Data Acquisition and Duplication

Module 04

Data Acquisition and Duplication

Data acquisition is the process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Electronic evidence is fragile by nature and it can be very easily modified, destroyed, or damaged. Even the boot process can delete temporary files, modify stamps, or alter other data to writing data, and then create new files to the drive using the boot process.

Lab Objectives

The objective of this lab is to help students learn to **monitor** a system **remotely** and to extract **hidden text strings** and other tasks that include:

- Creating a dd image file
- Image file conversion from E01 to dd format
- Mounting image files on a Linux workstation
- Converting image file to a bootable virtual machine
- Memory acquisition (RAM) on Windows and Linux workstations
- Investigating NTFS streams from hard drives to create customized image files
- Investigating hidden text strings
- Extracting the hidden content from hard drives

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

To carry out the lab, you need:

- A computer running **Windows 10**, **Ubuntu**, and **Windows Server 2016** virtual machines
- A web browser with internet access
- Administrative privileges to run tools

Lab Duration

Time: 130 minutes

Overview of Data Acquisition and Duplication

Data acquisition is the process of gathering evidence or information. This can be done by using established methods to acquire data from a suspected storage media in order to get access to information about the crime or other incident and potentially using that data as evidence to convict a suspect.

Data duplication is a critical process in any computer forensic investigation. Many duplication tools are available that can duplicate or create a copy of data. To start an investigation, a person who wants to examine data on a suspect machine needs to create an image of the disk.

Lab Tasks

Recommended labs to assist you in data acquisition and duplication:

- Creating a dd Image of a System Drive
- Converting Image File from E01 Format to dd Format
- Mounting Images on a Linux Forensic Workstation
- Converting Acquired Image File to a Bootable Virtual Machine
- Acquiring RAM from Windows and Linux Workstations
- Creating Customized Images from an Image Containing NTFS File System
- Viewing Contents of Forensic Image File

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on the forensic investigation.

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

Lab

1

Creating a dd Image of a System Drive

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

ICON KEY

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

Lab Scenario

Jason, a forensics investigator, is appointed to examine a suspect's computer. Examining suspect's machine directly would result in loss of data and hence it is necessary to generate a forensic copy/image of the suspect machine's hard disk. The investigator needs to perform forensic examination on the acquired evidence file and retrieve potential artifacts that could be useful for investigation.

As a forensics investigator, you need to know how to create a dd image of any system drive.

Lab Objectives

The objective of this lab is to help you understand how to create a dd image of system drive using dd tool in Windows OS.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

This lab requires:

- A system running **Windows 10** virtual machine
- A system running **Windows Server 2016** virtual machine
- Administrative privileges to execute the commands
- A web browser with internet access
- **dd.exe** installer for Windows located at **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\dd**

Note: You can download the latest Windows based version of **dd** tool from the link http://www.chrysocome.net/dd on Windows machine

If you are using the latest version of tool 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 physical acquisition of a system drive/disk using the dd command.

Lab Tasks

TASK 1

Introduction to the Lab

1. Physical acquisition of the suspect disk/drive usually requires an external data storage medium, such as a hard disk or a pen drive, to collect the image generated during physical acquisition process.
2. In this lab, we will be performing physical acquisition of the primary disk/internal disk (**PHYSICALDRIVE0**) of the **Windows 10** virtual machine using **dd** command. Acquisition usually requires an external data storage device for storing the image. However, since this is a lab environment, we are using a secondary physical disk (**PHYSICALDRIVE1**, created during the lab setup) assuming it as an external storage device to store the image. Therefore, we will be treating this disk as an external disk for this lab.

TASK 2

Copy the Tool and List the Drives

3. Login to the **Windows 10** virtual machine.
4. Before beginning this lab, copy **dd** folder from **Z:\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools** and paste it onto **Desktop**.

FIGURE 1.1: Copy dd Folder onto Desktop

5. To obtain information about the available drives on Microsoft Windows, we will issue the **wmic** command in **Windows PowerShell**.
6. To launch PowerShell as an administrator, right-click on the **Windows** icon and select **Windows PowerShell (Admin)**.

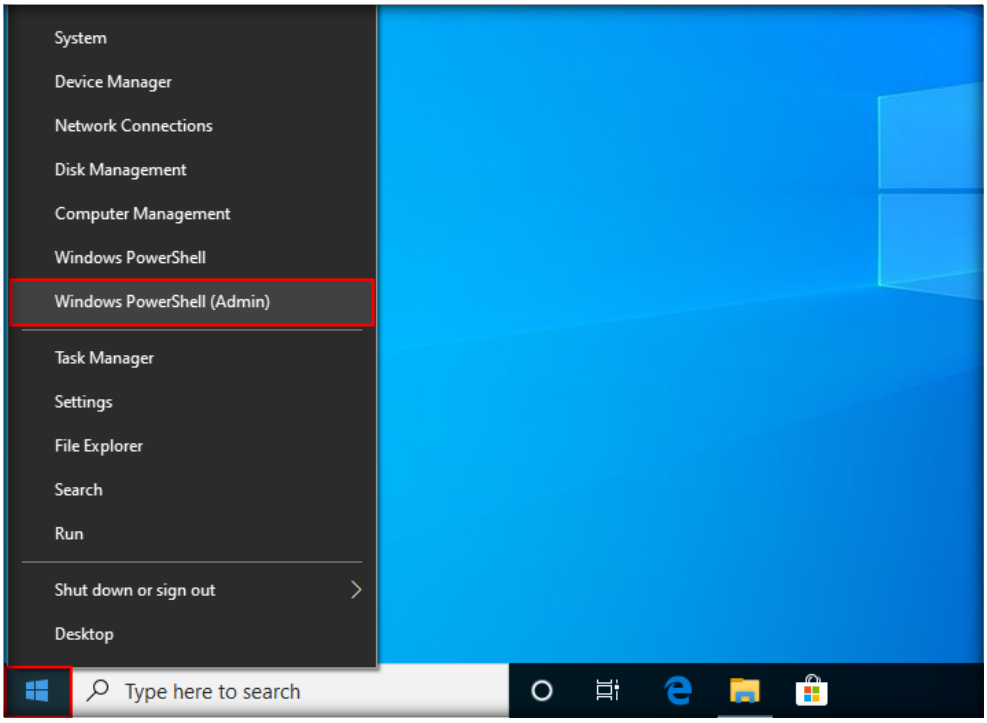


FIGURE 1.2: Launch Windows PowerShell

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

7. **Windows PowerShell** appears; type the command **wmic diskdrive list brief /format:list** and press **Enter**.

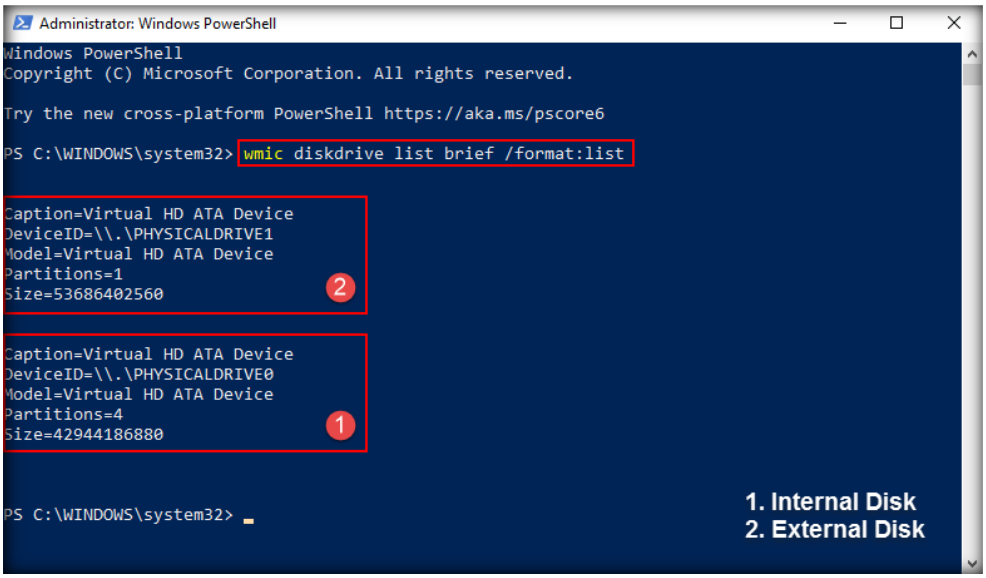


FIGURE 1.3: View Physical Disks Information using WMIC Utility

TASK 3

Create image file using dd command

8. Now, use **cd** command to navigate to the directory **C:\Users\Admin\Desktop\dd**.

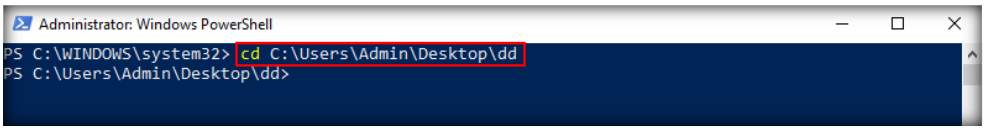


FIGURE 1.4: cd into dd Folder

9. Next, type the command .**dd.exe if=\\.\PHYSICALDRIVE0 of=F:\Windows_Evidence_002.dd bs=512k --size --progress** and press **Enter**. This begins to create a physical image of the drive **PHYSICALDRIVE0** in the **Forensic Disk** (**F:** in this lab) as shown in the following screenshot:

Note: The drive letter of the forensic disk may vary in your lab environment. You need to enter the letter that is associated with the forensic disk.

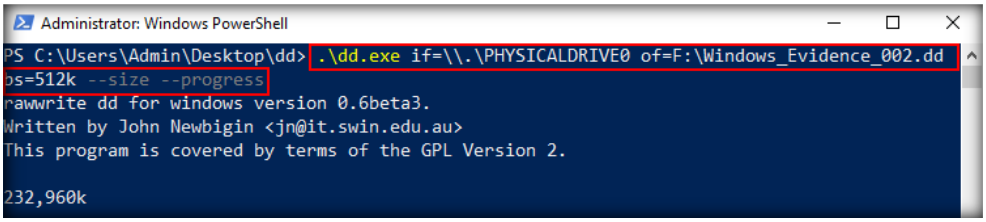


FIGURE 1.5: Creating dd Image Using dd Utility

10. It takes some time for the tool to create the image. Upon successfully creating the image, it displays the number of records in and the number of records out, as shown in the following screenshot:

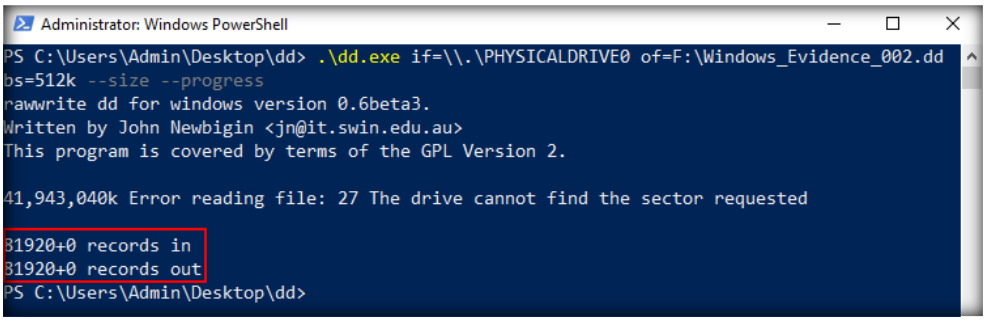


FIGURE 1.6: Imaging Process Completed

11. Navigate to the **Forensic Disk** (**F:** drive in this lab) to see the captured **dd image** file, as seen in the screenshot below:

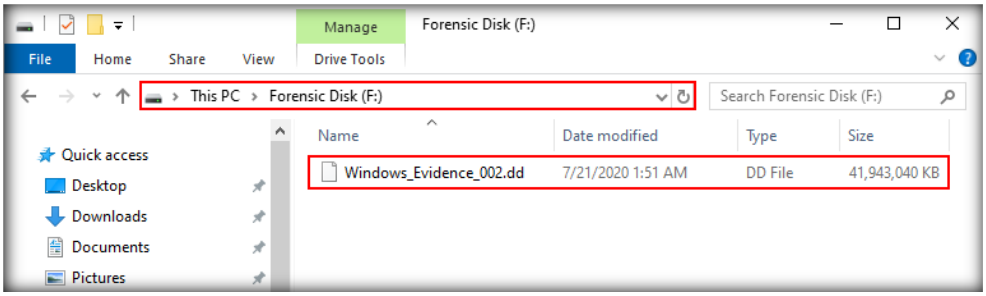


FIGURE 1.7: Location of dd Image

12. This image becomes the main source of examination for investigators in real-time. Depending on the type of forensic workstation and the investigator's requirements, these images are either examined directly through forensic tools or further converted into other forensic tool formats and bootable images.

Note: Delete this image file, in case you are running short of space for the upcoming labs.

13. This way, you can create a **dd image** of system drive during investigation process.

Lab Analysis

Analyze the file attributes and file systems of the disk partition image and document the results related to the lab exercise. Give your opinion of the target's file system.

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

Lab

2

Converting Image File from E01 Format to dd Format

E01 and dd are forensic image file formats to store bit-by-bit copy of storage devices such as hard disks, USB drives, etc.

ICON KEY

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

Lab Scenario

James, a forensics investigator, is appointed to examine an E01 format forensic image file on a Linux workstation. But forensic examination of E01 image file works perfectly only when the forensics workstation is Windows-based, not Linux-based. To examine E01 file format image file on a Linux workstation, the investigator needs to convert the E01 image file to dd file format.

As a forensics investigator, you should know how to convert the E01 file format to dd file format.

Lab Objectives

The objective of this lab is to help you understand how to convert E01 file format to dd file format using Linux commands.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

This lab requires:

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

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 xmount tool. It helps you understand how to convert E01 image file to dd image file on the Linux workstation for further analysis.

Lab Tasks

TASK 1

Converting E01 file format to dd file format

1. Make sure that the **Windows Server 2016** virtual machine is **powered on** before beginning this lab.
2. Login to the **Ubuntu Forensics** virtual machine.
3. Click on the **Files** icon in the **Launcher** panel to launch the **File Manager**.

FIGURE 2.1: Launch File Manager

4. **File manager** window will appear pointing to **Home** directory. Click on the bookmarked **chfi-tools on 10.0.0.16** directory.

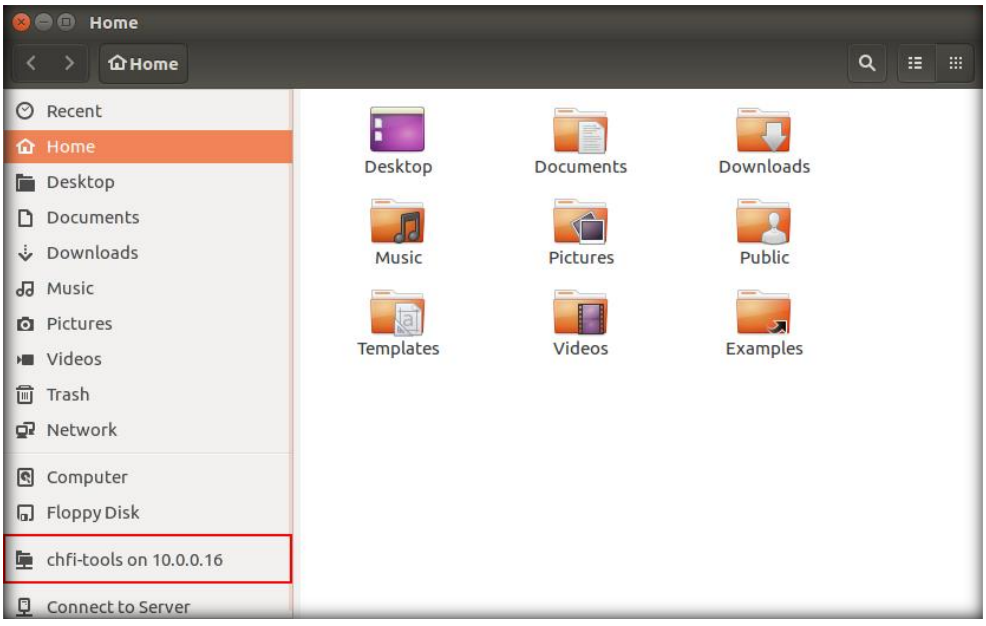


FIGURE 2.2: Enter CHFI-Tools Directory

5. **CHFI-Tools** shared folder appears, as shown in the following screenshot:

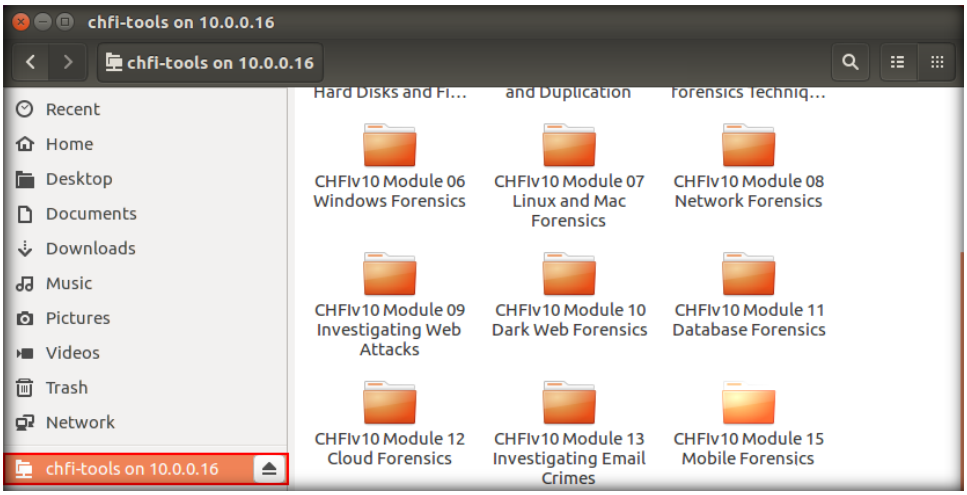


FIGURE 2.3: CHFI-Tools Shared Folder

6. Next, go to **Evidence Files → Forensic Images**. You will be able to view the **Windows_Evidence_001.E01** file in the images.

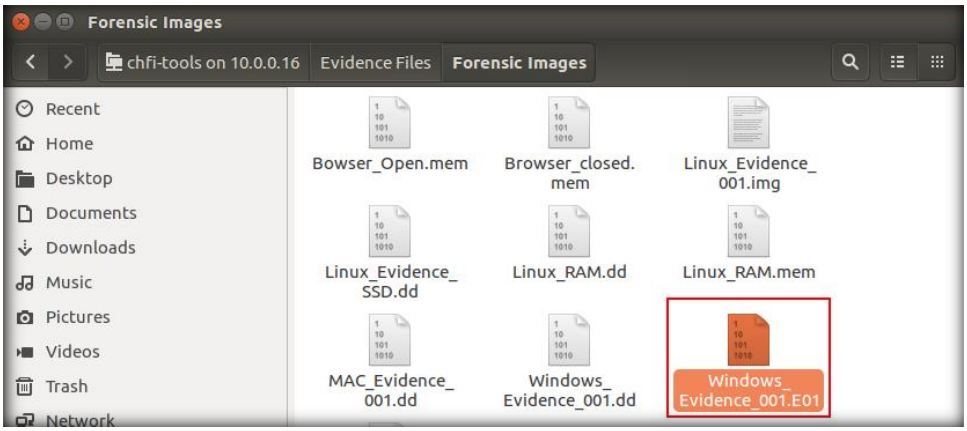


FIGURE 2.4: View the Specified Image File

7. In this lab, we are going to convert an image file with **E01** file format to **dd** file format. To do this, we need to install **xmount** tool.
8. Click on the **Terminal** icon from the launcher panel to launch the command line terminal.

