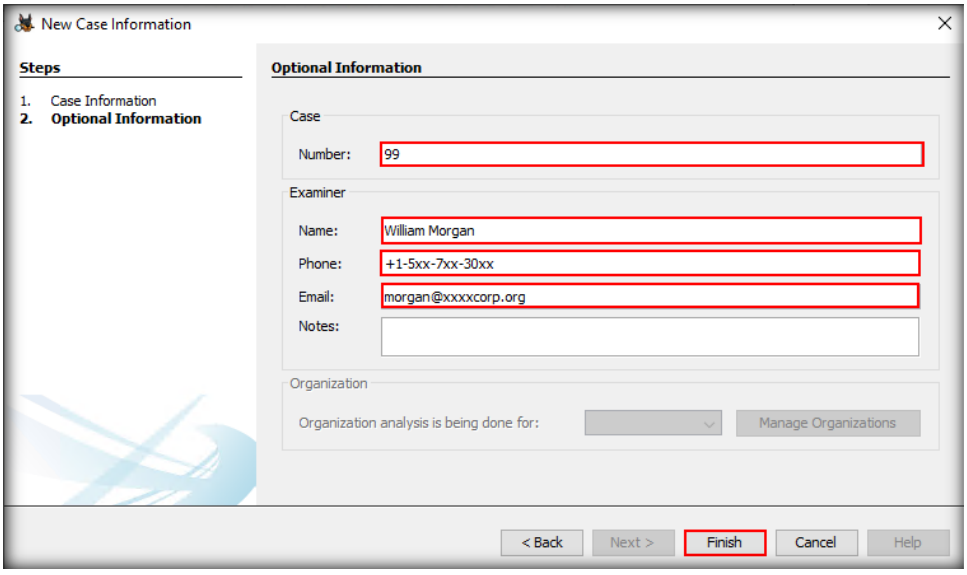

FIGURE 1.3: Autopsy Optional Information Section

8. The application takes some time to create the case. After the creation of the case, the **Add Data Source** window appears, where the **Select Type of Data Source to Add** section is displayed first. Ensure that the **Disk Image or VM File** option is selected and click **Next**.

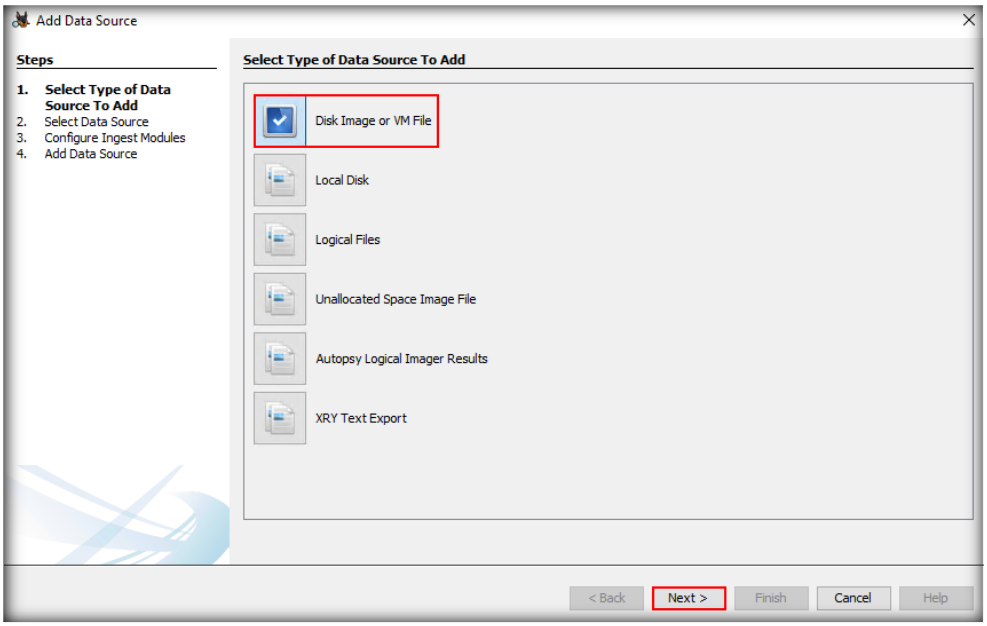

FIGURE 1.4: Add Data Source window showing the Select Type of Data Source to Add section

9. The **Select Data Source** section now appears. Click **Browse**.

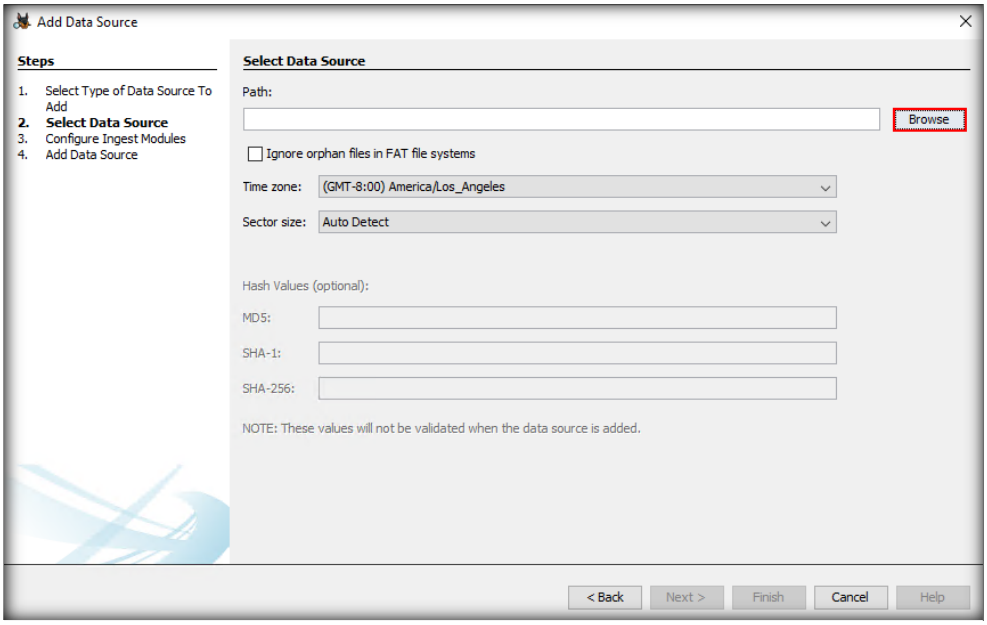

FIGURE 1.5: Select Data Source section

10. An **Open** window appears. Navigate to the location **C:\CHFI-Tools\Evidence Files\Forensic Images**, select the file **Windows_Evidence_SSD_TE.dd**, and click **Open**.

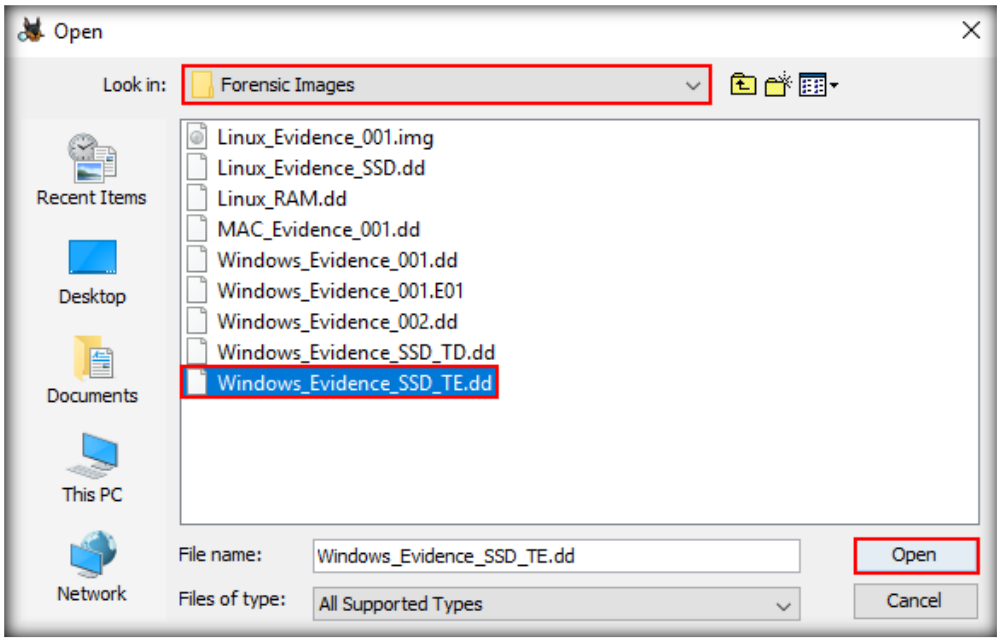

FIGURE 1.6: Autopsy Open Window

11. The **Select Data Source** section now displays the path to the **Windows_Evidence_SSD_TE.dd** file in the **Path** field. Click **Next**.

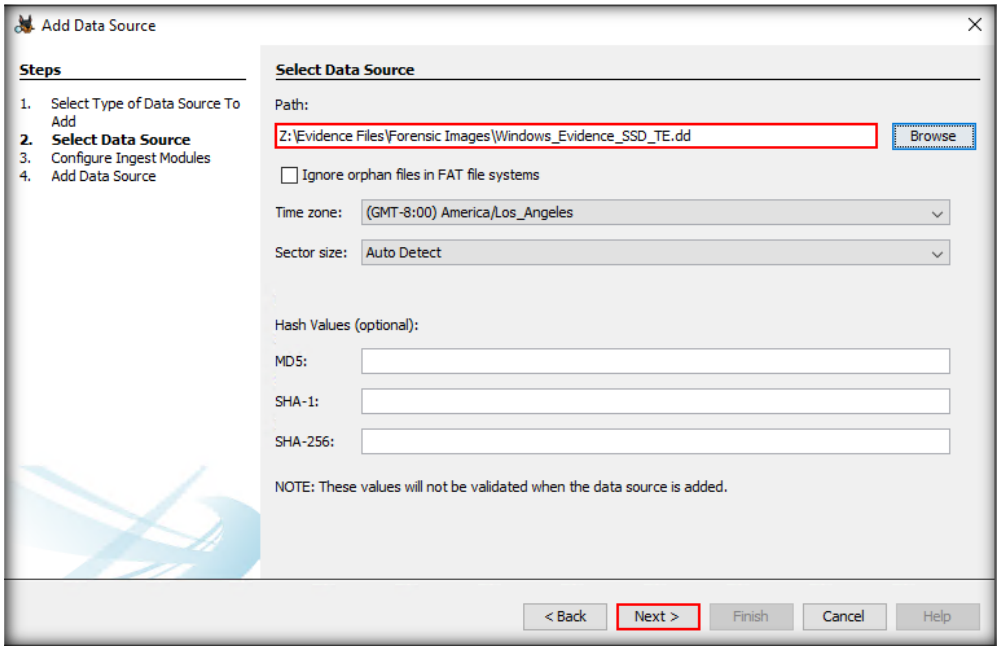

FIGURE 1.7: Autopsy Select Data Source Section

12. The **Add Data Source** window now displays the **Configure Ingest Modules** section which contains a list of options that are checked. Select these options according to your requirement. You may also leave these options set to default. Click **Next**.

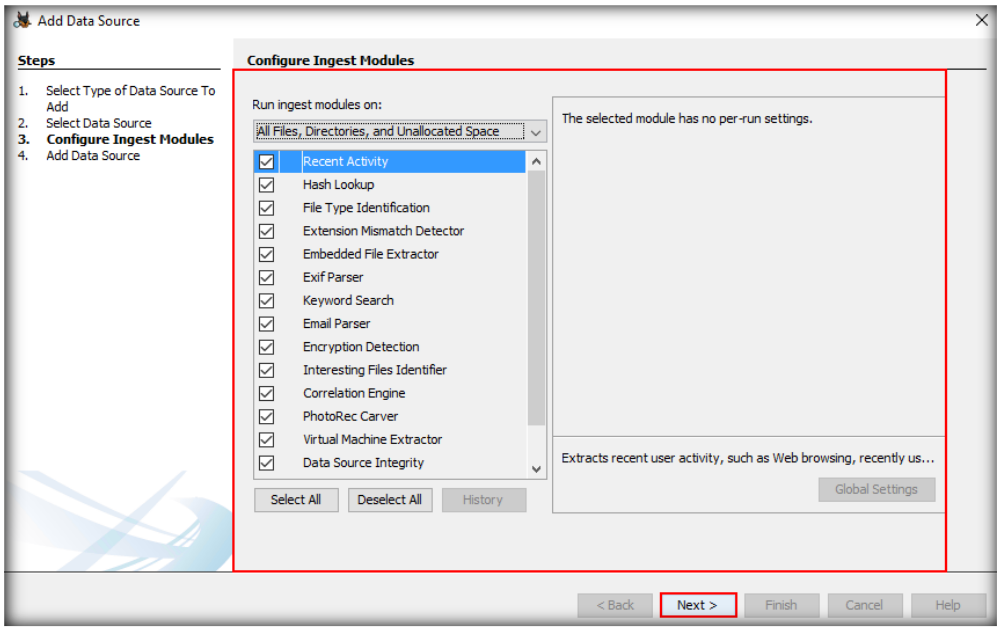

FIGURE 1.8: Configure Ingest Modules Section

13. The **Add Data Source section** appears, displaying the following message: **Data Source has been added to the local database. Files are being analyzed.** Click **Finish**.

Note: The Autopsy tool will take time to analyze the image file. View the status at the lower-right corner of the Autopsy window. Once the analysis is complete, the status disappears.

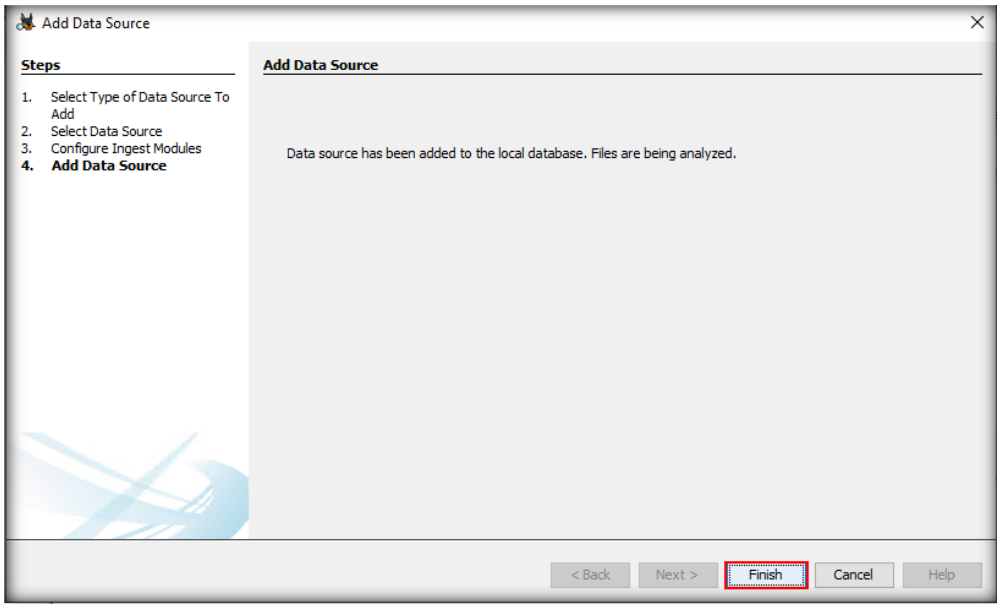

FIGURE 1.9: Add Data Source Section

14. The application will now take you to its main window. Expand the **Data Sources** node in the left pane of the window. The **Data Sources** option lists the name of the image file that you have analyzed (in this case, it is **Windows_Evidence_SSD_TE.dd**).

15. Click the image file name (**Windows_Evidence_SSD_TE.dd**) to view its contents in the right pane of the tool window. The image file contains folders that store data related to files, processes, services, tools, etc., stored/used on a Windows system.

Note: Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is completed.

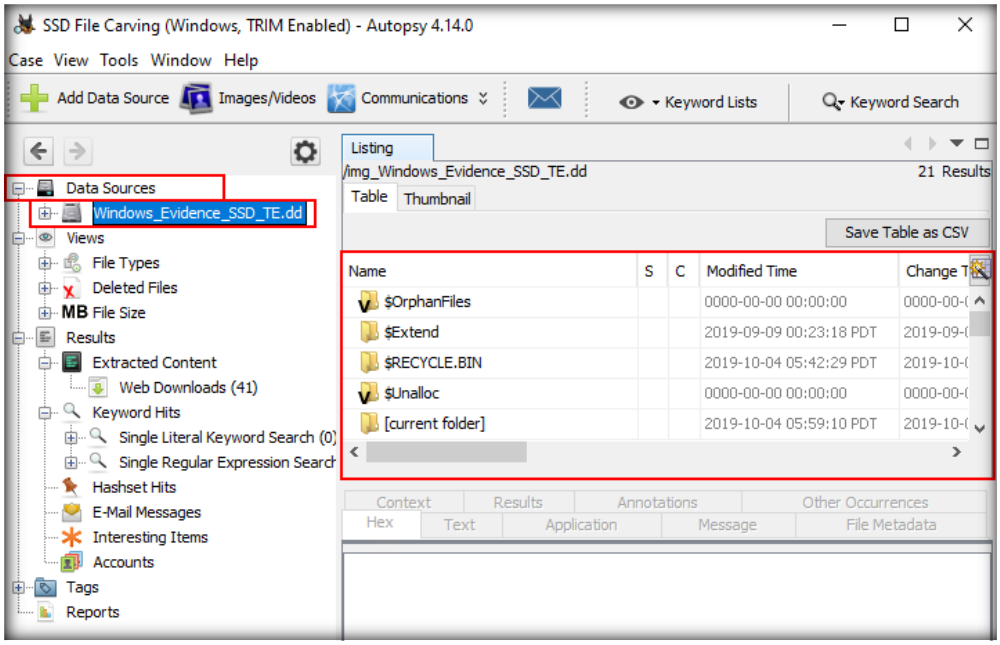

FIGURE 1.10: Viewing Contents of Windows_Evidence_SSD_TE.dd File

16. You may also view these contents by expanding the image file. So, expand the image node.

17. Our goal here is to recover carved files. The tool takes around 10–15 minutes to analyze the image and attempts to retrieve deleted and carved files from the image.

18. However, since this is a case that involves the use of a TRIM-enabled SSD image file as an evidence file, we observe that the tool does not carve any files. Hence, this demonstrates that file carving is not possible when TRIM is enabled on an SSD image file. You may now close all the windows pertaining to **Autopsy**.

19. We shall now move to retrieving data from a TRIM-disabled SSD image file. The steps below describe SSD file carving on a Windows file system when TRIM is disabled.

TASK 2

Perform File Carving on Windows File System (Trim Disabled)

20. On **Windows Server 2016** virtual machine, re-launch the Autopsy tool by double-clicking on the tool's shortcut icon located on **Desktop**.
21. The main window of **Autopsy** will open, along with its **Welcome** window.
22. Click the **New Case** option in the **Welcome** window.

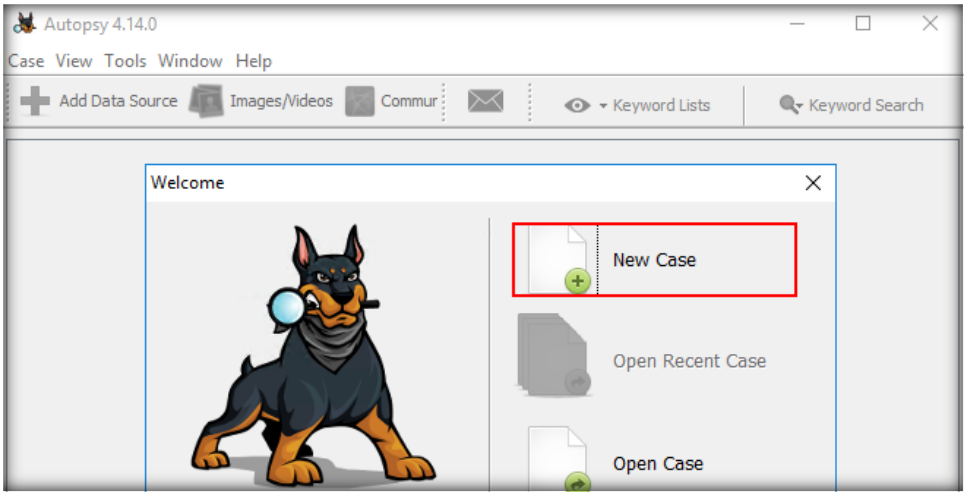

FIGURE 1.11: Autopsy Welcome Window

23. A **New Case Information** window opens, prompting you to input the **Case Name** and **Base Directory**. The base directory is the location where the case data is to be stored. The case name may be entered according to your identification purpose. In this lab, we assign the case name as **SSD File Carving (Windows, TRIM Disabled)**.
24. We will save the case data in the **Image File Analysis** folder located on **Desktop**. So, assign this folder as the **Base Directory** and click **Next**.

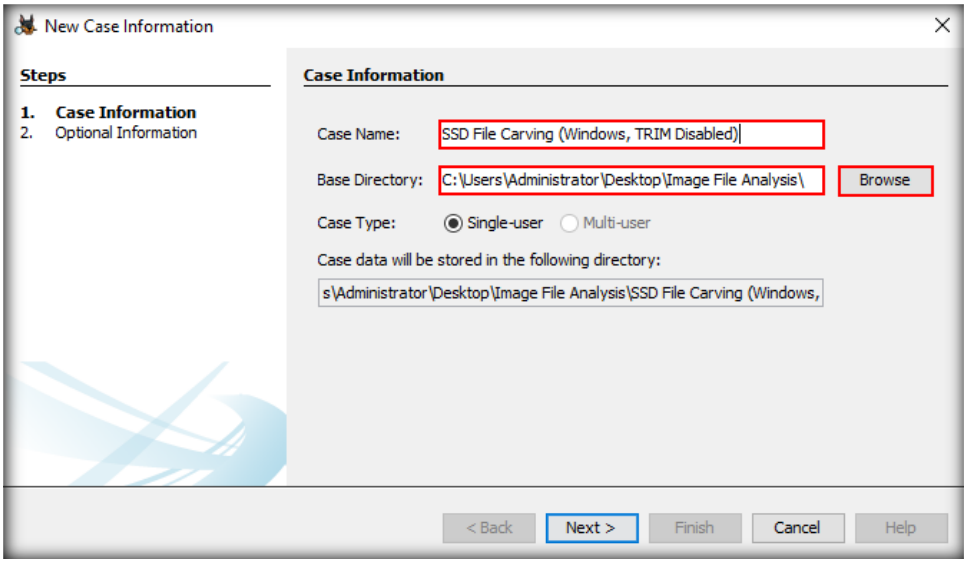

FIGURE 1.12: Autopsy New Case Information Window

25. The **Optional Information** section appears. Provide the **Case Number** and **Examiner Details** (here, we have entered the **Case Number** as **100**). You may enter your details in the **Examiner** section. Click **Finish**.

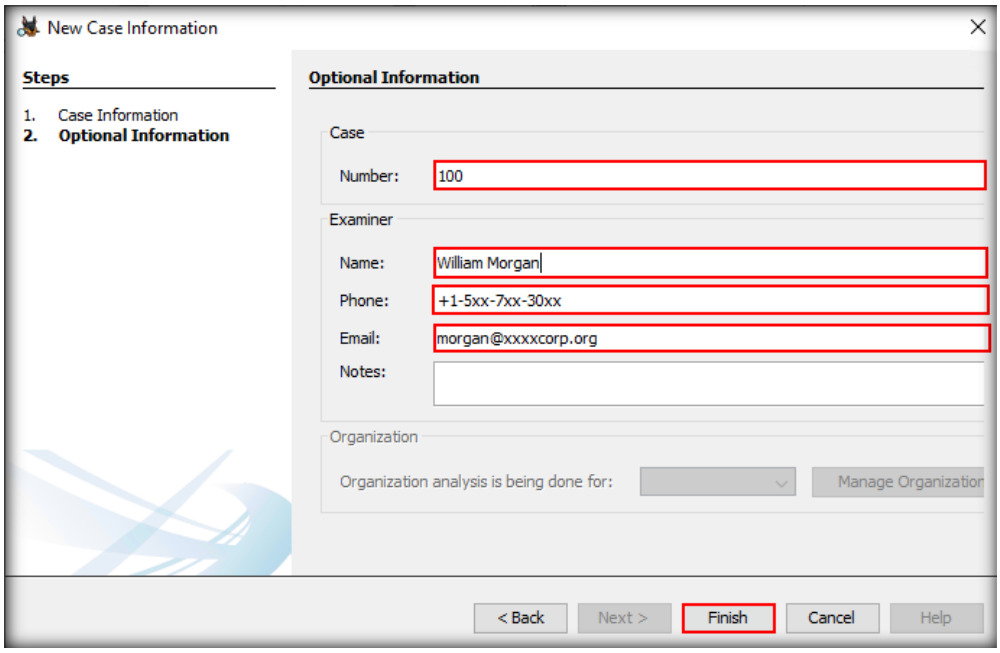

FIGURE 1.13: Autopsy Optional Information Section

26. The application takes a moment to create the case. After creation of the case, the **Add Data Source** window opens, where the **Select Type of Data Source to Add** section appears first. Ensure that the option **Disk Image or VM File** is selected. Click **Next**.

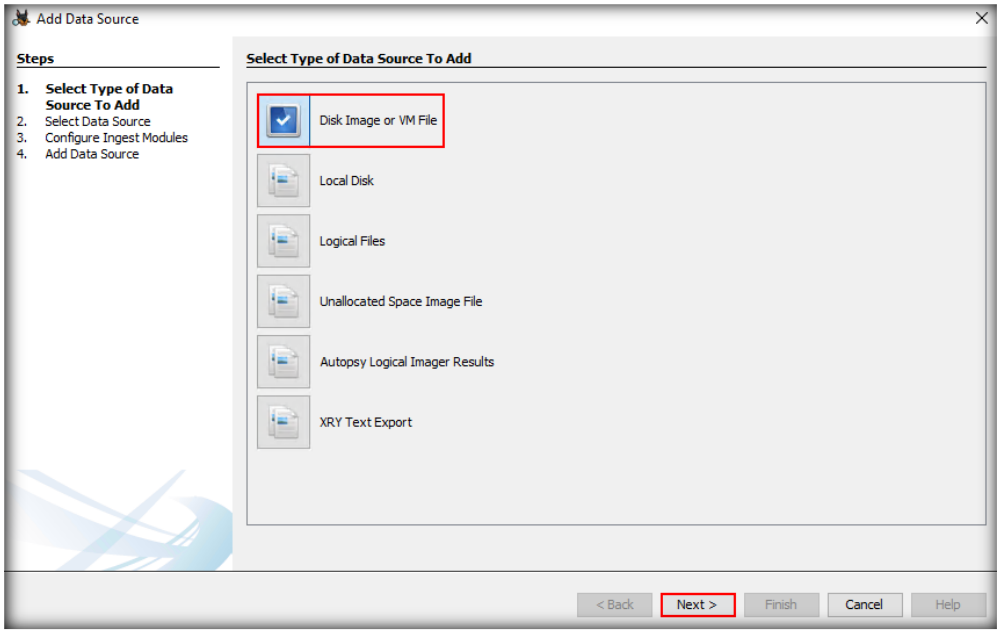

FIGURE 1.14: Autopsy Add Data Source Window - Select Type of Data Source to Add Section

27. The **Select Data Source** section appears. Click **Browse**.

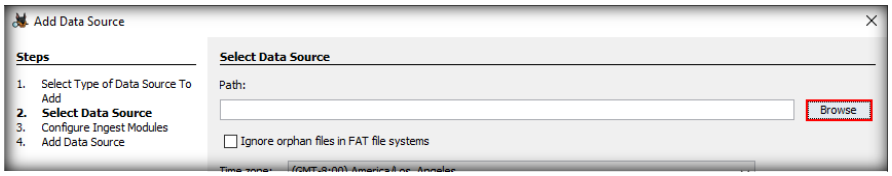

FIGURE 1.15: Select Data Source section

28. An **Open** window appears. Navigate to the location **C:\CHFI-Tools\Evidence Files\Forensic Images**, select the **Windows_Evidence_SSD_TD.dd** file, and click **Open**.

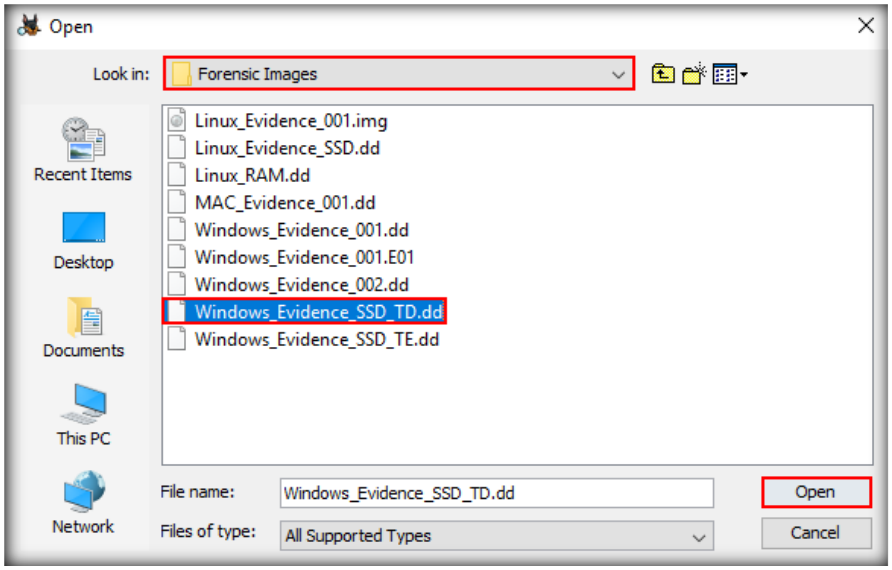

FIGURE 1.16: Autopsy Open Window

29. The **Select Data Source** section now displays the path to the **Windows_Evidence_SSD_TD.dd** file. Click **Next**.

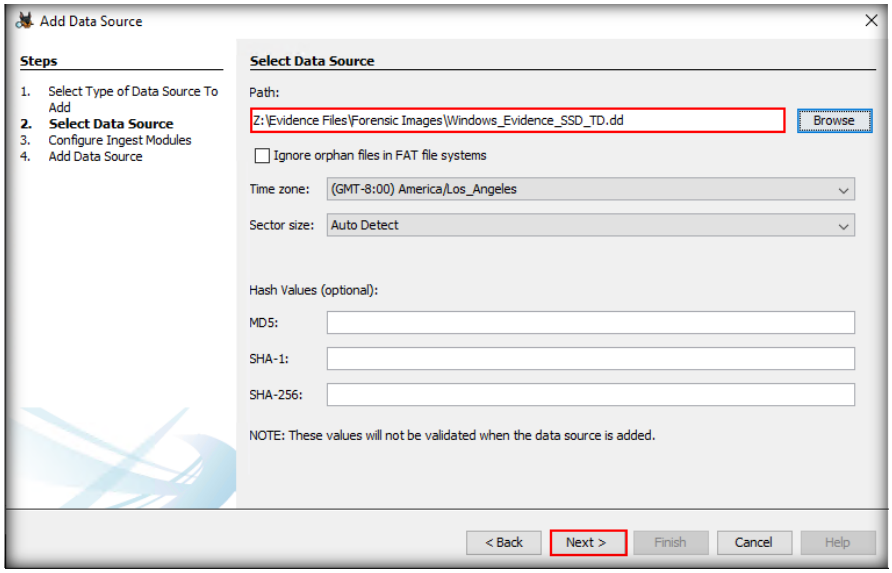

FIGURE 1.17: Select Data Source Section

30. The **Add Data Source** window now displays the **Configure Ingest Modules** section, which contains a list of options that are checked. Select the options according to your requirement. You may also leave these options set to default. Click **Next**.

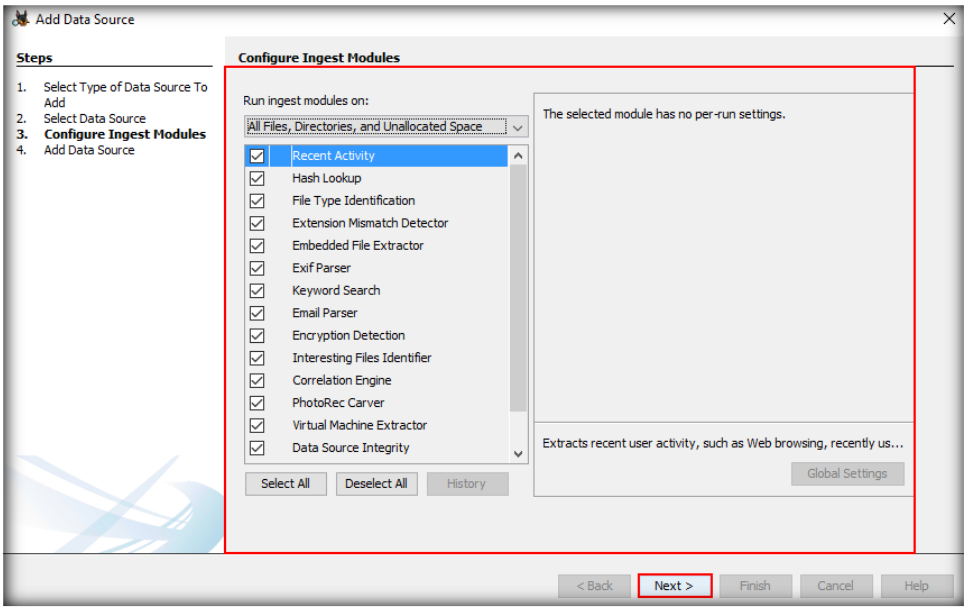

FIGURE 1.18: Configure Ingest Modules Section

31. The **Add Data Source** section now appears with a message that reads **Data Source has been added to the local database. Files are being analyzed.** Click **Finish**.

Note: The tool will take time to analyze the image.

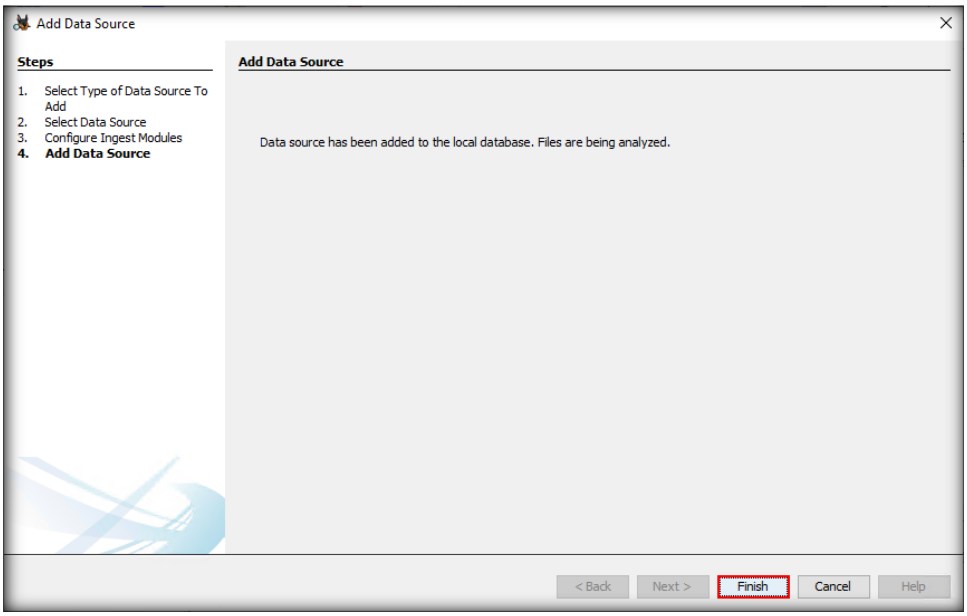

FIGURE 1.19: Add Data Source Section

32. The application now takes you to its main window. Expand the **Data Sources** node in the left pane. The **Data Sources** option lists the name of

the image file that you have analyzed (in this case, it is **Windows_Evidence_SSD_TD.dd**).

33. Click the image file name (here, **Windows_Evidence_SSD_TD.dd**) to view its contents in the right pane of the tool window. The image file contains folders that store data related to files, processes, services, tools, etc., stored/used on a Windows system.

Note: Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is completed.

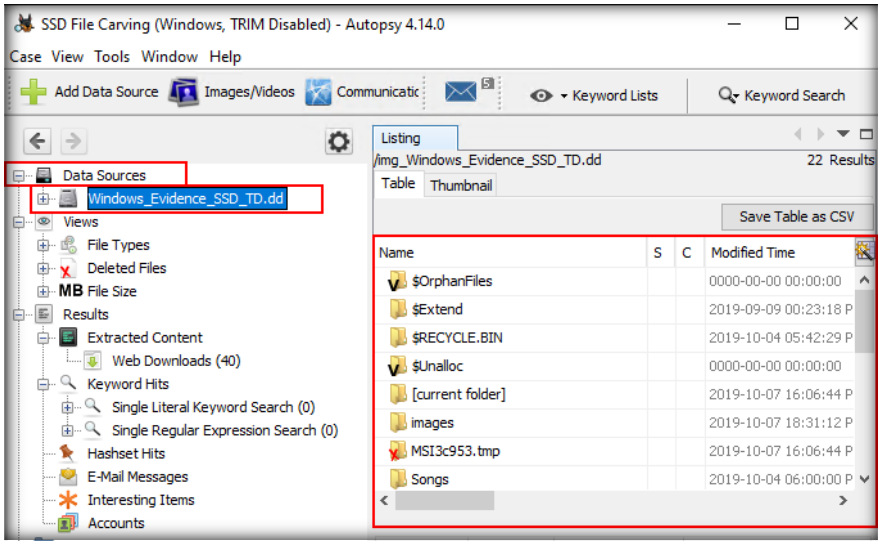

FIGURE 1.20: Viewing Contents of Windows_Evidence_SSD_TD.dd Image File in right pane

34. Here, the goal of our task is to retrieve carved files. The tool takes about 10–15 minutes to load the **CarvedFiles** folder. Upon loading the **CarvedFiles** folder, the tool displays it both in the right pane of the window and under the **Windows_Evidence_SSD_TD.dd** node, if you expand it.