FIGURE 2.5: Click on the Terminal

9. Command line terminal launches. You require root privileges in the terminal to install an application.
10. So, type **sudo su** and press **Enter**. You will be prompted to enter the password. Type **toor** as the password and press **Enter**.
11. Now, you will enter the **root** terminal as shown in the following screenshot:

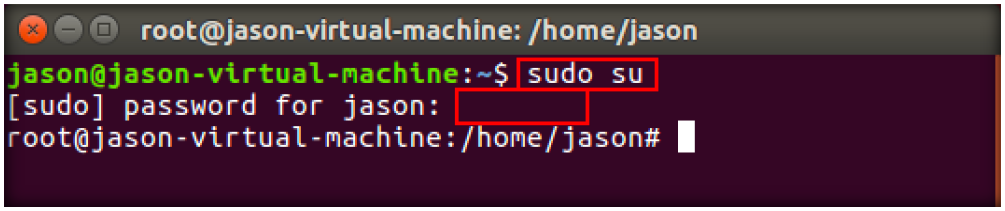


FIGURE 2.6: Run as super user

12. To install **xmount**, type the command **apt-get install -y xmount** and press **Enter**.

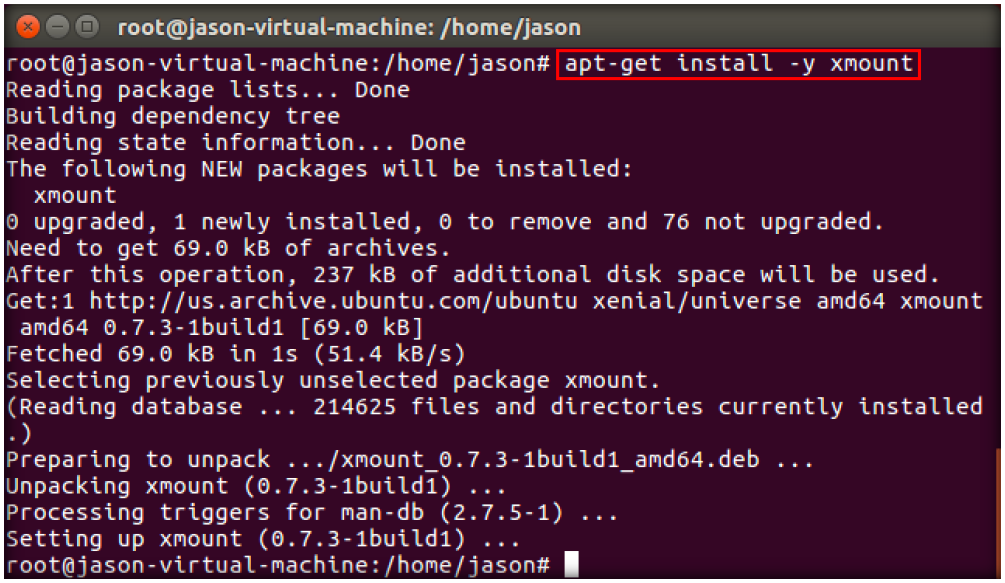


FIGURE 2.7: Installation of xmount Tool

Note: If you face any issues with the internet connectivity, run the commands **ifdown -a** followed by **ifup -a**; and then run the command **apt-get install -y xmount**.

Note: The **apt-get install -y xmount** command will not execute in case another process is using the apt command. In this scenario, restart the **Ubuntu Forensics** virtual machine and then run the command for **xmount** so that it executes successfully as shown in the above screenshot.

13. It is not possible to mount the evidence file from the shared directory; therefore, **copy** the **Windows_Evidence_001.E01** file from the shared directory into the **Home** directory of Ubuntu.

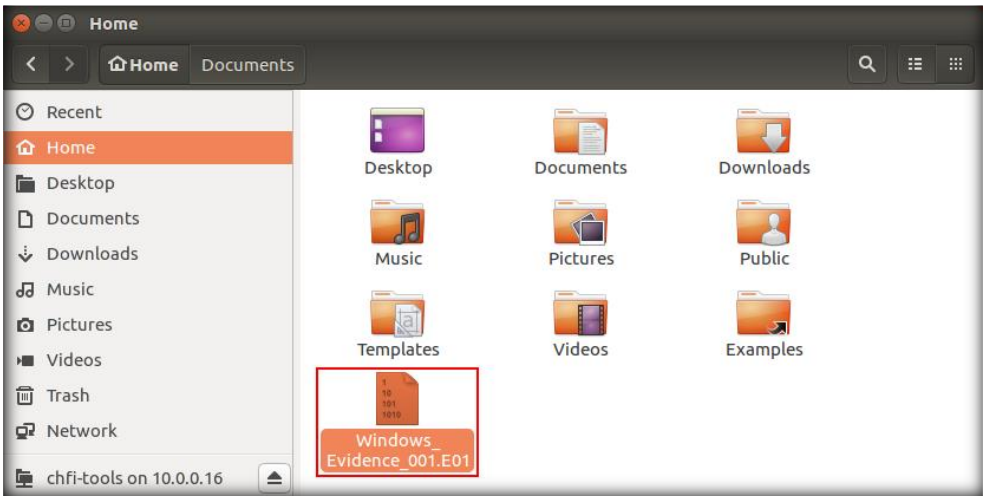


FIGURE 2.8: Copy Image File to Home Directory

14. To convert the E01 file using xmount and mount it, **execute** the command **xmount --in ewf Windows_Evidence_001.E01 /home/jason/Documents** in the terminal. This command converts the E01 file to dd file and mounts it onto **Documents** folder.

Note: Make sure that the mount directory is empty before executing the command. You may also create a new empty folder and provide the location of the created empty folder for mount directory.

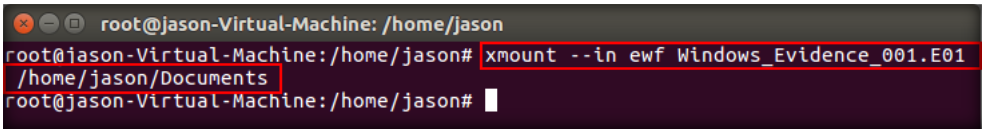


FIGURE 2.9: Converting E01 to dd Using xmount

15. The mounted drive (here, **Documents**) will be created on the system.

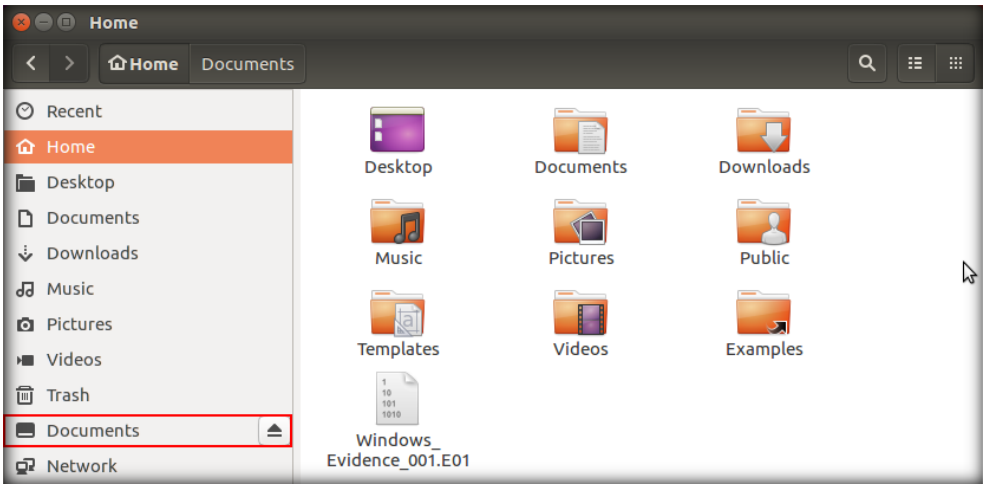


FIGURE 2.10: Click on the Mounted Documents Directory

16. Click on the mounted **Documents** directory to find **Windows_Evidence_001.dd** file, as shown in the following screenshot:

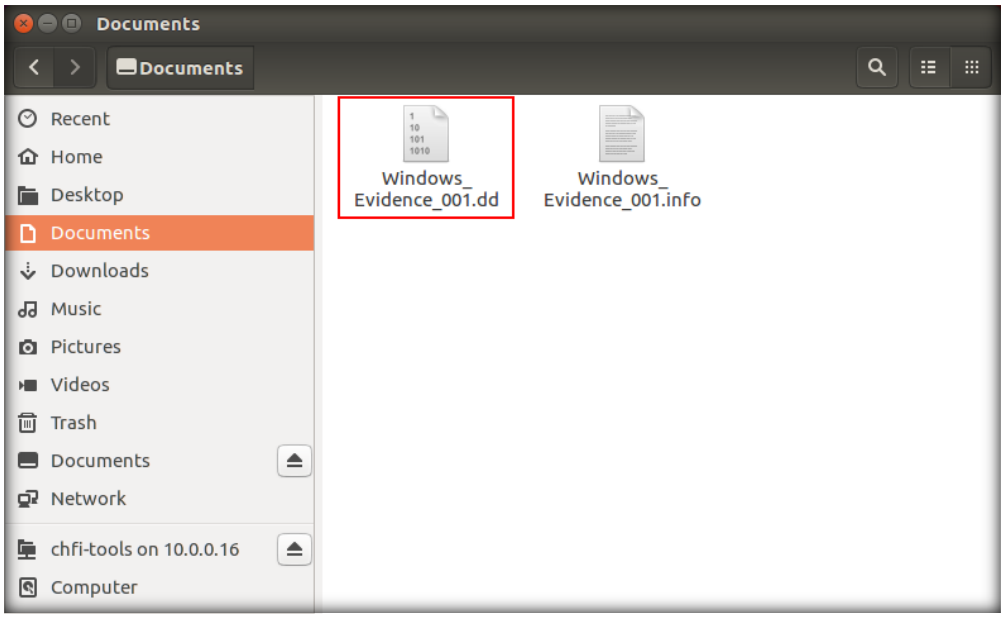


FIGURE 2.11: View the dd File

17. This way, you can convert the E01 file into dd file format for further examination.
18. The next task of an investigator would be to mount this file on the machine and view its contents. Mounting evidence files is covered in the next lab.

Lab Analysis

Analyze the file attributes and file systems of the disk partition image and document the results related to the lab exercise. Give your opinion of the target's file system.

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

Lab

3

Mounting Images on a Linux Forensic Workstation

Linux workstations can support various file systems and contains advanced tools that can help conduct forensic investigation.

Forensic image files are mounted on a drive to access and analyze files/folders present within the image file.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Forensic investigators generate image file of the evidence gathered from a hard drive to conduct investigation. In order to access and examine the files present in the image file, the investigator should mount the image file using different tools.

In some cases, the investigator ends up in a situation where he/she cannot use their preferred tool. Therefore, the forensic investigator should know how to mount different forensic file image formats on different workstations using different tools.

In this scenario, we consider mounting image files on a Linux forensic workstation.

Lab Objectives

The objective of this lab is to help you understand how to mount image files on a Linux forensic workstation:

- Mount a dd image file using mount command
- Mount a dd image file using a loop device

Lab Environment

This lab requires:

- A system running **Ubuntu Forensics** virtual machine
- A system running **Windows Server 2016** virtual machine
- Administrative privileges to install and run tools

- A web browser with internet access

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

Lab Duration

Time: 15 minutes

Overview of the Lab

In this lab, we shall demonstrate how to mount image files on a Linux forensic workstation.

Lab Tasks

TASK 1

Mount a dd Image using mount command

1. Make sure that the **Windows Server 2016** virtual machine is powered **on** before beginning this lab.
2. Login to the **Ubuntu Forensics** virtual machine.
3. This lab is a continuation of the previous lab. In the previous lab, we saw how to convert an E01 image to dd image. In this lab, we will see how to mount this converted image to view its contents.
4. So, click on the **Terminal** icon from the launcher panel to launch the command line terminal.

FIGURE 3.1: Click on the Terminal

5. Command line terminal launches. You require root privileges in the terminal to install an application.
6. Therefore, type **sudo su** and press **Enter**. You will be prompted to enter the password. Type **toor** as the password and press **Enter**.

7. Now, you will enter the **root** terminal as shown in the following screenshot:

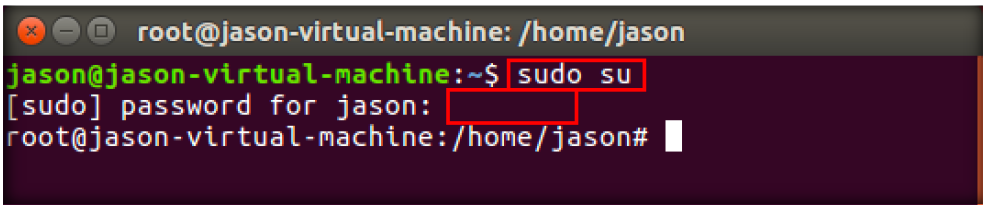


FIGURE 3.2: Run as super user

8. If you have not shut down the **Ubuntu forensics** virtual machine, and the **Windows_Evidence_001.dd** file is still mounted on **Documents** directory, skip to **Step no. 10**.

9. If you have rebooted the machine, the mounted image would disappear, and you need to again convert the E01 file using xmount and mount it. Therefore, type **xmount --in ewf Windows_Evidence_001.E01 /home/jason/Documents** and press **Enter**. This command converts the file and mounts it to **Documents** folder.

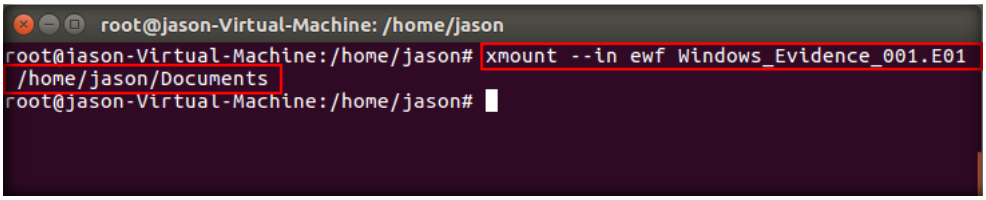


FIGURE 3.3: Converting E01 to dd Using xmount

10. The dd file appears in the **Documents** directory, as shown in the following screenshot:

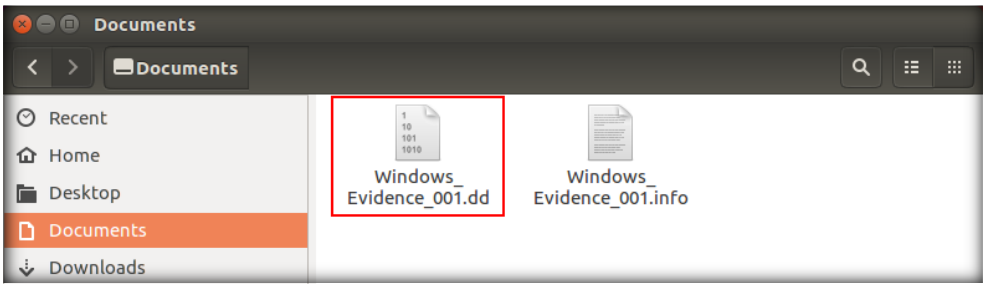


FIGURE 3.4: View the dd File

11. Next, we will mount this image. In this lab, we are going to create a directory named **dd** within the **/mnt** directory and mount the image on this directory.

12. To create the directory, issue the command **mkdir /mnt/dd**.

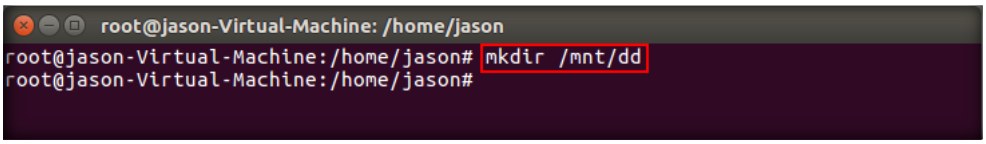


FIGURE 3.5: Create a Directory Using mkdir

13. To mount the image located at **/home/jason/Documents/** onto **/mnt/dd** in **read-only** mode, type the command **mount -o ro /home/jason/Documents/Windows_Evidence_001.dd /mnt/dd/** and press **Enter**.

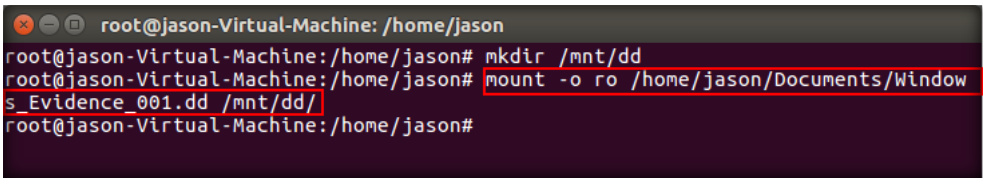


FIGURE 3.6: Command to Mount the Image File

14. Now the image is successfully mounted on the dd directory. To view the contents of the image through the command line terminal, type **ls -la /mnt/dd/** and press **Enter**.

15. A list of all the files pertaining to the image appears as shown in the following screenshot:

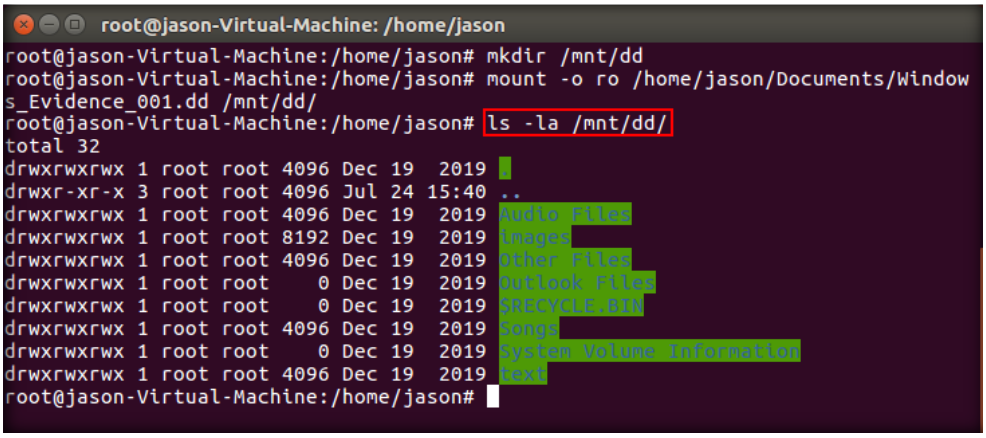


FIGURE 3.7: View All the Files in the Image File

16. To view these files in the file manager, click on the **Files** icon in the **Launcher** panel to launch the **File Manager**.

FIGURE 3.8: Launch File Manager

17. **File manager** window will appear pointing to **Home** directory. Click on **Computer** from the left pane.