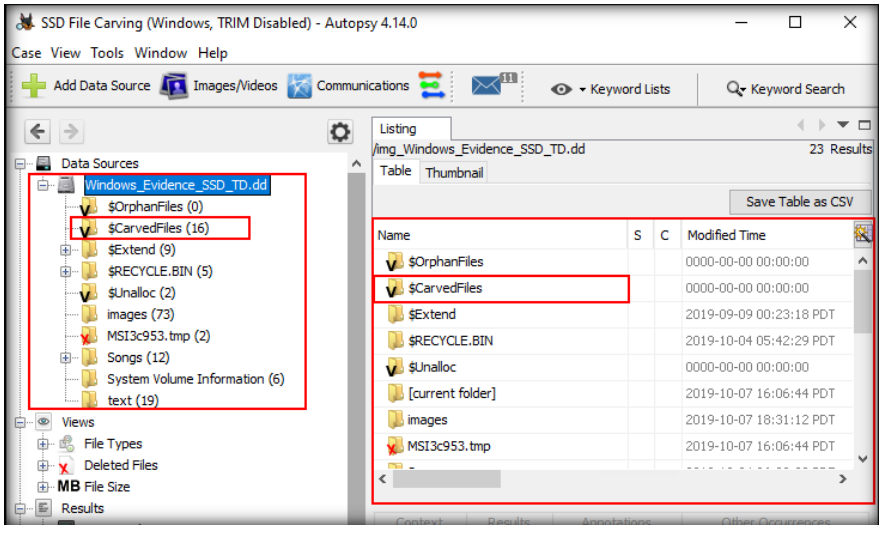

FIGURE 1.21: CarvedFiles Folder loaded

35. To find the carved files, double-click the **CarvedFiles** folder in the right pane of the window. The tool lists a number of carved files, which are all identified by a cross-mark coupled with a knife icon against the file names.

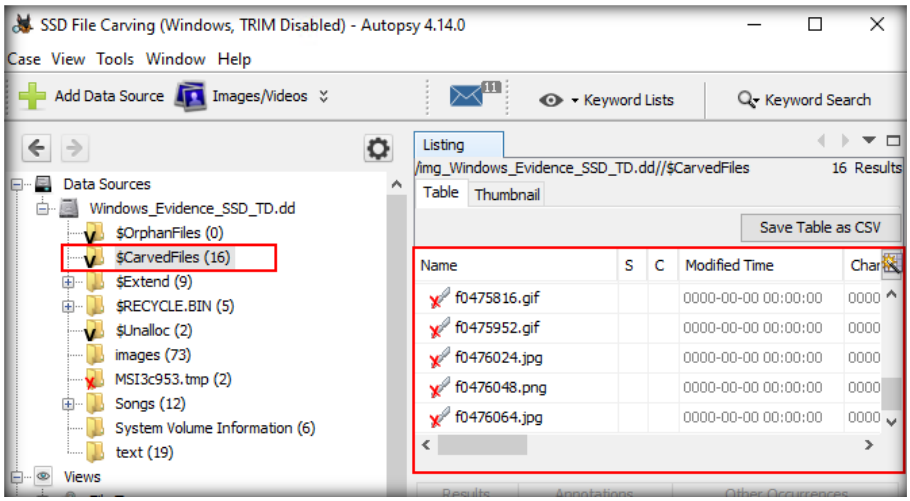

FIGURE 1.22: Viewing Content(s) of CarvedFiles Folder

Note: Once the carved files are loaded, you will also find them under the **Deleted Files** option. Expand the **Deleted Files** node to find the category **All** under it. Select **All** and then scroll down the list of files in the right pane to locate those carved files. Hence, you can alternatively recover those carved files from **All** under **Deleted Files**.

36. To view the content of a carved file, select the file. Its content will be displayed in the lower pane of the tool window. Here, we have selected the file **f0475952.gif**; the content of this file is displayed in the lower pane of the window.

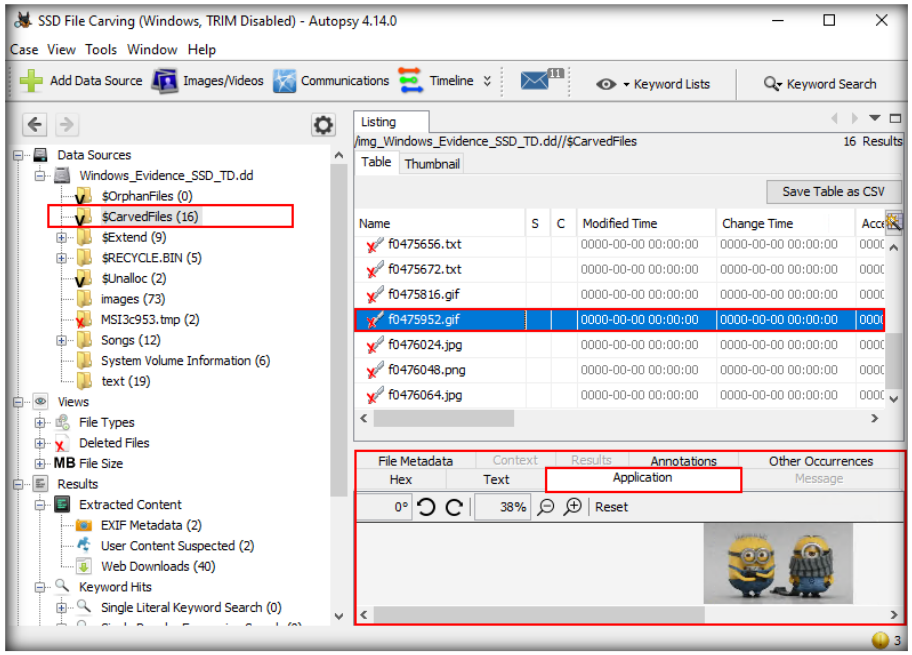

FIGURE: 1.23: Viewing Carved File Content

Note: When you select a carved file, the tool will display its content(s) under the **Application** tab of the lower pane by default. You may also click on the **Hex, Text, File Metadata**, and other tabs to view the respective data stored under them.

37. Now, to recover the selected carved file, right-click on it and then click **Extract File(s)** from the context menu.

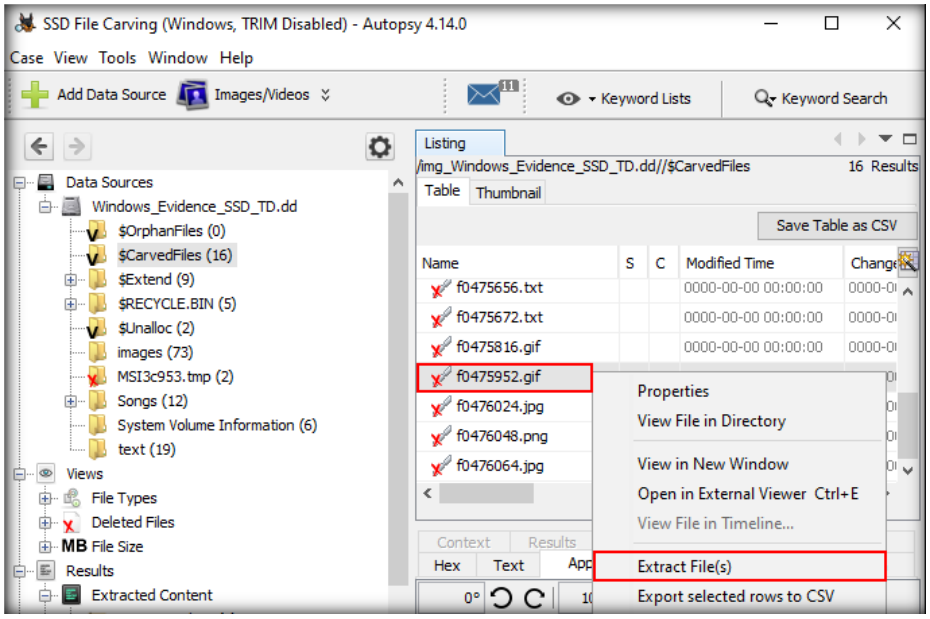

FIGURE 1.24: Extracting a selected Carved File

38. A **Save** window opens, showing the default location where the file will be exported. This default location is the **Export** sub-folder that exists within the case folder created in the **Image File Analysis** folder on the Desktop. Click **Save** to export the file.

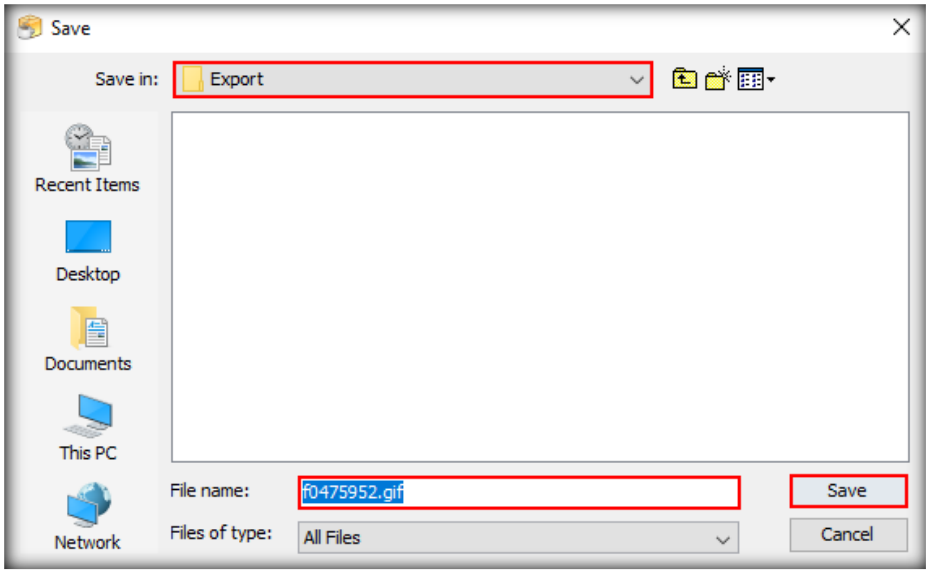

FIGURE 1.25: Saving a Carved File

39. A pop-up appears, indicating that the file has been extracted. Close the pop-up or click **OK**.

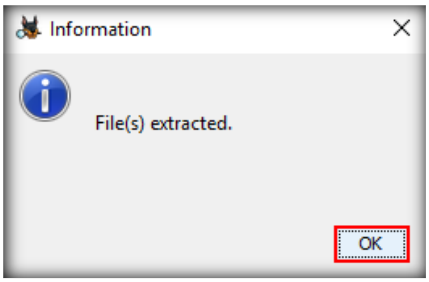

FIGURE 1.26: File(s) extracted pop-up

40. Now, manually navigate to the location where the carved image file has been saved. The location is **C:\Users\Administrator\Desktop\Image File Analysis\SSD File Carving (Windows, TRIM Disabled)\Export**.

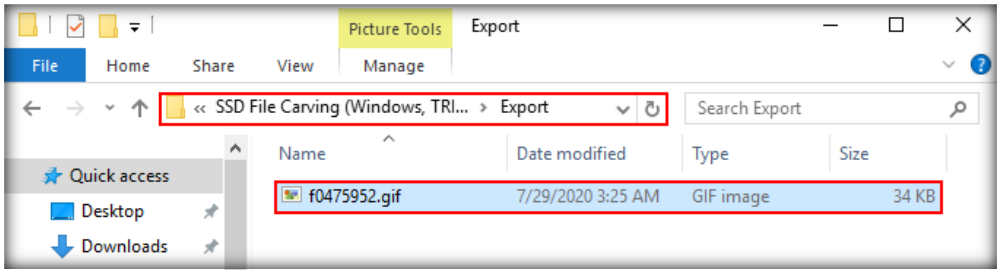

FIGURE 1.27: Location of Exported Image File

41. In this case, we were able to retrieve and view the file's content(s) because it has been acquired from the disk when **TRIM** was disabled on it.

42. Similarly, you can also retrieve and view the contents of other carved files.

Lab Analysis

Analyze and document the results related to this lab exercise. Submit your opinion and experience with Autopsy for Windows file carving.

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

Lab

2

SSD File Carving on a Linux File System

File carving is a technique to recover files and fragments of files from unallocated hard disk space in the absence of file metadata. SSD file carving on a Linux file system is performed using the forensics tool Autopsy.

ICON KEY

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

Lab Scenario

Sam, a forensic investigator, is supposed to perform file carving on a forensic image file of an SSD acquired from a Linux file system. Law enforcement agents acquired the image from the machine of a suspect who is accused in performing nefarious activities. Now, the forensic investigator should use file carving techniques to recover more data related to the case. To do so, the investigator should possess knowledge of the file system structure to identify and recover files and fragments of files from the unallocated space of the SSD in the absence of file metadata.

As a forensics investigator, you should know how to perform SSD file carving on a Linux file system.

Lab Objectives

The objective of this lab is to help you understand how to perform SSD file carving on a Linux file system.

Lab Environment

This lab requires the following:

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

Note: You can download the latest Windows-based version of **Autopsy** from https://www.autopsy.com/download/

If you use 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: 20 minutes

Overview of the Lab

This lab familiarizes you with the Autopsy tool and helps you understand how to recover data from a Linux file system on an SSD when the TRIM functionality is disabled.

Lab Tasks

TASK 1

File Carving on Linux File System (Using Windows)

1. Login to **Windows Server 2016** virtual machine.
2. Double click the **Autopsy 4.14.0** shortcut icon located on **Desktop** to launch the application.
3. The main window of **Autopsy**, along with its **Welcome** window, will open.
4. Click on the **New Case** option in Autopsy **Welcome** window.

FIGURE 2.1: Autopsy Welcome window

5. A **New Case Information** window opens, prompting you to input the **Case Name** and **Base Directory**. The base directory is the location where the case data is to be stored. The case name may be entered according to your identification purpose. In this lab, we assign the case name as **SSD File Carving (Linux File System)**.

6. We will save the case data in the **Image File Analysis** folder located on **Desktop**. So, assign this folder as the **Base Directory** and click **Next**.

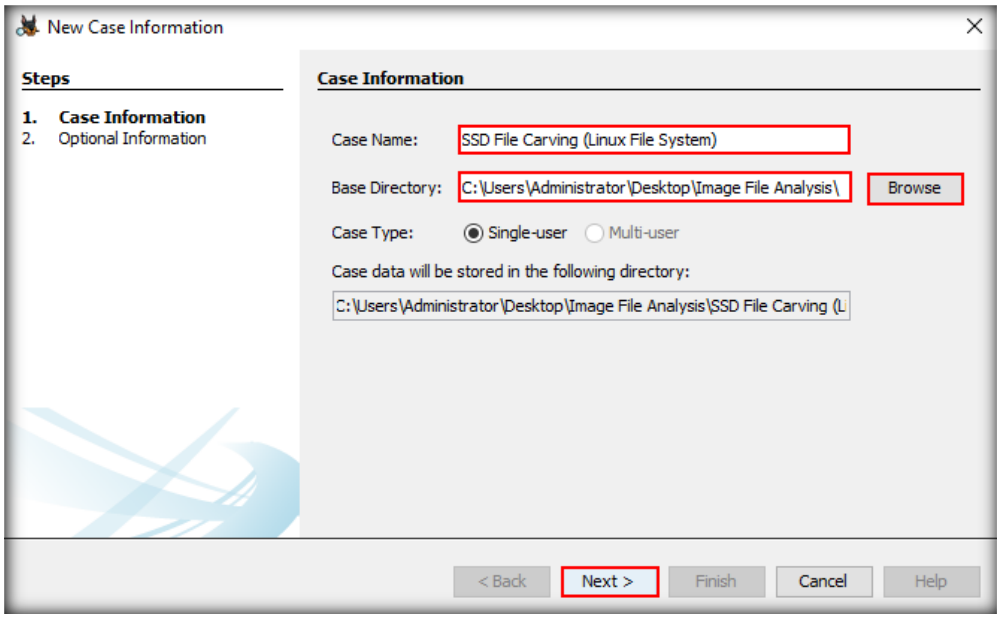

FIGURE 2.2: Autopsy New Case Information Window

7. The **Optional Information** section appears. Provide the **Case Number** and **Examiner Details** (here, we have entered the **Case Number** as **101**). You may enter your details in the **Examiner** section. Click **Finish**.

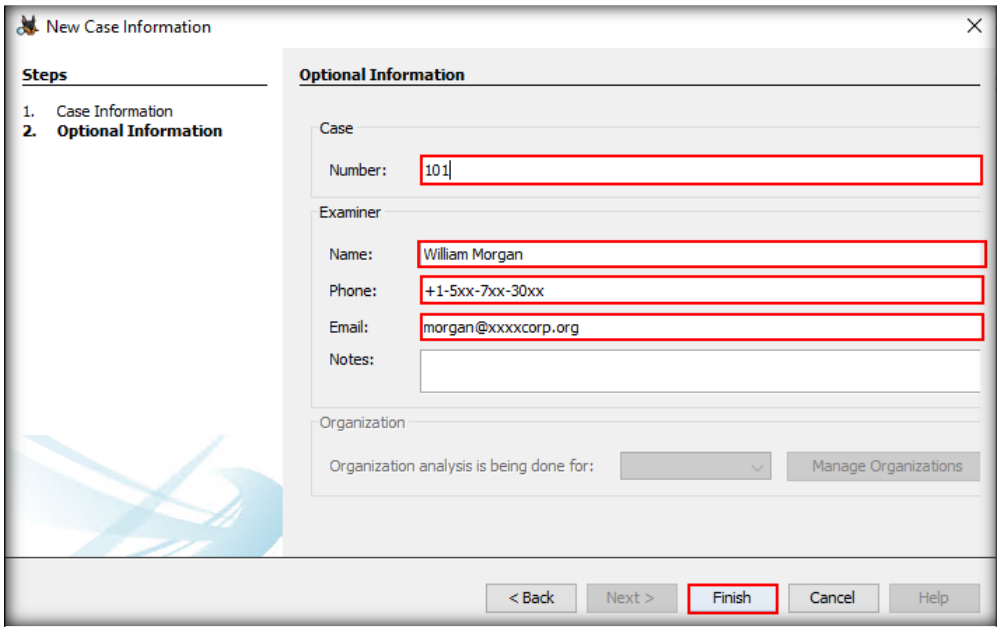

FIGURE 2.3: Autopsy Optional Information Section

8. The application takes a moment to create the case. Subsequently, the **Add Data Source** window appears, displaying the **Select Type of Data Source to Add** section. Ensure that the option **Disk Image or VM File** is selected and click **Next**.

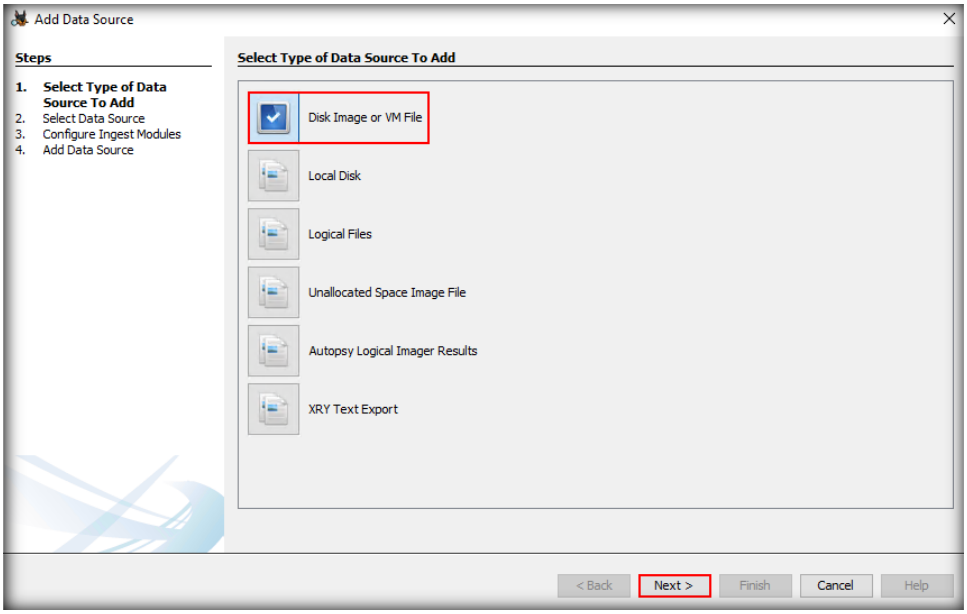

FIGURE 2.4: Autopsy Add Data Source window – Select Type of Data Source to Add section

9. The **Select Data Source** section appears. Click **Browse**.

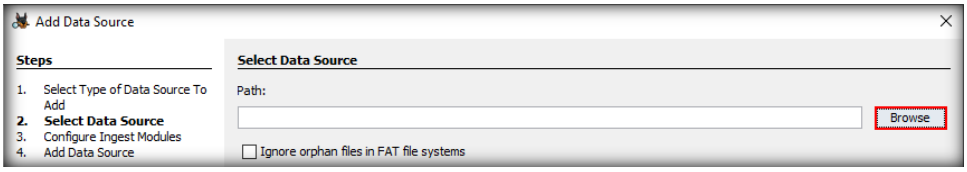

FIGURE 2.5: Autopsy Select Data Source section

10. An **Open** window appears. Navigate to the location **C:\CHFI-Tools\Evidence Files\Forensic Images**, and select the file **Linux_Evidence_SSD.dd**. Click **Open**.

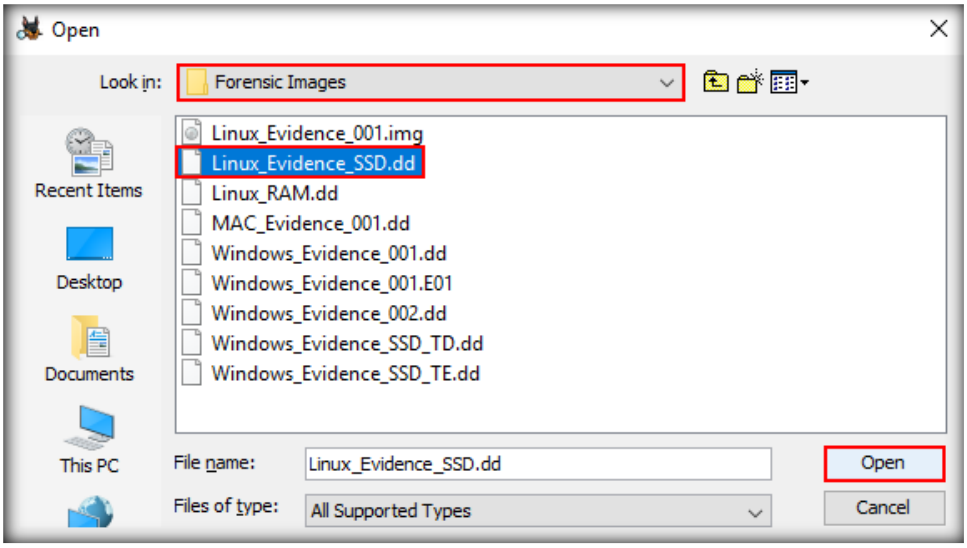

FIGURE 2.6: Autopsy Open window

11. The **Select Data Source** section now displays the path to the **Linux_Evidence_SSD.dd** file in the **Path** field. Click **Next**.

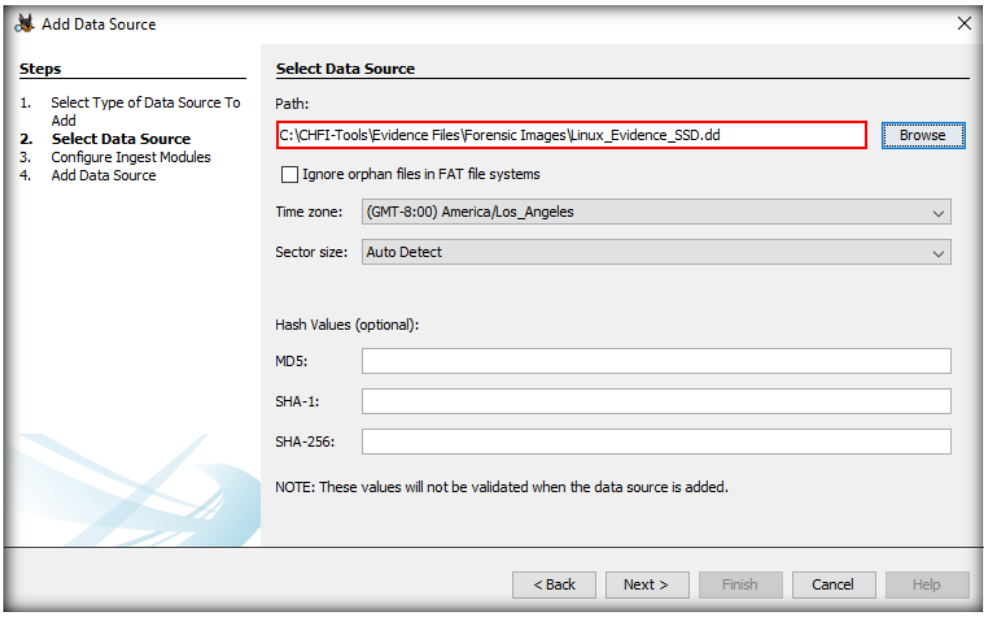

FIGURE 2.7: Autopsy Select Data Source section

12. The **Add Data Source** window now displays the **Configure Ingest Modules** section, which contains a list of options that are checked. Select the options according to your requirement. You may also leave these options set to default. Click **Next**.

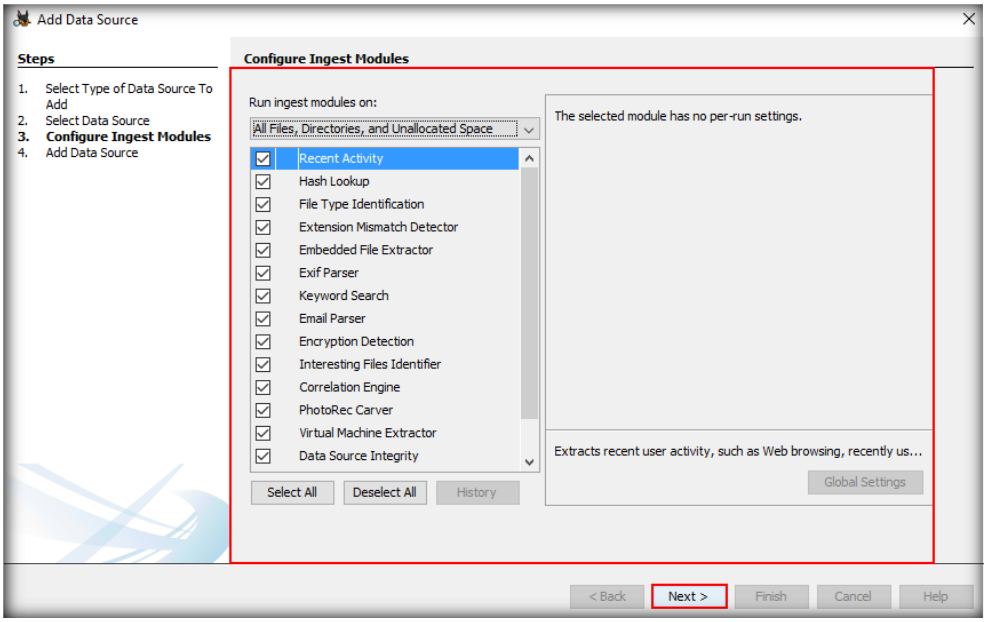

FIGURE 2.8: Configure Ingest Modules section

13. The **Add Data Source** section now appears, displaying the following message: **Data Source has been added to the local database. Files are being analyzed**. Click **Finish**.

Note: Autopsy tool will take some time to analyze the image

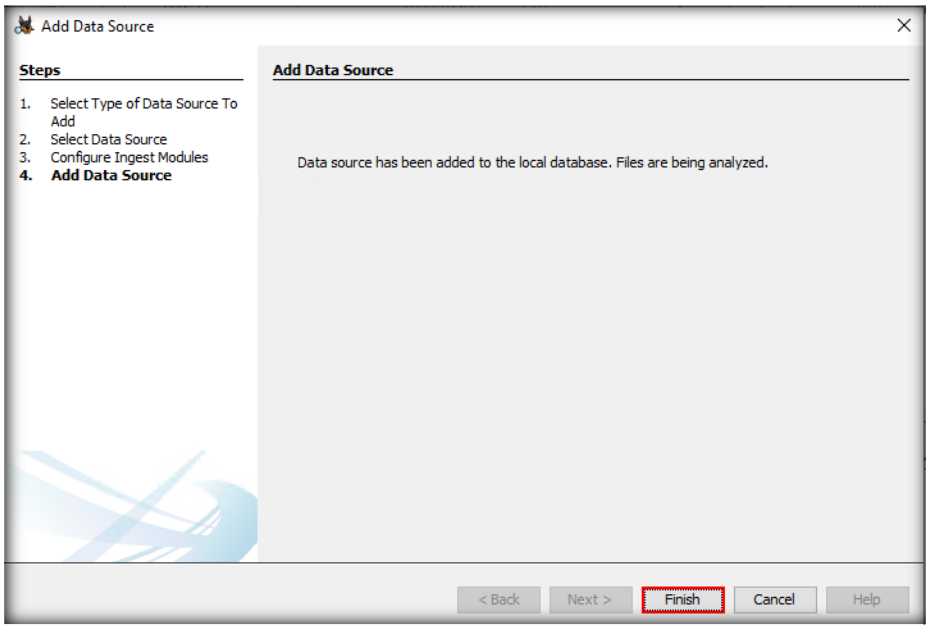

FIGURE 2.9: Add Data Source section

14. The tool will now take you to its main window. Expand the **Data Sources** node in the left pane of the window. The **Data Sources** option will list the name of the image file you have analyzed (in this case, it is **Linux_Evidence_SSD.dd**).

15. Click the image file name (here, **Linux_Evidence_SSD.dd**) to view its contents in the right pane of the tool window. It includes all the necessary operating system data.

Note: Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is completed.

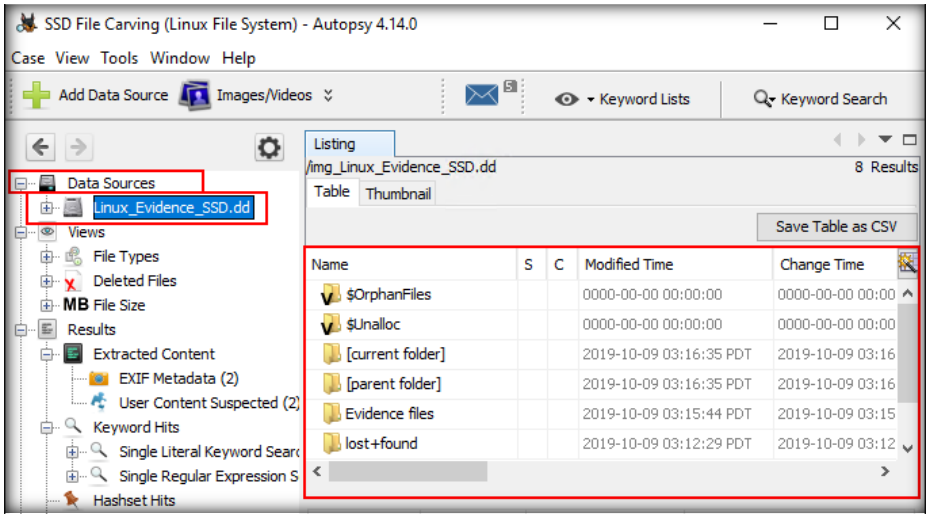

FIGURE 2.10: Viewing the contents of Linux_Evidence_SSD.dd

16. The image file contains folders that store data related to files, processes, services, tools, etc., used on a Linux system.

17. In this lab, our goal is to retrieve carved files. So, after clicking on the evidence file (i.e., **Linux_Evidence_SSD.dd**) in the left pane, we need to wait for 10–15 minutes to let the **Carved Files** folder be loaded in the right pane of the window.

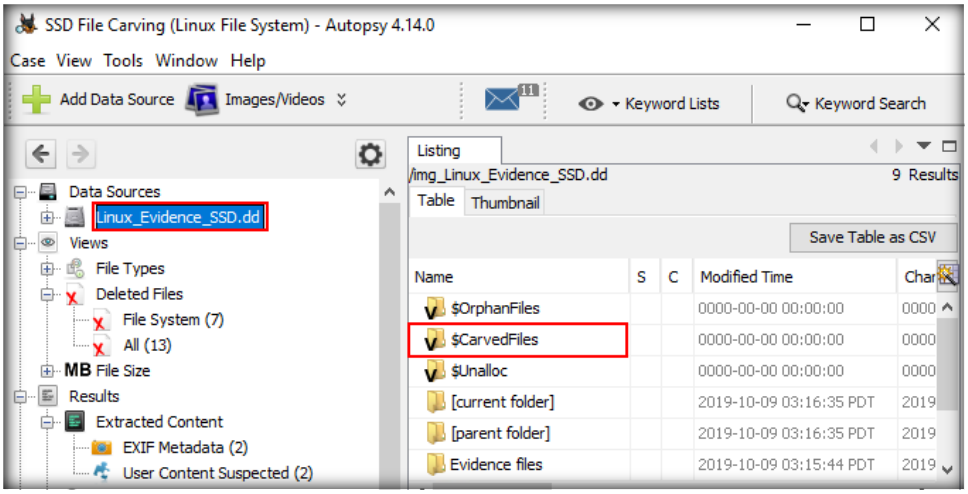

FIGURE 2.11: Carved Files Folder loaded

Note: As we can see in the screenshot above, the **Carved Files** folder has been loaded by the application in the right pane of the window after waiting for a few minutes.

18. Now, we will view the contents of **Carved Files**. Double click the **Carved Files** folder in the right pane of the window to find the carved image files stored within it.

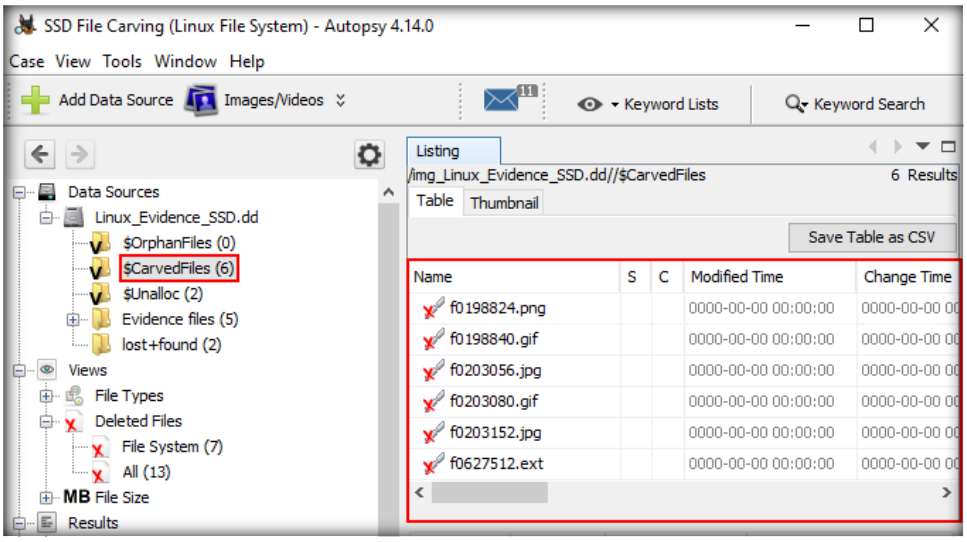

FIGURE 2.12: Viewing Contents of Deleted Files

19. Click on one of the carved image files (here, it is **f0203056.jpg**) to view its content and details in the lower pane of Autopsy's main window. By default, the

tool will display the image file's content under the **Application** tab, as highlighted in the screenshot below. Similarly, you may click the **Hex**, **Text**, **File Metadata**, and other tabs to view the respective data stored under them.