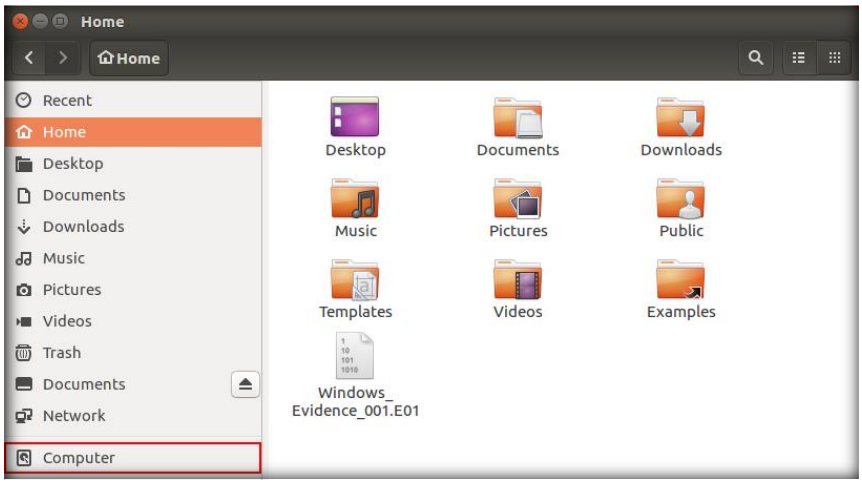


FIGURE 3.9: Click on the Computer

18. Now go to **mnt → dd** to view the files.

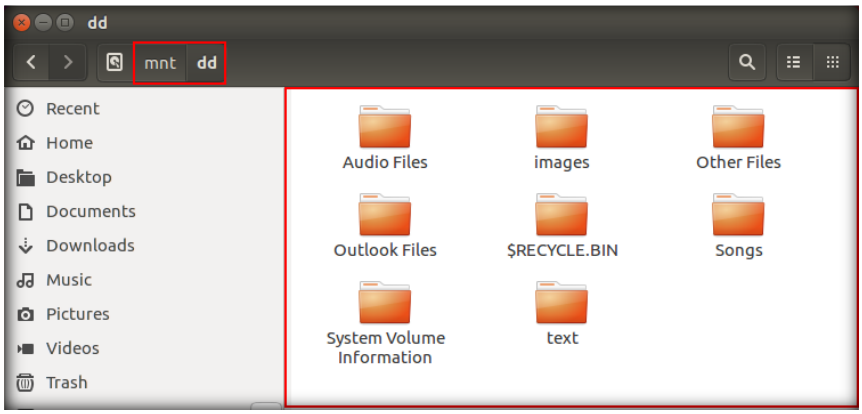


FIGURE 3.10: View Extracted Files from the Image File

TASK 2

Mount a dd Image Containing APFS File System using losetup

19. Our next task is to mount a dd image that contains **Apple File System**.
20. To begin the task, navigate to the shared directory **chfi-tools/Evidence Files/Forensic Images** and copy **MAC_Evidence_001.dd**.

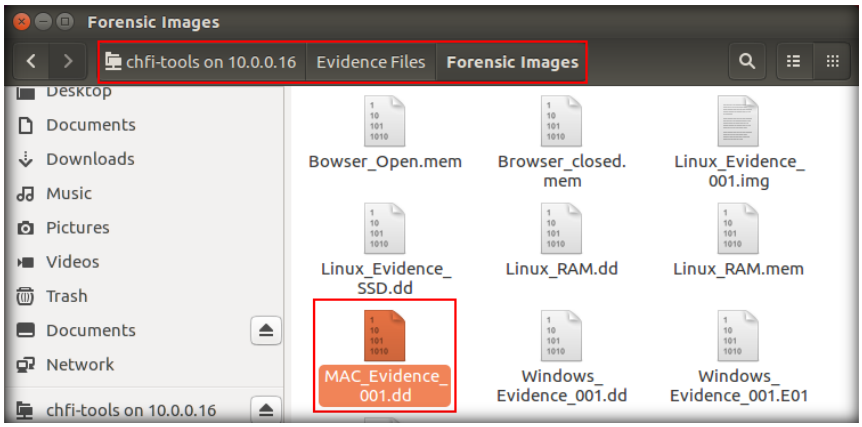


FIGURE 3.11: Forensic Images Directory

21. Paste the image file in the **Home** folder.

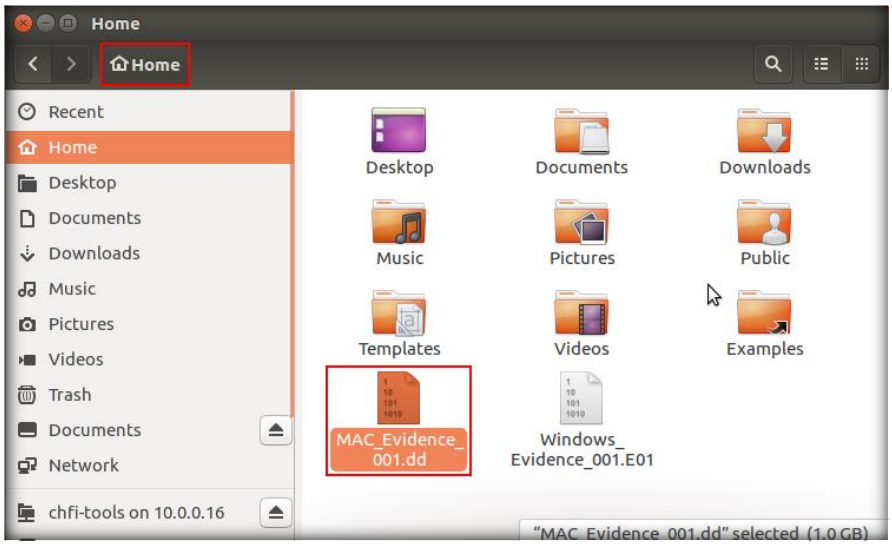


FIGURE 3.12: Image File Containing Apple File System

22. Next, we shall mount an image by attaching it to a loop device. Before attaching it, you need to find a free loop device.
23. The **losetup -f** command helps you identify the first unused loop device. Therefore, issue this command to view the unused loop devices.

Note: The unused loop device returned in the output might vary in your lab environment.

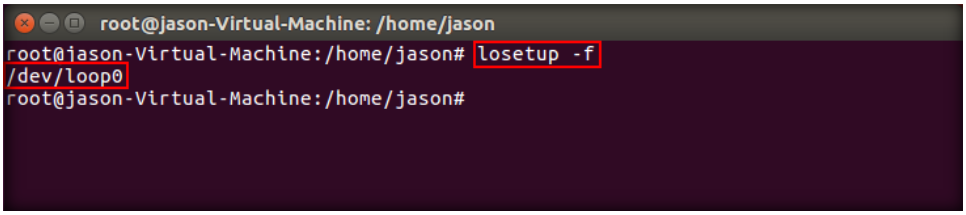


FIGURE 3.13: Command to Identify Unused Loop Device

24. In this lab, we will be considering **loop0** as the unused device. To attach the image to the loop device, type **losetup -r /dev/loop0 MAC_Evidence_001.dd** in the command line terminal and press **Enter**.
25. This mounts the image file (**MAC_Evidence_001.dd**) to the loop device **loop0**.

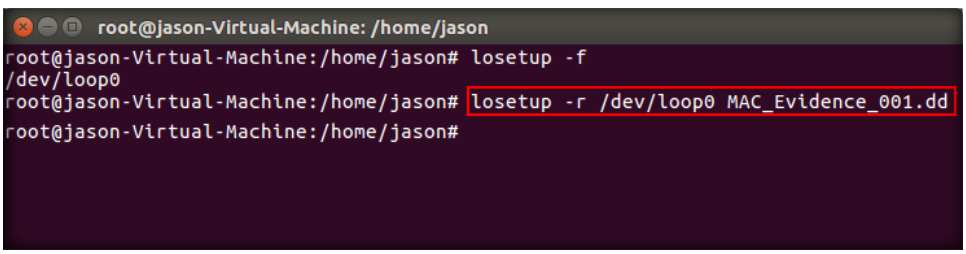


FIGURE 3.14: Image File Mounted to the Loop Device

26. To view the mounted image, click on the mount icon (named **Evidence Image**) on the **Launcher Panel**.

FIGURE 3.15: Mounted Image File

27. **Evidence Image** folder will appear displaying the contents of the image file, as shown in the following screenshot:

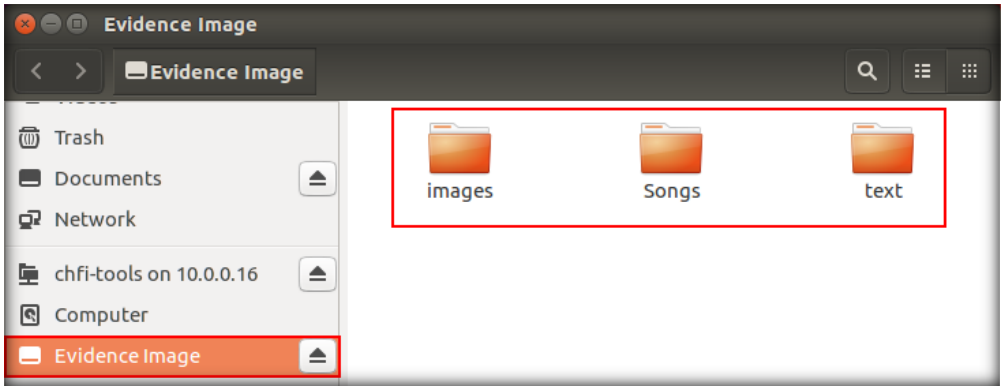


FIGURE 3.16: View the Contents of the Image File

28. Sometimes, images may contain hidden files and folders. To view them, press **Ctrl+H** on the keyboard.

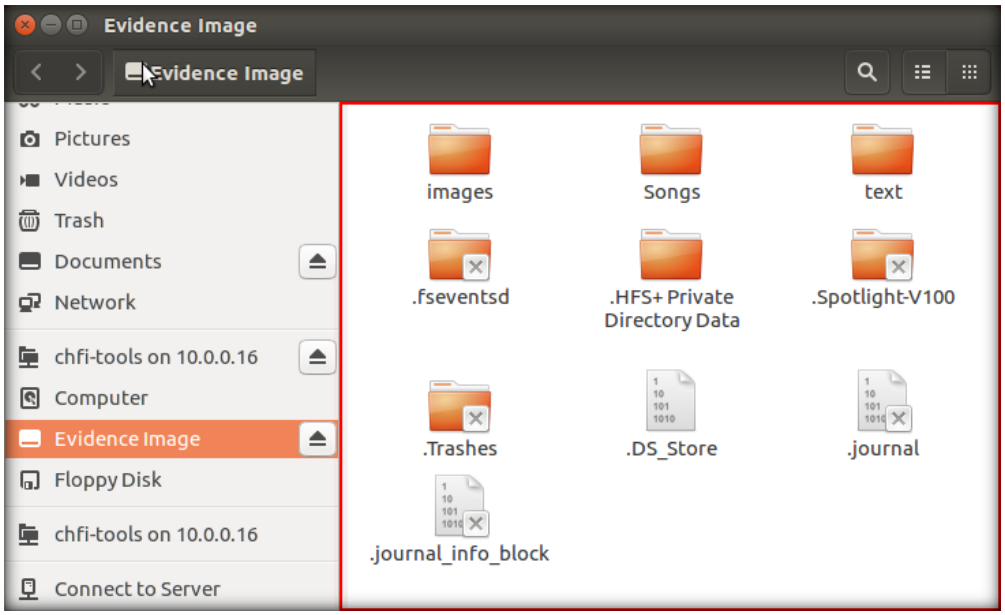


FIGURE 3.17: View Hidden Files

29. This way, you can mount an image file using **mount** and **losetup** commands. These images form the base of the investigation and help gain crucial insights related to the investigation.

Lab Analysis

Analyze the file attributes and file systems of the disk partition image and document the results related to the lab exercise. Give your opinion of the target file system.

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

Lab

4

Converting Acquired Image File to a Bootable Virtual Machine

A virtual machine runs a dedicated OS on shared physical hardware resources and provides the same functionality as an actual computer.

ICON KEY

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

Lab Scenario

During an investigation, the investigator needs to perform data acquisition on the suspect's machine in a forensically sound manner. In some cases, the investigator might need to create a live environment of the machine and boot the forensically acquired image file into the virtual machine so that the investigator can extract additional artifacts that may not have been discovered in the static analysis. These additional artifacts might serve as an evidence and help the investigator solve the case.

As a forensic investigator, you should know how to convert an acquired image file to a bootable virtual machine.

Lab Objectives

The objective of this lab is to help you understand how to convert an acquired image file to a bootable virtual machine.

Lab Environment

This lab requires:

- A system running **Ubuntu Forensics** virtual machine
- A system running **Windows Server 2016** virtual machine
- Administrative privileges to install and run tools

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

In the lab **Creating a dd Image of a System Drive**, we saw how to create a dd image of an entire disk. In this lab, we shall demonstrate how to convert that disk into a bootable virtual machine in order to launch the virtual machine and examine artifacts.

Lab Tasks

TASK 1

Convert Acquired Image to Bootable Virtual Machine

1. This lab requires a dd image of an entire physical disk. You can either use the disk that you created in the lab **Creating a dd Image of a System Drive** or the disk that is placed in **CHFI-Tools**.
2. Login to the **Ubuntu Forensics** virtual machine.
3. Converting an image to a bootable disk requires special tools like **qemu-utils** to be installed on the machine.
4. Therefore, launch a command line terminal, type the command **sudo apt-get install -y qemu-utils**, and press **Enter**. You will be asked to enter the password of root user; type **toor** in the **Password** field and press **Enter**.

   Note: If you get any error or unable to install **qemu-utils**, run the command **sudo apt-get update** and then run the command **sudo apt-get install -y qemu-utils**.
5. This begins to install the tool utilities, as shown in the following screenshot:

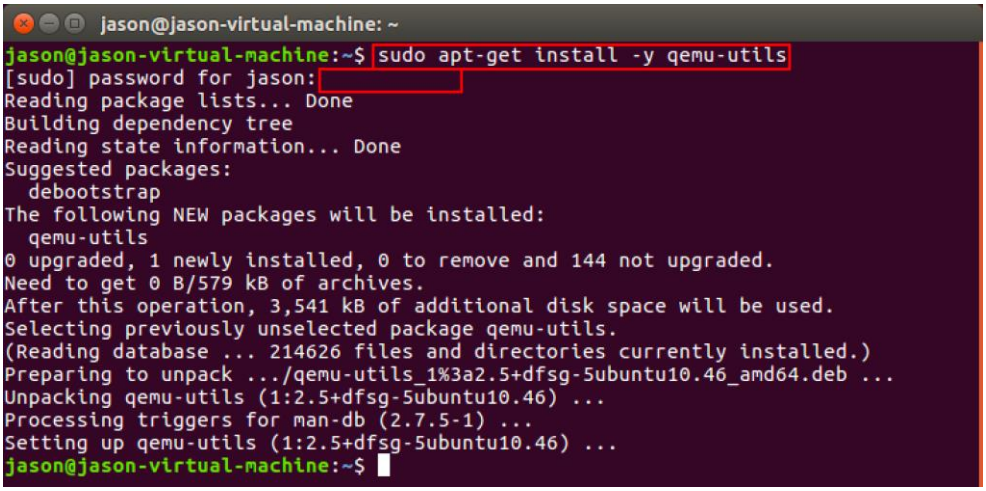


FIGURE 4.1: Download qemu-img Tool

6. Now, click on the **Files** icon in the **Launcher** panel to launch the **File Manager**.

FIGURE 4.2: Launch the File Manager

7. **File manager** window will appear pointing to **Home** directory. Click on the bookmarked **chfi-tools on 10.0.0.16** directory.

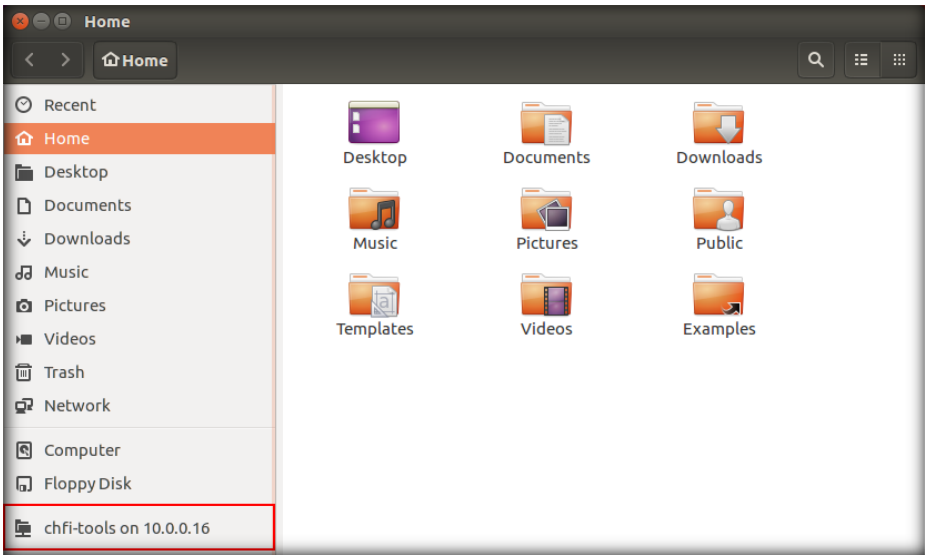


FIGURE 4.3: Click on the CHFI-Tools Directory

8. **CHFI-Tools** appear in the window; open **Evidence Files** folder.

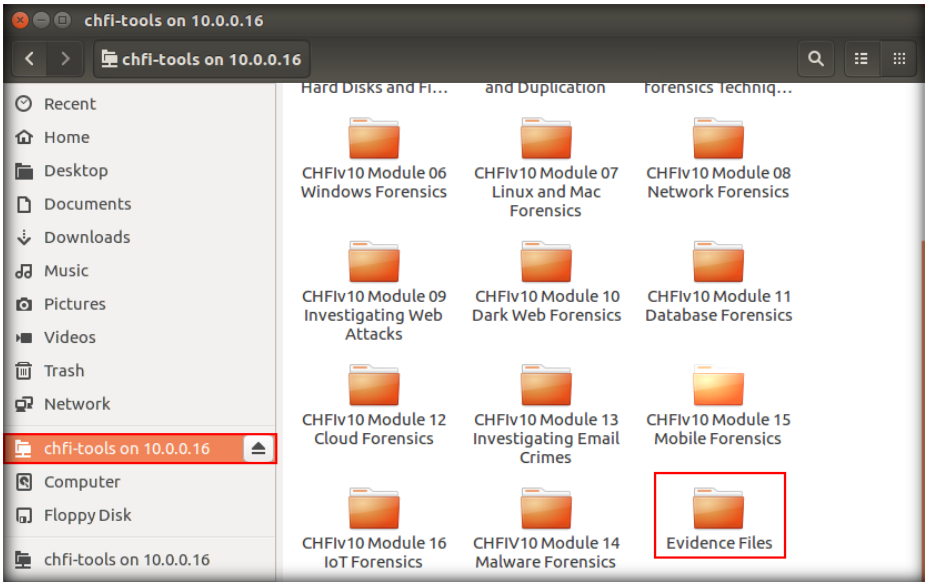


FIGURE 4.4: Open Evidence Files Folder

9. Now, right-click on **Forensic Images** folder and select **Open in Terminal** from the context menu.

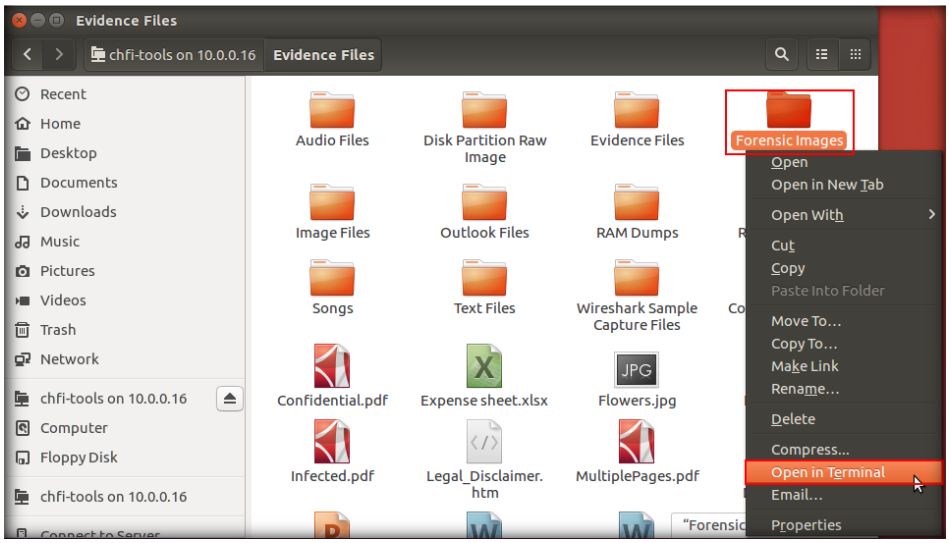


FIGURE 4.5: Open 'Forensic Images' Folder in Terminal

10. This will launch a terminal pointing to the **Forensic Images** folder.

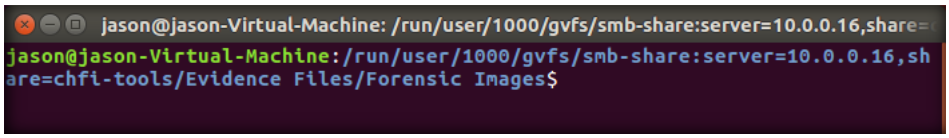


FIGURE 4.6: Path of the Evidence will Open in Terminal

11. Assuming that the virtualization platform used for forensics is Hyper-V, we shall convert the dd image to **vhdx** file.

12. To convert, type **qemu-img convert -f raw Windows_Evidence_002.dd -O vhdx /home/jason/Desktop/Windows.vhdx** and press **Enter**.

13. This takes some time and converts the raw dd image to a vhdx file named **Windows.vhdx** on the **Desktop**, as shown in the following screenshot:

Note: Using **qemu-img** tool, we cannot save the generated file (here, **Windows.vhdx**) directly to the network shared folder (i.e., **CHFI-Tools**) mounted on the virtual machine; therefore, you have to save the file on the virtual machine.

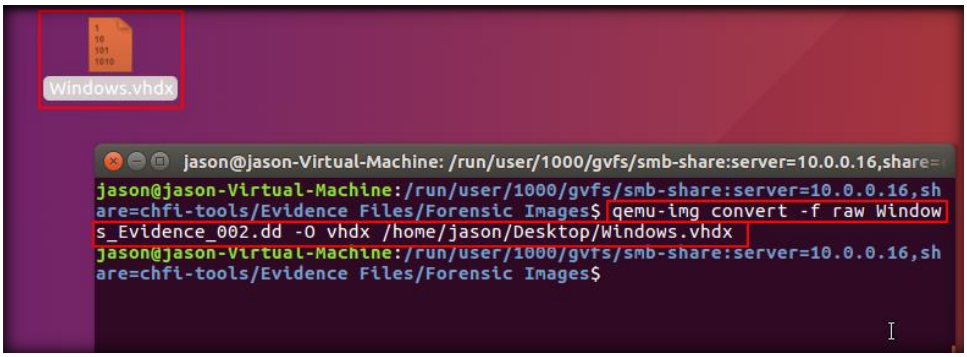


FIGURE 4.7: Conversion of dd Image to vhdx

14. Copy this output file to the **Forensic Images** sub-folder, which is a part of the **Evidence Files** sub-folder contained within the **CHFI-Tools** folder mounted on the virtual machine.

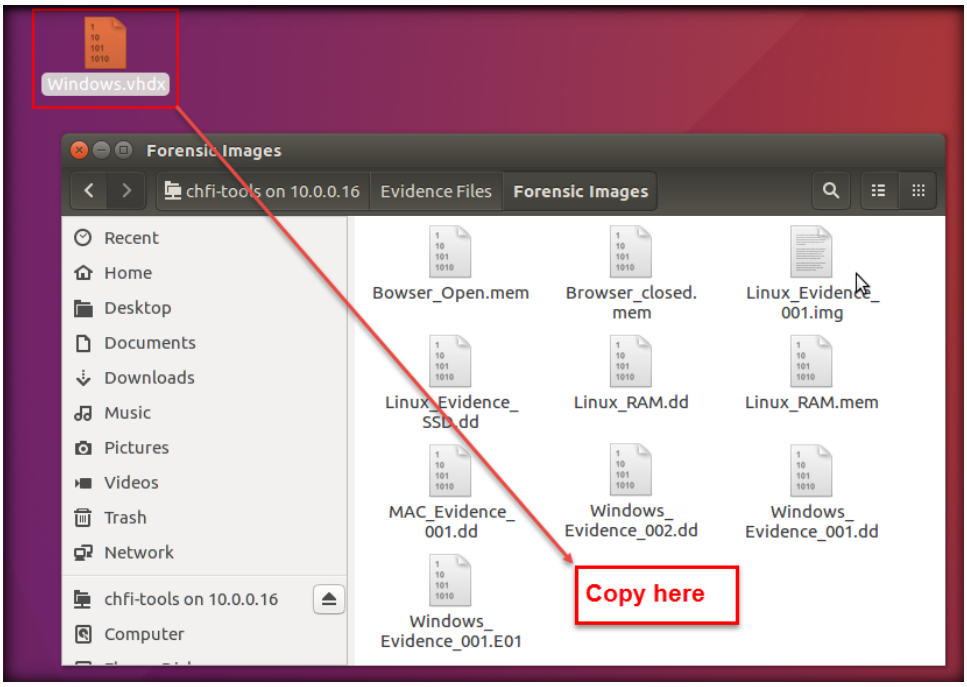


FIGURE 4.8: Copy vhdx file to the Forensic Images folder

15. Now, copy the image file (**Windows.vhdx**) folder from **Z:/Evidence Files** to any drive on the host machine.
16. Here we are choosing **E:** and creating a folder named **Windows Image** in **E:** to store the vhdx file.

TASK 2

Connect the Bootable Virtual Machine to Hyper-V

17. Click **Start → Windows Administrator Tools → Hyper-V Manager**.
18. Right-click on the **machine's name** (here, **WIN-P9394CKNU8T**) in the left pane of the window and then select **New → Virtual Machine...**

Note: Every machine has a unique name. Therefore, the name of your machine will differ from the name shown in the screenshot.

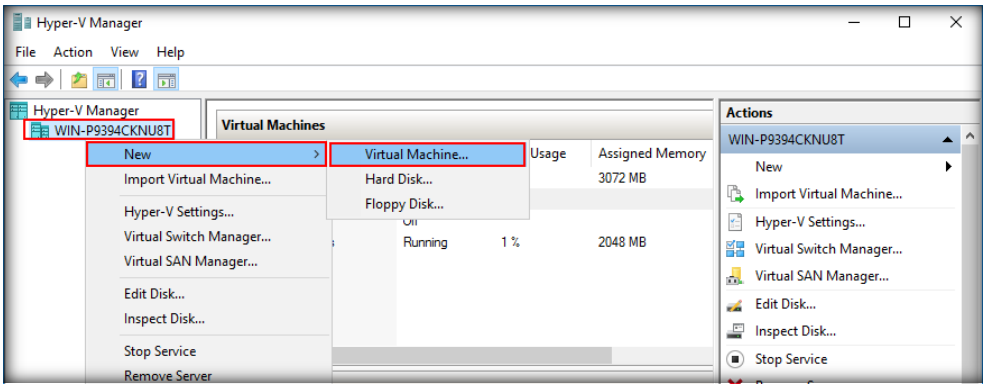


FIGURE 4.9: Hyper-V Manager

19. **New Virtual Machine Wizard** window will appear; click **Next**.

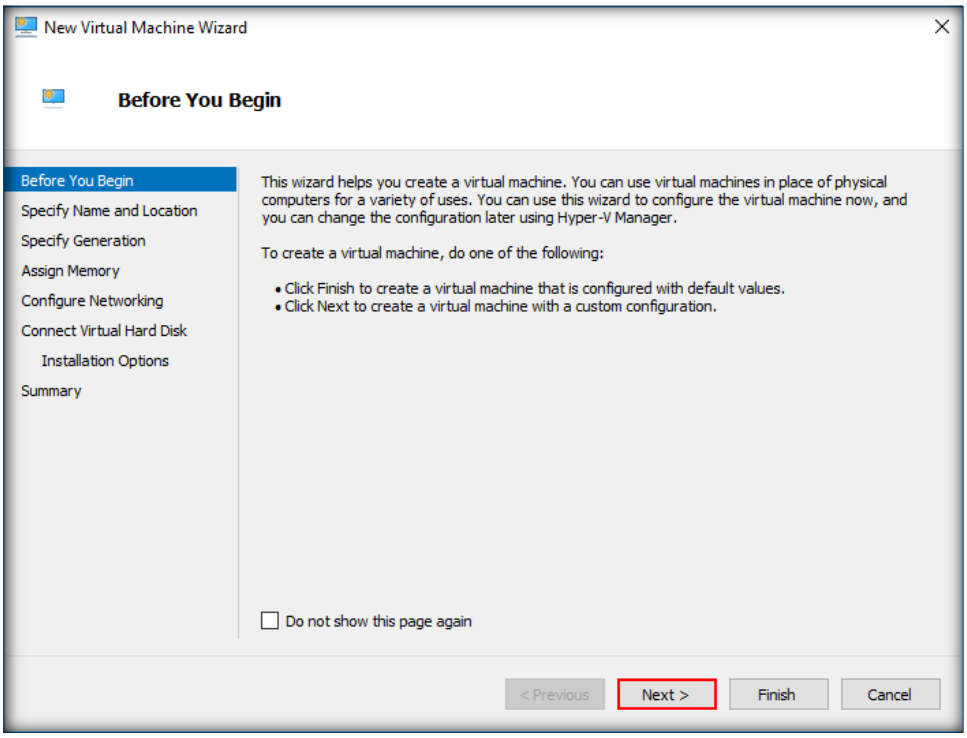


FIGURE 4.10: Before You Begin (New Virtual Machine Wizard)

20. **Specify Name and Location** section appears; assign the name of the virtual machine as **Windows Suspect Machine** and click **Next**.

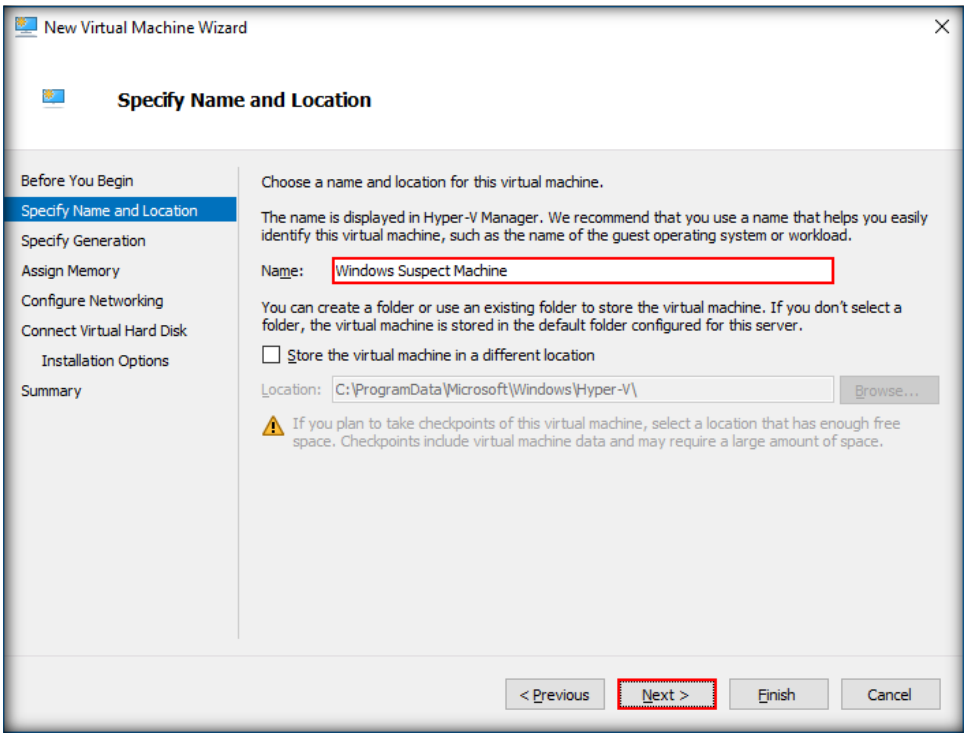


FIGURE 4.11: Specify Name and Location Window

21. **Specify Generation** section appears next; choose the generation of the virtual machine (here, **Generation 1**) and click **Next**.

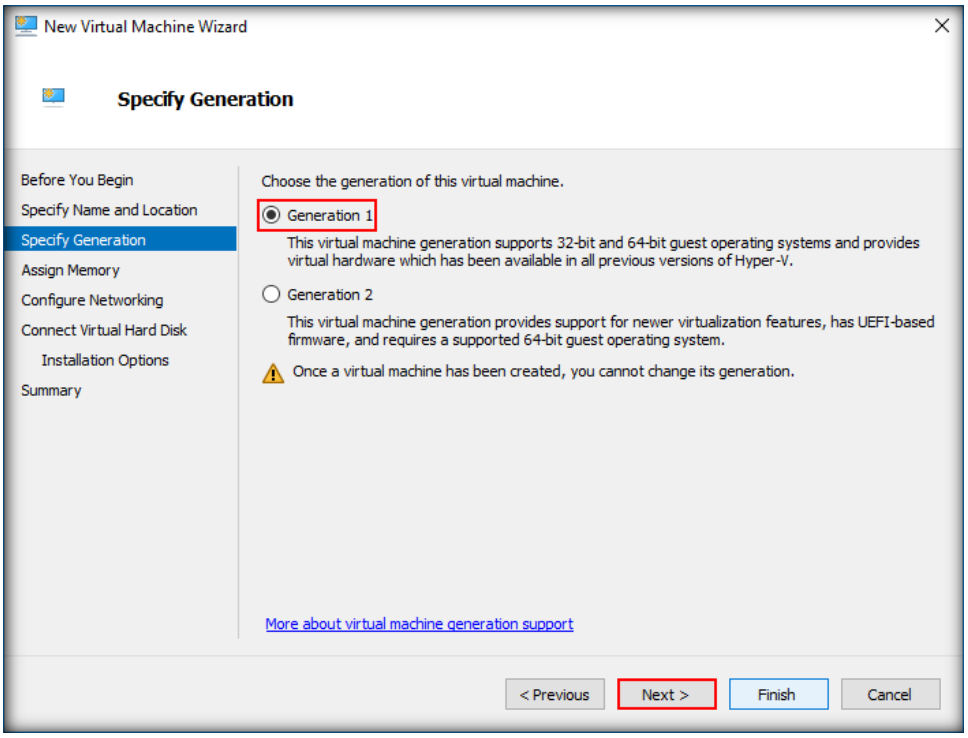


FIGURE 4.12: Specify Generation

22. The **Assign Memory** section will now appear; enter the **Startup memory** (RAM) as 1500 MB and click **Next**.

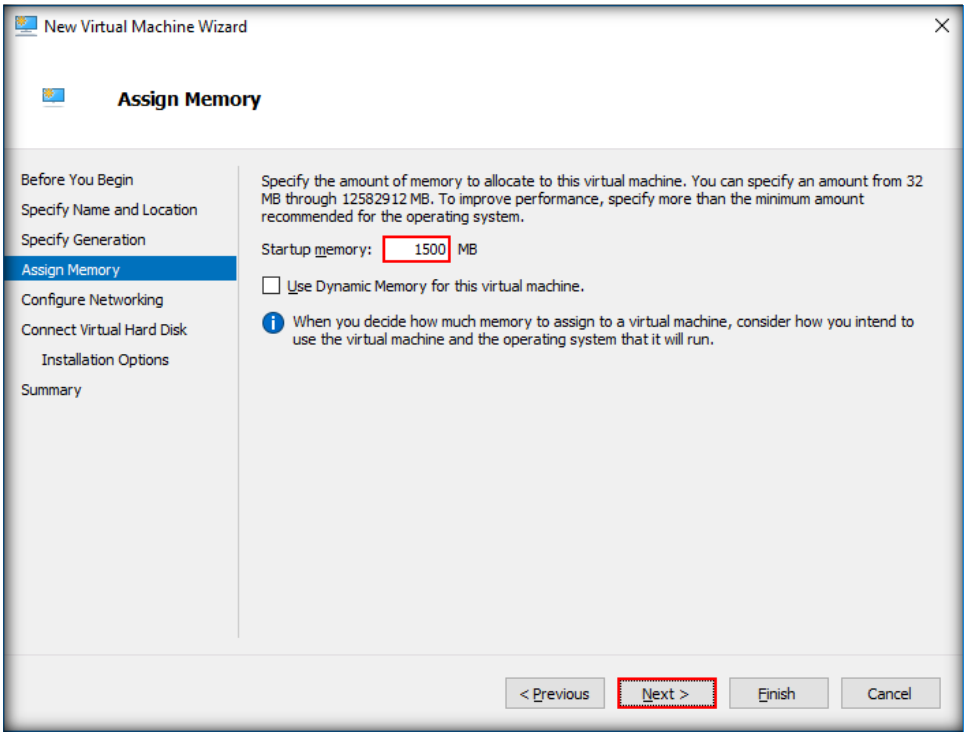


FIGURE 4.13: Assign Memory

23. Next, the **Configure Networking** section will appear. From the dropdown options for **Connection**, select **Not Connected** for the purpose of the static analysis. Click **Next**.