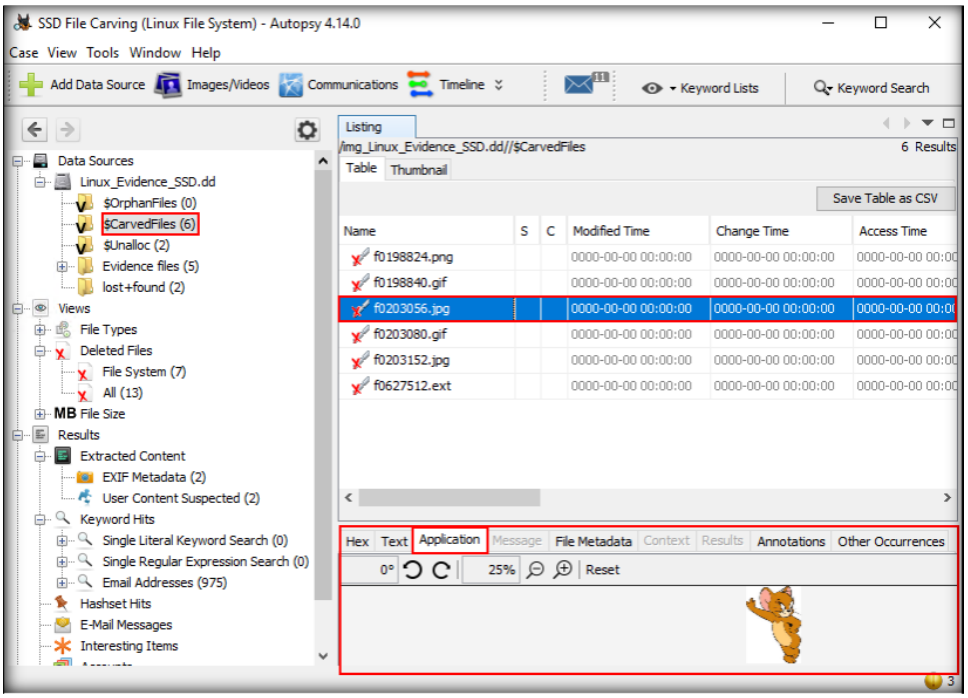

FIGURE 2.13: Viewing Content(s) of carved image files

20. To recover the selected carved file, right-click on the file and select **Extract File(s)** from the context menu.

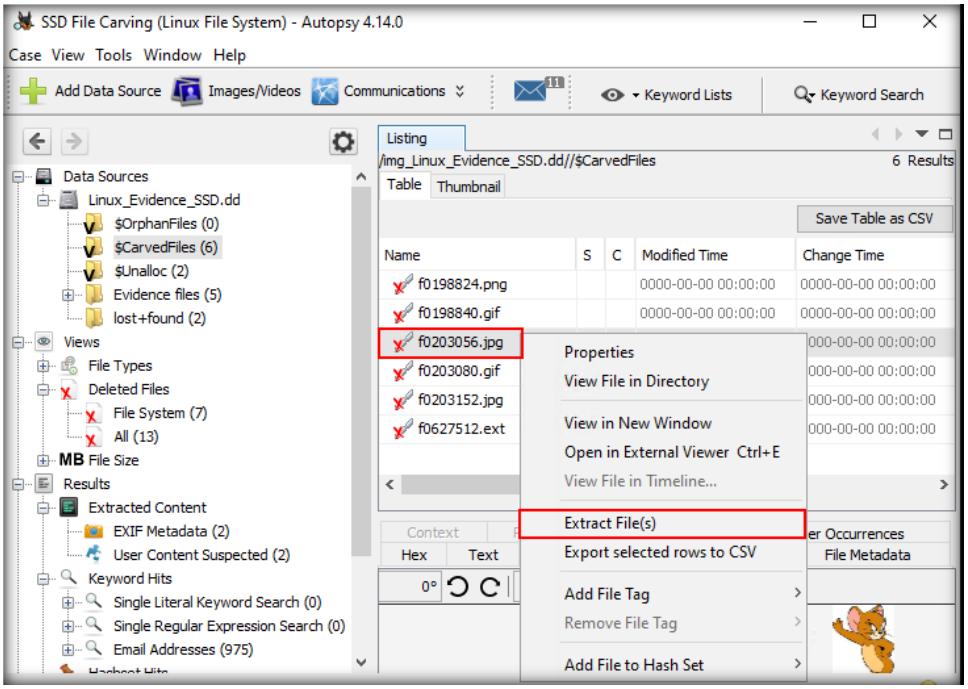

FIGURE 2.14: Recovering/Extracting a File

21. A **Save** window opens, showing the default location where the extracted file will be saved. This default location is the **Export** sub-folder within the case folder created on the Desktop. Click **Save** to export the file.

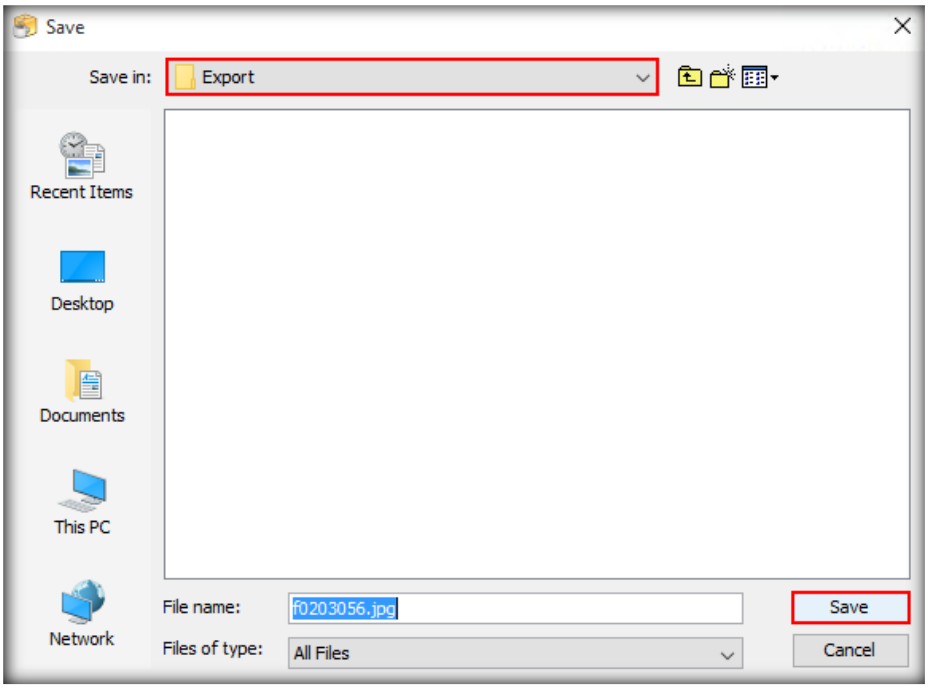

FIGURE 2.15: Exporting a file

22. A pop-up appears, indicating that the file has been extracted. Close the pop-up or click **OK**.

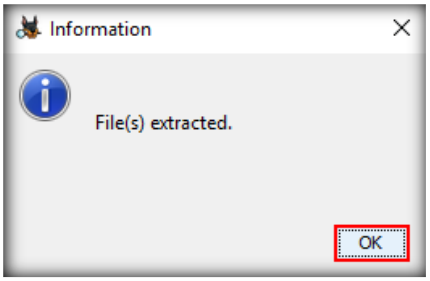

FIGURE 2.16: File(s) extracted pop-up

23. Now, manually navigate to the location where the exported image file has been saved. The location is **C:\Users\Administrator\Desktop\Image File Analysis\SSD File Carving (Linux File System)\Export**.

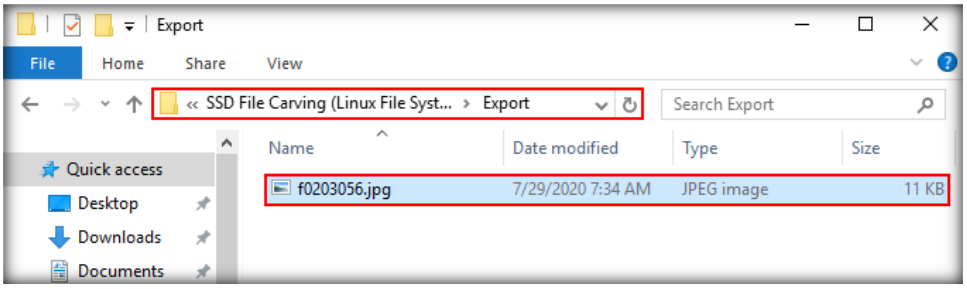

FIGURE 2.17: Image File saved to Export sub-folder in case folder

24. The image file has hence been recovered successfully.
25. Similarly, in this manner, you can recover other carved files.

Lab Analysis

Analyze and document the results related to this lab exercise. Submit your opinion and experience with Autopsy for Linux file carving.

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

Lab

3

Recovering Data from Lost/Deleted Disk Partition

When a partition is deleted from a disk, the files within the disk are lost, and the entries related to the deleted partition are removed by the computer from the MBR partition table. However, as long as the corresponding section of the disk is not overwritten, there is a chance to recover the deleted partition and the files within it.

ICON KEY

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

Lab Scenario

An attacker saved malicious files in one of the disk partitions of the victim's workstation system and executed them to steal sensitive business data. After committing the crime, the attacker deleted the entire disk partition in which they had saved the malicious files to prevent their crime and identity from being detected. The victim discovered that one of the disk partitions on their system was missing. They also found that the system was behaving suspiciously and reported the matter to their organization's cyber-security department. As a part of forensic investigation in this case, investigators must now recover the deleted disk partition so that the files that were stored in it (both normal and malicious files) can be retrieved and the malicious files can be sent for further investigation.

Lab Objectives

The objective of the lab is to help you understand how to recover data from lost/deleted partitions.

Lab Environment

This lab requires the following:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands

- A web browser with internet access
- **EaseUS Data Recovery Wizard** tool, which is already installed on your virtual machine

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

If you use 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: 20 minutes

Overview of the Lab

This lab familiarizes you with EaseUS Data Recovery Wizard and helps you understand how to recover a disk partition that may have been deleted by an attacker. A deleted disk partition may contain vital artifacts pertaining to an attacker's crime.

Lab Tasks

1. Login to **Windows 10** virtual machine.
2. Keep **Windows Server 2016** virtual machine powered **On** during this lab.
3. Before beginning this lab, create a folder named **Recovered Partition** in the **D** drive, (which has approximately 10 GB of free space).

TASK 1

Scan for Deleted Disk Partition Using EaseUS Data Recovery Wizard

4. Launch the **EaseUS Data Recovery Wizard** tool by double-clicking on its short-cut icon on the Desktop (since we have already installed the application in the lab **Recovering Data from a Windows Hard Disk** in **Module 02**).

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

5. The **EaseUS Data Recovery Wizard** tool window will open. Hover the mouse-pointer over **Lost Partition-1** so that you see the **Scan** button below it. Click **Scan**. Here, **Lost Partition-1** denotes the partition that was deleted/lost.

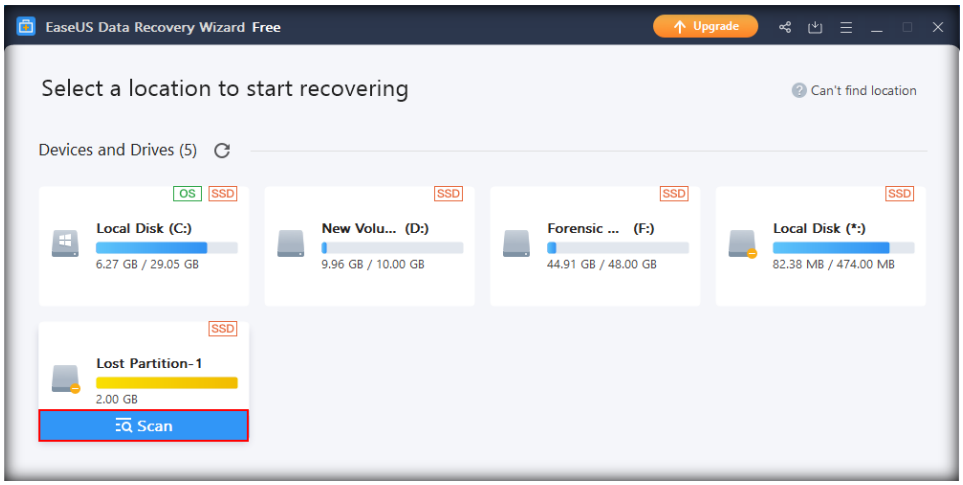

FIGURE 3.1: Select a location to start recovering

Note: If an **EaseUS Data Recovery Wizard** pop-up appears on the bottom right corner of the window, **close** it.

6. The tool will run an advanced scan, following which it will display an icon for the deleted partition (**Lost Partition-1**) in a new window. The Lost Partition-1 icon can be found in the left pane of the window at the top. Below **Lost Partition-1**, you will also find a folder named **Lost Files**, and the same can be found in the right pane, as shown in the screenshot:

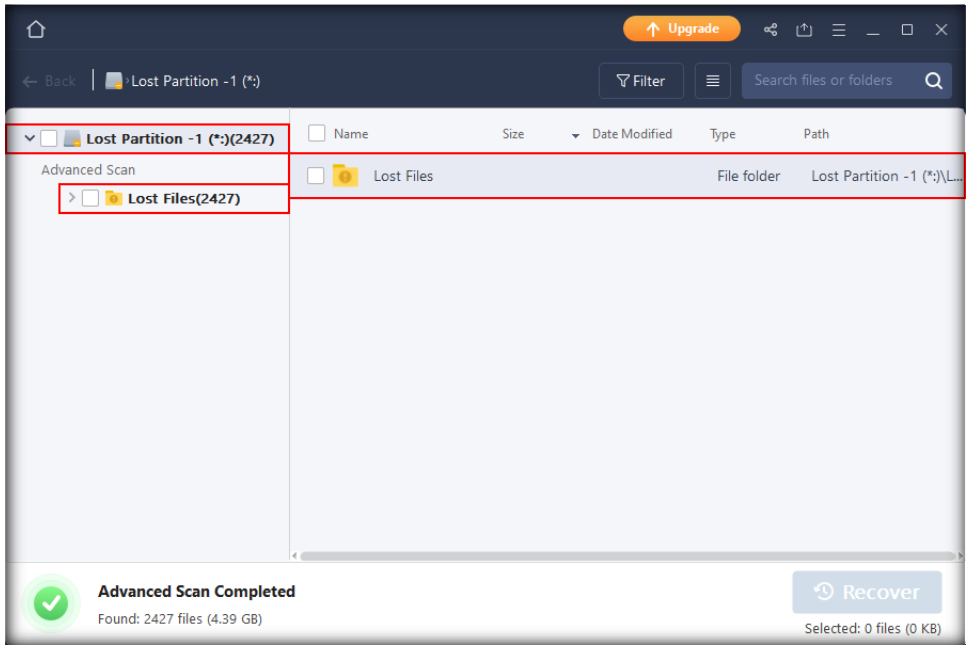

FIGURE 3.2: Advanced Scan Completed

Note: The number of files listed in the **EaseUS** window might differ in your lab.

7. To view the contents of the **Lost Files** folder, expand the **Lost Files** node. On expanding the node, the contents of the folder will be displayed as shown in the following screenshot:

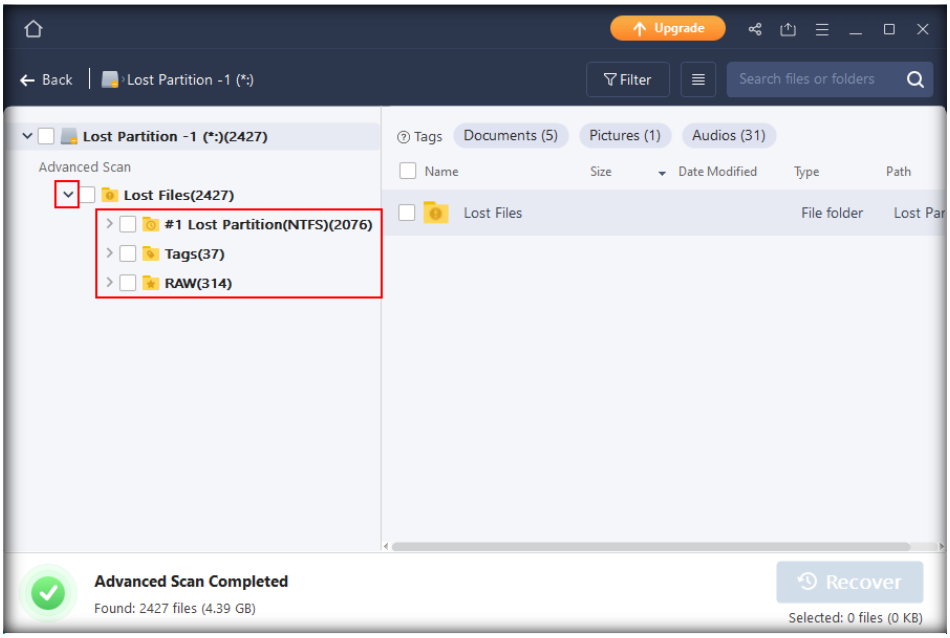

FIGURE 3.3: Expand Lost Files

8. Expand the **Lost Partition(NTFS)** folder to view the data that resides in it. Under the **Lost Partition** folder is a list of folders. Click on any one of them to view the contents. In this lab, we will view **Audio Files**.

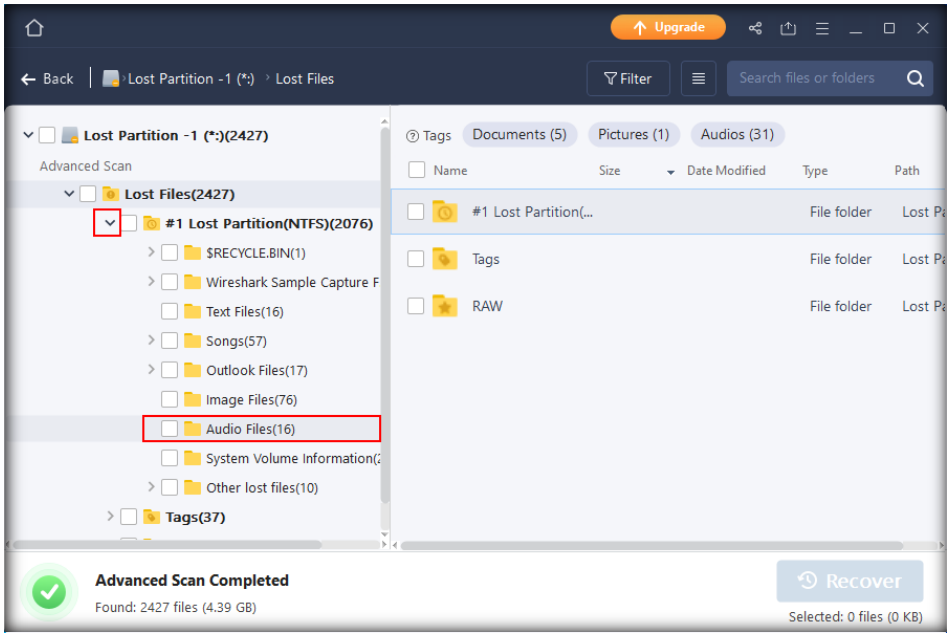

FIGURE 3.4: Find Evidence Files under Lost Partition (NTFS)

9. All the audio files will be listed in the right pane, as shown in the following screenshot:

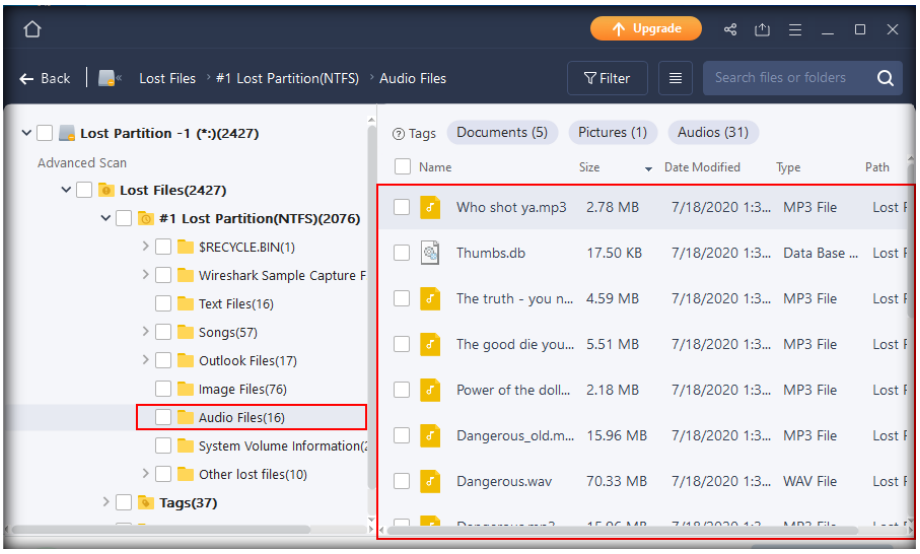

FIGURE 3.5: Viewing contents of Evidence Files folder

10. Similarly, the **Tags** and **RAW** folders are a part of the **Lost Files** folder. To view the contents under these folders, expand them. Further, to view the contents of the sub-folders of the Tags and RAW folders, click on those sub-folders so that their contents are listed in the right pane of the tool window.

TASK 2

Recover Deleted Partitions and Their Contents

11. Since the objective of this lab is to recover an entire lost/deleted partition, we will check the **Lost Partition-1** icon at the top in the left pane of the window. On checking the **Lost Partition-1** icon, all the data residing in that partition are checked, and the **Recover** button at the bottom right of the window is enabled.

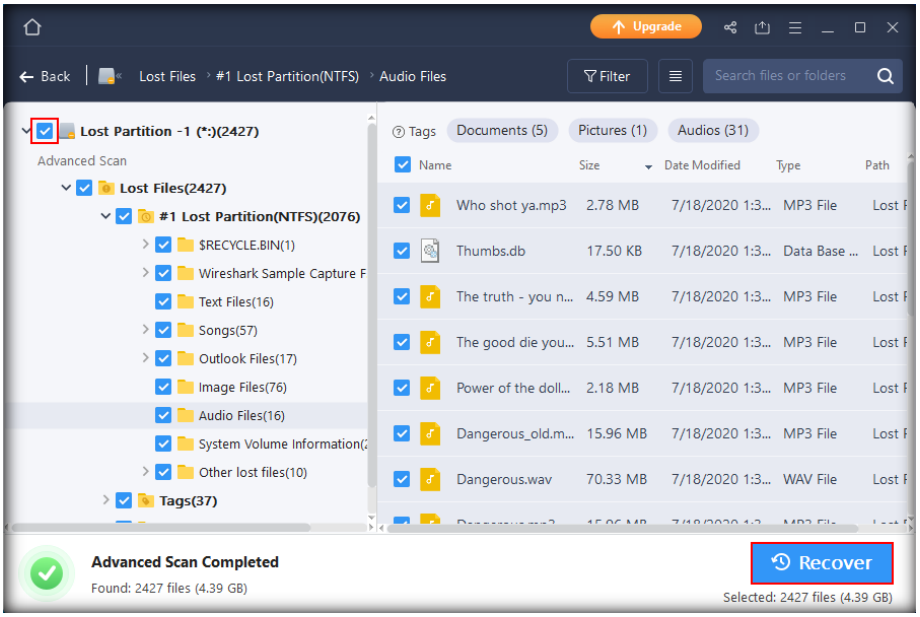

FIGURE 3.6: Check Lost Partition-1 icon to select all deleted partition data

12. Now, to recover the partition, click the **Recover** button

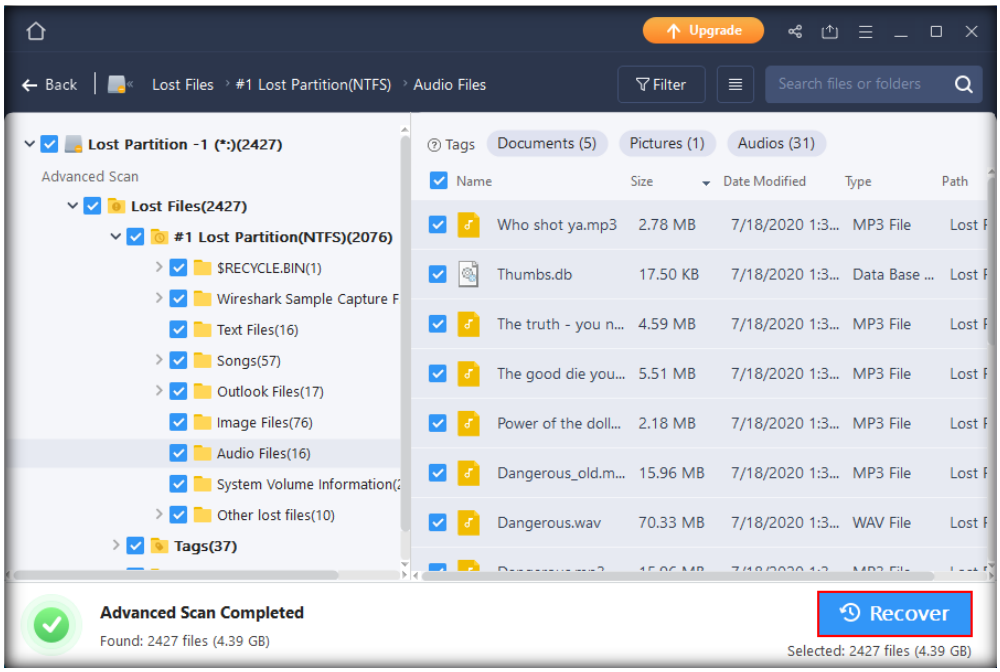

FIGURE 3.7: Click 'Recover' button

13. A **Browse for Folder** window appears. Under the **D** drive, select the **Recovered Partition** folder, which we had created at the beginning of the lab, and then click **OK**. All the data that was stored in the deleted partition will be recovered and saved to the **Recovered Partition** folder.

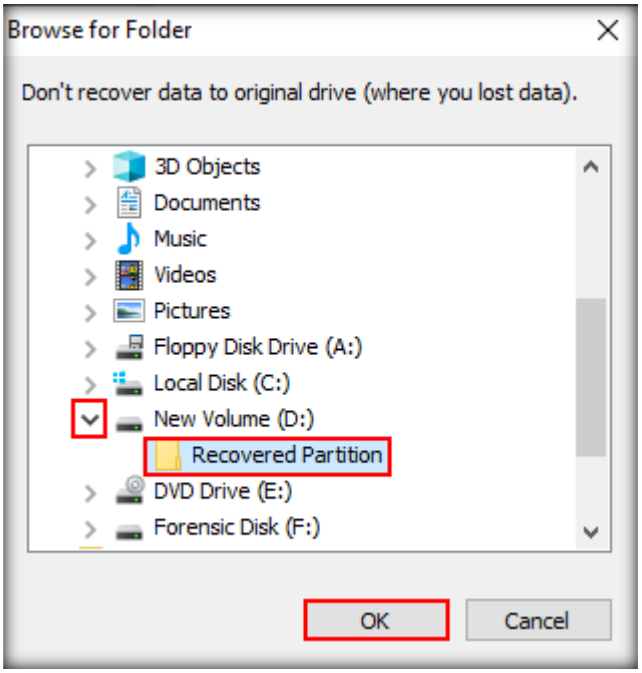

FIGURE 3.8: Select 'Recovered Partition' folder

14. **EaseUS** begins to recover the files as shown in the following screenshot:

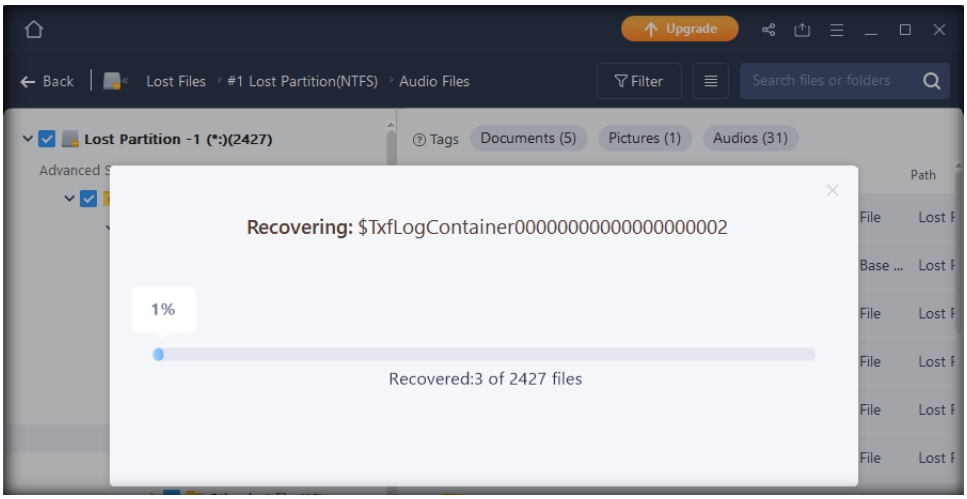

FIGURE 3.9: EaseUS recovering data

15. At a certain point, the application pauses the recovery and gives you two options. Since this is a trial version, you will not be able to recover all the files for free. You may click on **Continue Recovering** and buy a premium version or click on **Don't Recover Any More**. In this lab, we are choosing **Don't Recover Any More** option.

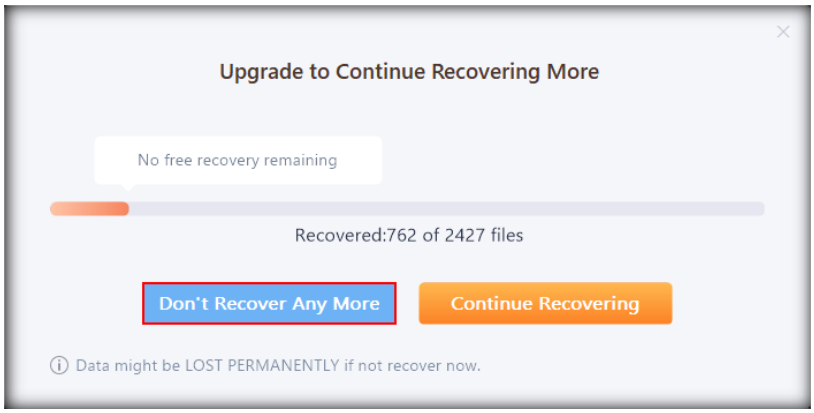

FIGURE 3.10: EaseUS Upgrade Window

16. Upon clicking **Don't Recover Any More**, the application automatically directs you to the location where the data from the deleted partition has been saved.

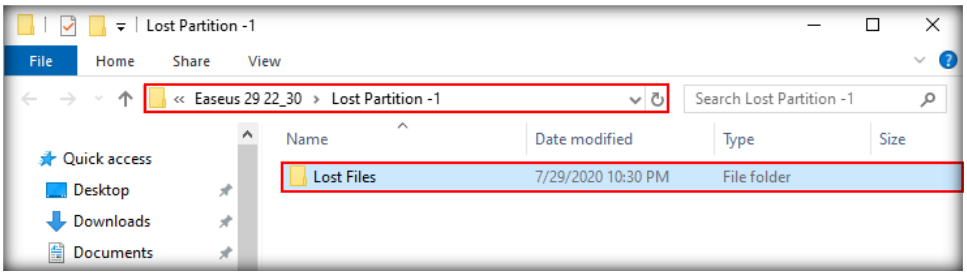

FIGURE 3.11: Recovered Partition folder

17. **EaseUS** auto-creates a series of sub-folders inside the **Recovered Partition** folder. The **Recovered Partition** folder will have an **EaseUS** folder in the following format: **Easeus [DD HH_MM]**, where **DD** denotes the **date**, **HH** denotes the **hours**, and **MM** denotes the **minutes**; all the recovered data will be saved in the **Easeus [DD HH_MM]** folder through a series of sub-folders.
18. In this manner, you can recover the contents of a deleted partition using **EaseUS Data Recovery Wizard**. **Close** the application.

Lab Analysis

Analyze and document the results related to this lab exercise. Submit your opinion and experience with the tool used.

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

Lab

4

Recovering Data from a Partition that is Deleted and Merged into another Partition

When a partition is deleted from a disk, the files within the disk are lost, and the entries related to the deleted partition are removed by the computer from the MBR partition table. However, as long as the corresponding section of the disk is not overwritten, there is a chance to recover the deleted partition and the files within it.

ICON KEY

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

Lab Scenario

An attacker saved malicious files in one of the disk partitions of the victim's workstation system and executed them to steal sensitive business data. After committing the crime, the attacker deleted the entire disk partition in which they had saved the malicious files to prevent their crime and identity from being detected. To complicate things further, the attacker merged this partition into another. The victim discovered that one of the disk partitions on their system was missing, and the size of another partition has increased by the size of the deleted partition. They reported the matter to the organization's cyber-security department. As a part of forensic investigation in this case, investigators must now recover data from the partition that existed earlier so that the files that were stored in it (both normal and malicious files) can be retrieved and the malicious program files can be taken up for further investigation.

Lab Objectives

The objective of the lab is to help you understand how to recover data from a partition that is deleted and merged into another partition.

Lab Environment

This lab requires the following:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands
- A web browser with internet access
- **R-Studio** located at **C:\CHFI-Tools\Module 05 Defeating Anti-Forensics Techniques\Partition Recovery Tools\R-Studio**

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques

Note: You can download the latest version of **R-Studio** from https://www.r-studio.com/Data_Recovery_Download.shtml

If you use 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: 20 minutes

Overview of the Lab

This lab demonstrates the following two tasks:

- Extend volume of a disk by merging a deleted partition into it.
- Recover the deleted partition after it is merged into another partition.

Lab Tasks

1. Login to **Windows 10** virtual machine.
2. Keep **Windows Server 2016** virtual machine powered **On** during this lab.
3. This lab is a continuation to the previous lab. In this lab, we will extend the **Forensic Disk** (**F** drive, which already has **48 GB** of storage space) partition by merging the unallocated space of **2 GB** into it. 2 GB is the space that was occupied by the partition that was deleted and will hence show as unallocated space in **Disk Management**.
4. Now, we shall see how to recover the deleted partition using **R-Studio**.

TASK 1

Merge the Deleted Partition

Note: The following operation is performed to create a scenario where the attacker has merged a deleted disk partition with an existing/primary partition, making the forensic investigation process complex.

5. Type **disk management** in the **Search bar** and press **Enter**. Click **Create and format hard disk partitions** option as shown in the below screenshot.

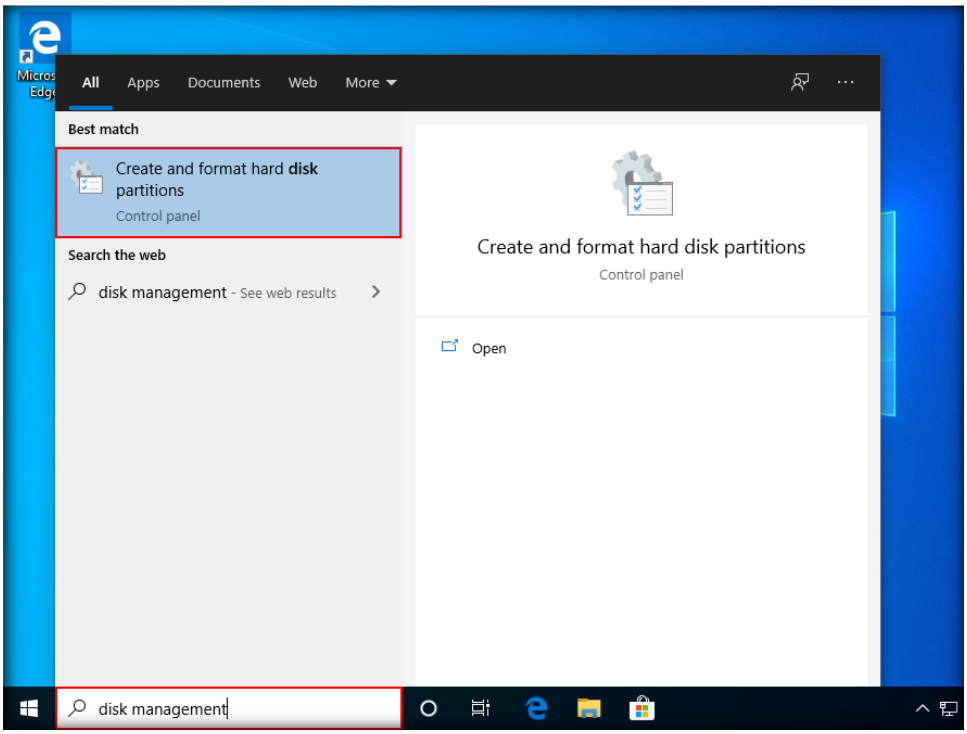

FIGURE 4.1: Search bar

6. The **Disk Management** window appears, where you will find a partition named **Forensic Disk** (**F:**) with **48 GB** of storage listed alongside an unallocated space of **2 GB** in Disk 1 .

7. To extend the volume of the **Forensic Disk** partition, right-click on it and select **Extend Volume...** from the context menu.