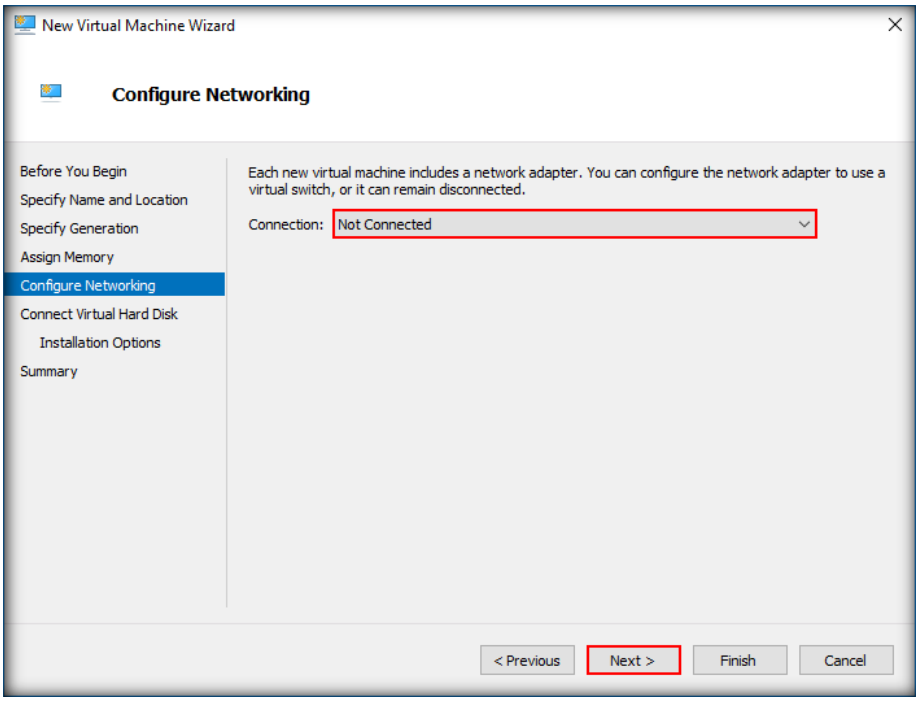


FIGURE 4.14: Configure Networking

24. Now, **Connect Virtual Hard Disk** section appears. Select **Use an existing virtual hard disk**, browse to the location where you have saved the converted vhdx image on the host machine and click **Next**.

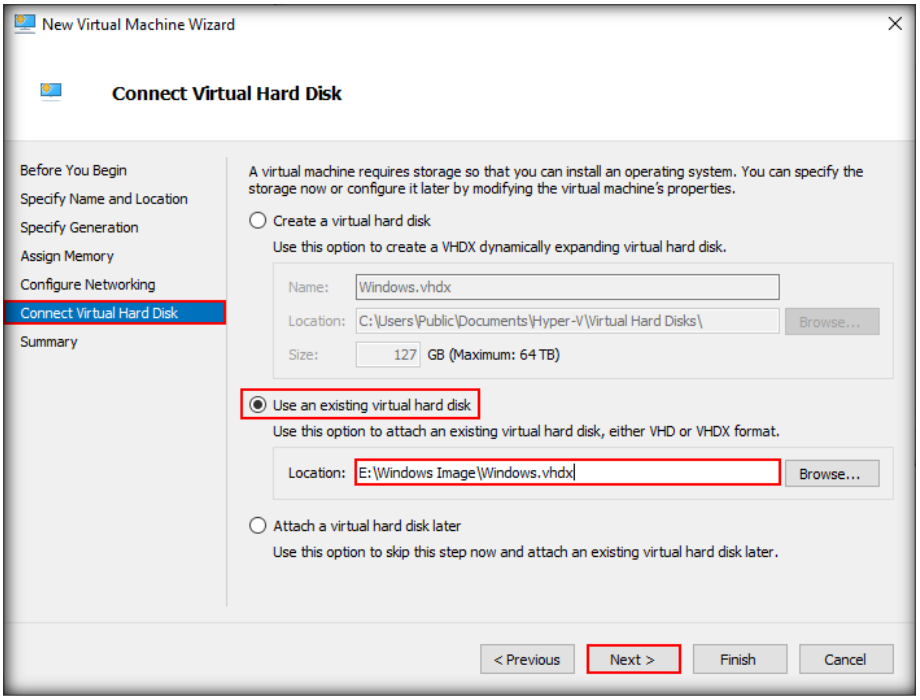


FIGURE 4.15: Connect Virtual Hard Disk

25. The **Summary** section will appear, where under **Description**, you can review the details of the virtual machine. Click **Finish** once done with the review.

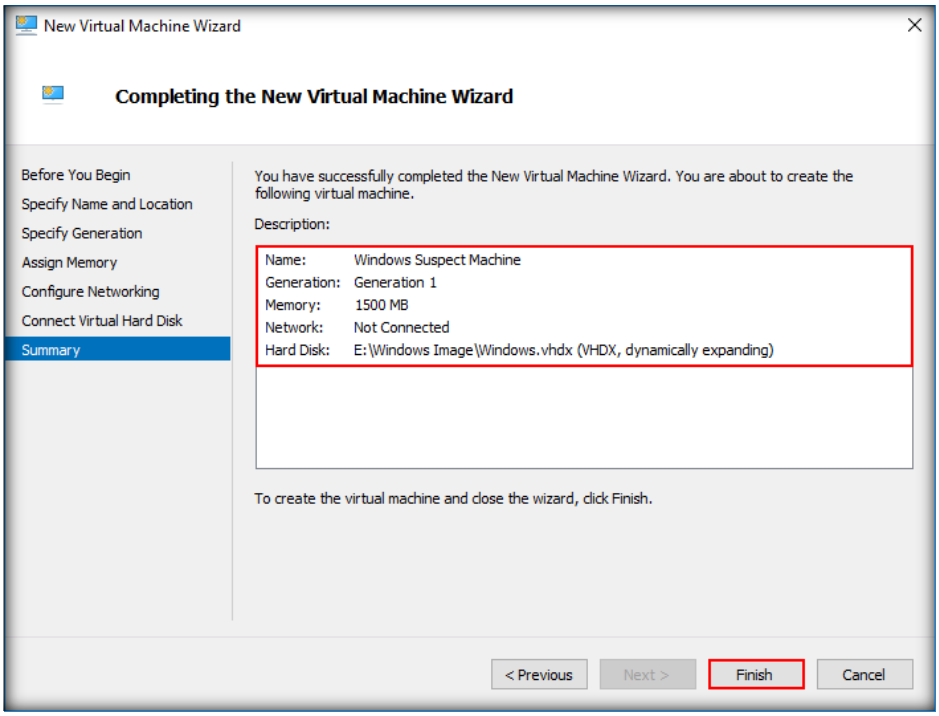


FIGURE 4.16: Summary

26. The created vhdx file is now attached to the virtual machine. Right click on the newly created virtual machine (here, it is **Windows Suspect Machine**) and click **Connect**.

Note: You may turn off the **Ubuntu Forensics** virtual machine before starting this virtual machine to regulate the usage of RAM on the host machine.

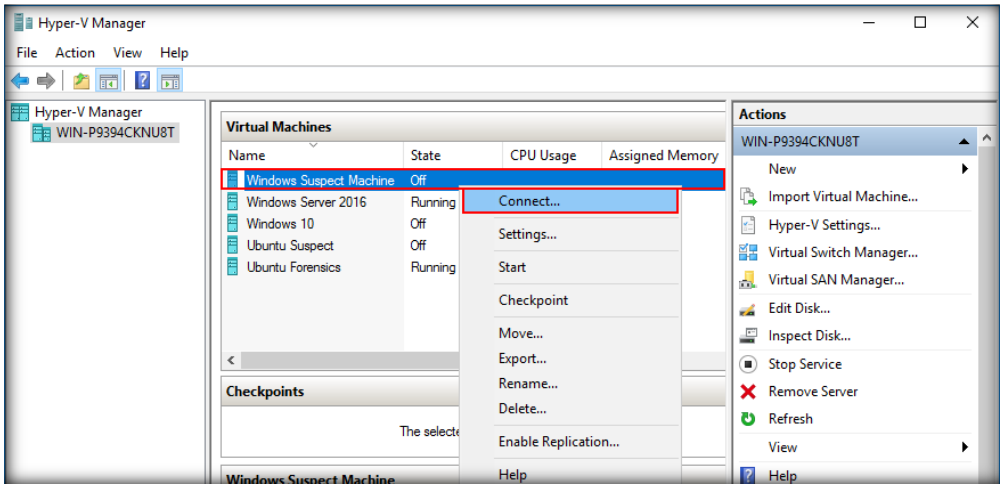


FIGURE 4.17: Connect to the created virtual machine

27. A black virtual machine window will appear; click on **Start** button from the toolbar to boot the virtual machine.

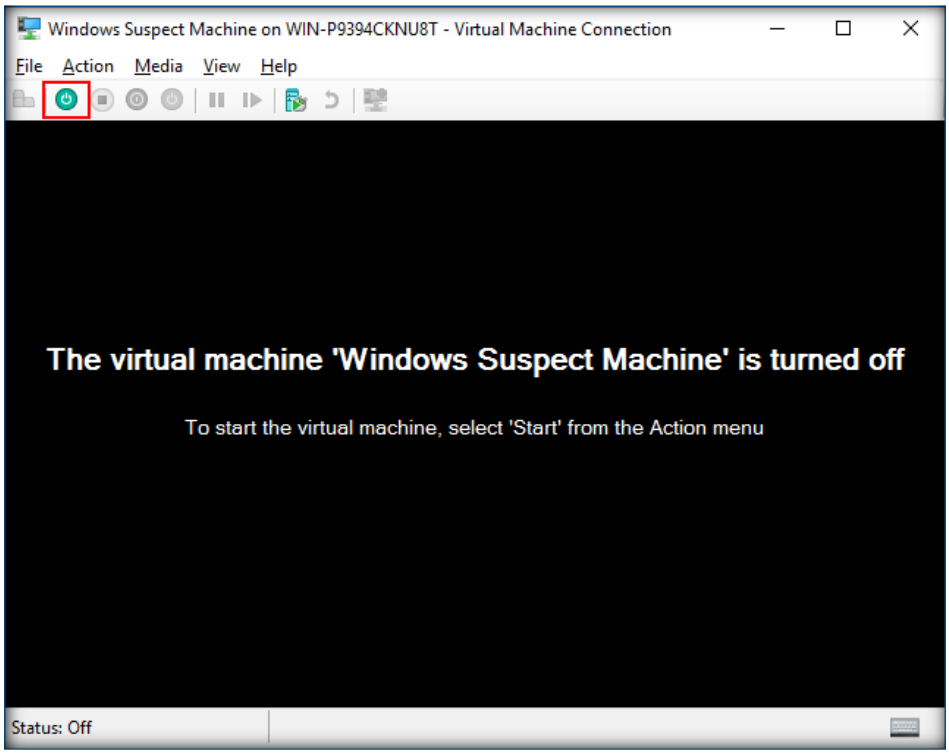


FIGURE 4.18: Start the Machine

28. The machine's lock screen appears; click on the screen to access the login window.

FIGURE 4.19: Click on the lock screen

29. The machine's login screen appears; type the **Password** as **Test@123** and press **Enter**.

Note: In real-time, the investigator needs to obtain the password for the machine from its owner.

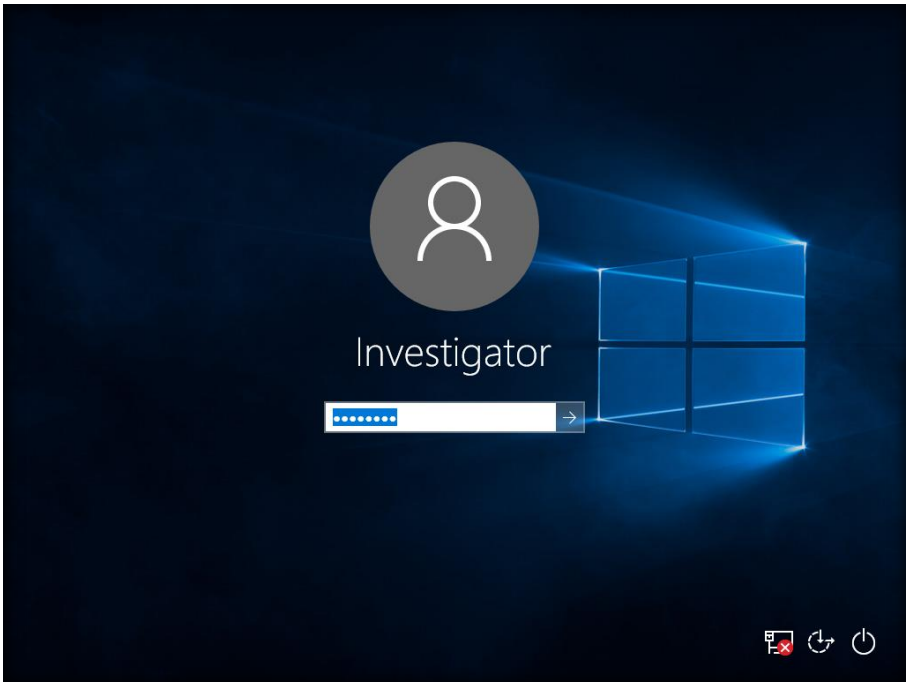


FIGURE 4.20: Enter Machine Password

30. In the end, the vhdx file obtained from conversion of the dd file is loaded successfully to **Windows 10**, as shown in the screenshot:

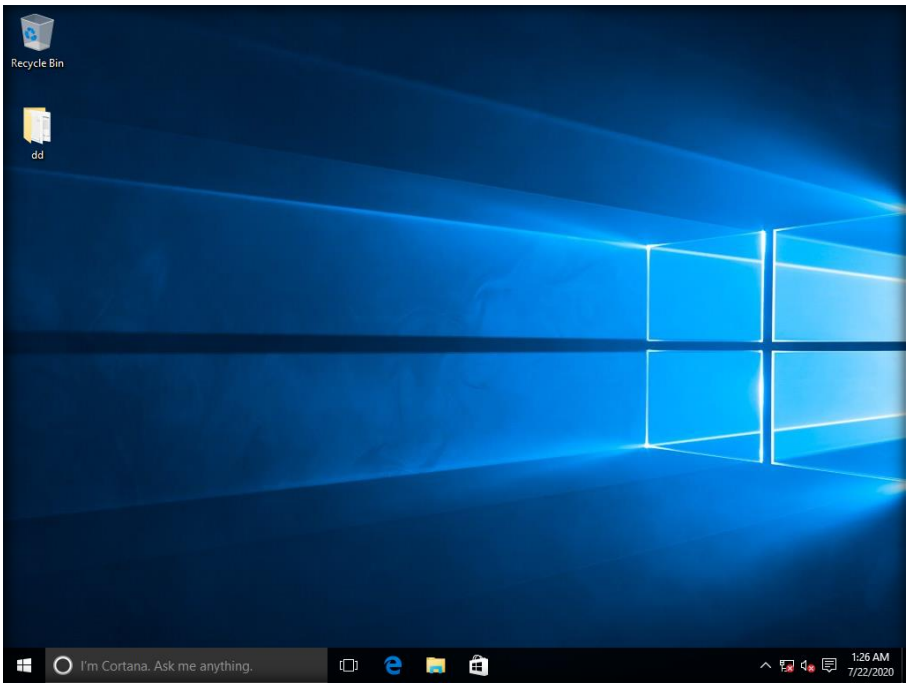


FIGURE 4.21: Successfully Booted the vhdx File

Note: After a complete analysis of suspect machine, delete the virtual machine from Hyper-V.

Lab Analysis

Analyze the file attributes and file systems of the disk partition image and document the results related to the lab exercise. Give your opinion of the target file system.

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

Lab

5

Acquiring RAM from Windows and Linux Workstations

RAM (Random Access Memory) is a volatile-memory storage found in computing devices that temporarily holds the data your device needs to access.

ICON KEY

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

Lab Scenario

James, a forensic investigator, is performing live analysis on a suspect's computer. In this process, the investigator needs to primarily capture the RAM dump of the machine as RAM contains volatile data that is lost when the machine loses power. In this scenario, the investigator performs RAM acquisition on both Windows and Linux workstations.

To be an expert forensic investigator, one must understand how to acquire a RAM dump from Windows and Linux OSes.

Lab Objectives

The objective of this lab is to help students learn how to perform RAM acquisition on Windows and Linux workstations.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

This lab requires:

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

- **Belkasoft RAM Capturer** tool located at **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\Belkasoft RAM Capturer**

Note: You can also download the latest version of **Belkasoft RAM Capturer** from https://belkasoft.com/get?product=ram

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

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

Lab Duration

Time: 30 minutes

Overview of the Lab

This lab familiarizes you with the **Belkasoft RAM Capturer** tool, which helps perform RAM acquisition on Windows systems; LiME and fmem do the same on Linux systems.

Lab Tasks

1. Login to the **Windows 10** virtual machine.
2. Make sure that the **Windows Server 2016** virtual machine is also turned **on**.
3. Before beginning this lab, navigate to the directory **Z:\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools**, copy **Belkasoft RAM Capturer folder** and paste it onto **Desktop**.

TASK 1

Acquire RAM on Windows 10

4. Now navigate to the directory **Desktop → Belkasoft RAM Capturer folder → x64** and double-click **RamCapture64.exe** to launch the application.

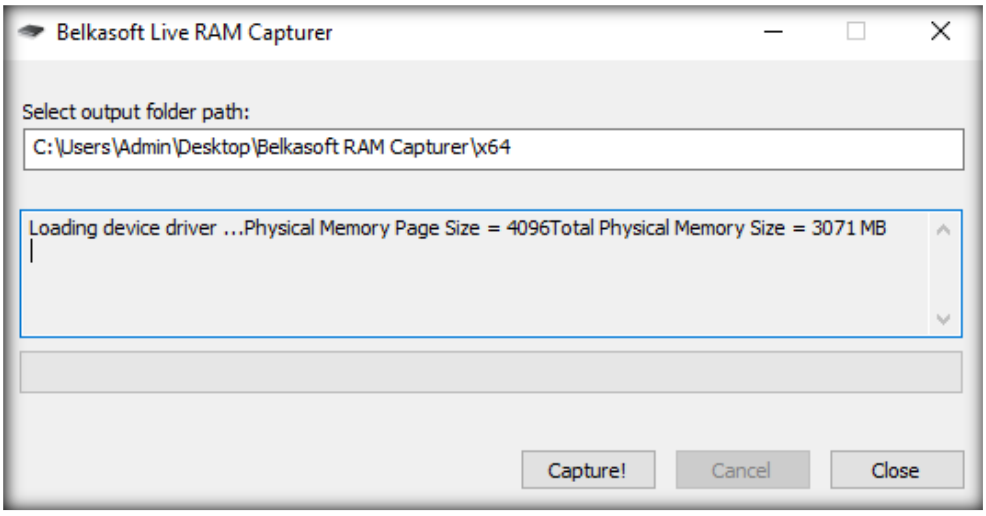


FIGURE 5.1: Belkasoft Live RAM Capturer

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

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

5. You need to assign a folder to store the captured RAM. Therefore, navigate to the **Forensic Disk** (**F Drive**) and create a folder named **Windows RAM**.
6. Now, enter the path for the output (here, **F:\Windows RAM**) under **Select output folder path** field and click **Capture!**

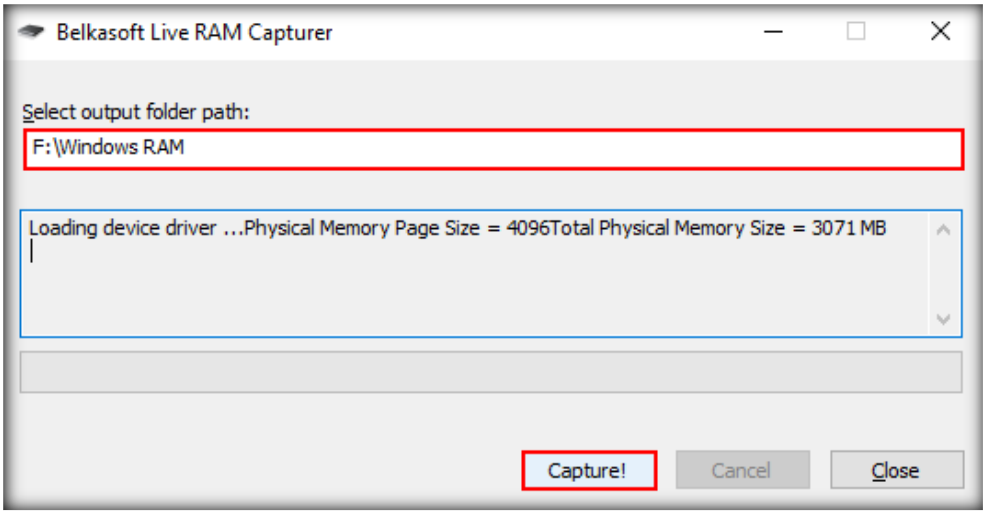


FIGURE 5.2: Provide Output Folder Path

7. The application begins to capture the RAM, as shown in the following screenshot:

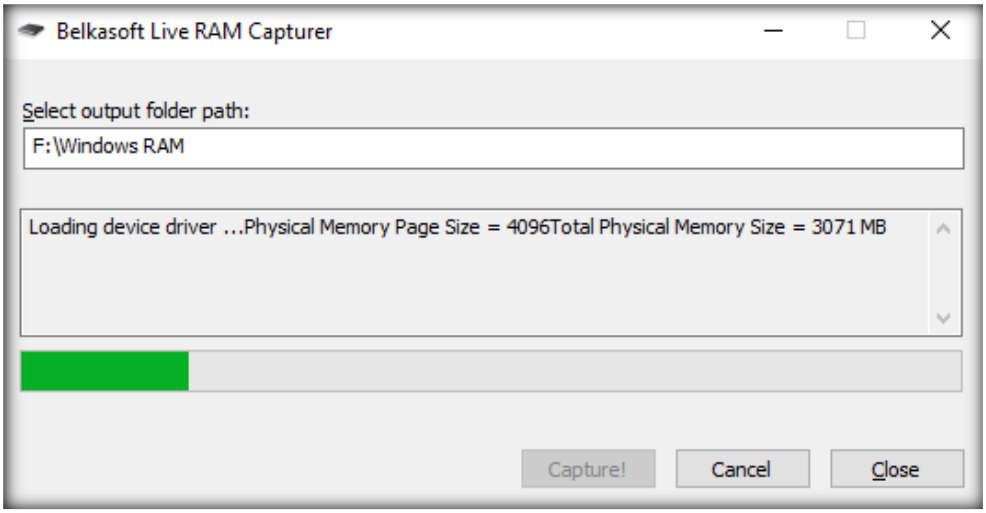


FIGURE 5.3: Capturing RAM

8. Once the memory dump is successfully created, click **Close** to close the application.

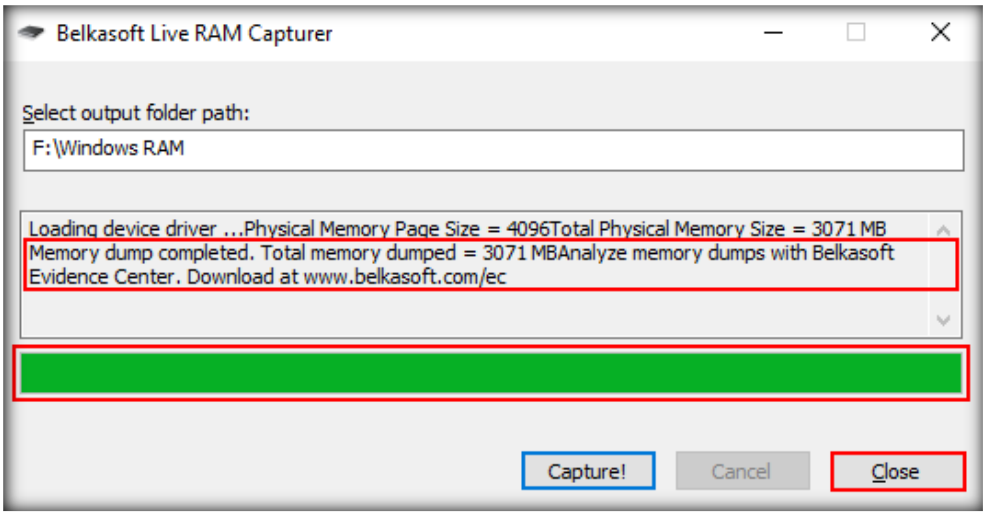


FIGURE 5.4: RAM Dump Created

9. Navigate to **F:\Windows RAM** to view the created memory dump. The dump is saved in the **yyyymmdd.mem** format, where yyyy refers to the year, mm refers to the month, and dd refers to the date.

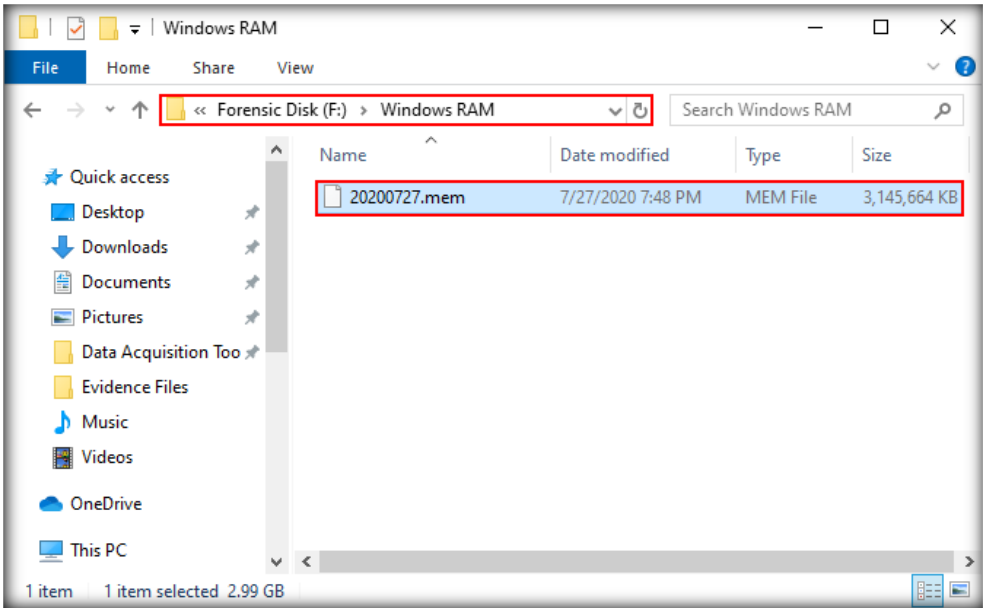


FIGURE 5.5: Captured RAM File

10. This way, you can capture the memory dump of a suspect Windows machine. These dumps act as important source of evidence for the investigators while investigating volatile memory.
11. You may now turn the **Windows 10** virtual machine **Off** in order to optimize RAM on the main machine.
12. Keep the **Windows Server 2016** virtual machine powered **on** during this lab.

TASK 2

Local Acquisition of RAM on Ubuntu

13. Now, we shall see how to dump RAM on Ubuntu machines. Therefore, login to the **Ubuntu Suspect** virtual machine. Also make sure to power **on** the Ubuntu Forensics virtual machine.
14. Click on the **Files** icon in the **Launcher** panel to launch the **File Manager**.

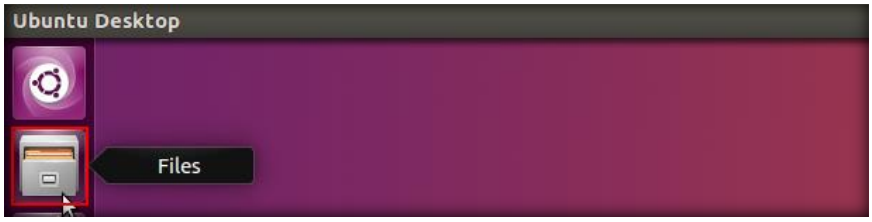


FIGURE 5.6: Launch File Manager

15. **File manager** window will appear pointing to **Home** directory. Click on the bookmarked **chfi-tools on 10.0.0.16** directory.

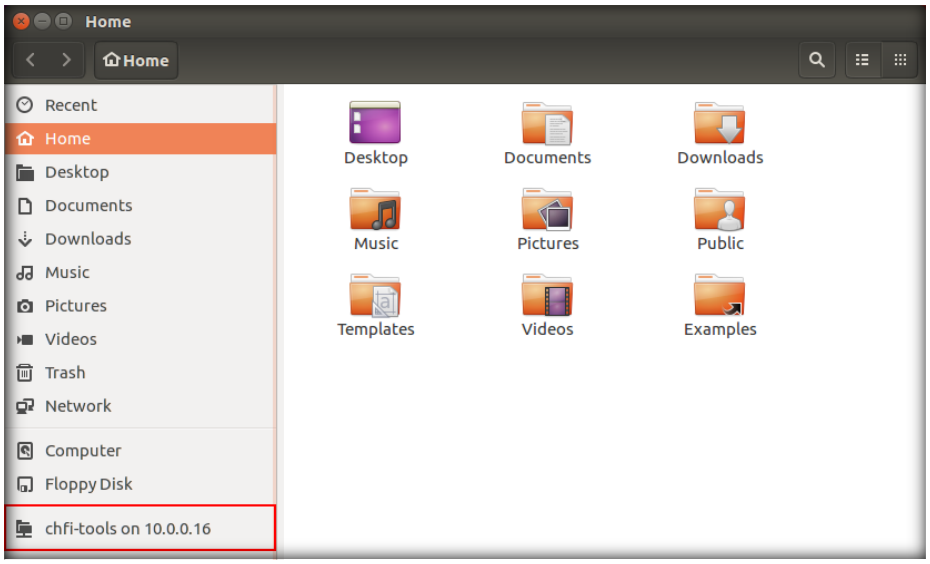


FIGURE 5.7: Click on the CHFI-Tools Folder

16. **CHFI-Tools** will appear in the window, as shown in the following screenshot:

FIGURE 5.8: View contents in the CHFI-Tools Folder

17. Now, go to **CHFIv10 Module 04 Data Acquisition and Duplication → Data Acquisition Tools**, copy **fmem** and **LiME** folders and paste them in the **Home** directory.

FIGURE 5.9: Copy fmem and LiME Tools

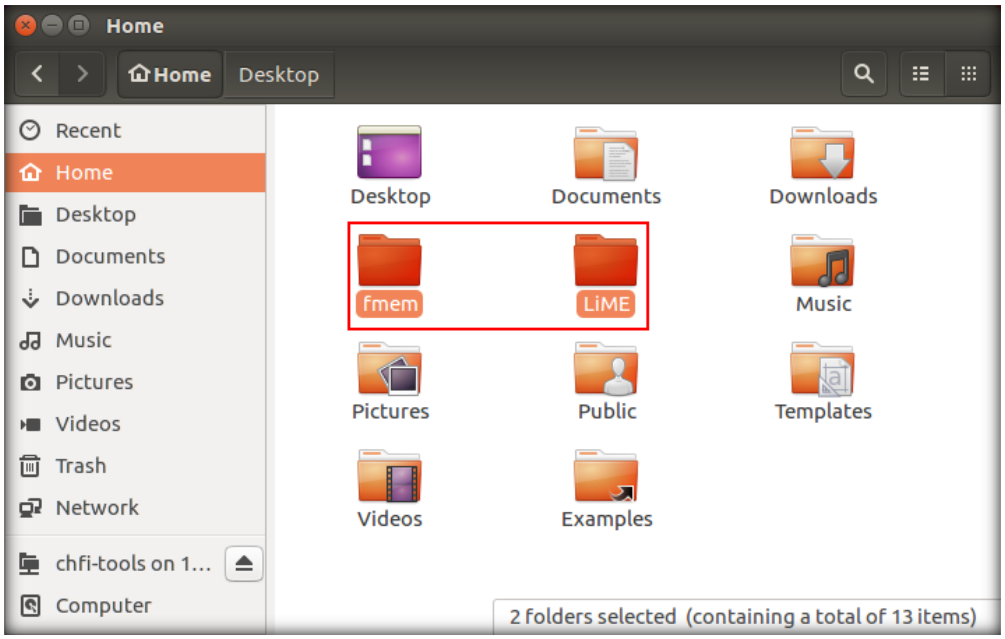


FIGURE 5.10: Paste the fmem and LiME Tools in Home Directory

18. Now, click on the **Terminal** icon from the launcher panel to launch the command line terminal.

FIGURE 5.11: Launch Terminal

19. Command line terminal launches. You require root privileges in the terminal to install an application.
20. So, type **sudo su** and press **Enter**. You will be prompted to enter the password. Type **toor** as the password and press **Enter**.
21. Now, you will enter the **root** terminal, as shown in the following screenshot:

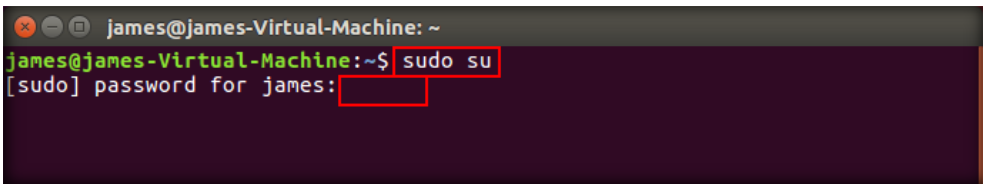


FIGURE 5.12: Run as super user

22. Before you start acquiring RAM on this machine, you need to install **fmem**
23. Type **cd fmem/** and press **Enter**.

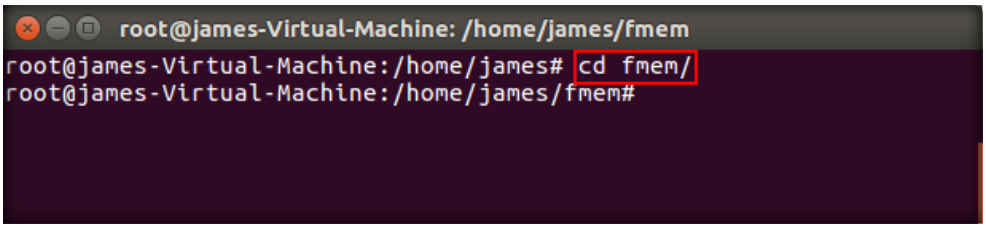


FIGURE 5.13: cd into Fmem Folder

24. You need to make sure that all the dependencies are met before installing fmem. Therefore, type **apt install -y build-essential** in the terminal and press **Enter**.

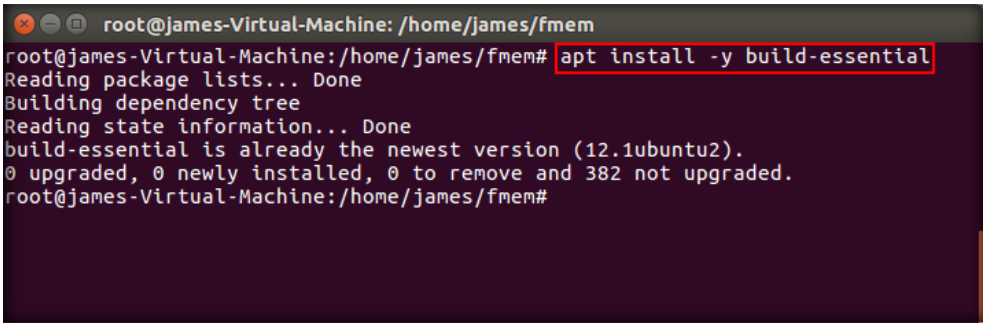


FIGURE 5.14: Install Dependencies

Note: If the **apt install -y build-essential** command is not executing, then restart the **Ubuntu Suspect** virtual machine, acquire root privileges, run the command **cd fmem/**, and then run the above command so that it executes successfully.

Note: If you are experiencing issues with internet connectivity, then run the commands **ifdown -a** followed by **ifup -a**, and then run the command **apt install -y build-essential**.

25. Type **make** and press **Enter** to build all the necessary libraries associated with fmem from the source code.

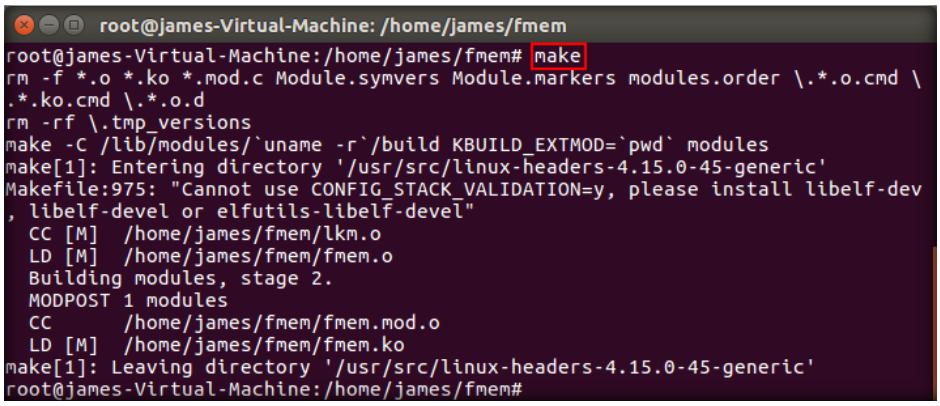


FIGURE 5.15: Build Necessary Libraries Associated with fmem Using Make Command

26. Now, type **bash run.sh** and press **Enter** to install the fmem tool.

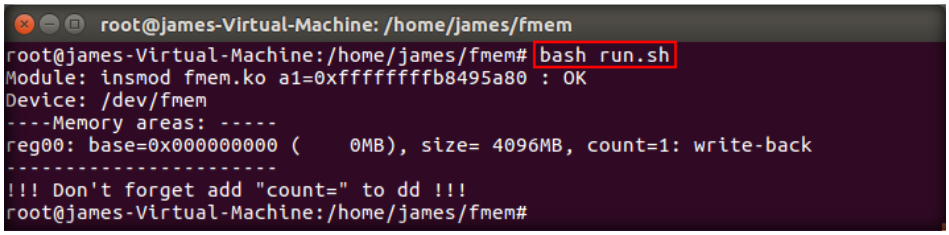


FIGURE 5.16: Install fmem Tool

27. In this lab, we are going to acquire RAM using local acquisition and remote acquisition methods. We will be using **dd** and **LiME** to acquire RAM locally, and **dd** to acquire RAM remotely.