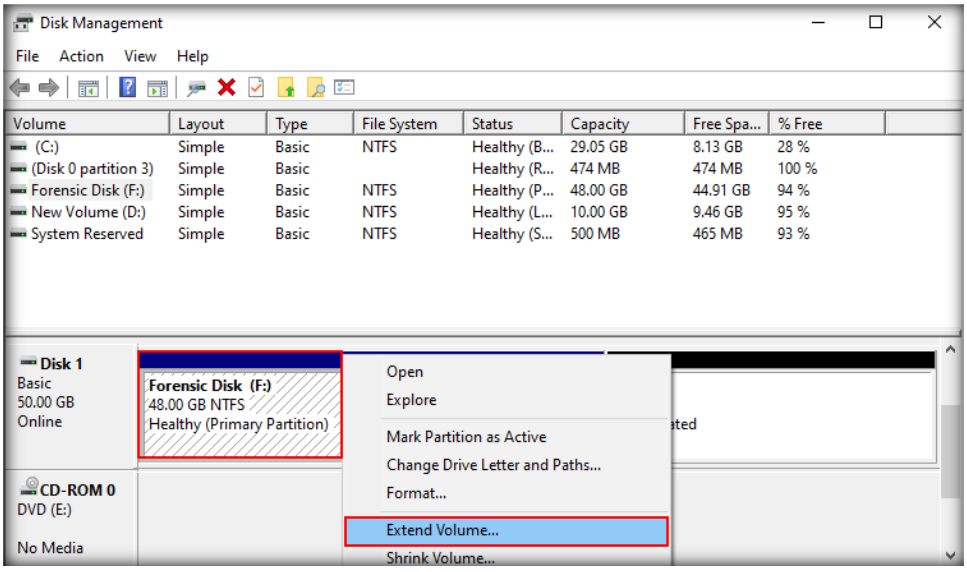

FIGURE 4.2: Disk Management window

8. The **Extend Volume Wizard** appears. Click **Next**.

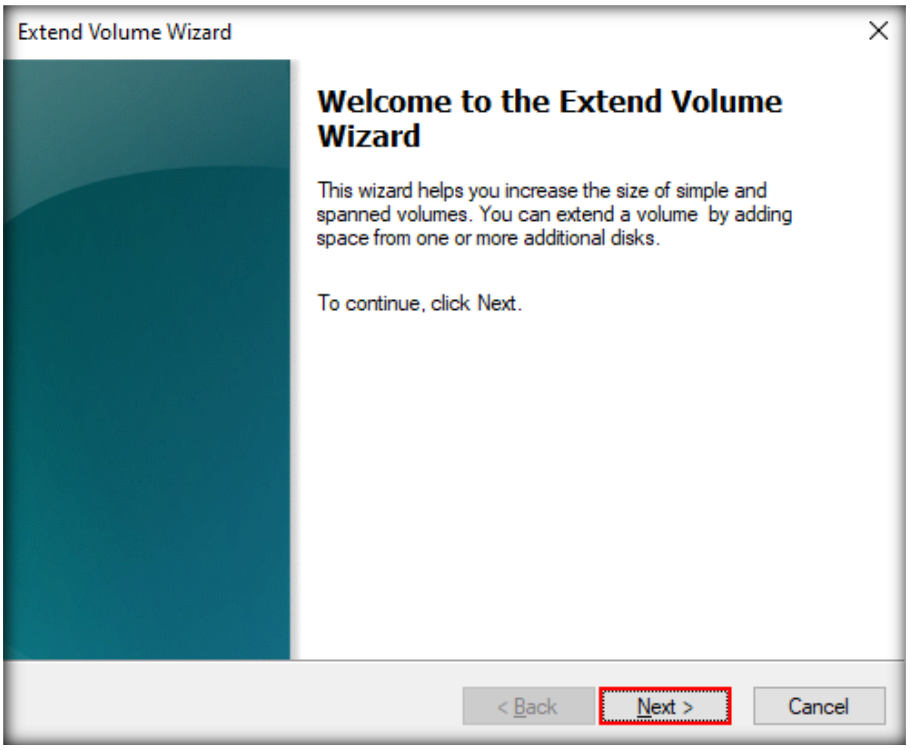

FIGURE 4.3: Extend Volume Wizard

9. The **Select Disk** section of the wizard appears, where you will find the unallocated space in **Disk 1** (**~2 GB**) selected by default. Click **Next**.

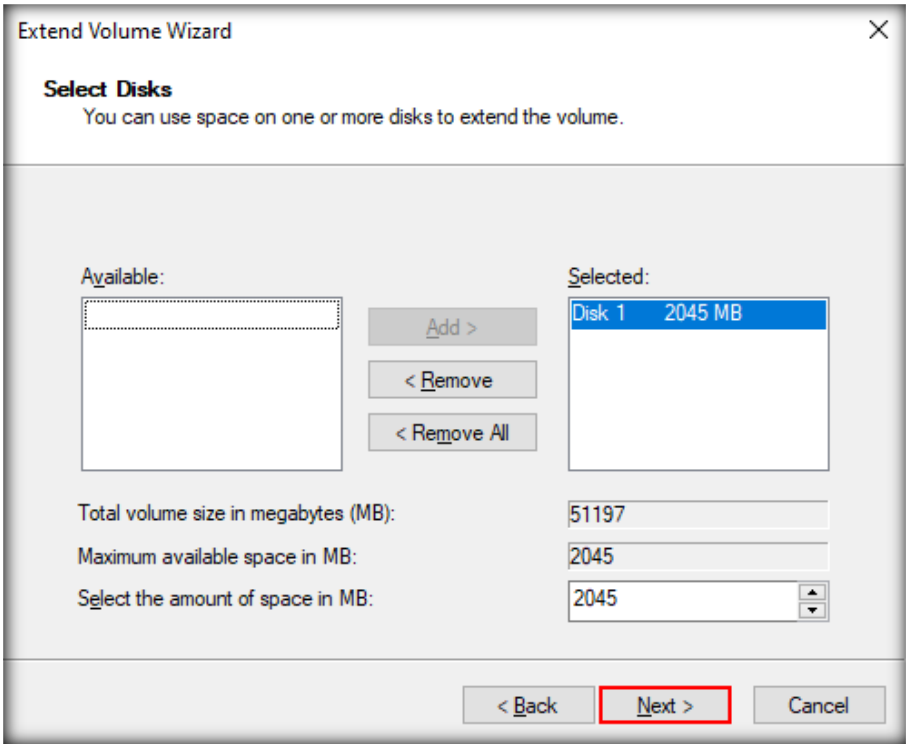

FIGURE 4.4: Select disks to extend the volume

10. The final step of the wizard appears, displaying the disk that was selected in the previous step. Click **Finish**.

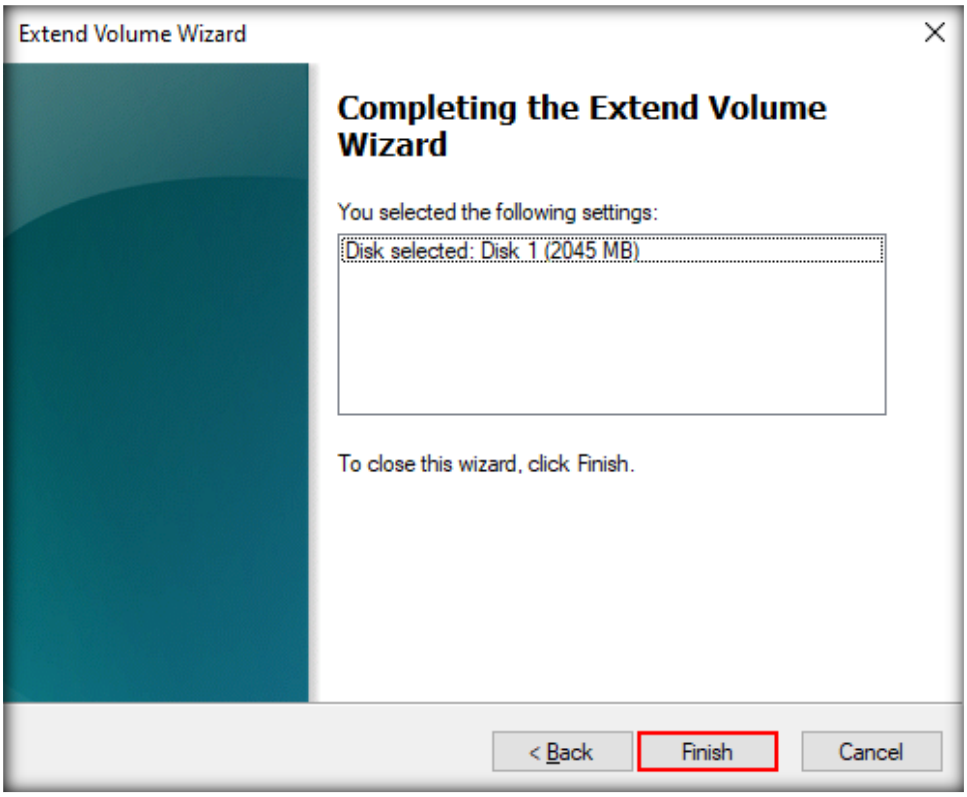

FIGURE 4.5: Click 'Finish' to extend the volume

11. Now, launch **File Explorer** and click on **This PC**. You should be able to observe that the size of the **Forensic Disk (F:)** has increased to **49.9 GB** (**~50 GB**) since we have merged the unallocated space of **2 GB** into it.

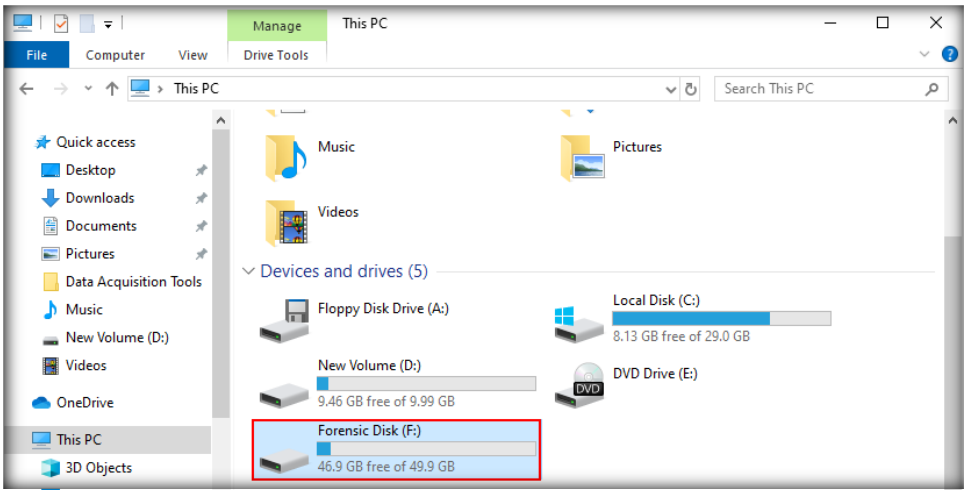

FIGURE 4.6: Unallocated partition merged

TASK 2

Recover Files Using R-Studio

12. We have finished the task of merging the deleted partition into an active partition. Now, we shall recover the files of this partition, (which was deleted and merged into another partition).

13. Navigate to **Z:\CHFIv10 Module 05 Defeating Anti-Forensics Techniques\Partition Recovery Tools\R-Studio** and double-click the **RStudio8.exe** file. An R-Studio pop-up appears, prompting you to choose a language. Select **English** and click **OK**.

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

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

14. Click **Next** and follow the wizard-driven instructions to install the application.

FIGURE 4.7: R-Studio Welcome window

15. In the last step of the installation, check **Launch R-Studio** and click **Finish**.

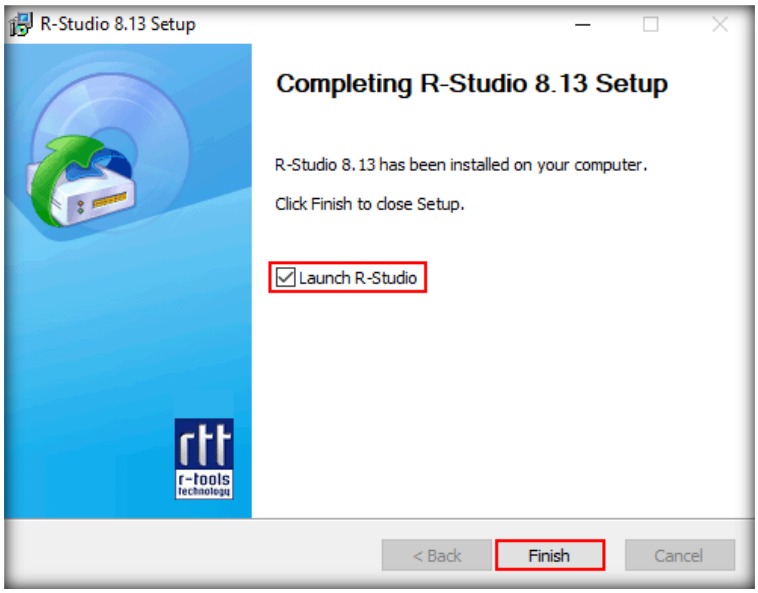

FIGURE 4.8: Checking "Launch R-Studio"

16. Now, the registration window for the tool appears. Click **Demo** to continue.

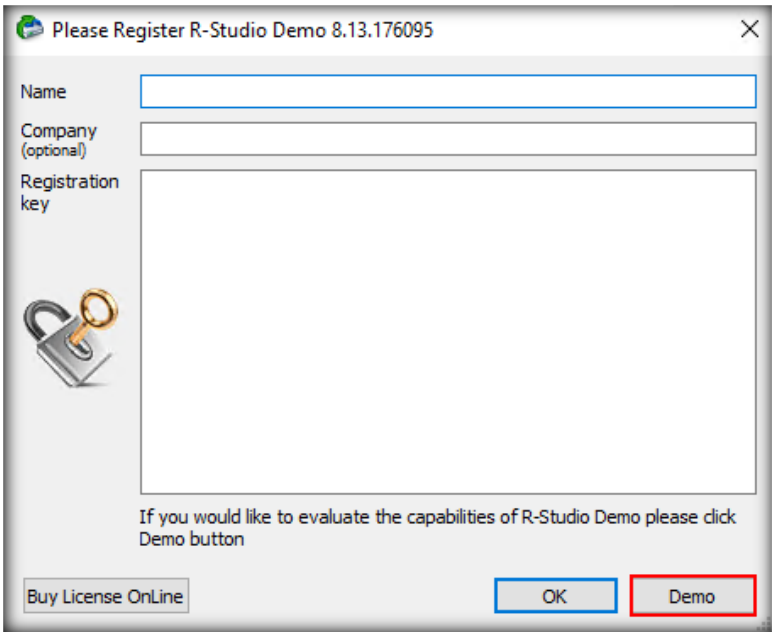

FIGURE 4.9: Click Demo

17. The main window of the tool will now open. We must check for a partition that has been deleted and recover the data in the deleted partition. To check for a deleted partition, we first select an existing partition (here, **F: Drive**) and then click on the **Scan** icon on the toolbar, as shown in the screenshot:

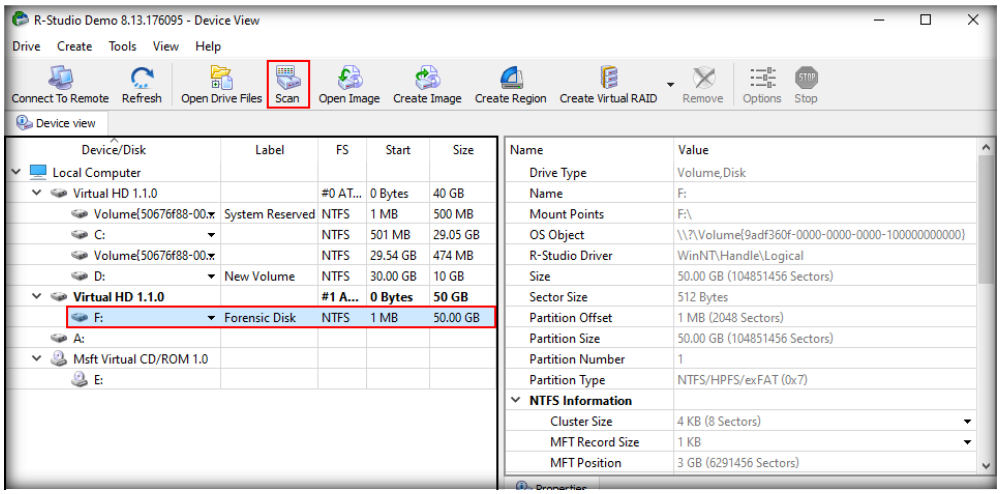

FIGURE 4.10: Scanning a drive

Note: When you select a listed drive/partition, the right pane of the window will display the properties pertaining to that drive/partition, as seen in the screenshot above.

18. The **Scan** window will now appear. Ensure that the **Detailed (Scan progress and found objects. Slower.)** option is selected, and then click the **Scan** button.

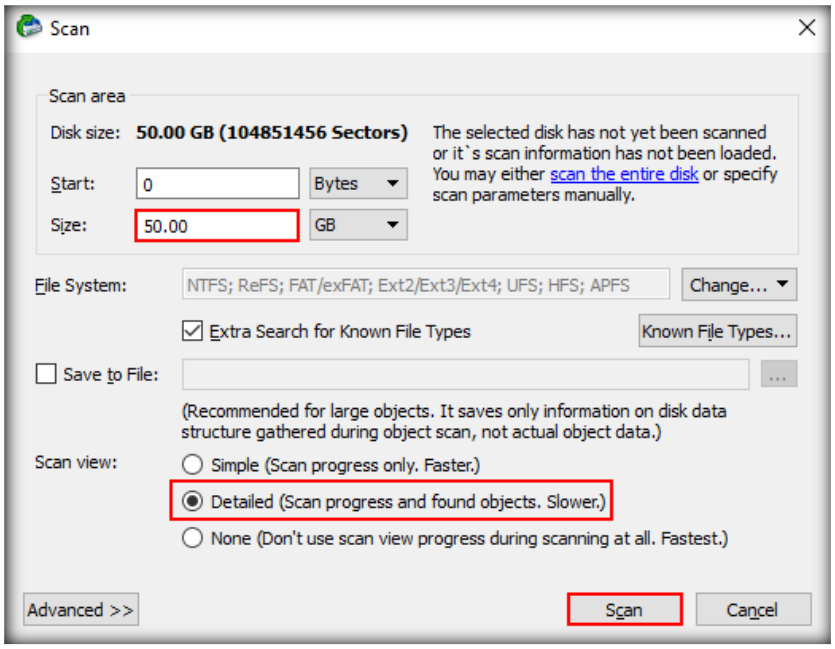

FIGURE 4.11: Scan Window

19. The tool will now start performing a **scan**, and detailed scan information will be displayed in the right pane of the tool window. You can also observe the scan's progress at the bottom of the window.

Note: The scan duration will depend on the storage capacity of the drive being scanned.

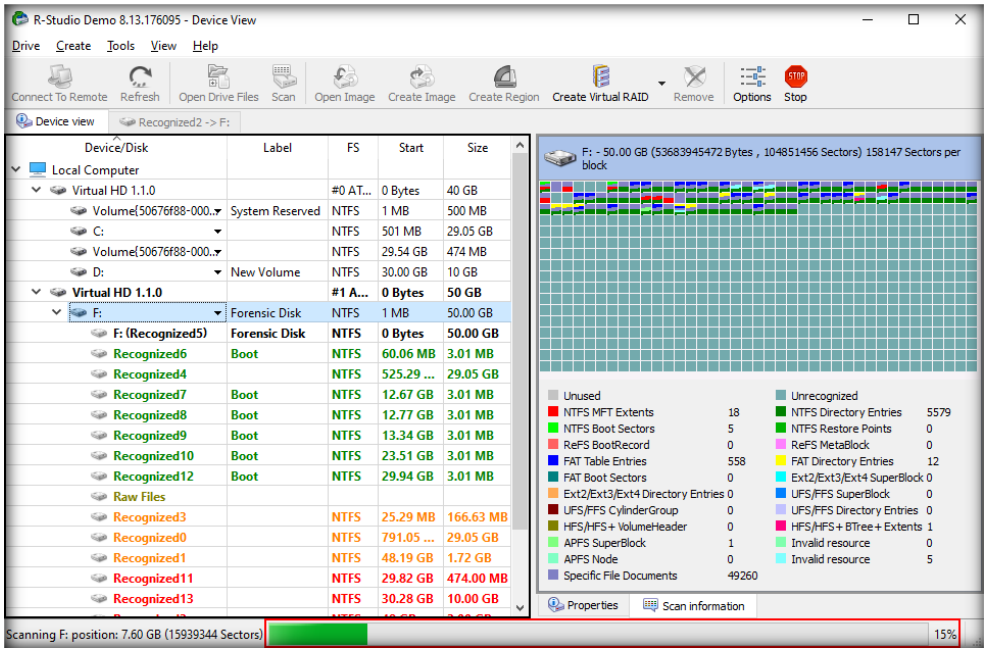

FIGURE 4.12: Scanning Information and Progress

20. Upon completing the scan, the tool will list **Recognized Partition(s)** below the drive that we selected for scanning (here, below the **F:** drive).

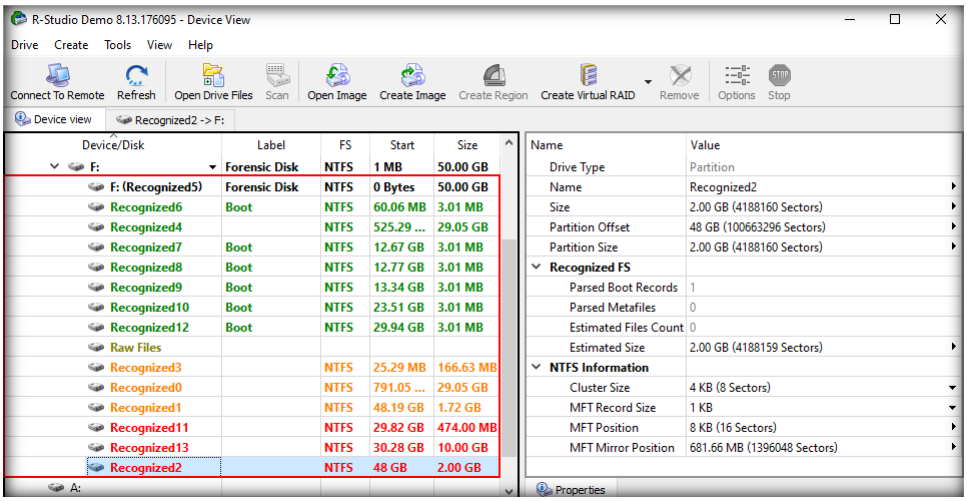

FIGURE 4.13: Recognized Partition(s) list

21. Under the **F:** drive, examine the partition that has been listed as **Recognized2**; the tool shows its size to be **2 GB**, which is unknown space. This indicates that **Recognized2** is the lost/deleted partition with a size of **2 GB** that was merged into the existing **F:** drive, which had a size of **48 GB**, to make it appear as a single disk partition of **50 GB**.

Note: In this lab, the partition has been identified as **Recognized2** by the application. The recognized partition's number might vary in your lab environment.

22. To view the contents of the lost/deleted partition (**Recognized2**), double click it.

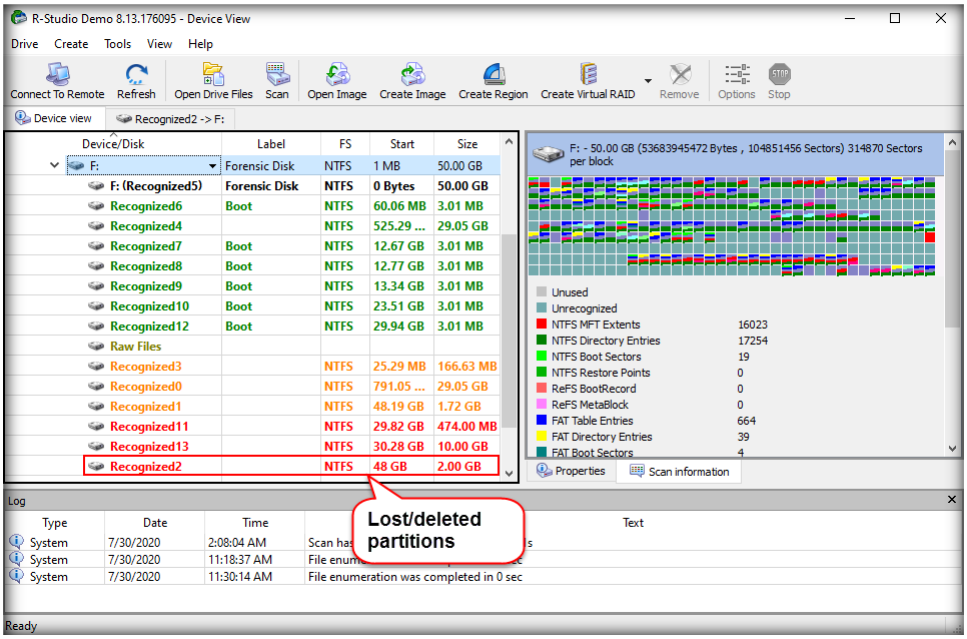

FIGURE 4.14: Lost/Deleted Partition

23. You can now view all the contents of the partition as shown in the following screenshot:

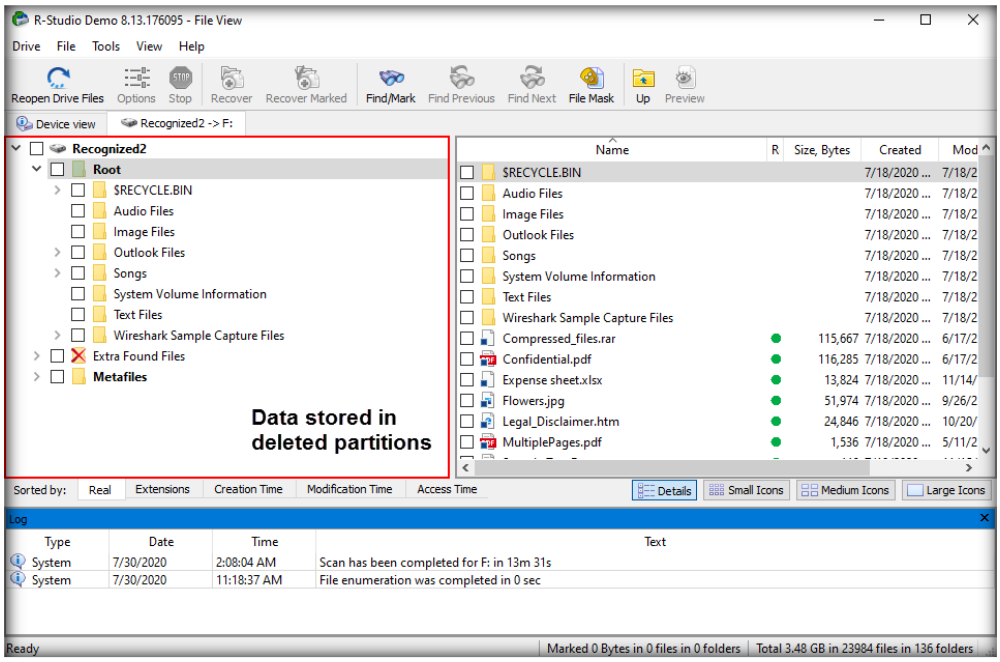

FIGURE 4.15: Viewing data in the deleted partition

24. If you wish to view the contents of a folder that was stored in the deleted partition, then click on that folder; its contents will be displayed in the right pane of the window. For the purpose of this lab, we shall view the contents of the **Audio Files** folder.

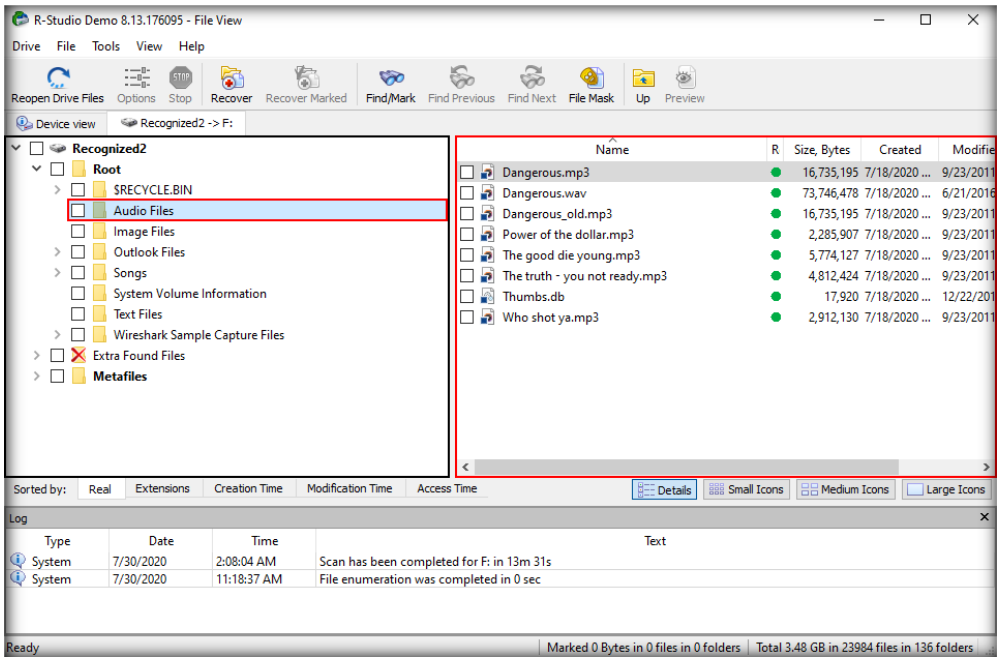

FIGURE 4.16: Viewing Contents of Evidence Files

25. Since the objective of this task is to recover an entire deleted partition, we will be recovering the entire **Recognized2** partition.

26. Check the **Recognized2** icon at the top in the left pane of the window so that all the folders in the partition are selected for recovery. Next, click on **Recover Marked** in the toolbar.

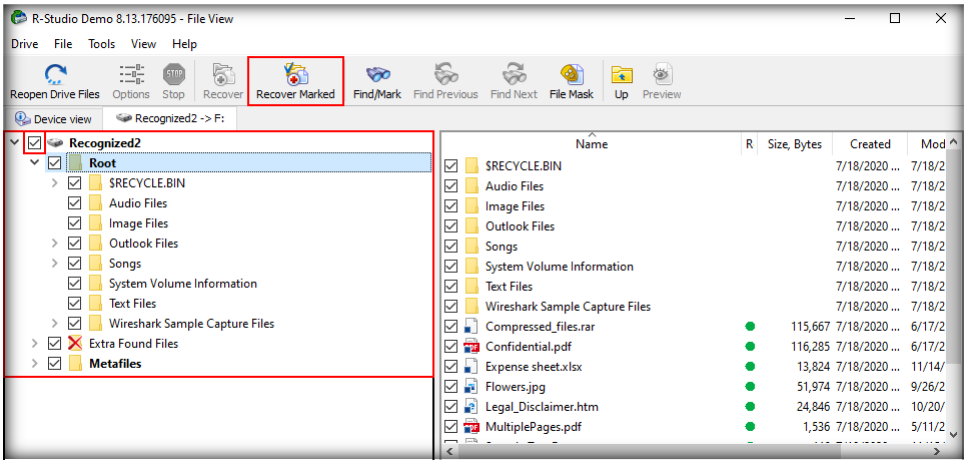

FIGURE 4.17: Checking the Recognized Partition icon

27. A **Recover** window appears. In the **Output folder** field at the top, we need to provide the output directory where the recovered partition data will be saved. We will set the output directory path as **D:\Recovered Partition**. In the same window, under the **Main** tab, check the options according to your requirement and then click **Ok**.

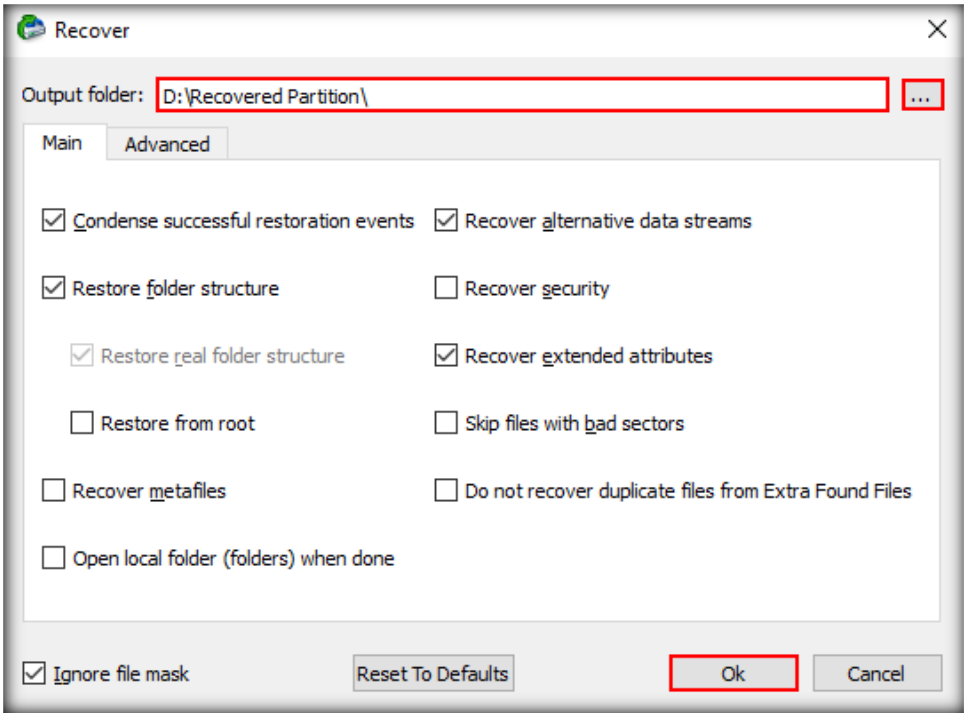

FIGURE 4.18: Providing Output Directory to recover data

28. If an **R-Studio Demo** dialog-box appears prompting you to choose whether to remove attributes or leave the settings as is, check **Apply the answer to all the recovered files** and click **Continue**.

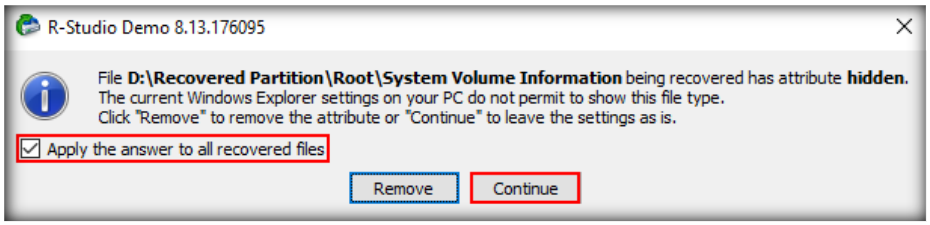

FIGURE 4.19: R-Studio Demo dialog box

29. R-Studio creates a folder named **Root** inside **D:\Recovered Partition**. The data from the lost/deleted partition will be recovered and saved to this folder, i.e., **D:\Recovered Partition\Root**.

30. Since this is a demo version of the tool, files greater than 256 KB in size will not be recovered. If you see an R-Studio Demo pop-up stating that files exceeding the 256 KB limitation cannot be recovered, check **Don't show this message again** and click **Skip**, as shown in the screenshot:

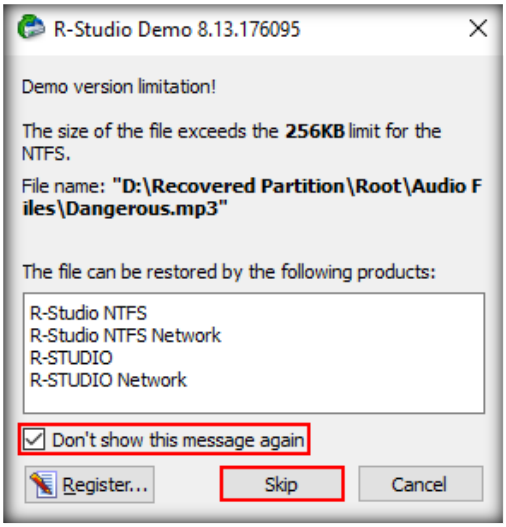

FIGURE 4.20: R-Studio 256KB limitation pop-up

31. R-Studio begins to recover the files and displays the status as shown in the following screenshot:

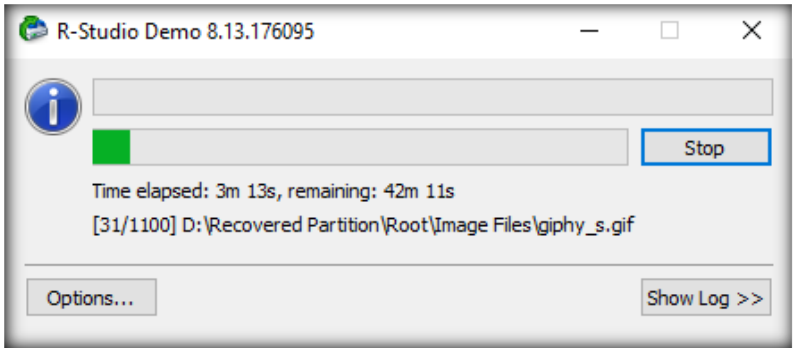

FIGURE 4.21: R-Studio starts to recover files

32. Upon completing the recovery process, you will be able to find the recovered data in **D:\Recovered Partition\Root**.