28. To acquire RAM locally, type **dd if=/dev/fmem of=/home/james/ubuntu_local_ram.dd bs=1MB** and press **Enter**.

29. This begins to dump RAM of the machine in the **Home** folder with the name **ubuntu_local_ram.dd**.

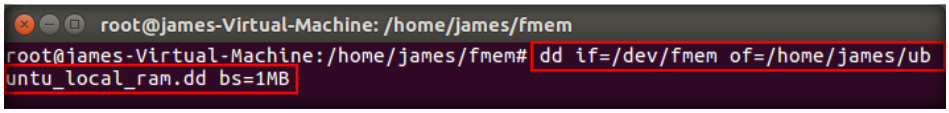


FIGURE 5.17: Create RAM Dump Using dd Command

30. It takes some time to complete the **acquisition procedure**. Upon dumping the RAM successfully, you will see the stats of the operation as shown in the following screenshot:

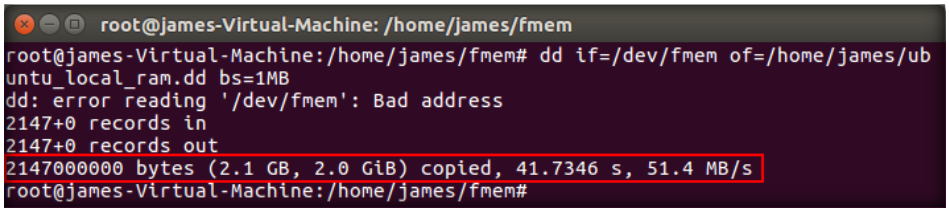


FIGURE 5.18: RAM Dump Created Successfully

31. Now, navigate to the **Home** folder to view the created **ubuntu_local_ram.dd** file.

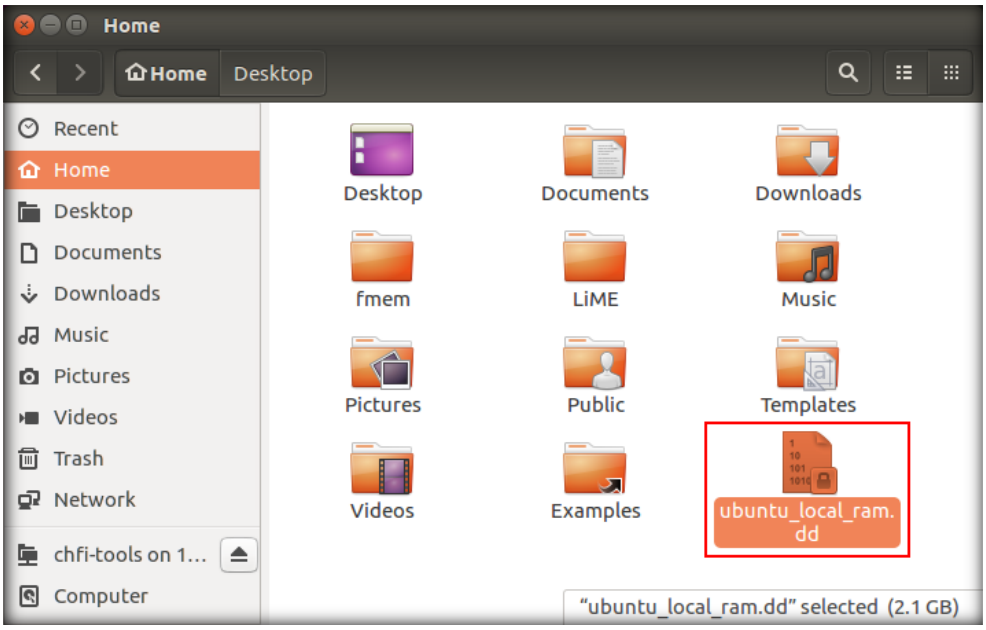


FIGURE 5.19: RAM Dump Created via Local Acquisition

32. Next, we shall install LiME tool on the machine to use it for acquiring RAM. Therefore, launch a new terminal, acquire root privileges, type **cd /home/james/LiME/src/**, and press **Enter**.

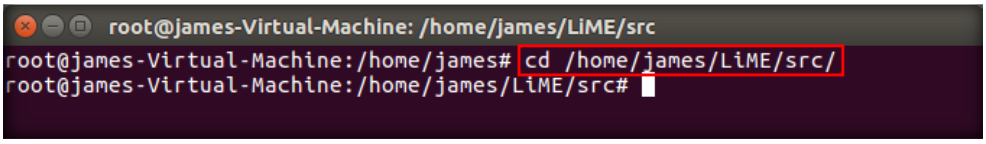


FIGURE 5.20: Install LiME Tool

33. Now, type **make** and press **Enter** to build all the necessary libraries associated with LiME from the source code.

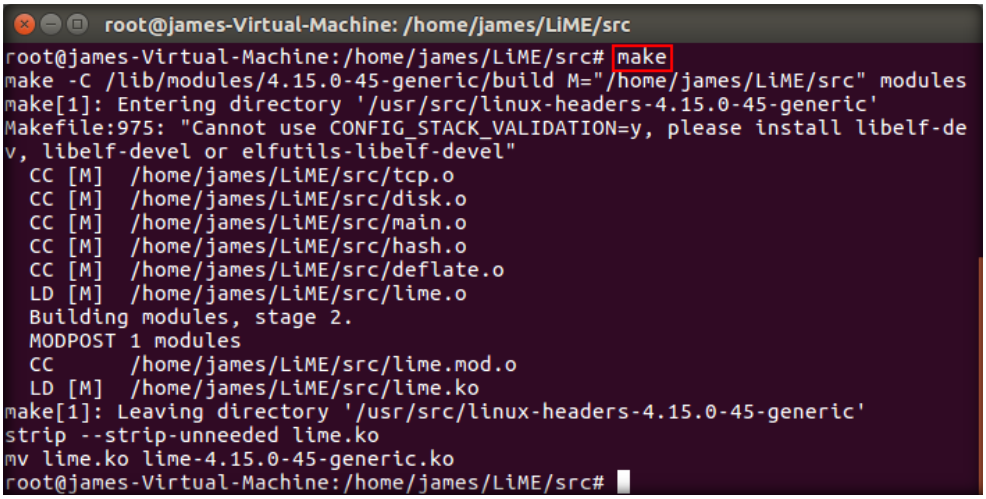


FIGURE 5.21: Build Necessary Libraries Associated with LiME Using Make Command

34. To acquire RAM locally, type **insmod lime-4.15.0-45-generic.ko "path=../../ubuntu_local_ram.mem format=lime"** and press **Enter**. This begins to dump the image of the RAM in lime format with the name **ubuntu_local_ram.mem** in the **Home** directory.

Note: The kernel module version varies depending on the Ubuntu OS version installed on the suspect machine. In this case, it is **4.15.0-45-generic**.

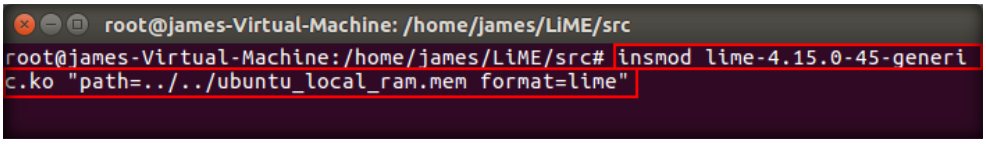


FIGURE 5.22: Perform Local Acquisition of RAM

35. **LiME** takes a considerable amount of time to acquire the image. Navigate to **Home** directory to see the RAM dump as shown in the screenshot below.

Note: Since this is a lab demonstration, it is recommended to abort the process after some time in order to save time for the forthcoming labs.

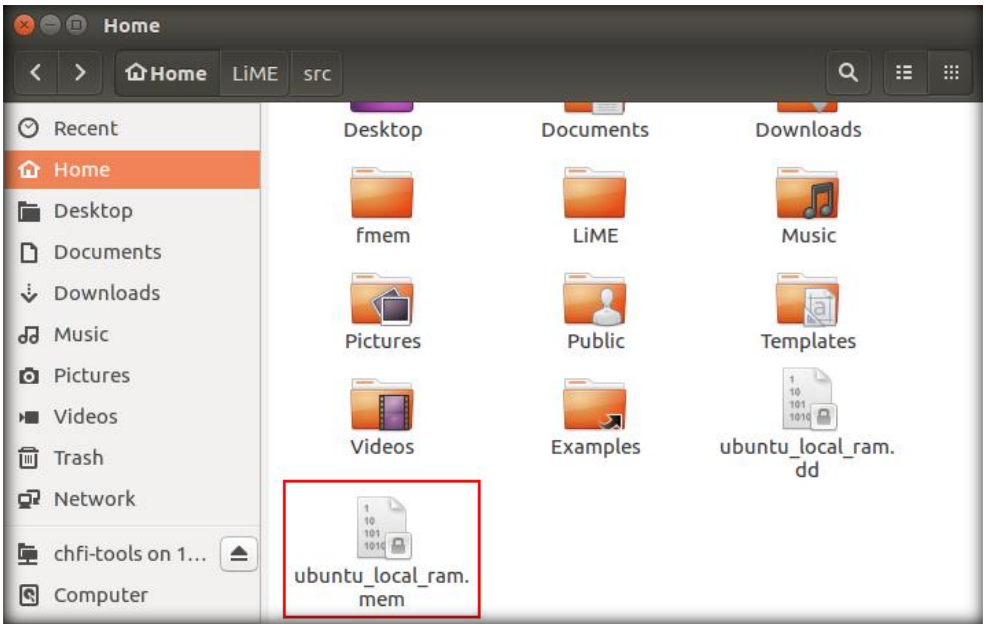


FIGURE 5.23: RAM dump created Using LiME

TASK 3

Remote Acquisition of RAM on Ubuntu

36. We have successfully demonstrated how to acquire RAM locally on an Ubuntu suspect machine using dd and LiME. Next, we shall perform **remote RAM acquisition** using **dd** and **netcat**.

37. First, login to the **Ubuntu Forensics** virtual machine, launch a command line **terminal**, and enter the **root** shell.

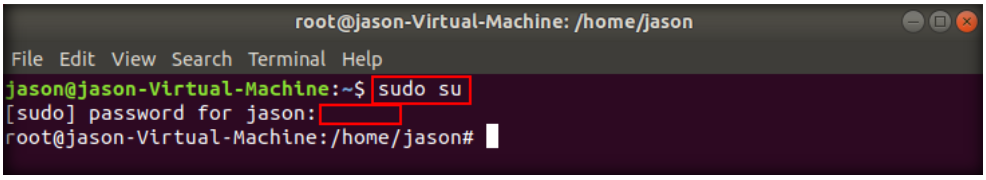


FIGURE 5.24: Run as super user

38. Type **nc -l 1234 > ubuntu_remote_ram.dd** and press **Enter**. This initiates the **netcat listener** on port **1234**.

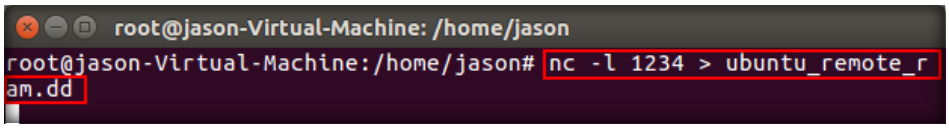


FIGURE 5.25: Initiate netcat Listener

39. Now switch to the **Ubuntu Suspect** virtual machine. In the root terminal, type **dd if=/dev/fmem bs=1024 | nc 10.0.0.9 1234** and press **Enter**.

40. By entering this command, you are redirecting the output of the dd command to **10.0.0.9**, which is the IP address of the **Ubuntu Forensics** virtual machine.

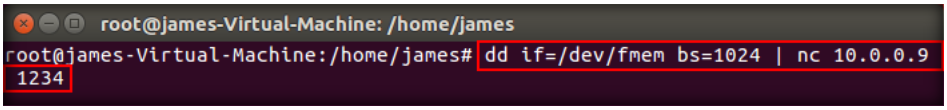


FIGURE 5.26: Capture RAM Using dd Command

41. Once you hit **Enter**, the image acquisition process initiates. Upon acquiring the RAM, you will see the statistics of the operation as shown in the following screenshot:

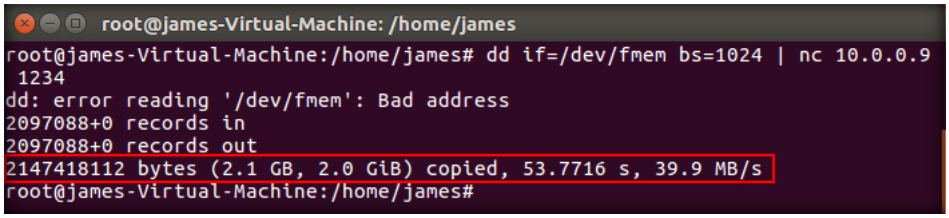


FIGURE 5.27: RAM Dump Created

42. Now, switch back to the **Ubuntu Forensics** virtual machine and go to the **Home** directory. You can observe the RAM image of the **Ubuntu Suspect** virtual machine is dumped with the name **ubuntu_remote_ram.dd**, as shown in the following screenshot:

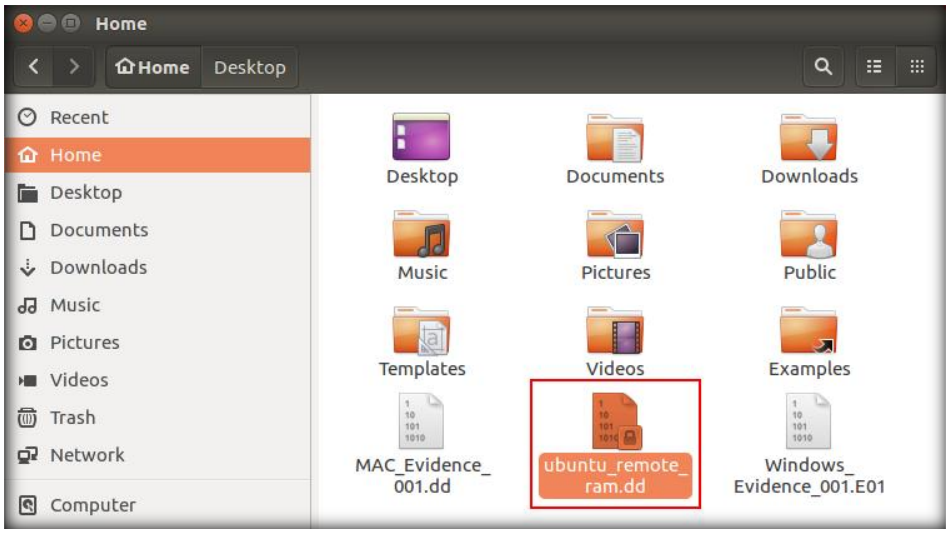


FIGURE 5.28: RAM Image File Acquired via Remote Acquisition

43. This way, you can acquire RAM locally and remotely using **dd** and **LiME**. Examining such RAM files is demonstrated in **CHFIv10 Module 06 Windows Forensics** and **CHFIv10 Module 07 Linux and Mac Forensics**.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Lab

6

Creating Customized Images from an Image Containing NTFS File System

NTFS (New Technology File System) is the file system used by the Windows NT Operating system for storing and retrieving files on a hard drive.

ICON KEY

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

Lab Scenario

NTFS has become the default storage format across various devices. It supports features such as compression and encryption, which help users hide data. Therefore, investigators need a deep knowledge of how the format works.

To be an expert forensic investigator, one must understand how to acquire a file from the storage device, analyze the file systems, and collect the data from them.

Lab Objectives

The objective of this lab is to help students learn how to analyze NTFS file system using **DiskExplorer for NTFS**.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

This lab requires:

- A computer running a **Windows Server 2016** virtual machine.
- Administrative privileges to execute the commands
- A web browser with internet access
- **DiskExplorer for NTFS** installer located at **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\DiskExplorer for NTFS**

Note: You can also download the latest version of **DiskExplorer for NTFS** from https://www.runtime.org/diskexpl.htm

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

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

Lab Duration

Time: 15 minutes

Overview of the Lab

This lab familiarizes you with the **DiskExplorer for NTFS** tool and helps you understand how to investigate an NTFS file system and copy hex data from it by importing a raw forensic image into the application.

Lab Tasks

TASK 1

Launching DiskExplorer Tool

1. Login to the **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\DiskExplorer for NTFS**.
3. Double-click **Setup.exe** to launch the setup and follow the wizard-driven installation steps to install the application.