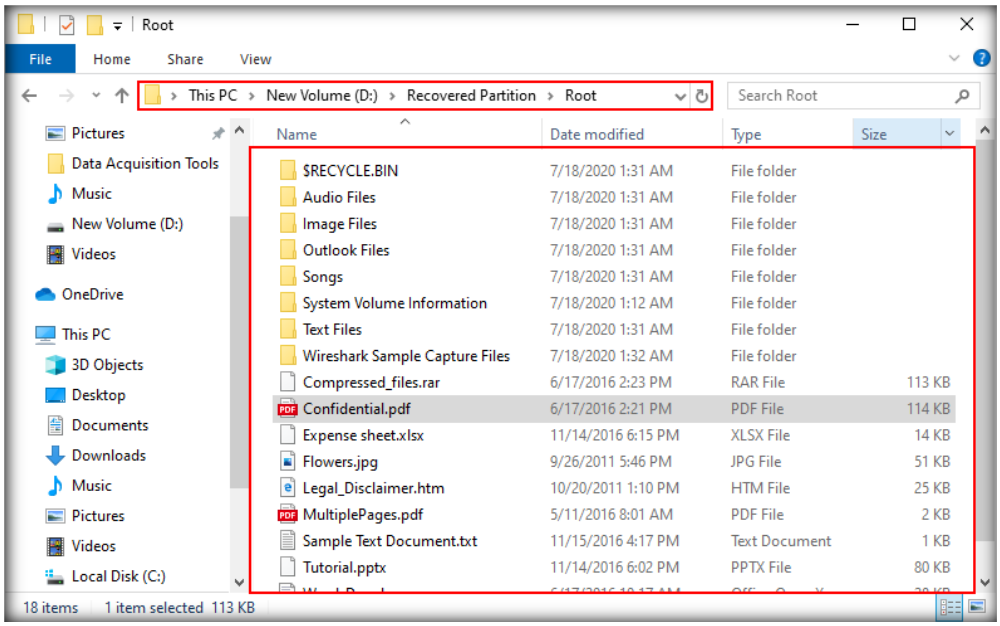

FIGURE 4.22: Recovered Partition Data in Output Directory

33. In this manner, you can recover data from a partition that is deleted and merged into another partition using **R-Studio**.

Lab Analysis

Analyze and document the results related to this lab exercise. Submit your opinion and experience with Recovering Deleted/Lost Partition.

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

Lab

5

Cracking Application Passwords

Passwords are typically a string of characters used to verify the identity of a user during an authentication process.

ICON KEY

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

Lab Scenario

An investigation into a case of theft of intellectual property and trade secrets belonging to an investment-banking organization has led forensic investigators to a personal computer belonging to the perpetrator. The perpetrator has stored all the stolen information in the form of various documents on their computer and has set passwords for those documents to prevent them from being accessed by others. With the help of law enforcement authorities, forensic investigators seized the perpetrator's machine to search through it for stolen information. During the course of investigation, the investigators found some password-protected files, the passwords for which must be cracked in order to gain access to the sensitive information that belongs to the investment-banking organization. How should the investigators proceed to crack the passwords of the protected documents?

As an expert forensic investigator, you must know how to crack the passwords of password-protected files and applications.

Lab Objectives

The objective of this lab is to help you understand how to crack the passwords of password-protected files and applications.

Lab Environment

This lab requires the following:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands
- A web browser with internet access

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics

- **Passware Kit Forensic** installer located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Passware Kit Forensic**

Note: You can download the latest version of **Passware Kit Forensic** from https://www.passware.com/kit-forensic/

If you use 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 Passware Kit Forensic tool and helps you understand how to crack passwords of password-protected applications/files on a computer for purposes of forensic investigation.

Lab Tasks

1. Login to **Windows 10** virtual machine.
2. Keep **Windows Server 2016** virtual machine powered **On** during this lab.

TASK 1

Install and Launch the Passware Kit Forensic Tool

3. Navigate to **Z:\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Passware Kit Forensic** and double-click **passware-kit-forensic-demo.msi** to launch the setup. Follow the wizard-driven installation steps to complete the installation.

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

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

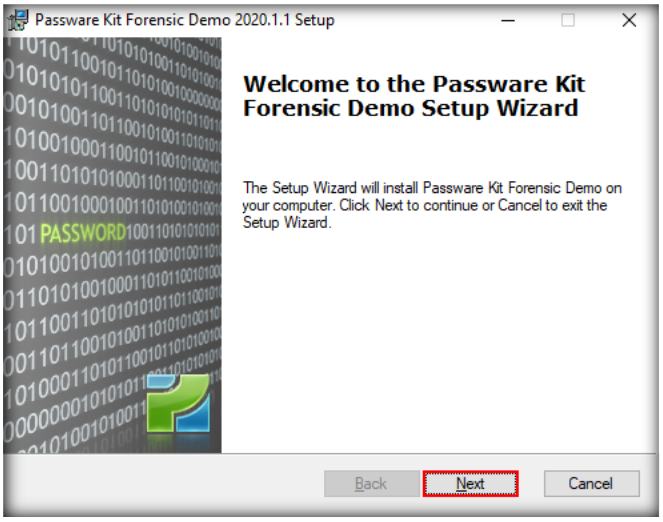

FIGURE 5.1: Setup wizard for Passware Kit Forensic Demo

4. During the final step of installation, ensure that the **Run Passware Kit Forensic Demo** option is checked. Click **Finish**.
5. The Passware Kit Forensic GUI appears, as shown in the following screenshot:

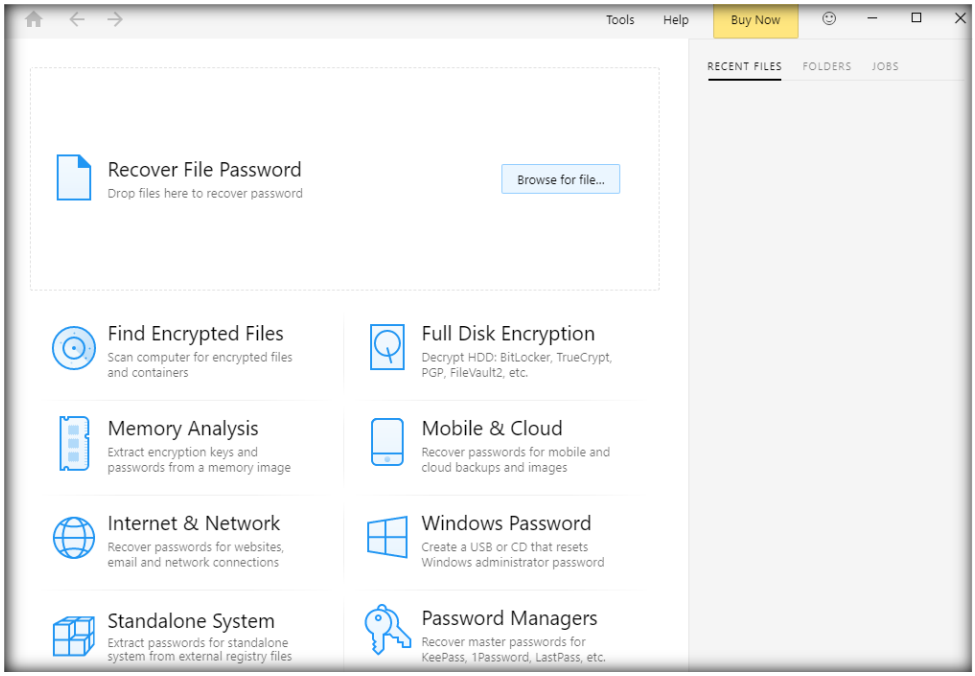

FIGURE 5.2: Passware Kit Forensic Demo GUI

TASK 2

Crack the Password of a Word Document

6. Click the **Recover File Password** option from the main window of the tool.

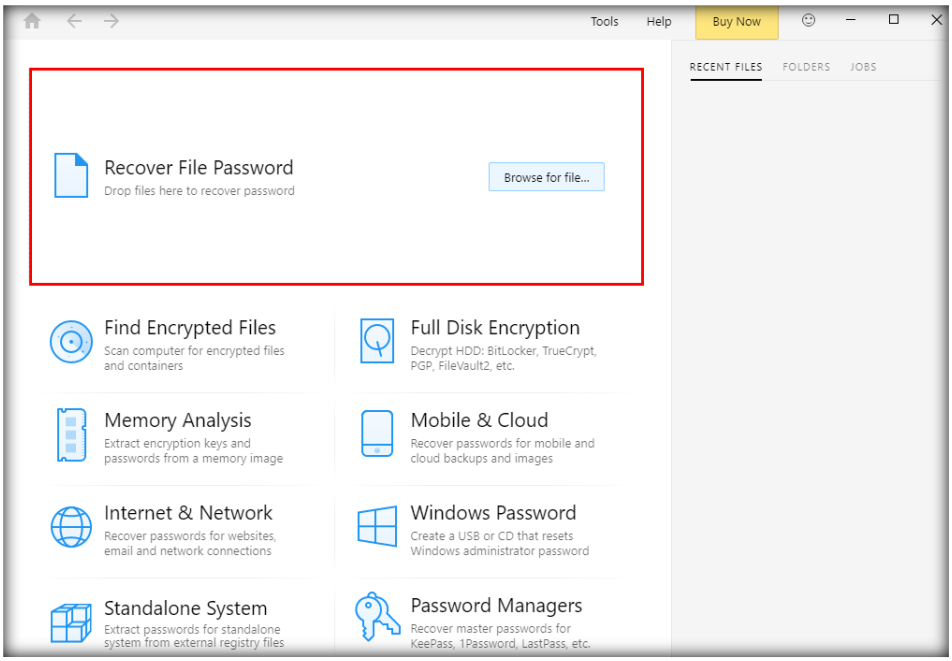

FIGURE 5.3: Recover File Password option

7. Navigate to the location **Z:\Evidence Files**, select the file **Sample_1.docx**, and click **Open**.

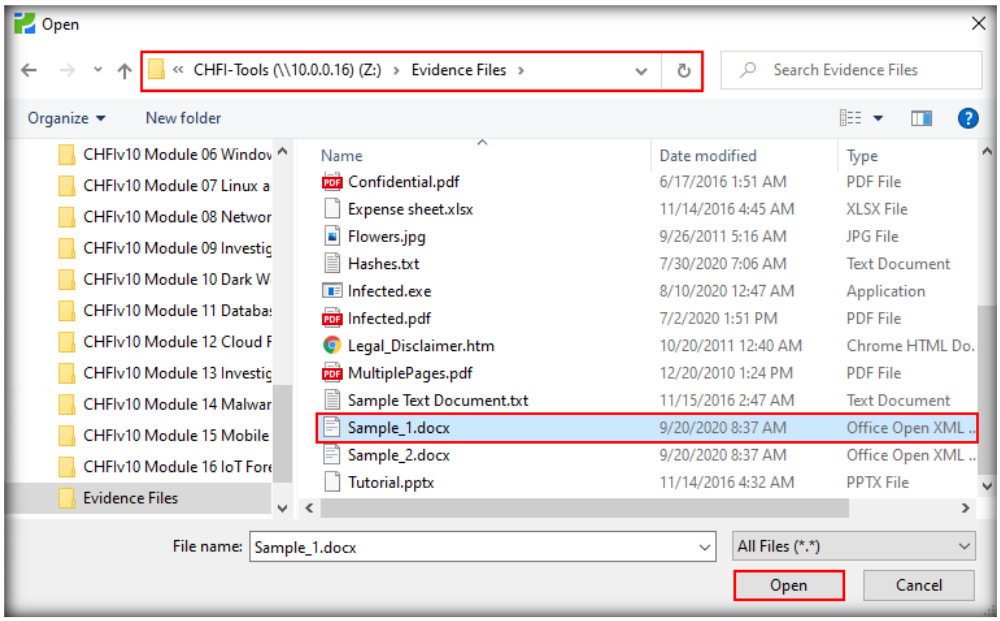

FIGURE 5.4: Selecting the password-protected file Sample_1.docx

8. Upon uploading the file to the application, the **Recover File Password** window wizard appears, where you need to select the **Use Predefined Settings** option.

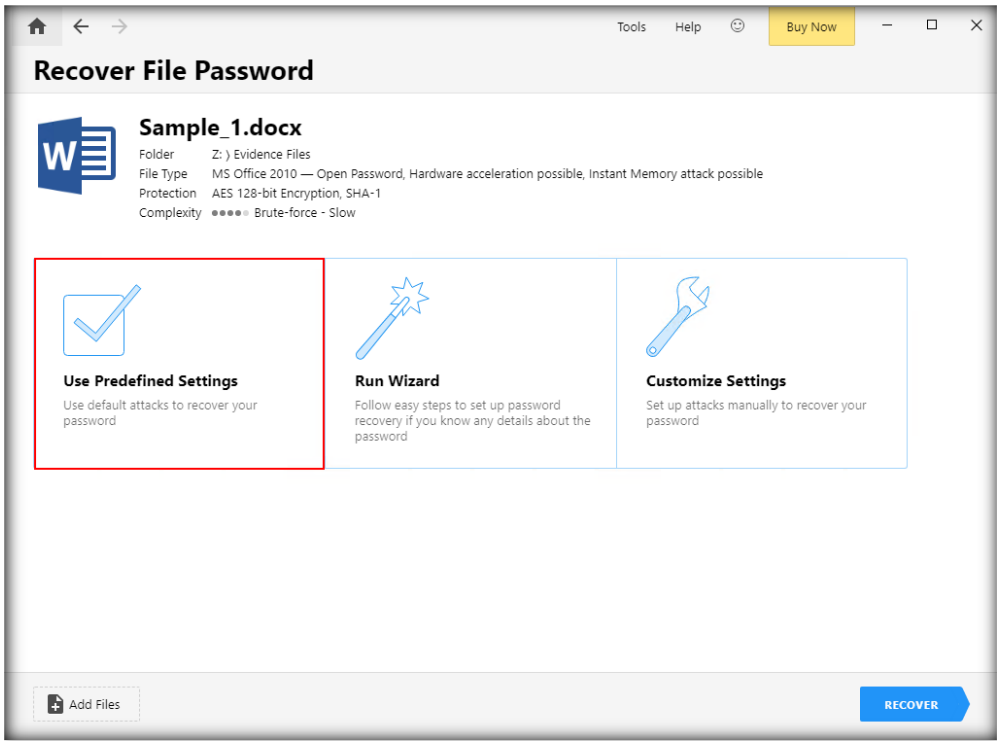

FIGURE 5.5: Use Predefined Settings option

9. The tool will take some time to crack the password. The time required is proportional to the number and types of characters used in the password.

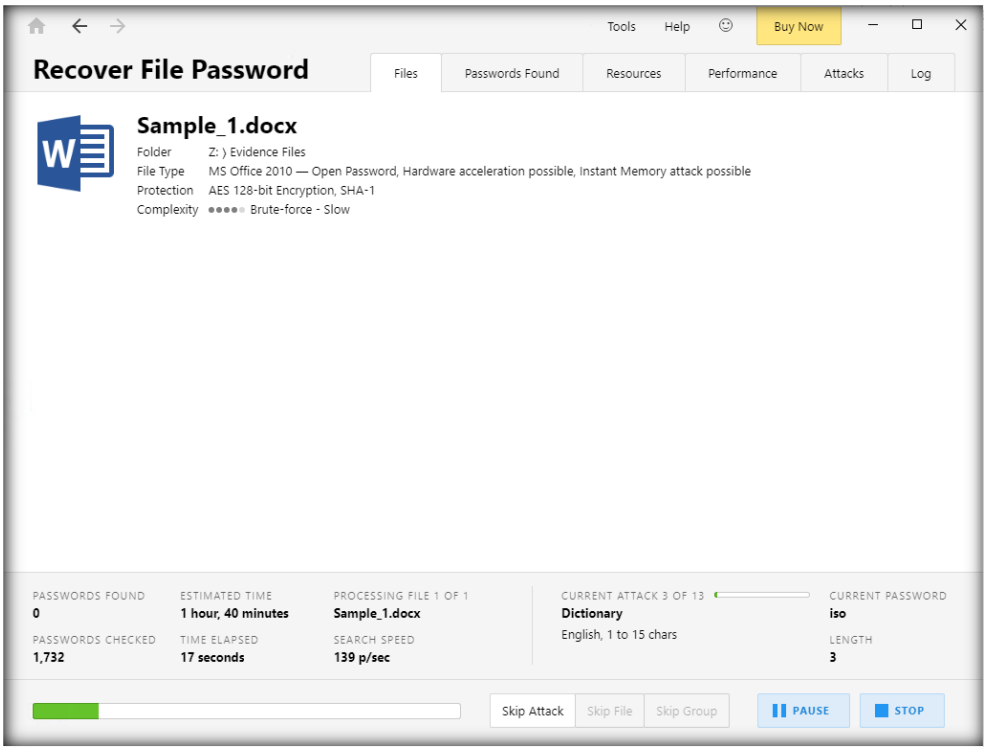

FIGURE 5.6: Password cracking screen

10. After analysis, the tool displays the **cracked password**, as shown in the screenshot:

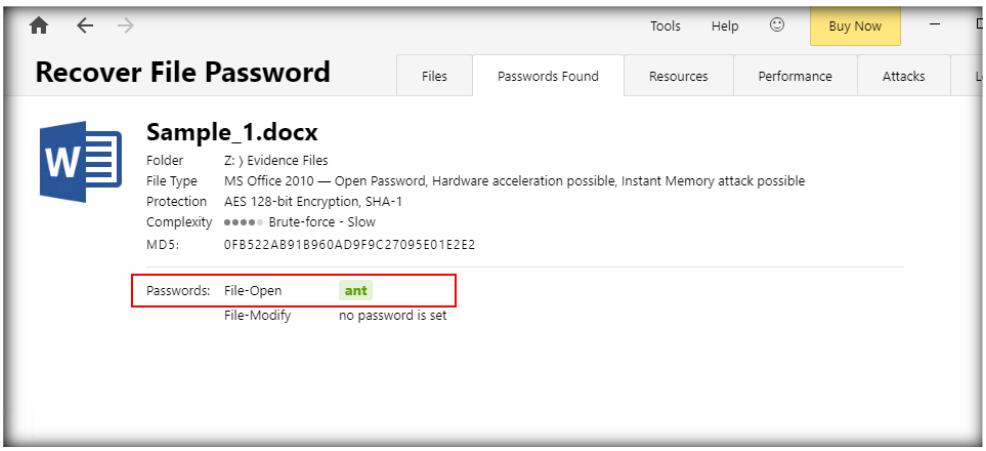

FIGURE 5.7: File password recovered

11. Close the Application. Now, we shall examine how to crack a **compressed password-protected** file.

TASK 3

Crack the Password of a Compressed File

12. To crack the password of a compressed folder or RAR file, navigate to **Z:\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Advanced Archive Password Recovery**, and double-click the **archpr_setup_en.msi** setup file.

13. Click **Next** and follow the wizard-driven installation steps to install the application.

FIGURE 5.8: Setup wizard for Advanced Archive Password Recovery

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

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

14. During the final step of installation, ensure that **Run Advanced Archive Password Recovery** is checked, and click **Finish**.

15. The **Advanced Archive Password Recovery** GUI appears, as shown in the following screenshot:

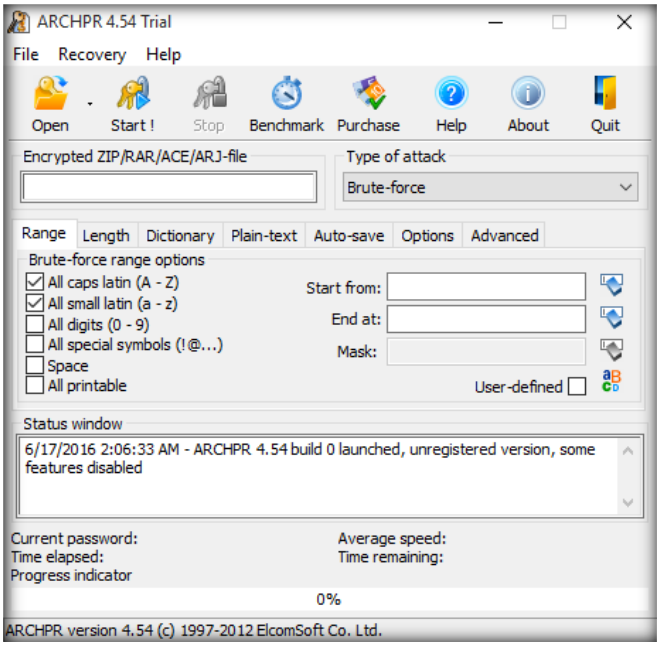

FIGURE 5.9: Advanced Archive Password Recovery GUI

16. Now, set a range for brute-force attack options by checking the options under the **Range** tab. For the demonstrative purpose of this lab, we are checking the **All digits (0-9)** option while leaving all the other options unchecked. While running the lab in real time, you may check these options according to your requirement.

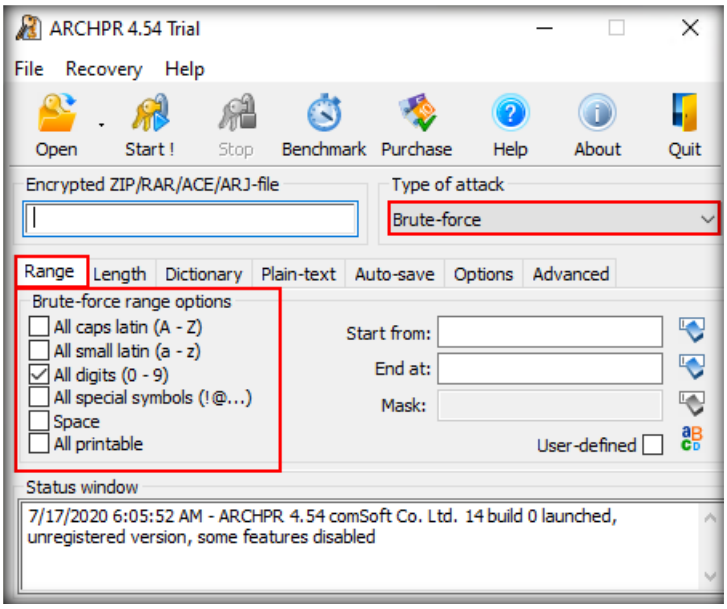

FIGURE 5.10: Set Range for Brute-force attack

17. From the toolbar of the tool window, click **Open** to add the WinRAR file you wish to crack.

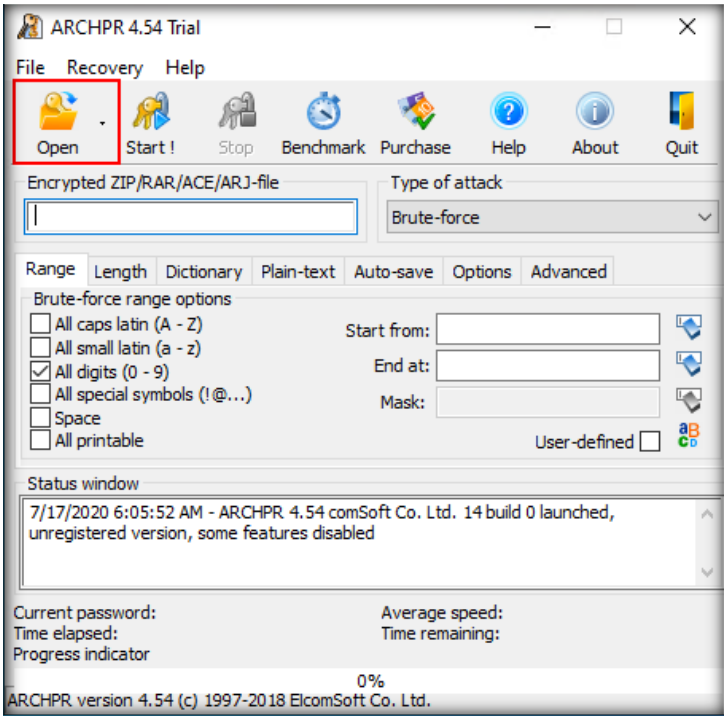

FIGURE 5.11: Clicking Open on the toolbar

18. An **Open** window appears. Navigate to the location **Z:\Evidence Files**, select the file **Compressed_files.rar**, and click **Open**.

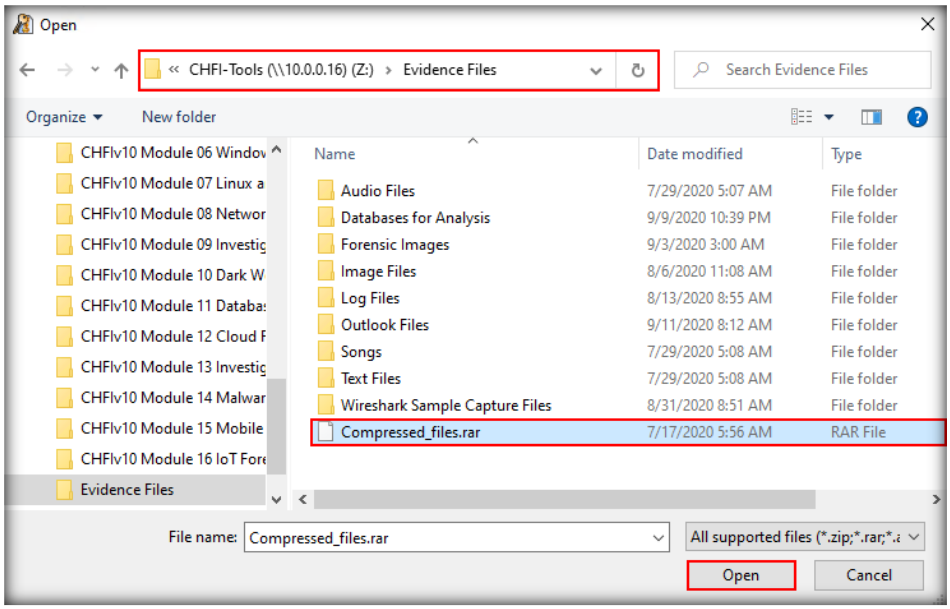

FIGURE 5.12: Selecting the Compressed_files.rar file

19. The tool cracks the password and displays it along with other details, as shown in the screenshot:

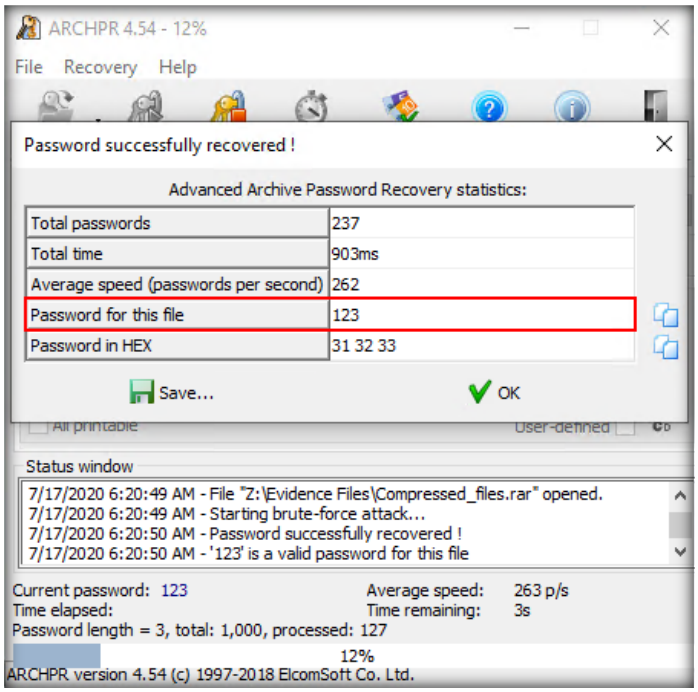

FIGURE 5.13: Password cracked and displayed

20. In a real scenario, you must set all the options as you will usually not have any clue regarding the password that protects the file. Therefore, the tool takes a large amount of time for cracking a password, if it is complex in nature.

TASK 4

Crack the Password of a Password-protected PDF File

21. Close the application.
22. We shall now crack the password of a **password-protected PDF** file.
23. To crack the password, we will use the **Advanced PDF Password Recovery** tool.
24. To install the tool, navigate to **Z:\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Password Cracking Tools\Advanced PDF Password Recovery**, double-click **apdfpr_setup_en.msi**.
25. Click **Next** and follow the wizard-driven installation steps to complete the installation of the tool.

FIGURE 5.14: Setup wizard for Advanced PDF Password Recovery

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

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

26. In the final step of installation, ensure that **Run Advanced PDF Password Recovery** is checked, and click **Finish**.

Note: Upon completion of the installation, if an **Elcomsoft Updater** window appears, close the window.

27. The **Advanced PDF Password Recovery** GUI appears, as shown in the following screenshot:

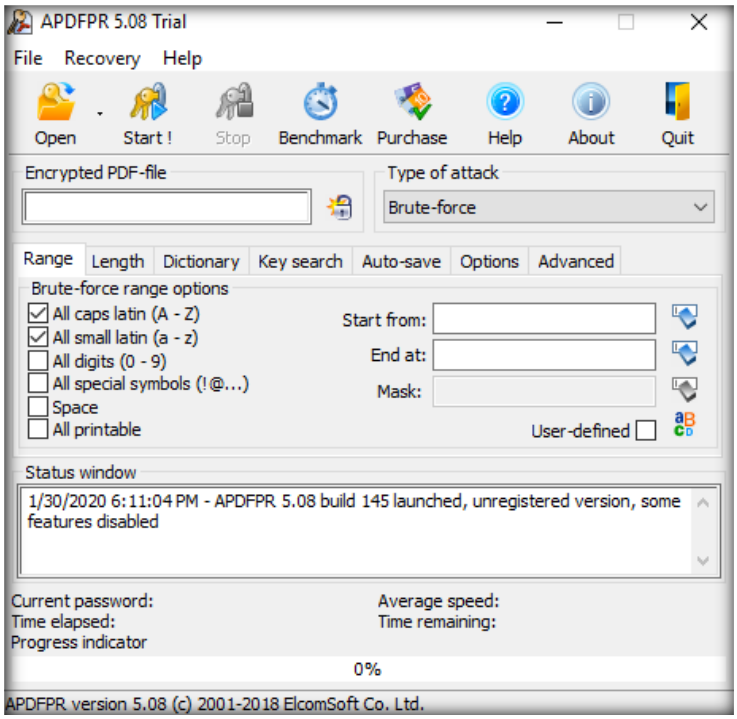

FIGURE 5.15 Advanced PDF Password Recovery GUI

28. Again, set the range for brute-force attacks by checking the options under the **Range** tab. For the demonstrative purpose of this lab, we are checking the **All small latin (a-z)** option while leaving the other options unchecked. While running the lab in real time, you may check the options according to your requirement.

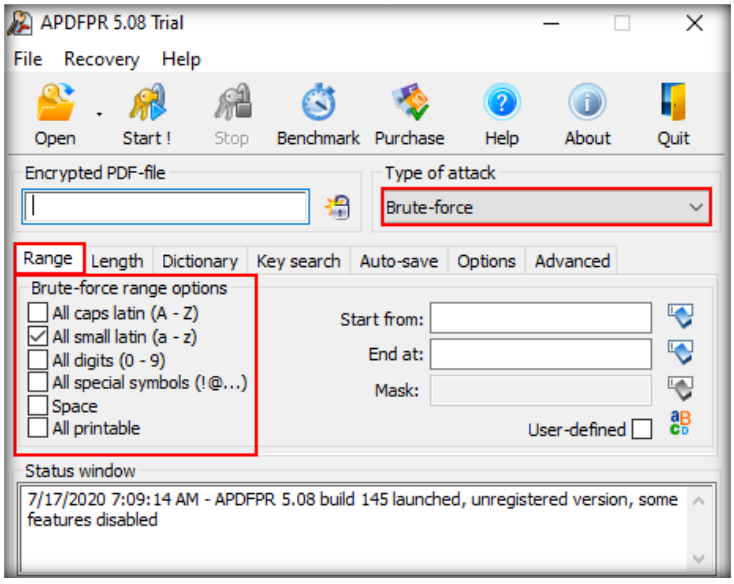

FIGURE 5.16: Setting the Range for Brute-force attack

29. From the toolbar of the tool window, click **Open** to add the PDF file you wish to crack.

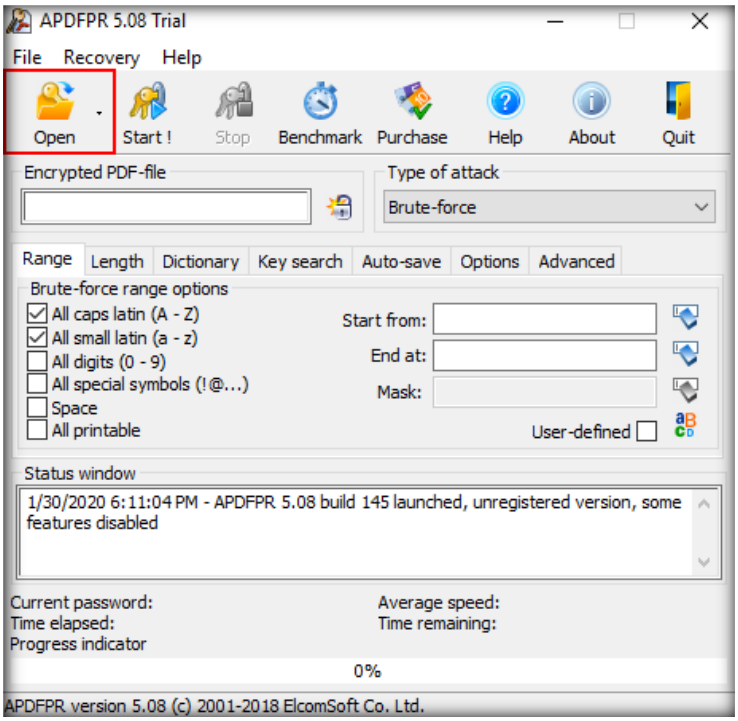

FIGURE 5.17: Clicking Open on the toolbar

30. An **Open** window appears. Navigate to the file location **Z:\Evidence Files**, select the file **Confidential.pdf**, and click **Open**.

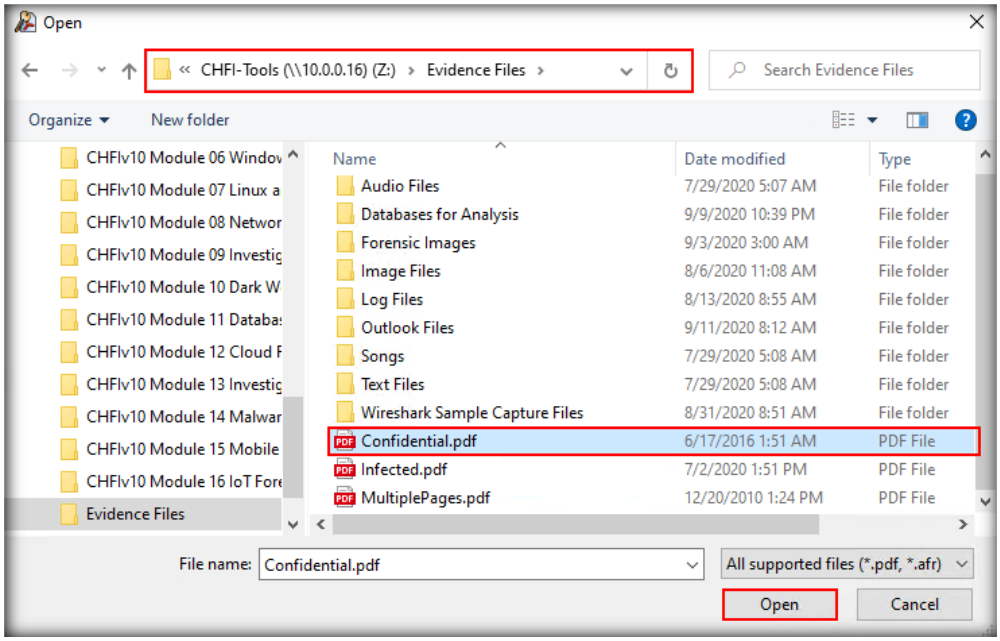

FIGURE 5.18: Selecting Confidential.pdf

31. An **APDFPR** pop-up appears with a message prompting you to enter the password for the document. Click the **Start recovery** button.

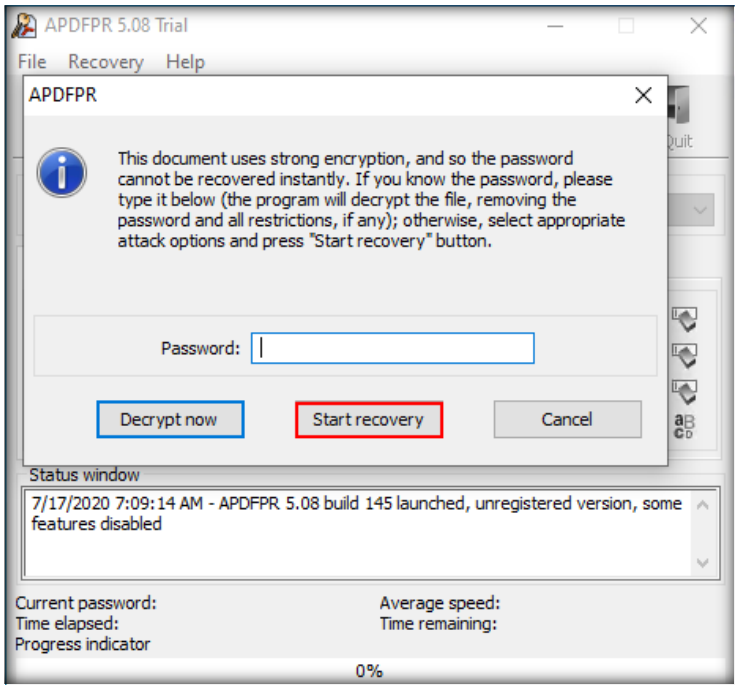

FIGURE 5.19: Clicking Start recovery in the APDFPR pop-up

32. After performing the analysis, the tool will display a window with the password for the **Confidential.pdf** file, as shown in the following screenshot:

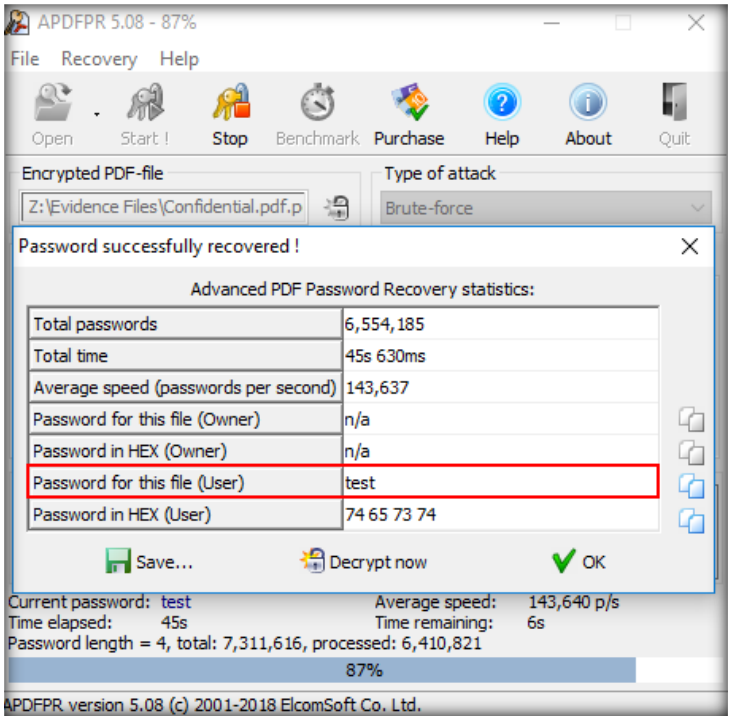

FIGURE 5.20: File Password Cracked and Displayed

33. In a real scenario, you must set all the options as you will usually not have any clue regarding the password that protects the file. Therefore, the tool takes a large amount of time for cracking a password, if it is complex in nature.

Lab Analysis

Analyze and document the results of 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

6

Detecting Steganography

Steganography is the process of hiding information or a file within another file. In other words, it is the process of disguising a harmful file as a safe file.

ICON KEY

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

Lab Scenario

Attackers occasionally attempt to deceive users and system security by hiding a malicious program with an apparently useful image or file. By doing this, they can avert security checks and lure victims into downloading and running malware as well as prevent forensic identification.

As an expert forensic investigator, you must be able to detect and analyze steganography files.

Lab Objectives

The objective of this lab is to help you analyze files hidden using steganography and find their impact on a system or network.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques

This lab requires the following:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands
- A web browser with internet access
- **Stegspy** tool located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\StegSpy**
- **Image Steganography** installer located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\Image Steganography**
- **OpenStego** installer located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\OpenStego**

- **DeepSound** installer located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\DeepSound**

Note: You can download the latest version of **StegSpy** from http://www.spy-hunter.com/stegspydownload.htm

You can download the latest version of **OpenStego** from https://github.com/syvaidya/openstego/releases

You can download the latest version of **DeepSound** from https://www.darknet.org.uk/2019/03/deepsound-audio-steganography-tool/

If you use 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: 20 minutes

Overview of the Lab

This lab familiarizes you with tools such as StegSpy, Image Steganography, OpenStego, and DeepSound and helps you understand how to identify messages or files with hidden content using these tools.

Lab Tasks

TASK 1

Detect Steganography

1. Login to **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\StegSpy** and double-click **StegSpy2.1.exe** to launch the tool.

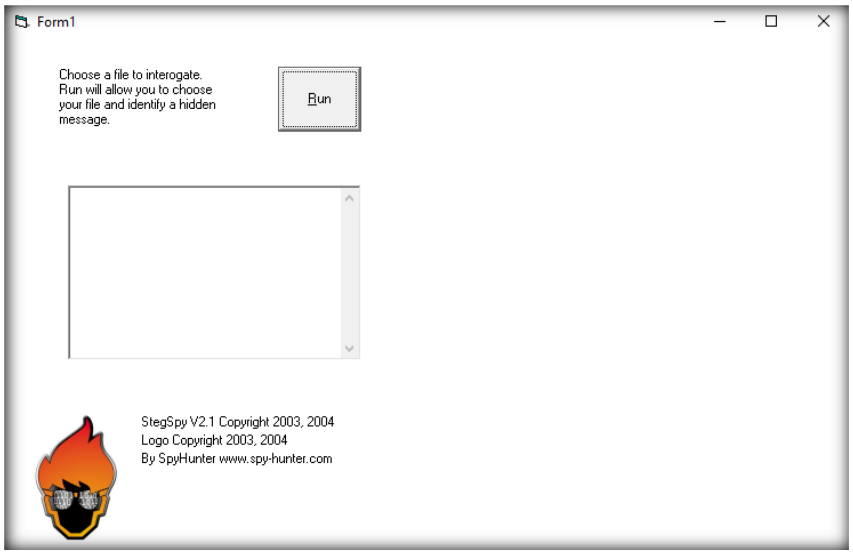

FIGURE 6.1: Main window of StegSpy

3. Click the **Run** button from the tool's main page to add the suspicious file.

FIGURE 6.2: Clicking the Run button

4. **Open** window appears. Navigate to the location of the suspicious file, **C:\CHFI-Tools\Evidence Files\Image Files**. Select the file **Model.png** and click the **Open** button.

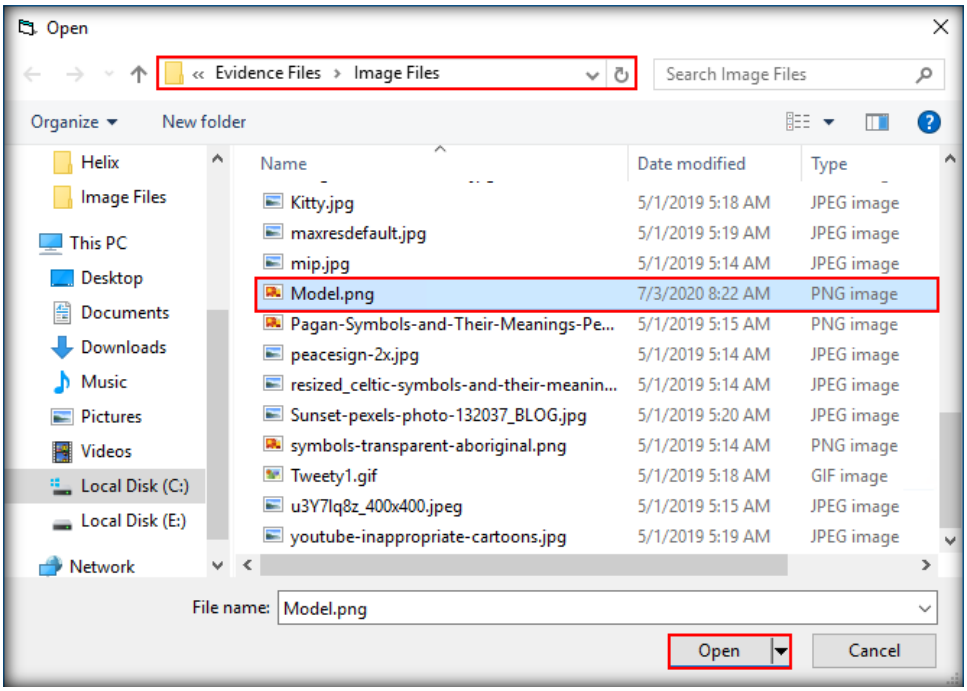

FIGURE 6.3: Selecting Model.png

5. The tool will scan the file and display the type of steganography technique used to hide another file in it.

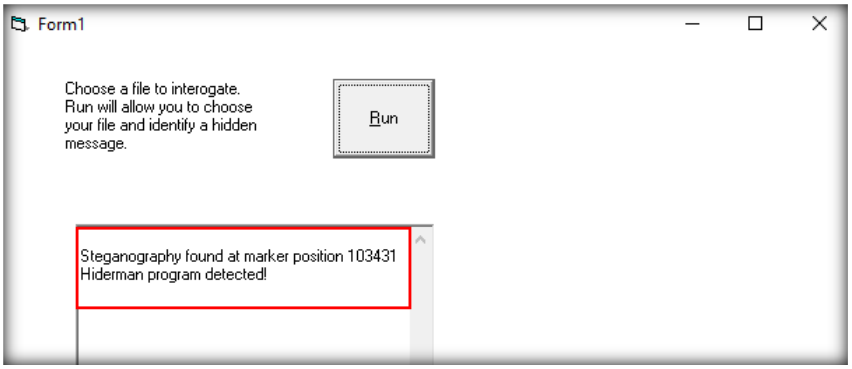

FIGURE 6.4: Displaying the steganography type

6. **Close** the application.
7. Alternatively, you can use online steganography detection tools such as McAfee's **Steganography Defense Initiative** to detect steganography in an image.
8. To perform steganography detection using this online platform, launch a web browser (here, **Firefox**) and browse the URL https://www.mcafee.com/enterprise/en-us/downloads/free-tools/steganography.html.

Note: Since we are demonstrating this task on a webpage, if McAfee removes it or changes the URL of the landing page in the future, the above-mentioned link might not work.

9. McAfee's **STEGANOGRAPHY DEFENSE INITIATIVE** webpage appears as shown in the following screenshot:

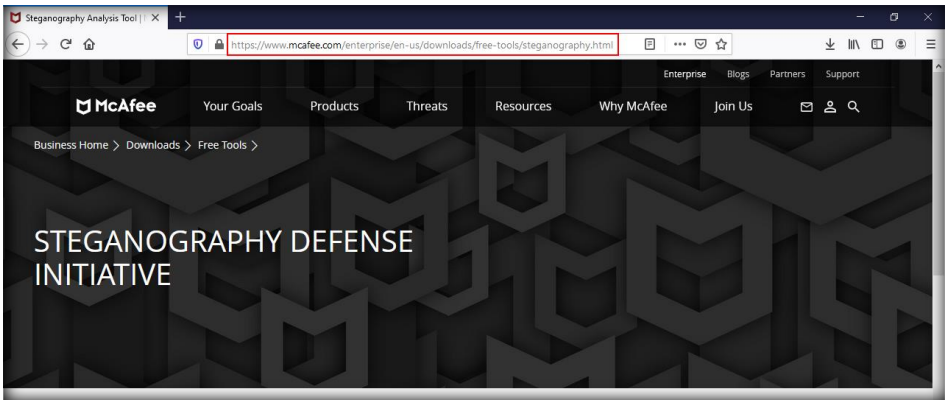

FIGURE 6.5: McAfee's STEGANOGRAPHY DEFENSE INITIATIVE Webpage

10. Scroll down the webpage and click on the box that reads **Drop here an image file to analyze for steganography** to upload the suspicious image.

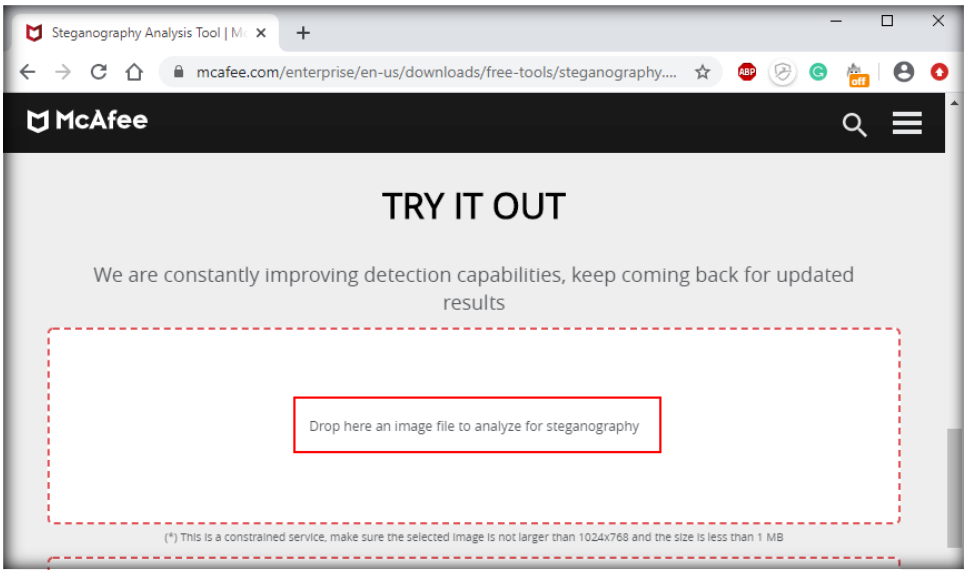

FIGURE 6.6: File Uploading and Results Box

11. An **Open** window appears. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files**, select **Model.png**, and click **Open**.

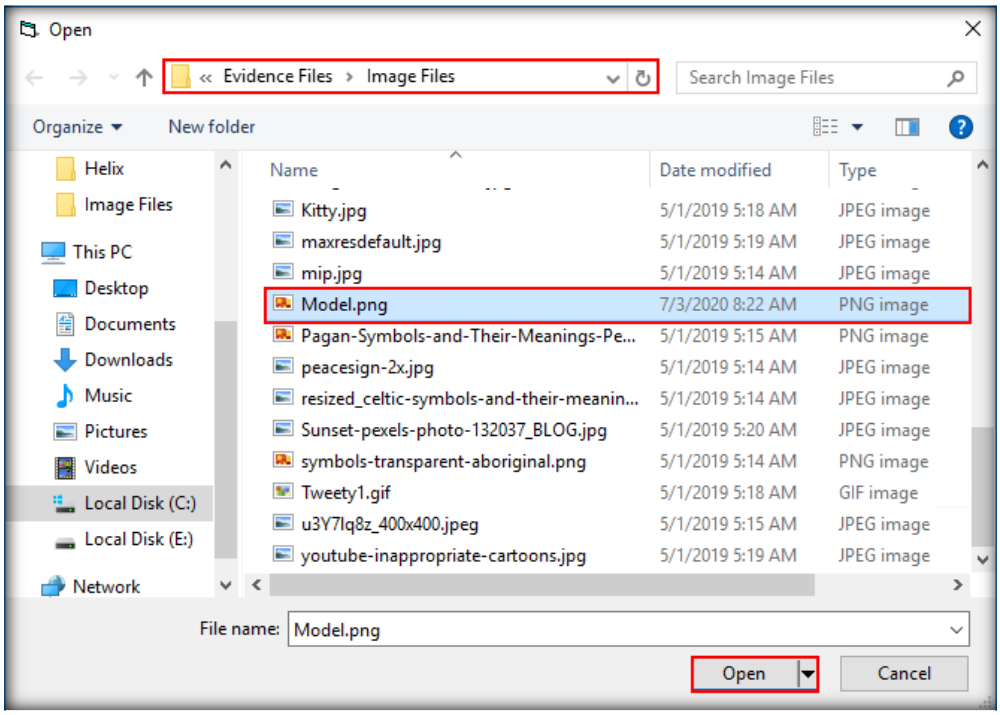

FIGURE 6.7: Selecting Model.png

12. The image gets uploaded on the webpage, and McAfee's website begins to scan it.

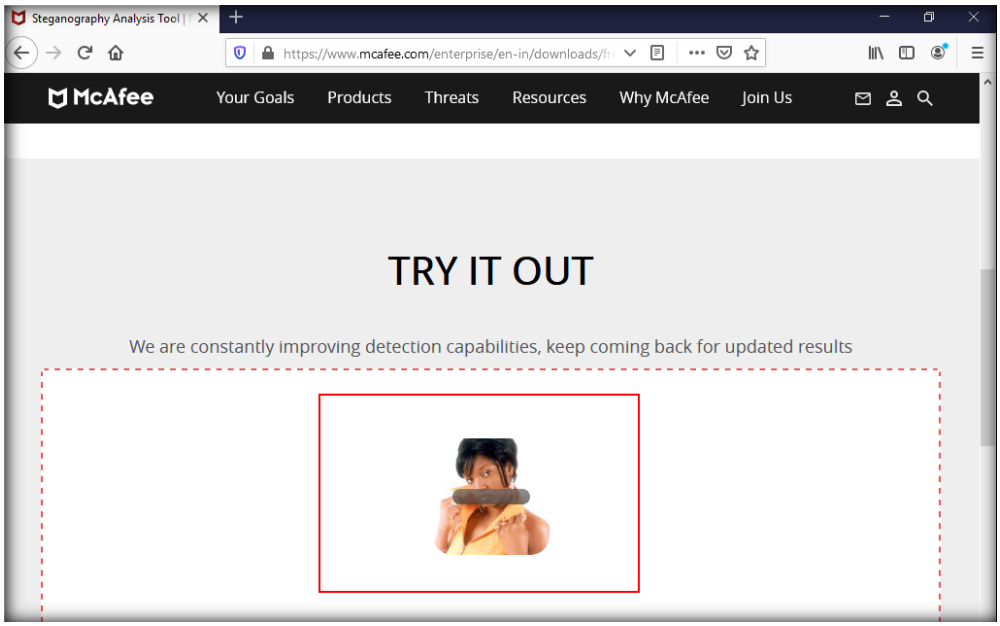

FIGURE 6.8: Uploaded Image

13. Once the scan is completed, the website returns a result indicating that the file **Model.png** contains significant traces of steganography in the image.

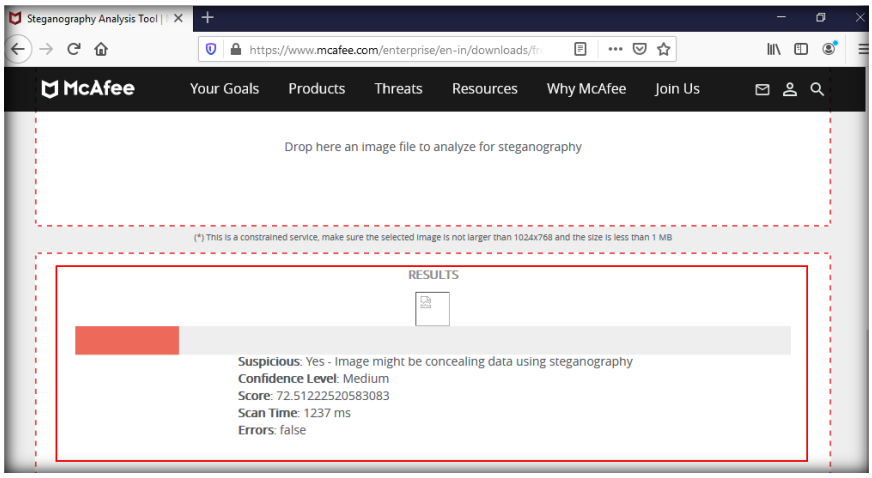

FIGURE 6.9: Result Section

14. **Close** the web browser.

TASK 2

Defeat Steganography

15. Now, we shall attempt to decode the content hidden in the image. We must keep attempting the use of various tools to detect the data hidden in the image. In this lab, we will use **Image Steganography** and **OpenStego** to uncover the hidden data.

16. Let us attempt to detect the hidden data using the **Image Steganography** tool. To install the tool, navigate to the location **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\Image Steganography**, double-click the **Image Steganography Setup.exe** file to launch the setup, and click **Install** in the setup window.

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

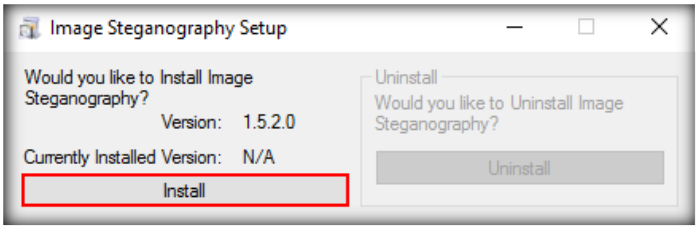

FIGURE 6.10: Image Steganography Setup dialog box

17. Upon completing the installation, an **Image Steganography Setup** pop-up appears. Click **Yes** to launch the tool.

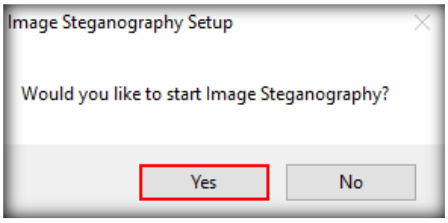

FIGURE 6.11: Image Steganography Setup dialog box appearing upon completion of the installation

18. The main window of **Image Steganography** appears, as shown in the following screenshot:

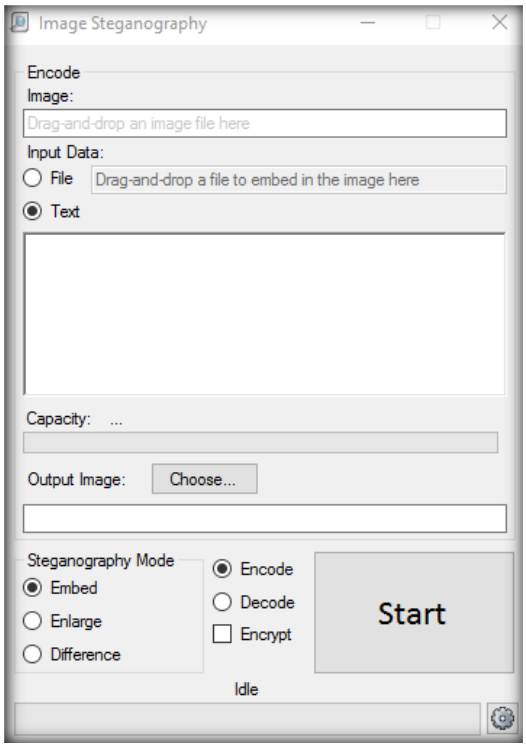

FIGURE 6.12: Image Steganography launch screen

19. Select the **Decode** option to extract the hidden file from the suspicious file.

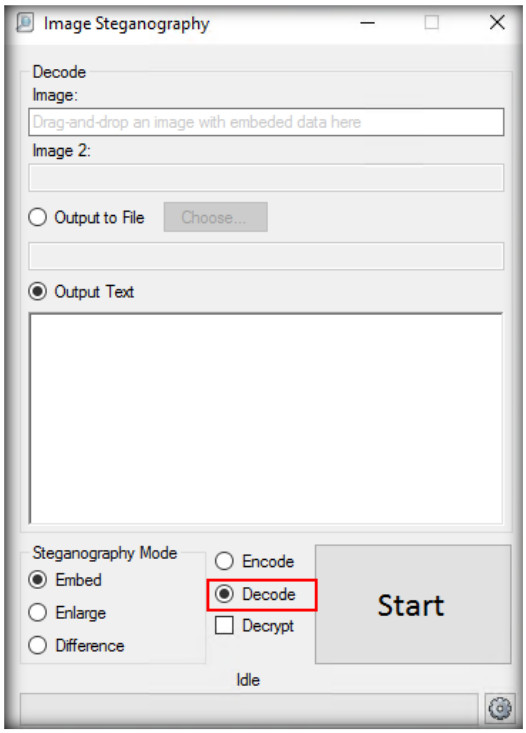

FIGURE 6.13: Selecting the Decode option

20. To attempt decoding the image, enter the location of the image, i.e., **C:\CHFI-Tools\Evidence Files\Image Files\Model.png** under the **Image** field in the **Decode** section, and click **Start**.

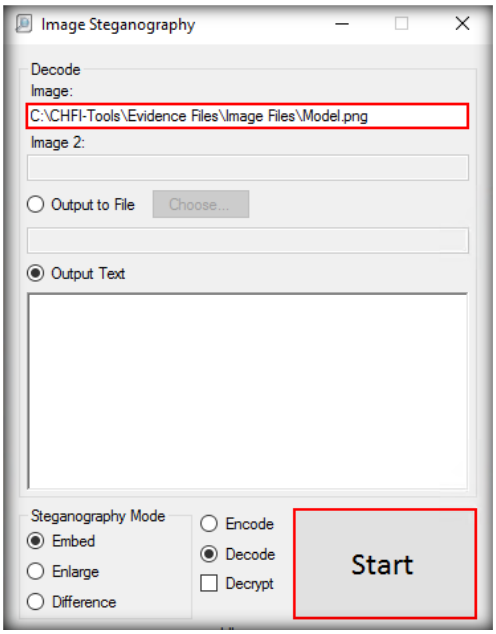

FIGURE 6.14: Clicking the Start button

21. The tool will attempt to analyze the file and display the result if it could decipher it; else, it will display a message indicating that the provided image is either corrupt or invalid.

22. In this case, the tool has failed to detect or extract the hidden content or file. It has displayed a message indicating that the provided input file is either corrupt or invalid. Click **OK**.

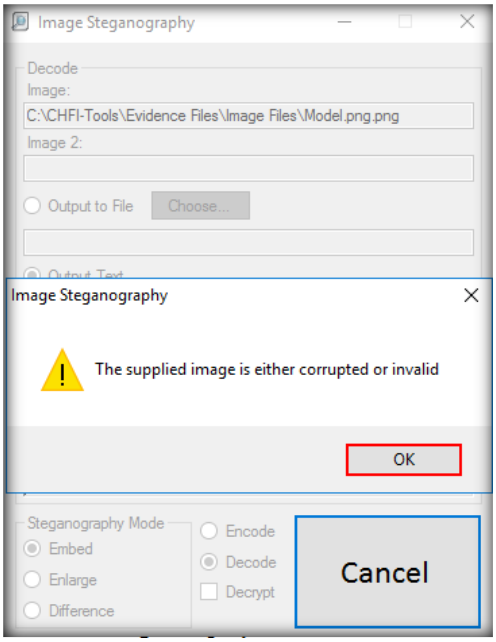

FIGURE 6.15: Image Steganography pop-up

23. **Close** the application.
24. We shall now attempt to extract the hidden file from the previously selected image (**Model.png**) by using the other tool, i.e., **OpenStego**.
25. To install **OpenStego**, navigate to **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\OpenStego**, and double-click the **Setup-OpenStego-0.6.1.exe** file.
26. The **OpenStego** setup wizard appears. Accept the license agreement and follow the wizard-driven installation steps to install the application.

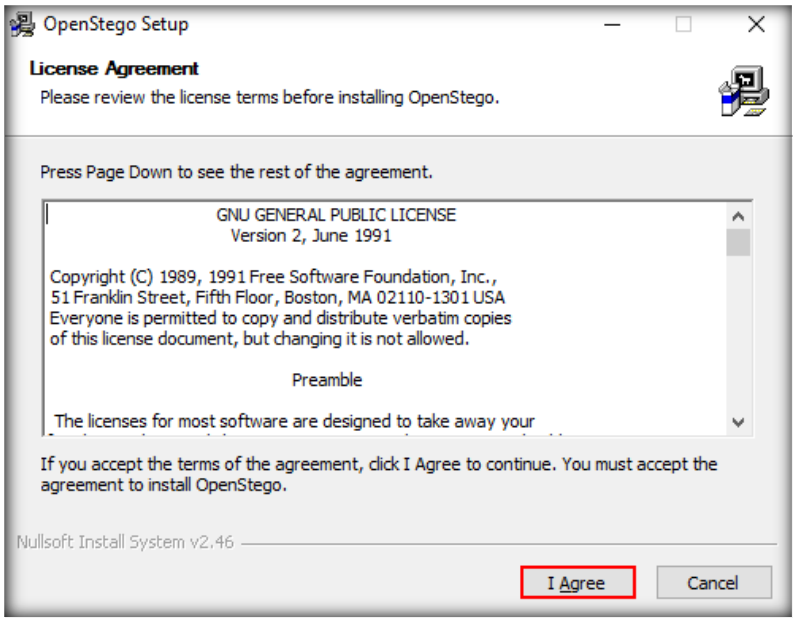

FIGURE 6.16: OpenStego setup wizard

Note: During installation of **OpenStego**, if an **OpenStego Setup** dialog-box appears asking if you would like to install **Java Runtime Environment (JRE)** version 1.5.0 or above, select **No** and then click **OK** in the subsequent **OpenStego Setup** dialog-box to proceed with the installation of the **OpenStego** application.

27. Navigate to the **Start** menu and click on **Run OpenStego** under the **Recently added** list.

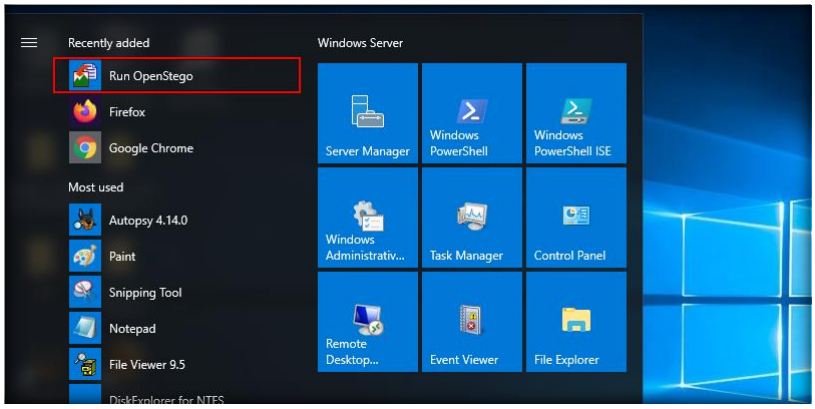

FIGURE 6.17: OpenStego GUI

28. The OpenStego GUI appears. Click the **Extract Data** button under the **Data Hiding** section to input the file containing steganography and extract the hidden data.

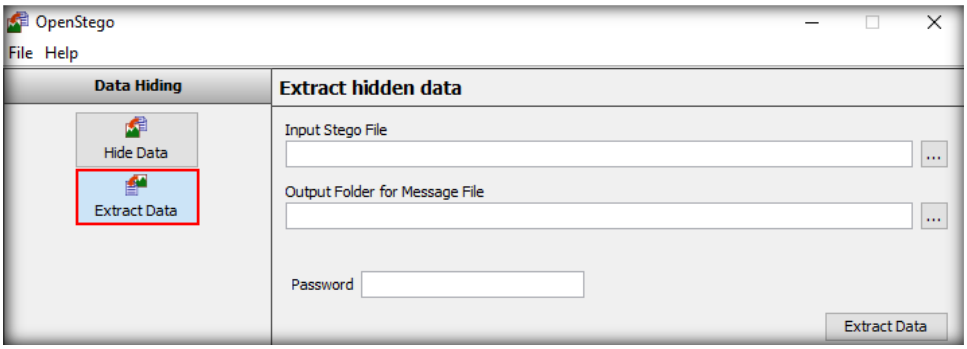

FIGURE 6.18: Clicking Extract Data

29. Provide the path of the file containing steganography in the **Input Stego File** field and specify a folder as an output directory in the **Output Folder for Message File** field. The path to the file containing steganography is **C:\CHFI-Tools\Evidence Files\Image Files\Model.png**. In this lab, we are setting the output folder as **Desktop**.

30. Click the **Extract Data** button.

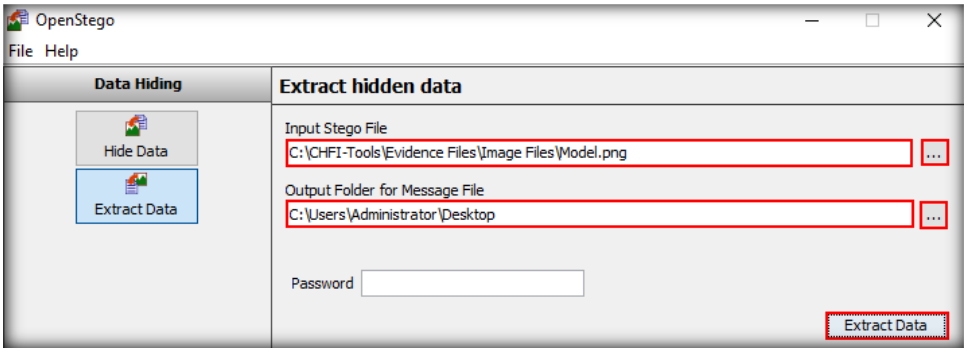

FIGURE 6.19: Providing the input file and output directory and clicking Extract Data

31. The tool will analyze the file and extract the hidden data successfully. It saves the extracted data to **Desktop**. Click **OK**.

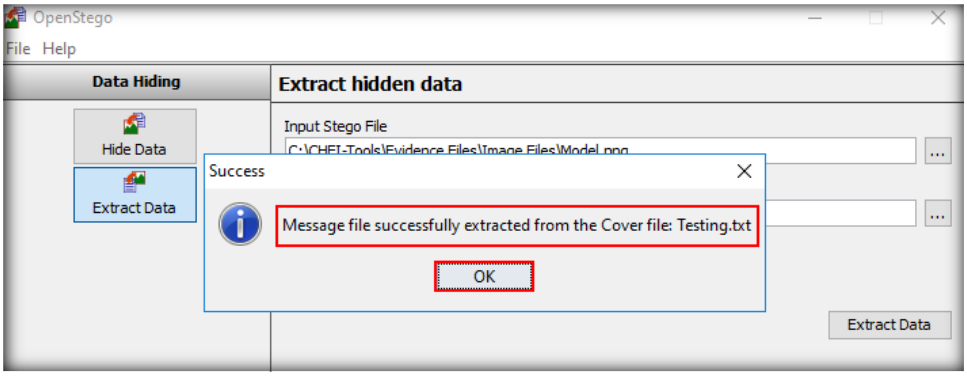

FIGURE 6.20: Success message pop-up

32. The hidden file has been extracted to **Desktop** as **Testing.txt**, which contains the text as shown in the following screenshot:

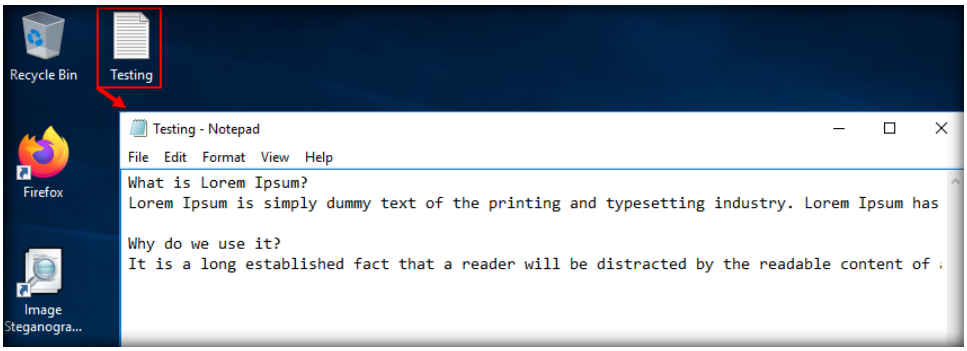

FIGURE 6.21: Extracted hidden file

33. In this manner, you can extract hidden data from an image file. Close the text file and **OpenStego** application.
34. During investigation, you might also come across audio files that contain hidden data.
35. In this section, you will learn the process of extracting hidden data from an audio file using **DeepSound**.

TASK 3

Analyze an Audio File

36. Navigate to the location of the file **DeepSound.msi**, **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Steganography Detection Tools\DeepSound**, double-click the **DeepSoundSetup.msi** file, and follow the wizard-driven instructions to install the application.

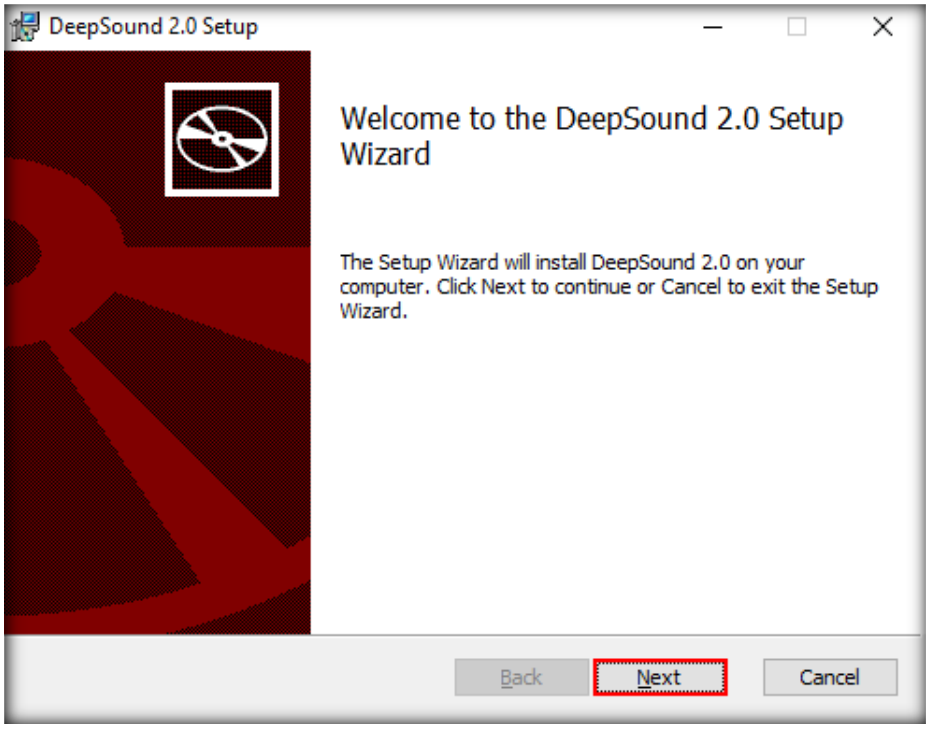

FIGURE 6.22: DeepSound welcome wizard

37. On completing the installation, either a dialog box would appear asking you to choose a browser and select OK, or a web browser would open automatically, displaying a webpage associated with the **DeepSound** application. **Close** the browser window.

38. Double-click the **DeepSound** icon located on the Desktop to launch the application.

39. The **DeepSound** GUI appears as shown in the following screenshot:

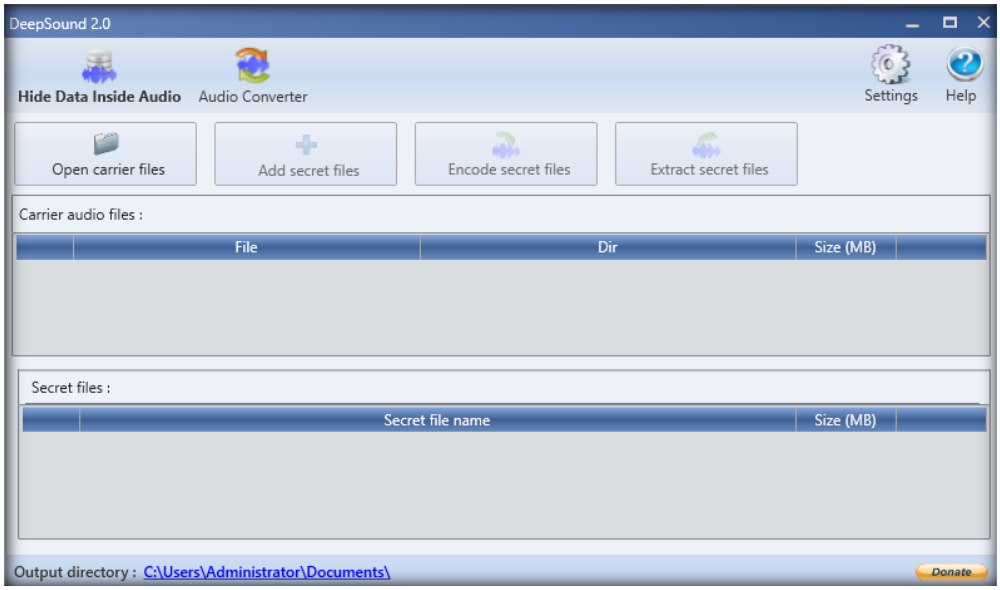

FIGURE 6.23: DeepSound GUI

40. Click the **Open carrier files** button to add the file containing steganography

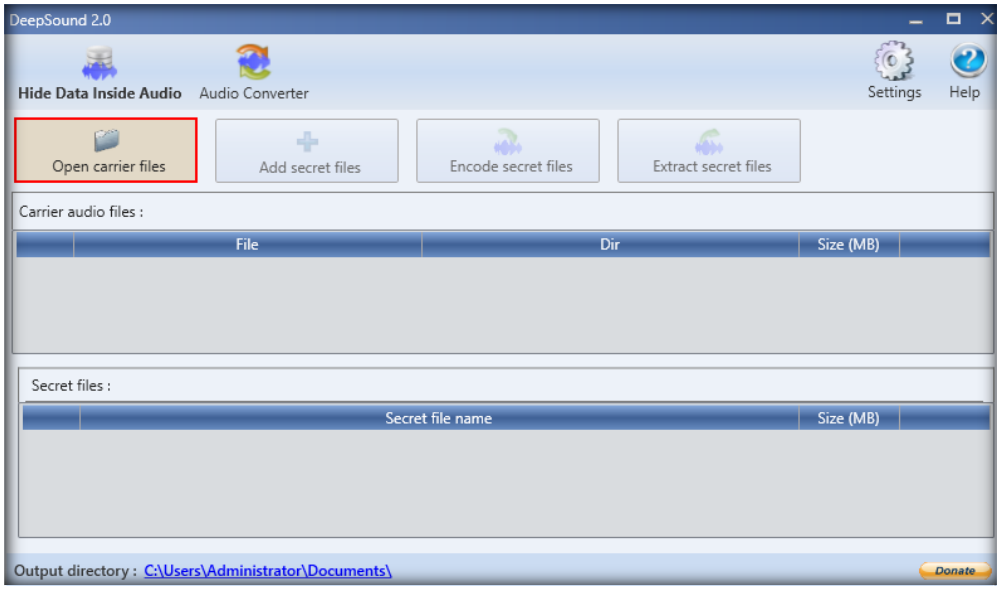

FIGURE 6.24: Click Open carrier files button

41. Navigate to the location **C:\CHFI-Tools\Evidence Files\Audio Files**; select the file containing steganography, **Dangerous.wav**, and click the **Open** button.

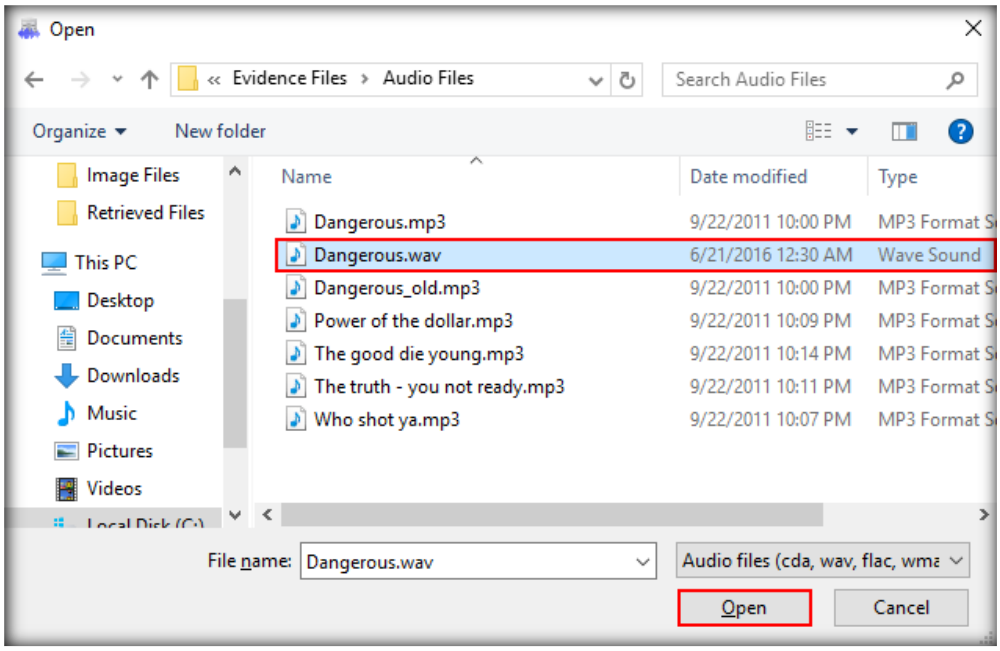

FIGURE 6.25: Opening Dangerous.wav

42. Click the **Extract secret files** button to start extracting the hidden files or data.

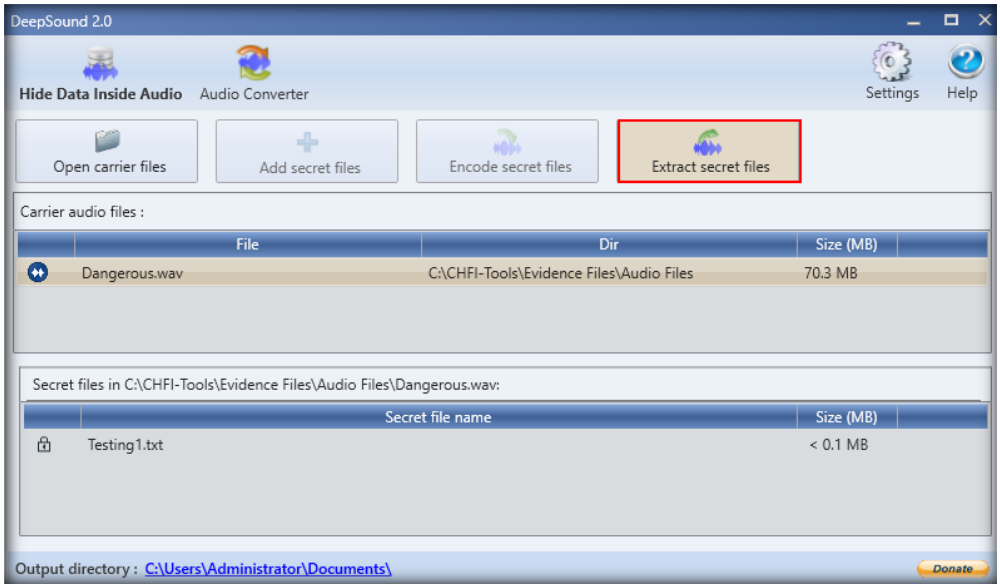

FIGURE 6.26: Extract secret files button

43. Post extraction, the tool will generate a message displaying the location of the extracted file. Click **OK**.

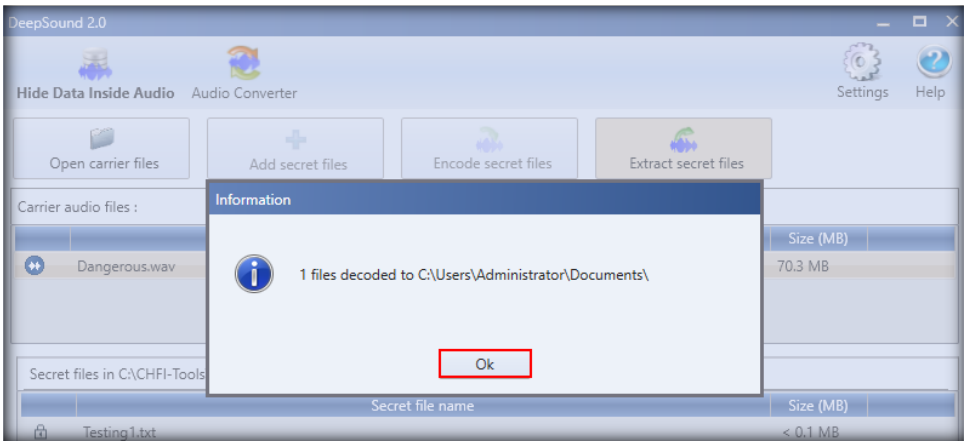

FIGURE 6.27: Hidden File extracted

44. To view the hidden file that was extracted in the previous step, navigate to the location displayed in the screenshot above, i.e., **C:\Users\Administrator\Documents**.

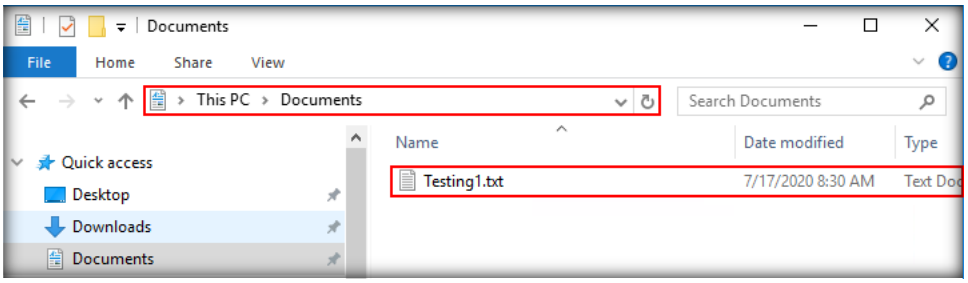

FIGURE 6.28: Extracted Hidden File in default destination

45. In this manner, you can detect and analyze data hidden in files of various format using steganography.

Lab Analysis

Analyze and document the results of 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

7

Detecting Alternate Data Streams

The use of Alternate Data Streams (ADS) is an anti-forensics technique that allows attackers to hide data in Windows NTFS; occasionally, these hidden Alternate Data Streams can be used to remotely exploit a web server.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

As part of a large criminal enterprise, attackers have stolen sensitive financial information of certain Europe-based MNCs by deceiving them through cyber-attacks. As part of their plan, the attackers used hidden ADS (Alternate data streams) to introduce and execute hidden rootkits and hacker tools in their target systems without being detected. A few days after the attacks, the MNCs discovered that their confidential financial information has been breached. The MNCs consulted expert forensic investigators to solve the case and secure their systems.

The challenge before the forensic investigators was to extract the information hidden in Alternate Data Streams that was used by the attackers to execute their plan. The hidden information extracted by forensic investigators from ADS can help the incident response teams of the MNCs in preventing the attackers from causing any further damage. As an expert forensic investigator, you must know how to extract information from hidden ADS.

Lab Objectives

The objective of this lab is to help you learn how to detect ADS.

Lab Environment

This lab requires the following:

- A computer running a **Windows 10** virtual machine
- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands

- A web browser with internet access
- **NoVirusThanks Stream Detector** located at **C:\CHFI-Tools\Module 05 Defeating Anti-Forensics Techniques\Alternate Data Stream Detection Tools**

Note: You can download the latest version of **NoVirusThanks Stream Detector** from https://www.novirusthanks.org/products/stream-detector/

If you use 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 concept of alternate data streams (ADS) and helps you understand how to detect ADS on a Windows system.

Lab Tasks

1. Login to **Windows 10** virtual machine.
2. Keep **Windows Server 2016** virtual machine powered **On** during this lab.

TASK 1

Detect Hidden Alternate Data Streams Using Windows PowerShell

3. In this lab, we will use Windows PowerShell to detect streams and view them. To launch PowerShell, right-click on the **Windows** icon and select **Windows PowerShell (Admin)**.

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

4. **Windows PowerShell (Admin)** launches. To identify hidden ADS through PowerShell, enter the command **gci -recurse | % { gi $_.FullName -stream * } | where stream -ne ':$Data'** and press **Enter**.

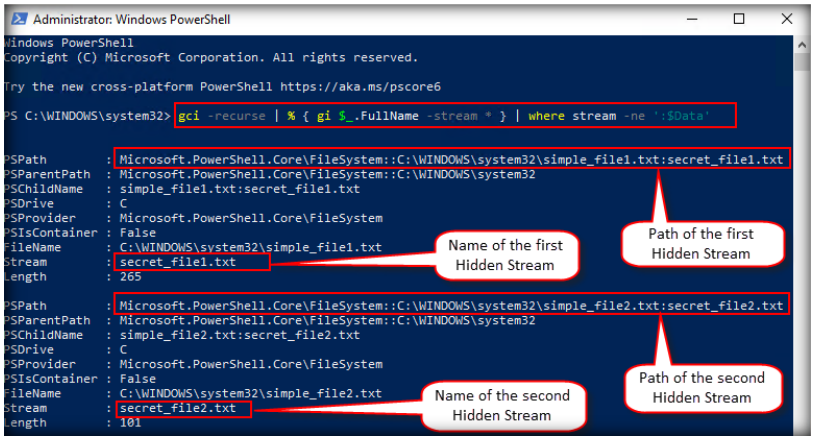

FIGURE 7.1: ADS in PowerShell

5. As seen in the above screenshot, running the command described in **Windows PowerShell** will detect the files containing ADS and display the results.

6. Now, we shall navigate to the path (here, **C:\Windows\System32**) where the text files **simple_file1.txt** and **simple_file2.txt** reside and open them.

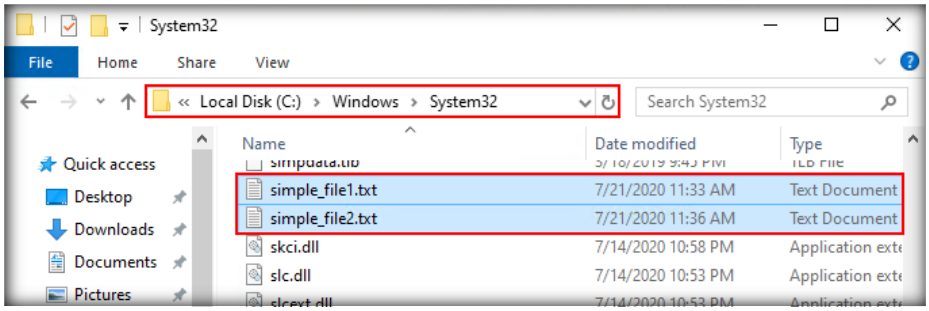

FIGURE 7.2: Files contains hidden ADS

7. The files, when opened, display the data they contain, but hidden alternate data streams cannot be viewed through Windows Explorer.

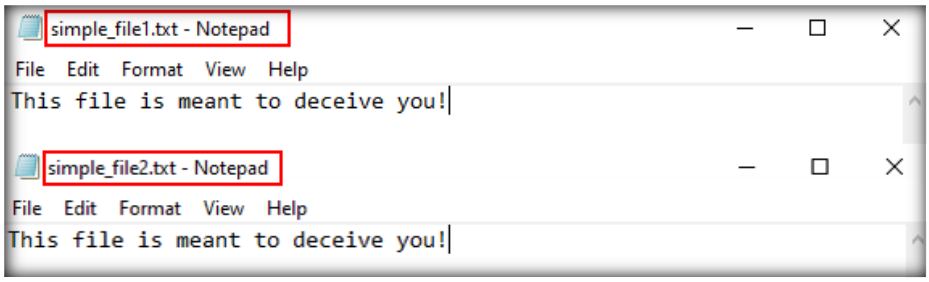

FIGURE 7.3: Opened Files

Note: For the demonstrative purpose of this lab, the simple files shown in the above screenshot display the line **This file is meant to deceive you!**. In a real scenario, files that contain ADS will display normal content that does not appear suspicious; attackers use files with normal content to hide their secret messages and prevent detection.

8. We shall now extract the hidden stream attached to the first file, i.e., **simple_file1.txt**. To extract the hidden stream, execute the command **get-content -path C:\WINDOWS\system32\simple_file1.txt -stream secret_file1.txt** in **Windows PowerShell**.

TASK 2

Extract and Display the Content Stored in hidden ADS

9. PowerShell will extract and display the content stored in the hidden stream as shown in the following screenshot:

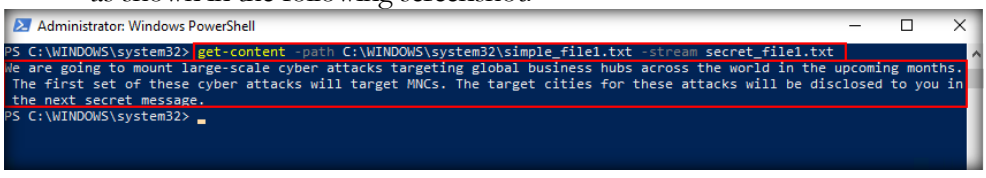

FIGURE 7.4: Content of the first stream

10. Similarly, we will now extract the hidden stream attached to the second file, i.e., **simple_file2.txt**. To extract the hidden stream, execute the command

get-content -path C:\WINDOWS\system32\simple_file2.txt -stream secret_file2.txt.

11. PowerShell will extract and display the content stored in the hidden stream as shown in the following screenshot:

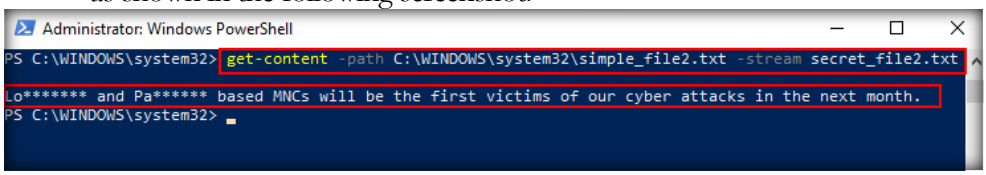

FIGURE 7.5: Content of the second stream

12. In this manner, we can use Windows PowerShell to identify streams and view ADS content.

TASK 3

Detect Hidden ADS Using NoVirusThanks Stream Detector

13. Now, we shall use **NoVirusThanks Stream Detector** to detect streams. To install, navigate to **Z:\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Alternate Data Stream Detection Tools\NoVirusThanks Stream Detector**, double-click on the **streamdetector_setup.exe** file to launch the setup, and follow the wizard-driven steps to install the application.

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, prompting you to enter the username and password for the **Windows Server 2016** virtual machine, enter the credentials and click **OK**.

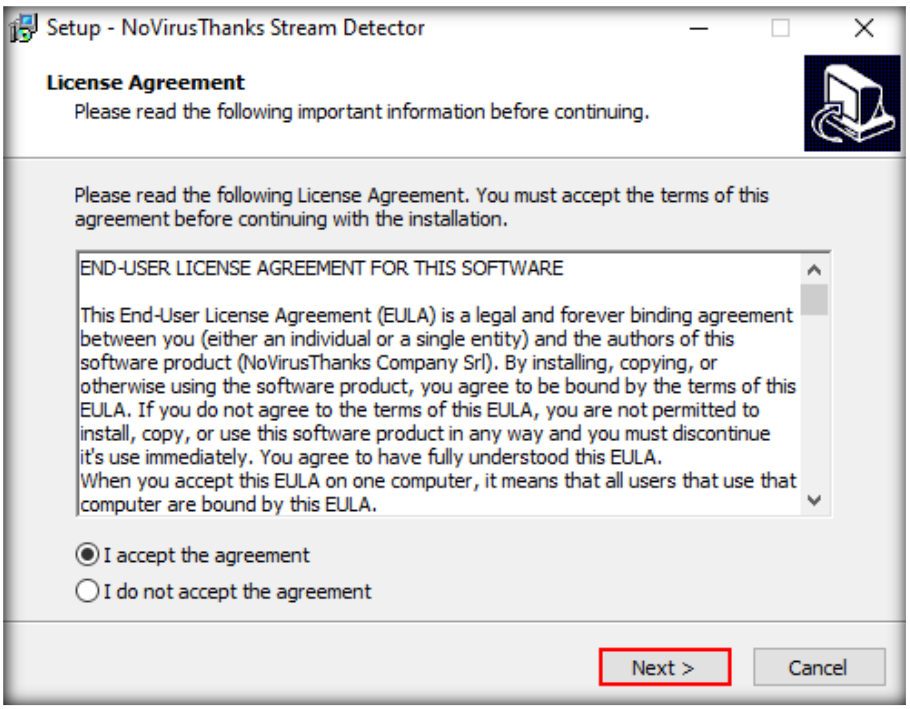

FIGURE 7.6: Setup wizard for NoVirusThanks Stream Detector

14. In the last step of the installation, ensure that **Open NoVirusThanks Stream Detector** is checked, and click **Finish**.

15. On completing the installation, the main window of **NoVirusThanks Stream Detector** appears, along with a browser window that displays a **novirusthanks** webpage. Close the web browser.

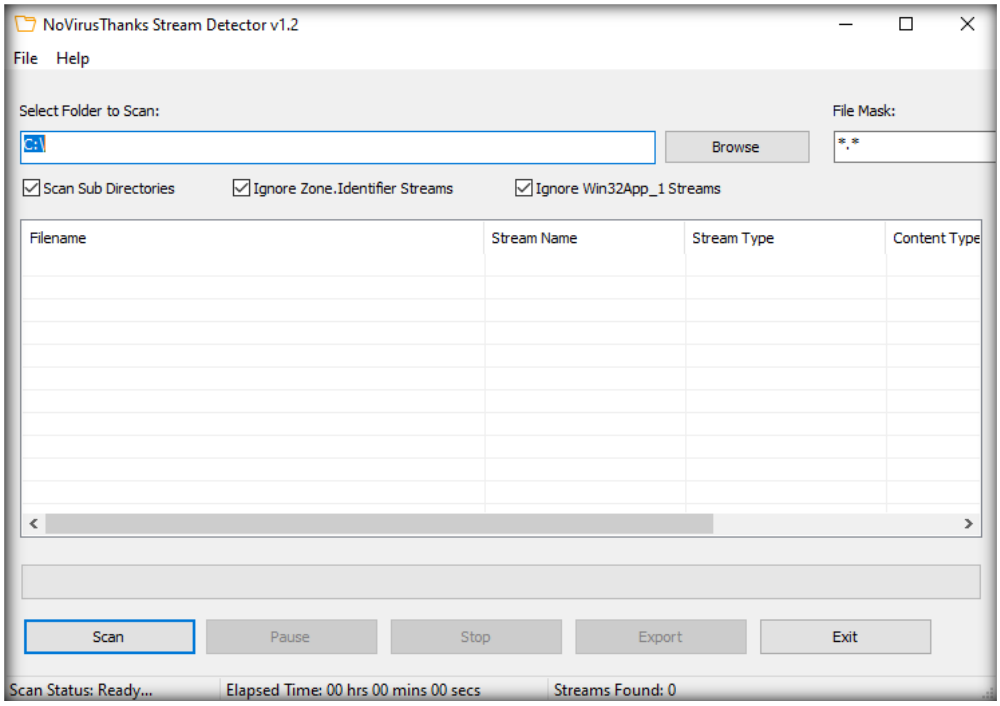

FIGURE 7.7: NoVirusThanks Stream Detector GUI

16. Now, we shall assign a folder to scan for ADS. In this lab, we will scan the files in **C:\Windows\System32**. So, click **Browse**.

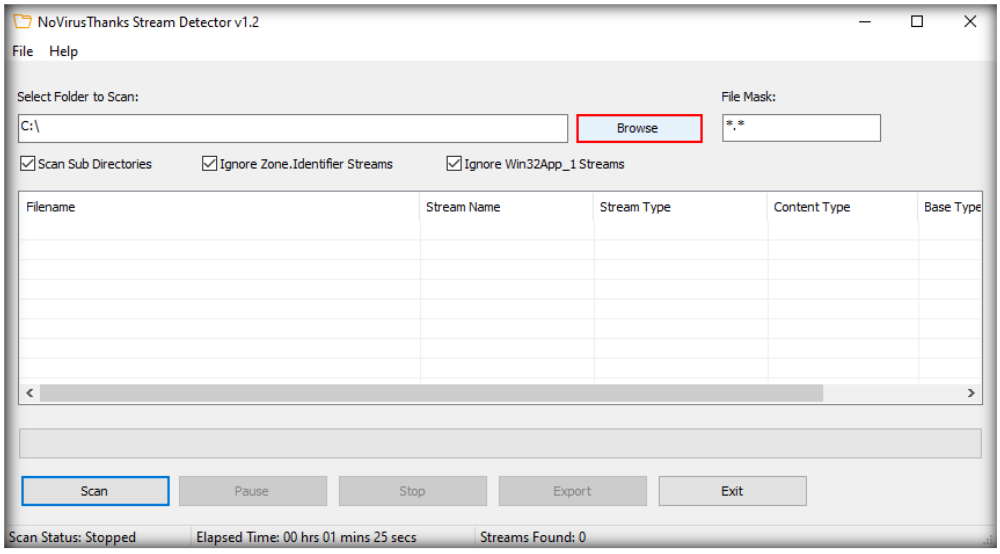

FIGURE 7.8: Clicking Browse

17. A **Browse for Folder** window will appear. Navigate and select the directory that you wish to scan for ADS (here, **C:\Windows\System32)** and click **OK**.

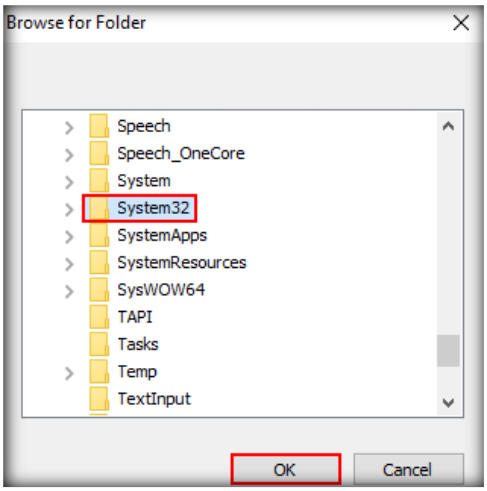

FIGURE 7.9: Browse for Folder window

18. The path of the selected folder will now appear in the **Select Folder to Scan** section. Click **Scan** to run a scan on the directory.

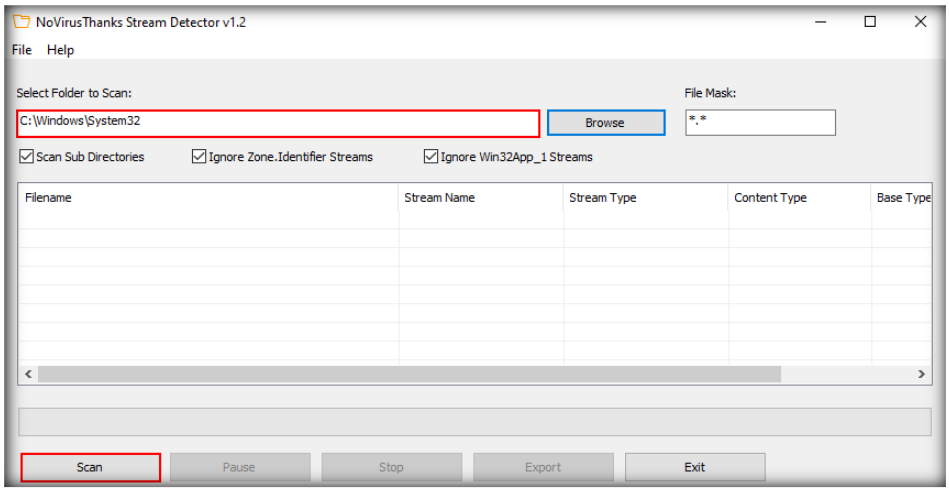

FIGURE 7.10: Scanning the browsed directory

19. The tool scans for ADS files. Upon completing the scan, it displays the streams present in the directory with details such as **Stream Name**, **Filename** (names of the files in which those streams exist), and **Size** of the files.

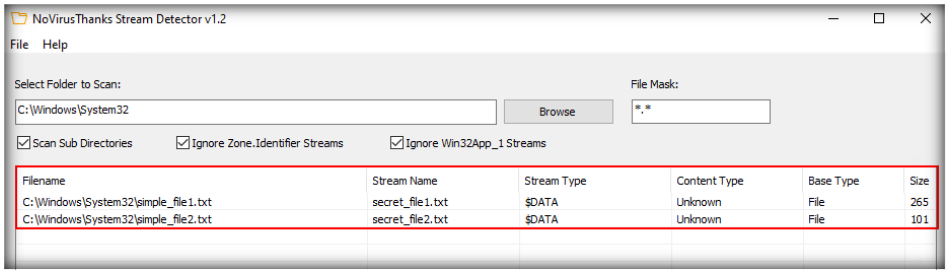

FIGURE 7.11: Hidden streams detected

20. If you wish to save the information displayed in the above screenshot, then click the **Export** button at the bottom of the window.

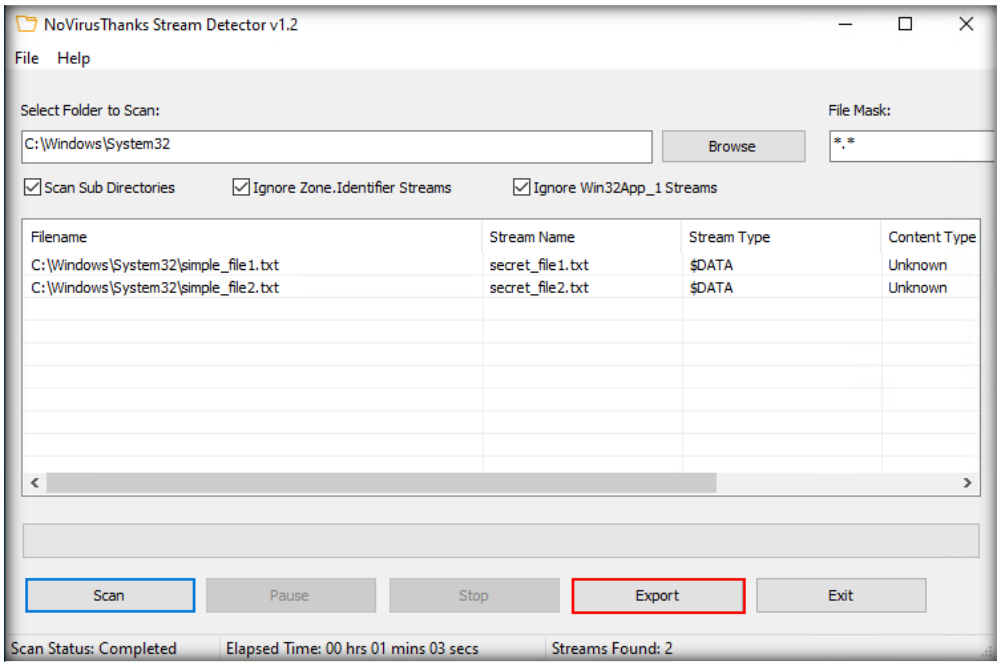

FIGURE 7.12: Clicking Export

21. A **Save file as...** window appears. Select the location where you wish to save the information (here, we will choose **Desktop** to save the information), leave the filename set to default, and click **Save**.

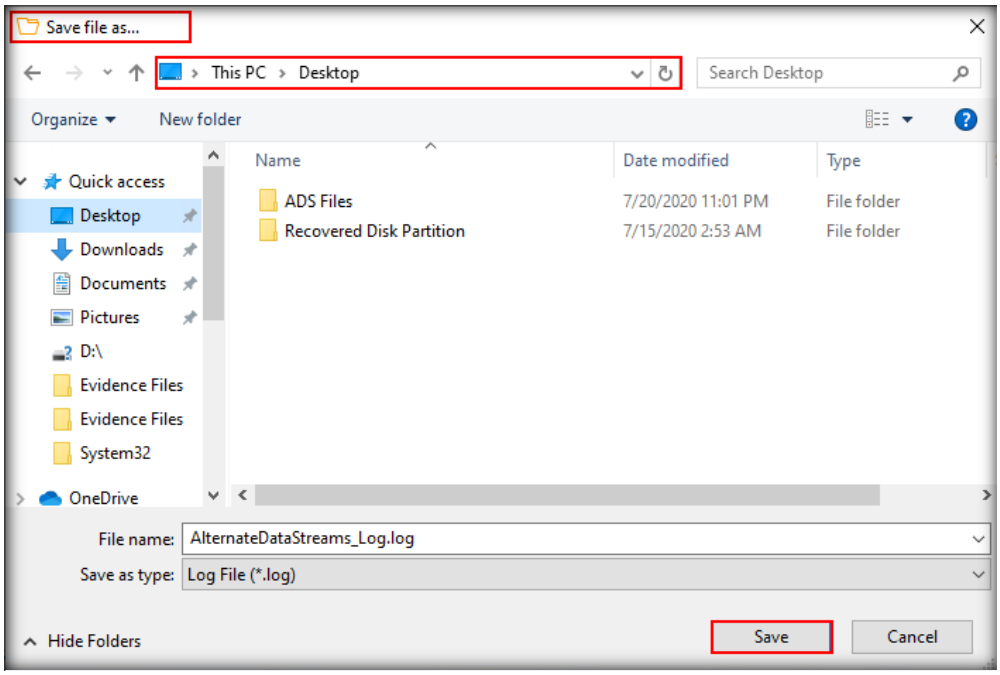

FIGURE 7.13: Save file as… window

22. The file will be saved and exported to **Desktop**. Navigate to **Desktop** and open the file to view the details of the files containing ADS.

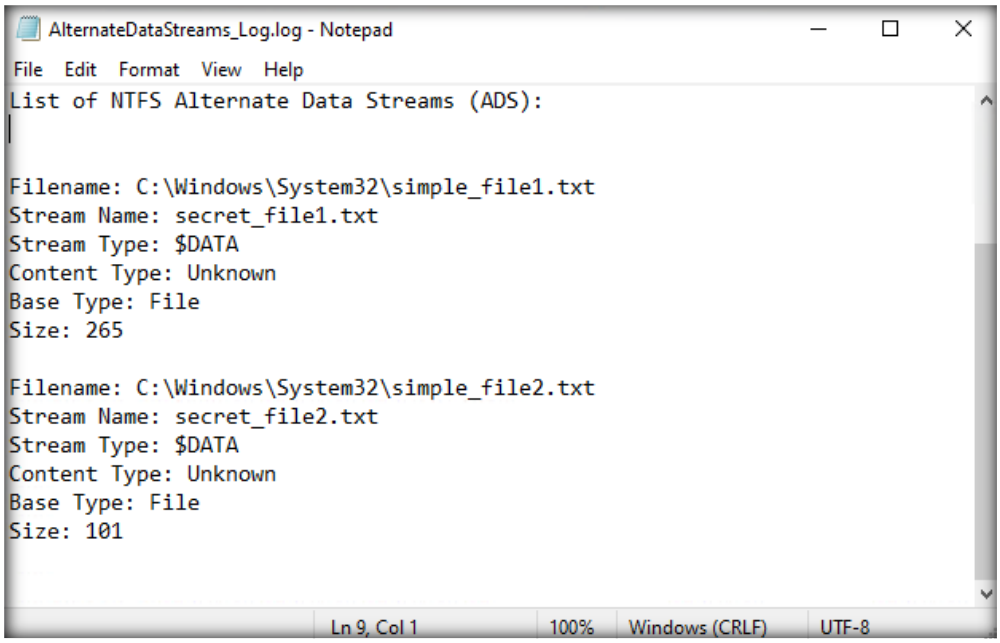

FIGURE 7.14: ADS Log

23. In this manner, you can detect streams on a machine and view them.

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

8

Detecting File Extension Mismatch

A file extension is an identifier specified as a suffix at the end of a filename. It helps identify the file type in operating systems such as Windows.

ICON KEY

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

Lab Scenario

An attacker has saved malicious files on a system for execution to steal sensitive user data. To mislead the firewall and anti-malware program on the system, they use the anti-forensics technique of changing the extension of those malicious files so that they remain undetected. The attacker may also have changed the extension of some of these malicious files to **.sys** to disguise them as system files and discourage the attention of forensic investigators. The investigators examining the system need to detect each of these malicious files so that they can be collected and studied for further investigation.

To be an expert forensics investigator, you should know how to detect files with extension mismatch using the proper tool(s).

Lab Objectives

The objective of this lab is to help you learn how to detect file-extension mismatch.

Lab Environment

This lab requires the following:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands
- A web browser with internet access
- **Autopsy** for Windows installed on your virtual machine

Note: You can download the latest Windows-based version of Autopsy from https://www.autopsy.com/download/

If you use 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: 25 minutes

Overview of the Lab

This lab familiarizes you with the concept of file-extension mismatch and, with the help of the Autopsy tool, helps you understand how to detect a file-extension mismatch.

Lab Tasks

TASK 1

Detect File-extension Mismatch Using Autopsy

1. Login to **Windows Server 2016** virtual machine.
2. Launch **Autopsy** by double-clicking on its shortcut icon on the **Desktop**. Upon launching Autopsy, the tool's main window will open, along with its **Welcome** window. In the **Welcome** window, click on **New Case**.

FIGURE 8.1: Selecting New Case

3. A **New Case Information** window opens, prompting you to input the **Case Name** and **Base Directory**. The base directory is the location where the case data is to be stored. The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as **File Extension Mismatch**.

4. We will save the case data in the **Image File Analysis** folder located in **Desktop**. So, assign this folder as the **Base Directory** and click **Next**.

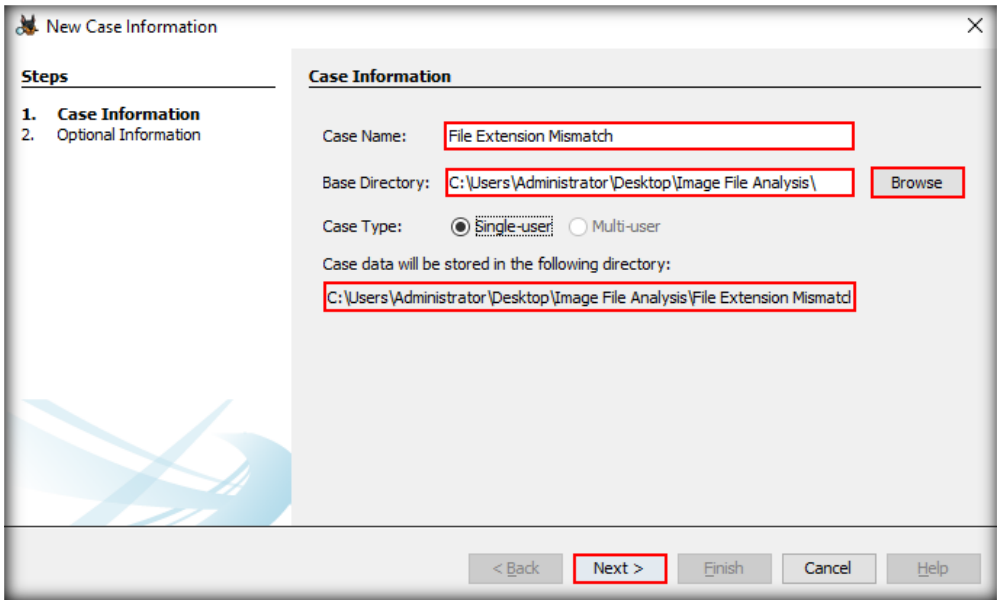

FIGURE 8.2: Case Information section

5. The **Optional Information** section appears. Enter the **Case Number** and **Examiner Details** (here, we have entered the **Case Number** as **102**). You may enter your details in the **Examiner** section. Click **Finish**.

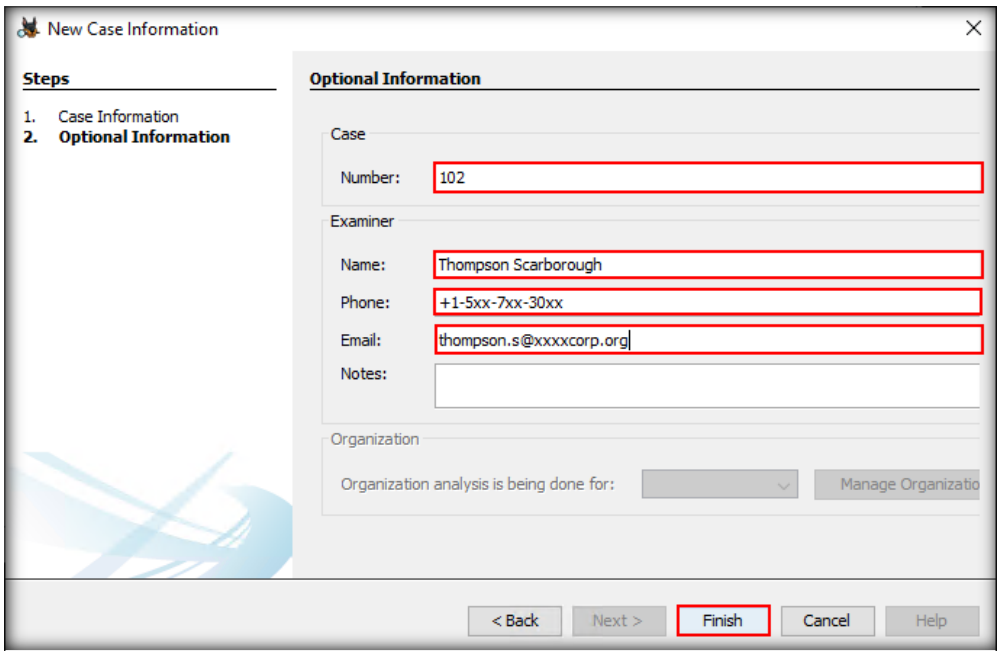

FIGURE 8.3: Optional Information section

6. The application will take a moment to create the case.

7. After creation of the case, the **Add Data Source** window appears. Under the **Select Type of Data Source to Add** section, ensure that the **Disk Image or VM File** option is selected. Click **Next**.

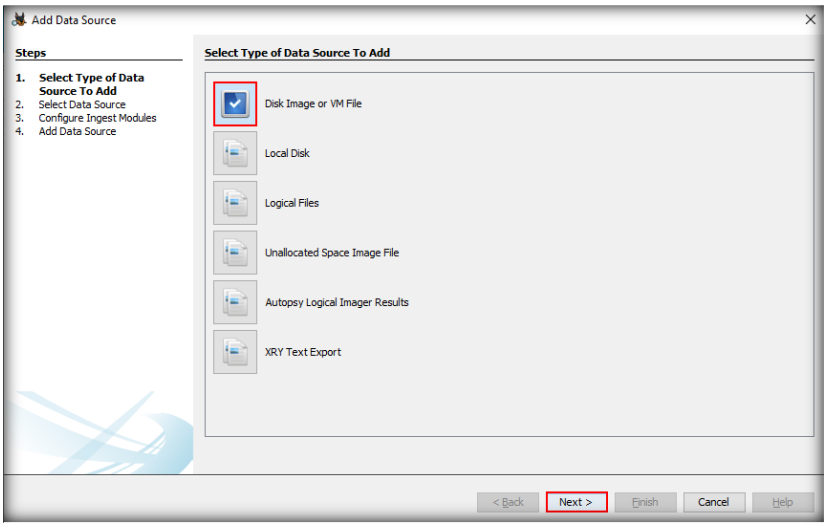

FIGURE 8.4: Selecting Disk Image or VM File

8. **The Select Data Source** section appears. Click **Browse** to choose the source image file, as highlighted in the screenshot:

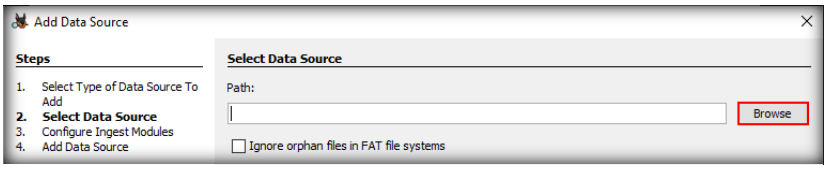

FIGURE 8.5: Select Data Source section

9. On clicking **Browse**, an **Open** window appears. Navigate to **C:\CHFI-Tools\Evidence Files\Forensic Images** and select the file **Windows_Evidence_001.dd**. Click **Open**.

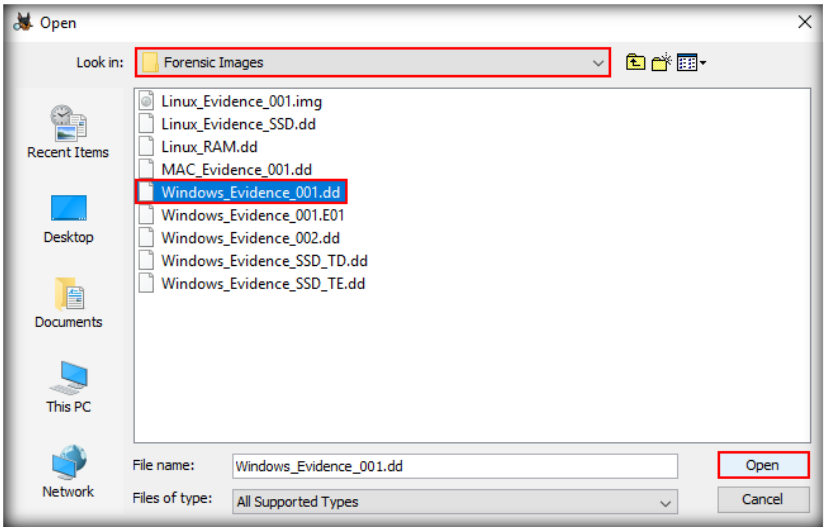

FIGURE 8.6: Selecting the source image file

10. Now, the path to the **Windows_Evidence_001.dd** file will be displayed in the **Path** field, as shown in the screenshot below. Click **Next**.

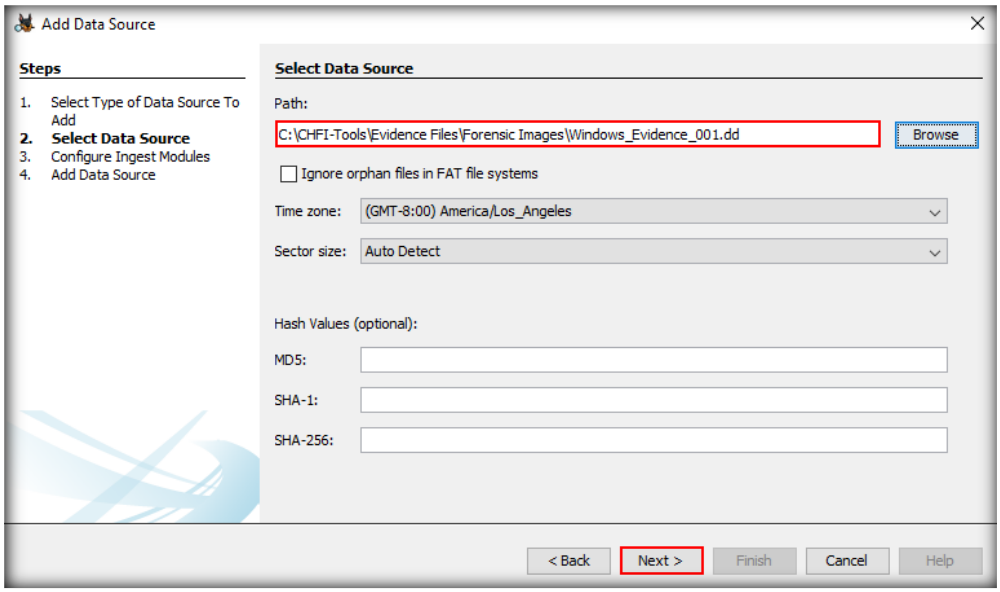

FIGURE 8.7: Select Data Source section

11. Now, the **Configure Ingest Modules** section appears. In the **Run ingest modules on:** column, select the options according to your requirement. Here, we have checked **File Type Identification, Extension Mismatch Detector** and **Embedded File Extractor** options. Once done, click **Next**.

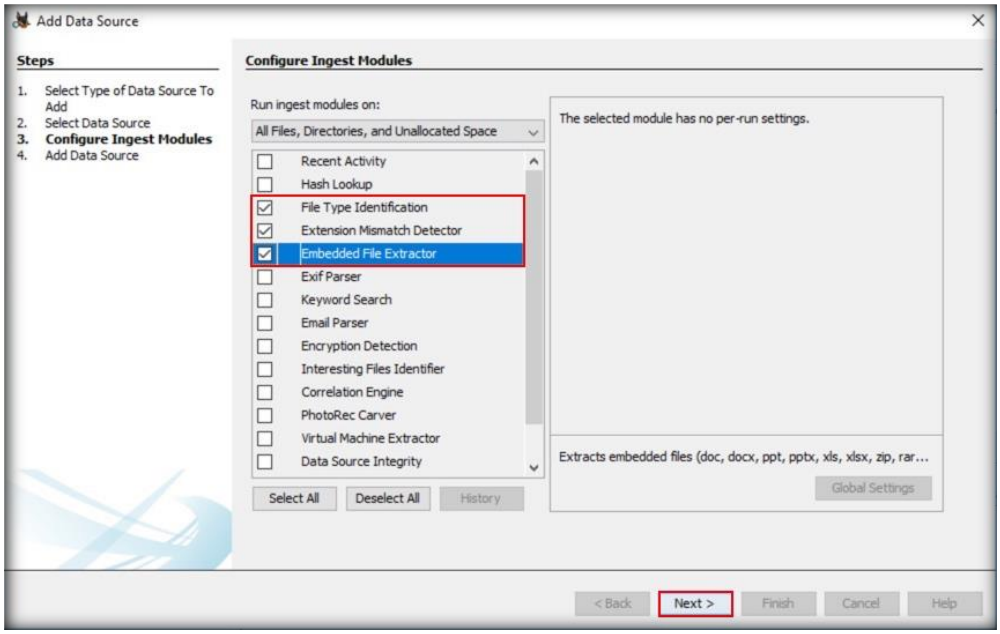

FIGURE 8.8: Configure Ingest Modules section

12. The **Add Data Source** section now appears, displaying the message **Data source has been added to the local database. Files are being analyzed.** Click **Finish**.

Note: The tool will take some time to analyze the provided image file.

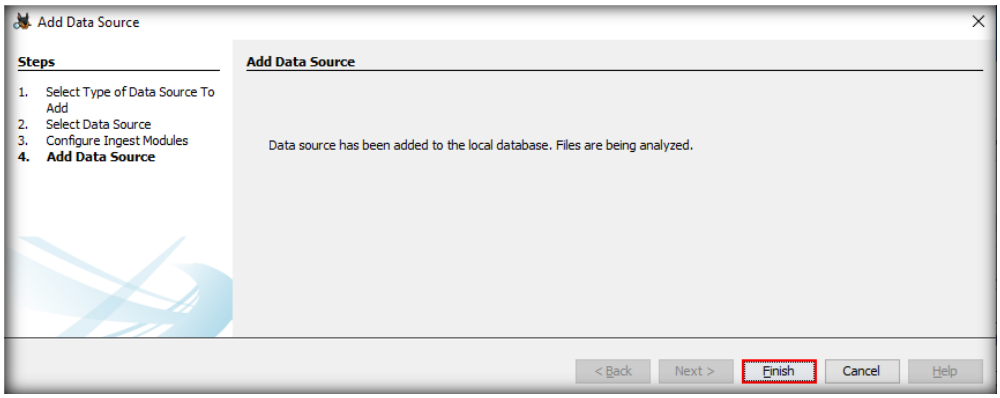

FIGURE 8.9: Add Data Source section

13. The tool will now take you to its main window. Expand the **Data Sources** node in the left pane of the window. The **Data Sources** option will list the name of the image file you have analyzed (in this case, it is **Windows_Evidence_001.dd**).

Note: Autopsy utilizes most of the virtual machine's resources while scanning the image. The machine might be unresponsive until the scanning is completed. It is recommended not to access the machine until the scanning is **100% completed**.

14. Click the image filename (here, **Windows_Evidence_001.dd**) to view its contents in the right pane of the tool window. It includes all the necessary operating system data.

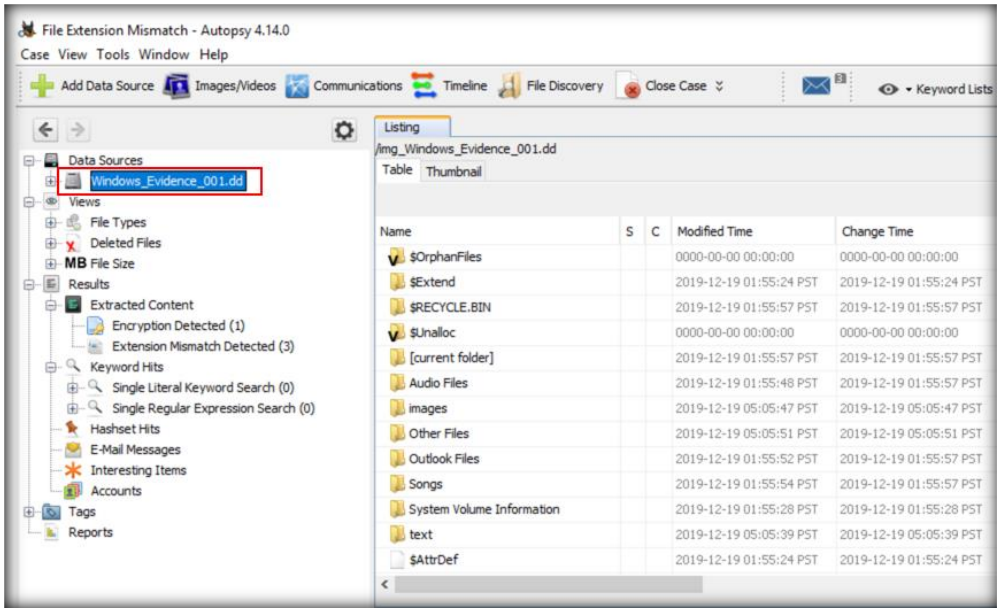

FIGURE 8.10: Extension Mismatch Detected loaded under Results tab

15. To view the files that have been detected with an extension mismatch, click the **Extension Mismatch Detected** category in the left pane. The tool will then display the files with extension mismatch in the right pane of the window, as shown in the following screenshot:

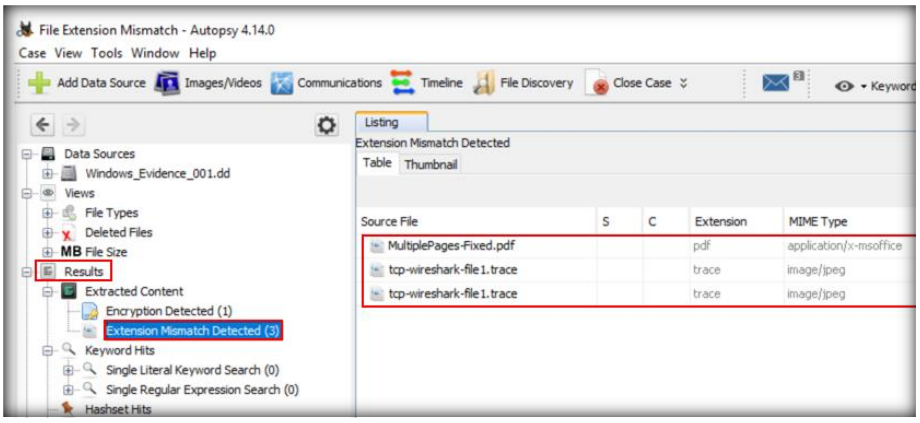

FIGURE 8.11: Files with extension mismatch in the right pane

Note: In the above screenshot, the **Extension** column in the right pane of the window displays the modified extensions of the files, while the **MIME Type** column displays their original extensions. As the extensions of the files have been modified, it means that they have been tampered with.

16. To view the content(s) of a file with extension mismatch, select the file; its contents will be displayed in the lower pane of the window, as shown in the following screenshot (here, we have selected the file **tcp-wireshark-file1.trace**. Selecting this file displays the image of an electronic circuit in the lower pane of the window. As can be seen in the screenshot below, **.trace** is the modified extension of this file, while **.jpeg** is its original extension.

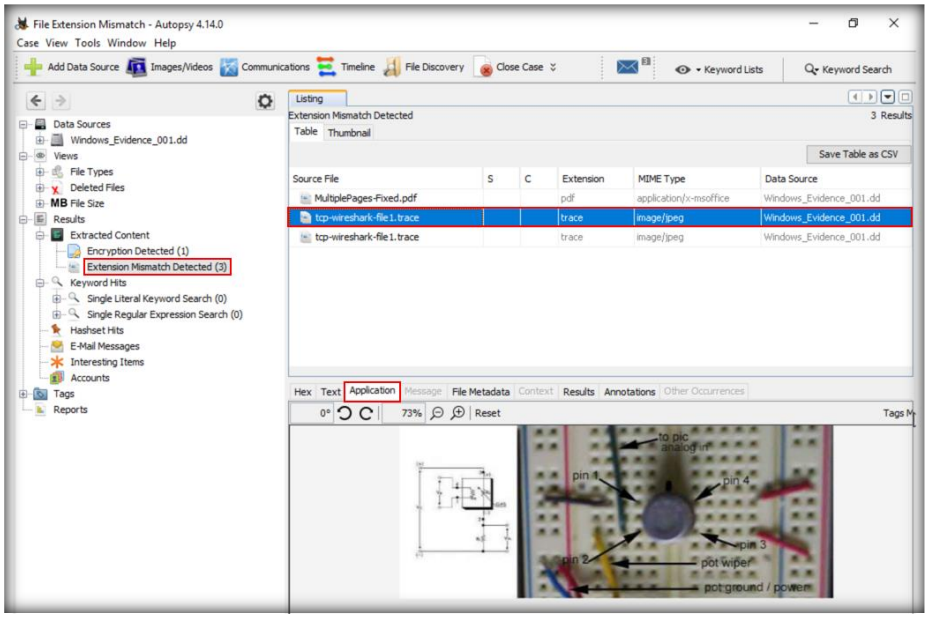

FIGURE 8.12: Viewing the content of a file

Note: When you select an image file, the tool will show you its content(s) under the **Application** tab of the lower pane of the window by default. You may also click on the **Hex, Text, File Metadata**, and other tabs to view the respective data stored under them.

17. In this manner, you can identify files with tampered extensions, view their original extensions, and perform further analysis if required.

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

9

Unpacking Program Packers

Using program packers is an effective anti-forensics technique for an attacker to prevent malicious programs on a system from being detected.

ICON KEY

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

Lab Scenario

An attacker saved a malicious program file in the workstation computer used by an accountant at a stockbroking company. The attacker had disguised the malicious file as a harmless file by using a program packer. The program packer allowed the malicious file to be executed on the system without being detected by the system's firewall and anti-malware program. The packed malicious file caused sensitive information stored on the target system to be compromised. The company consulted a forensic investigation agency to crack the case and secure its systems. As an expert forensic investigator, you must know how to unpack packed files.

Lab Objectives

The objective of the lab is to help you learn how to unpack packed program files.

Lab Environment

This lab requires the following:

- A computer running a **Windows Server 2016** virtual machine
- Administrative privileges to execute commands
- A web browser with internet access
- **Exeinfo PE** tool located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-Forensics Techniques\Program Unpacking Tools\ExeInfo PE**
- **UPX** located at **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-Forensics Techniques\Program Unpacking Tools\UPX**

Note: You can download the latest version of **Exeinfo PE** from http://exeinfo.atwebpages.com

Note: You can download the latest version of **UPX** tool from https://upx.github.io

If you use 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 process of identifying the packer used to pack a file by using ExeInfo PE and then unpacking the file using UPX.

Lab Tasks

TASK 1

Identify the Packer

1. Login to **Windows Server 2016** virtual machine.
2. In this lab, our first task is to identify the packer used to pack a file named **Infected.exe** located in **C:\CHFI-Tools\Evidence Files**.
3. We will use ExeInfo PE to perform this task. Navigate to **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-Forensics Techniques\Program Unpacking Tools\ExeInfo PE** and double-click the **exeinfope.exe** file to launch the tool.
4. The main window of the tool appears, as shown in the following screenshot:

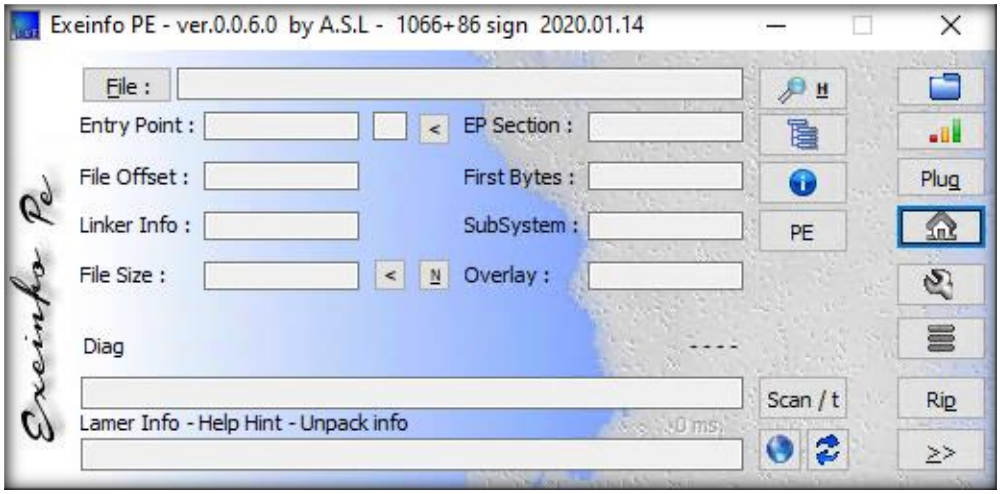

FIGURE 9.1: Exeinfo PE tool

5. Click on the **Open file** icon in the right pane of the main tool window, as highlighted in the screenshot:

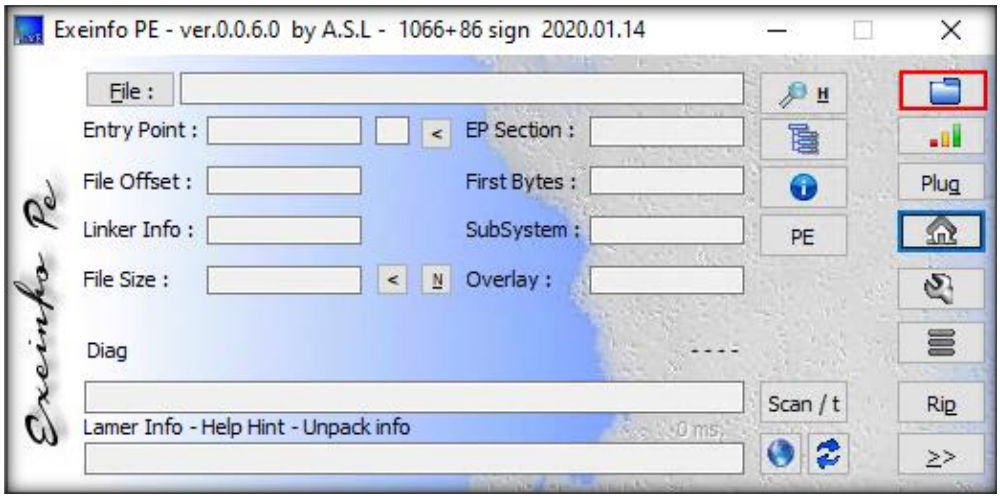

FIGURE 9.2: Clicking the Open file icon

6. The **Open EXE,DLL file** window will appear. Navigate to **C:\CHFI-Tools\Evidence Files**, select the file **Infected.exe**, and click **Open**.

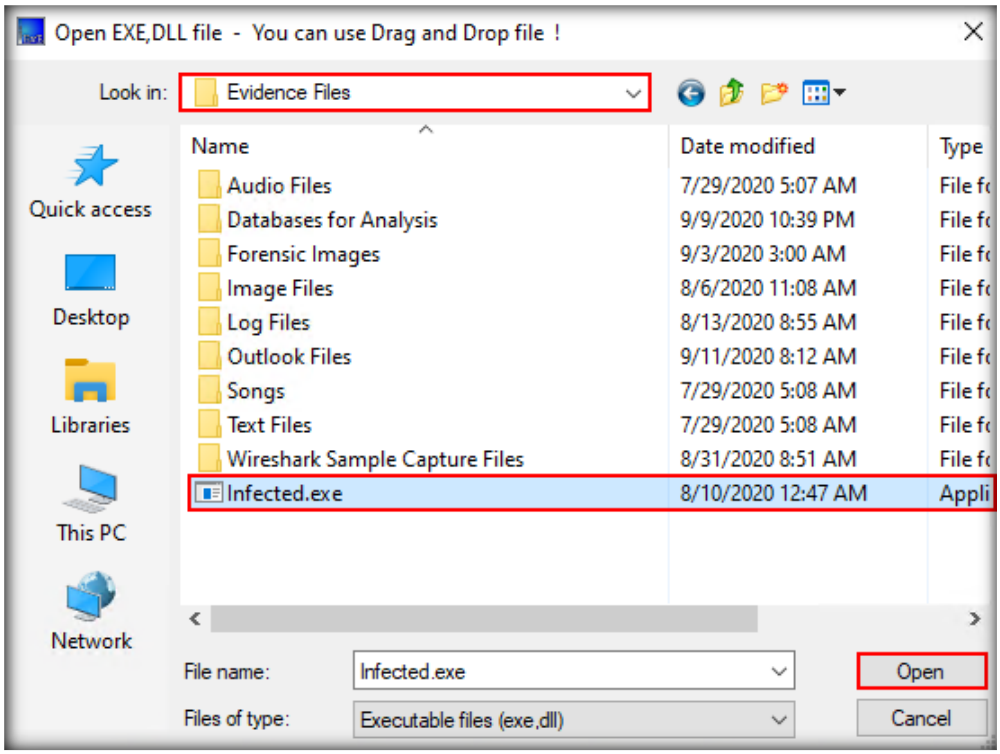

FIGURE 9.3: Open File window

Note: For the demonstrative purpose of this lab, the target evidence file has been named **Infected.exe**. In a real scenario, a malicious program file might bear a name that appears normal. Attackers disguise malicious files as normal files by using program packing tools so that they remain undetected by the firewall and anti-malware software on a system.

7. The tool's main window will now display the details of the application that was used to pack the selected executable file (i.e., **Infected.exe**).

FIGURE 9.4: Analyzing the executable file

8. From the above screenshot, it can be seen that the selected executable file was packed using the tool **UPX**. Therefore, we will be using the same tool (**UPX**) to unpack it. Close the **ExeInfo PE** window.

TASK 2

Unpack the File

9. We will run the UPX utility through **Command Prompt**. Navigate to **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Program Unpacking Tools**, select the **UPX** folder, hold the **Shift** key, and right-click on the **UPX** folder.
10. Select **Open command window here** from the context menu.

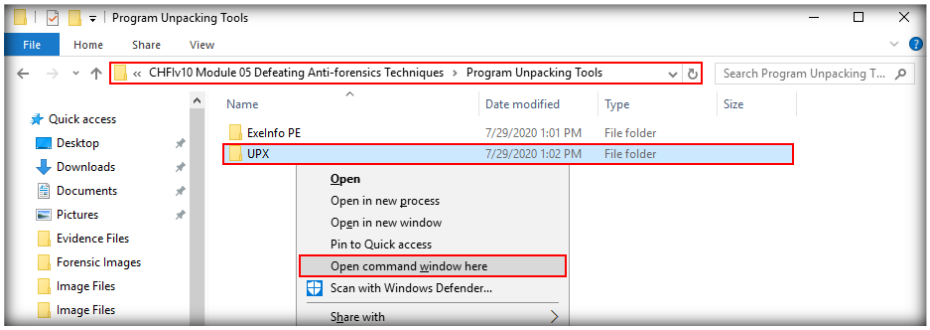

FIGURE 9.5: Selecting 'Open command window here'

11. **Command Prompt** opens, with the path set to **C:\CHFI-Tools\CHFIv10 Module 05 Defeating Anti-forensics Techniques\Program Unpacking Tools\UPX**.

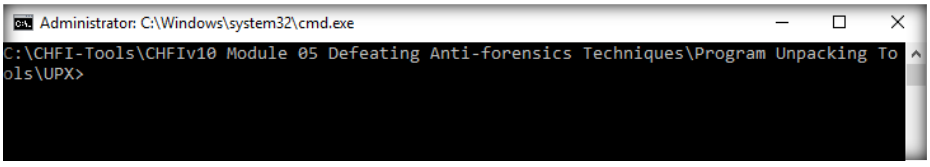

FIGURE 9.6: Command Prompt window

12. To unpack the target file, i.e., **Infected.exe** (located at **C:\CHFI-Tools\Evidence Files**), and save it as **Unpacked.exe**, run the command **upx.exe -d -o "C:\CHFI-Tools\Evidence Files\Unpacked.exe" "C:\CHFI-Tools\Evidence Files\Infected.exe"**.
13. The UPX tool **unpacks** the file successfully, as shown in the following screenshot:

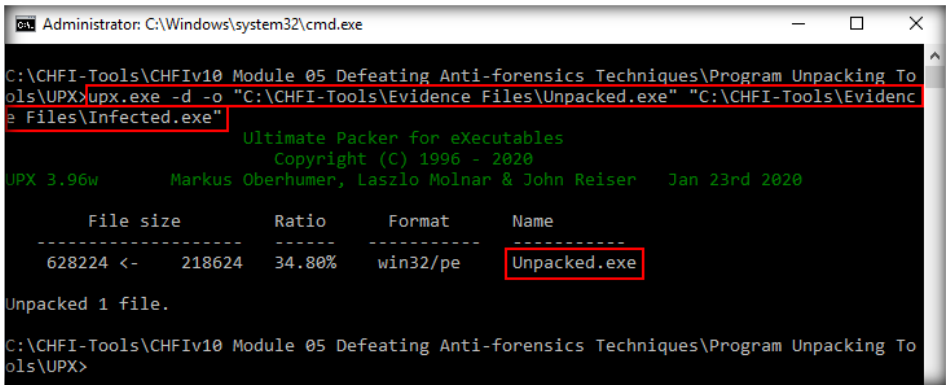

FIGURE 9.7: Running the UPX tool

14. The packed file has now been unpacked as **unpacked.exe** and saved to the **C:\CHFI-Tools\Evidence Files** directory, as shown in the screenshot:

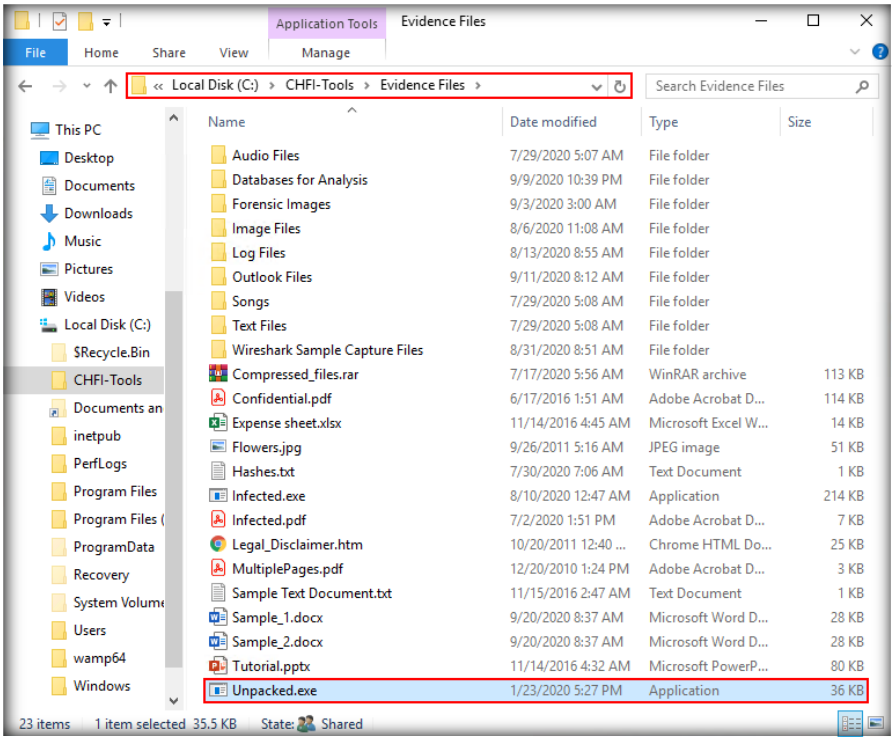

FIGURE 9.8: Location of the output file

15. This **Unpacked.exe** file is the original (uncompressed) file that was packed, and you can observe that its size is greater than that of the packed file.

16. In this manner, you can detect the packers used to pack files and unpack them using suitable tools.

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.