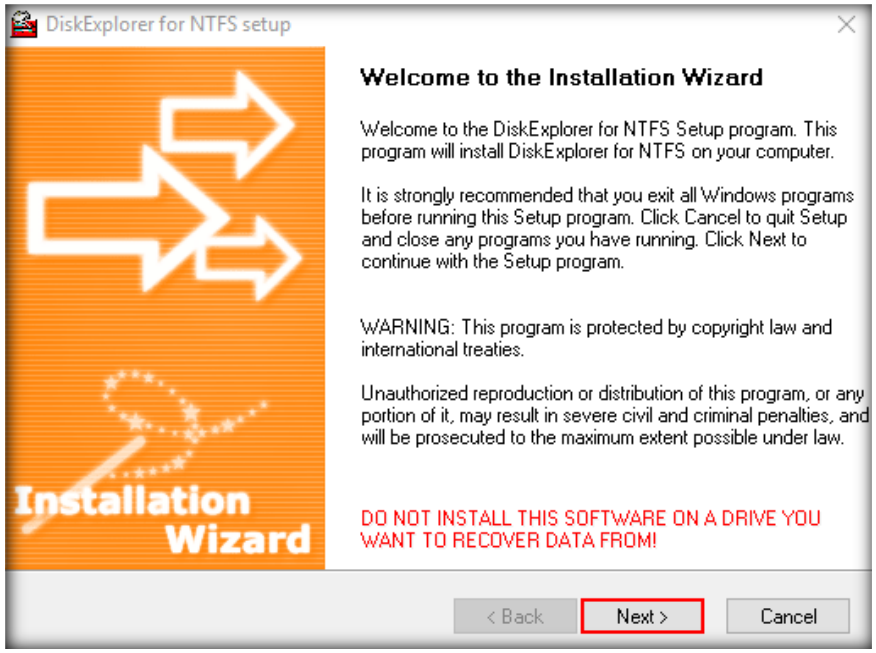


FIGURE 6.1: DiskExplorer for NTFS Installation Wizard

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

4. To launch the application, double-click the **DiskExplorer for NTFS** shortcut icon located on the Desktop.

5. The main window of **DiskExplorer for NTFS** appears, as shown in the screenshot:

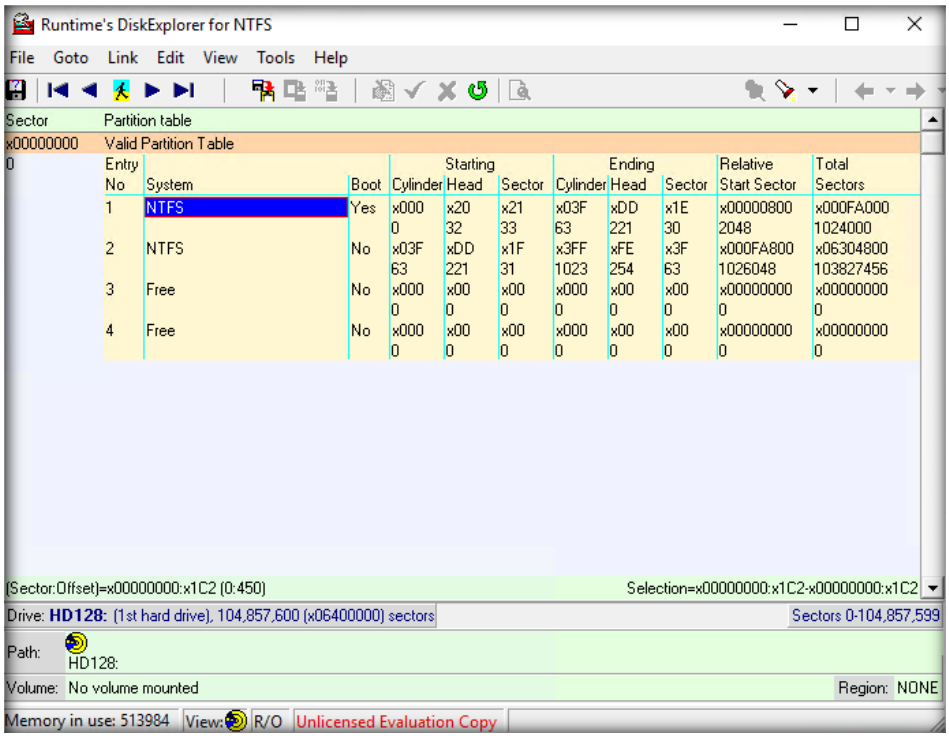


FIGURE 6.2: DiskExplorer for NTFS Main Window

TASK 2

Selecting an Image

6. Now, we will import a forensic image into this application. Go to **File** and select **Image...**.

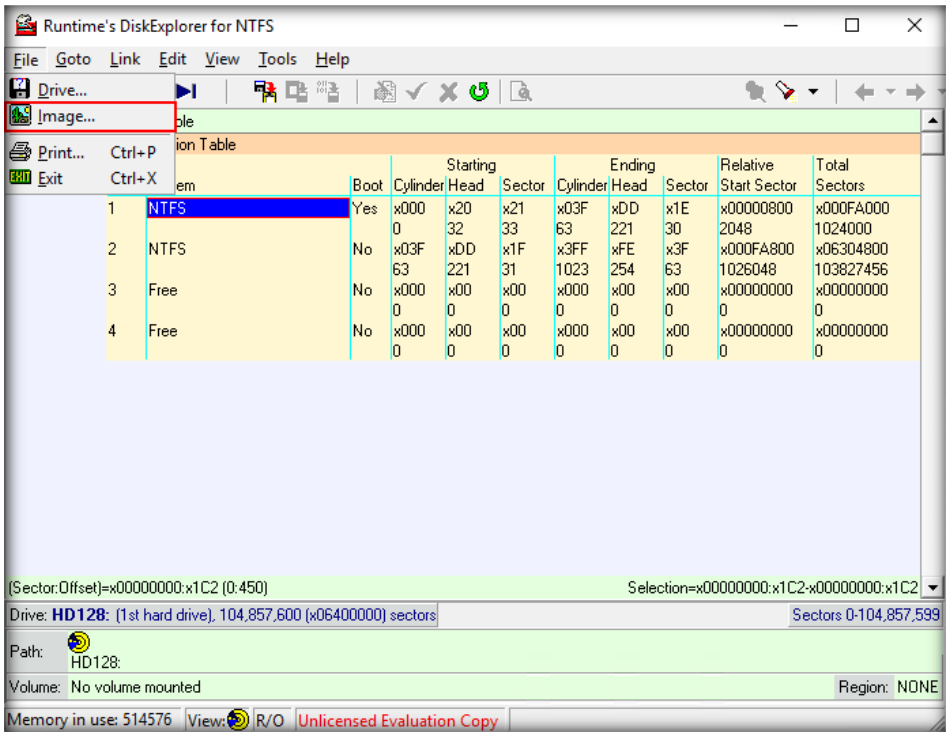


FIGURE 6.3: Select Image from the File Menu

7. **Select file to open as a drive...** window appears; in the **Files of type** drop-down list, select **All files (*. *)**, navigate to **C:\CHFI-Tools\Evidence Files\Forensic Images**, select **Windows_Evidence_001.dd**, and click **Open**.

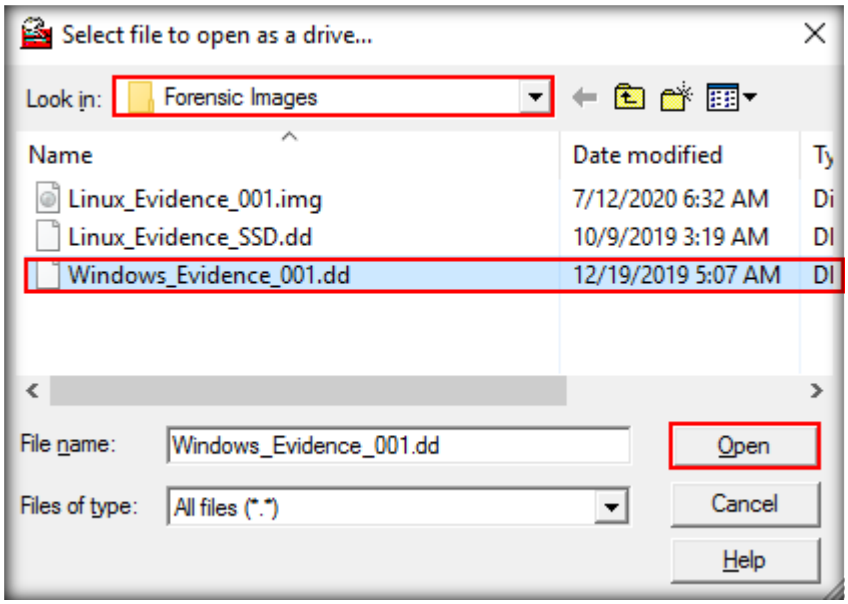


FIGURE 6.4: DiskExplorer for NTFS Evidence Image Selection

8. It will display the complete details of the image file in two sectors, **Valid** and **Invalid Boot Sector**, as shown in the figure below:

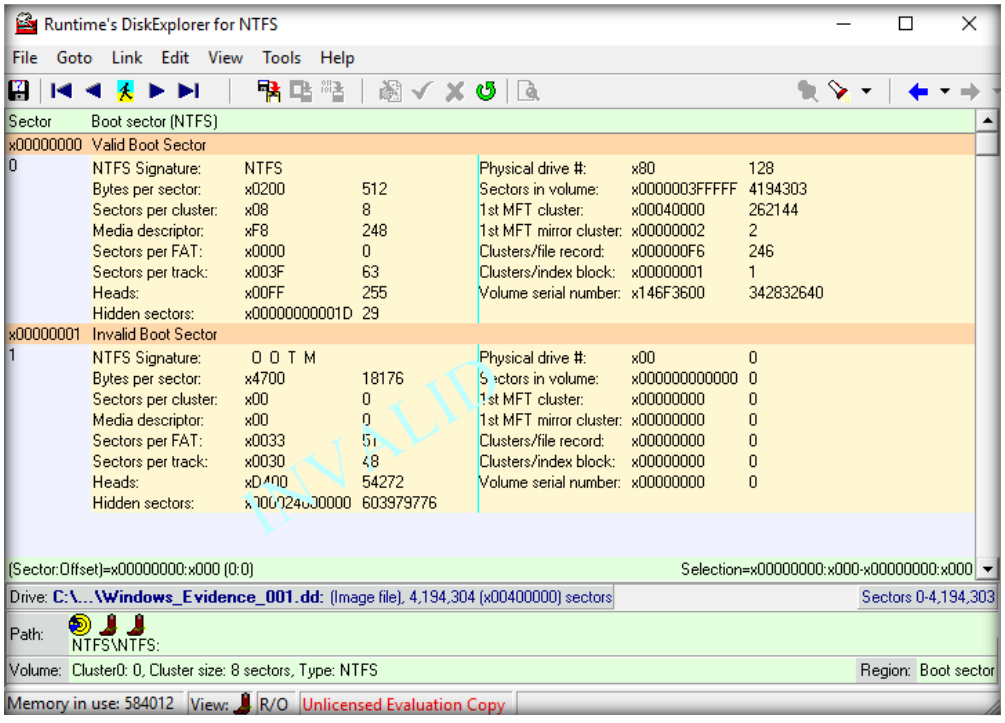


FIGURE 6.5: DiskExplorer for NTFS Boot Sector

TASK 3

Selecting the Sector

9. Now, click the **Sector** icon on the toolbar or navigate to **Goto → Sector** to view a specific sector.

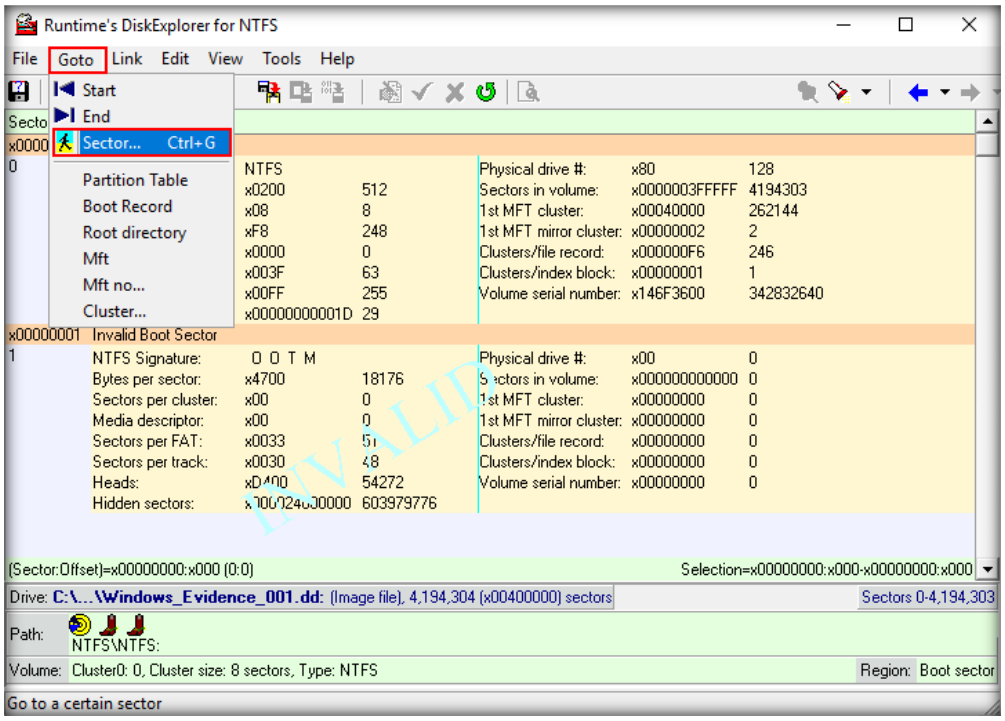


FIGURE 6.6: DiskExplorer for NTFS Sector Option

10. In the **Goto sector...** wizard, enter a **hex** value of your choice in the **Sector** or **Byte** section, to jump to a new position, and then click **OK**. (Here, we gave hex value as **00000002** in the **Sector** section).

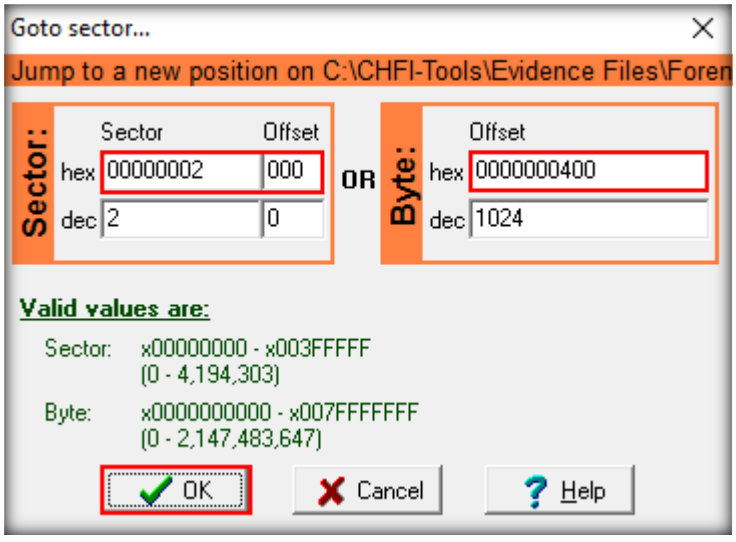


FIGURE 6.7: DiskExplorer for NTFS Goto Sector Wizard

The main characteristics of the NT file system are described by the boot record. The file system starts at the location of the boot sector and ends at this sector plus the sectors in the volume field. The volume is organized into clusters of multiples of 512 bytes.

Image files are files containing raw images of a drive. You can explore an image file as you can explore a physical or logical drive. Select File->Image or Drive->Image file to open an image file as a drive.

11. It will display the specified sector, as shown in the following screenshot:

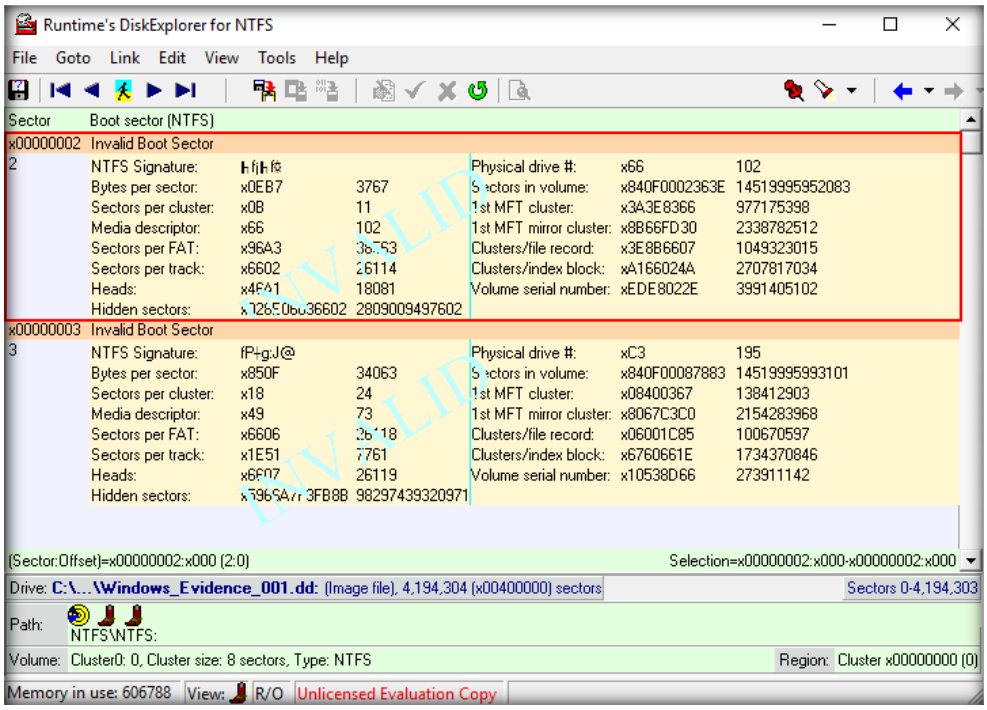


FIGURE 6.8: DiskExplorer for NTFS Window

TASK 4

Viewing the Hex Values of Selected Sector

12. Click **View → as Hex**, or alternatively you can press **F3** to view the hex values of the selected sector.

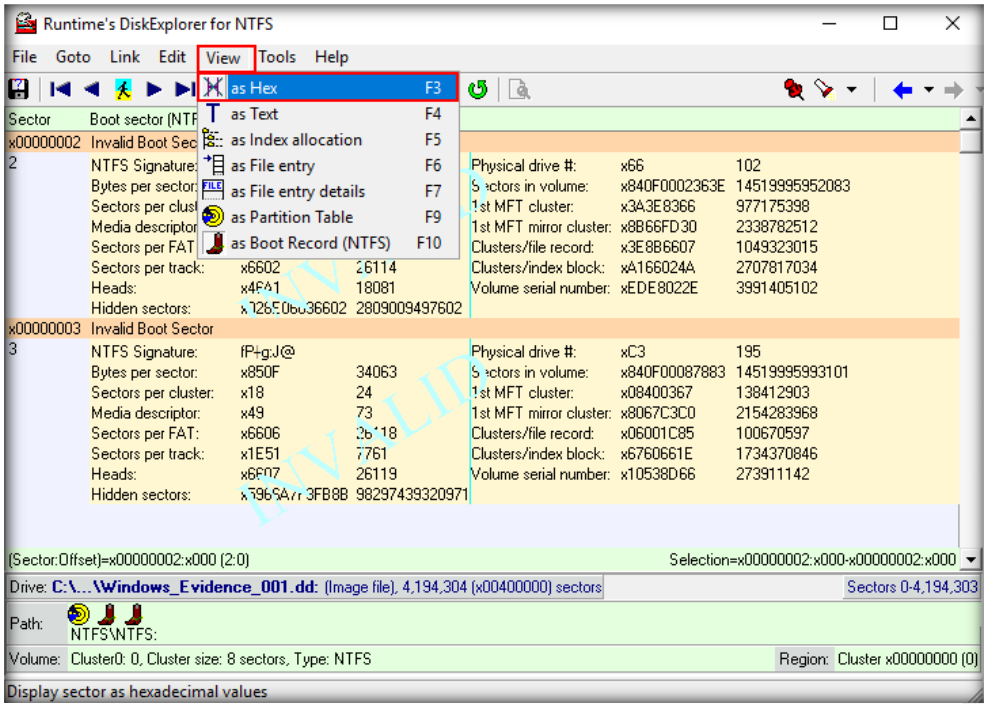


FIGURE 6.9: DiskExplorer for NTFS Hex Option

13. The screenshot below shows the **Hex view** of the selected sector:

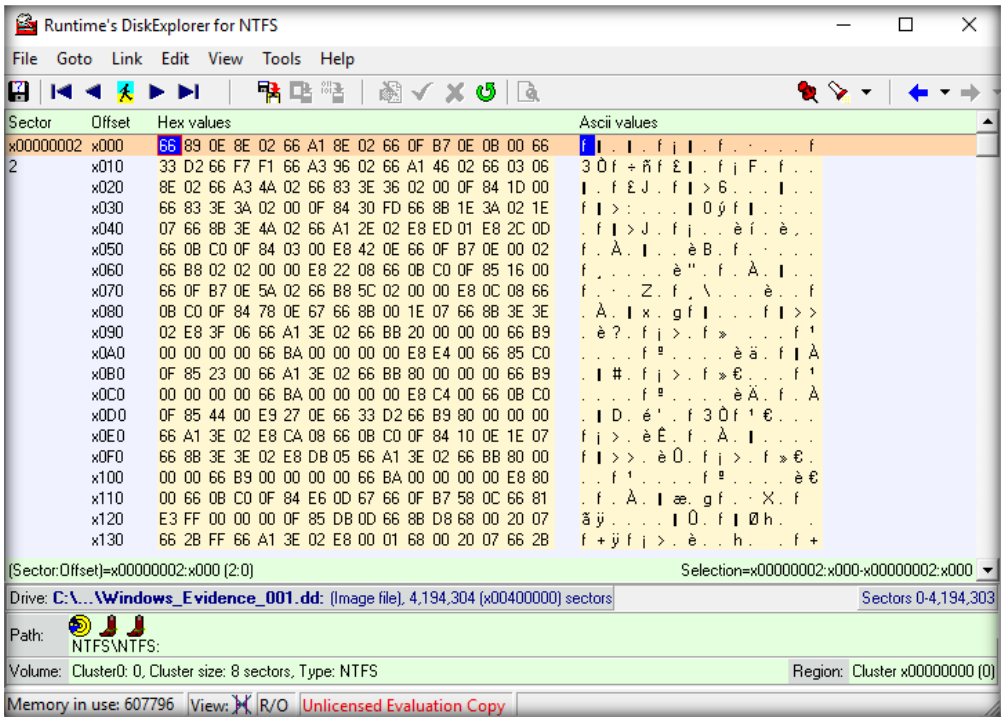


FIGURE 6.10: DiskExplorer for NTFS Hex View of Image Drive

14. You can copy the entire/required hex data for future reference. To copy the entire data, go to **Edit → Select All**.

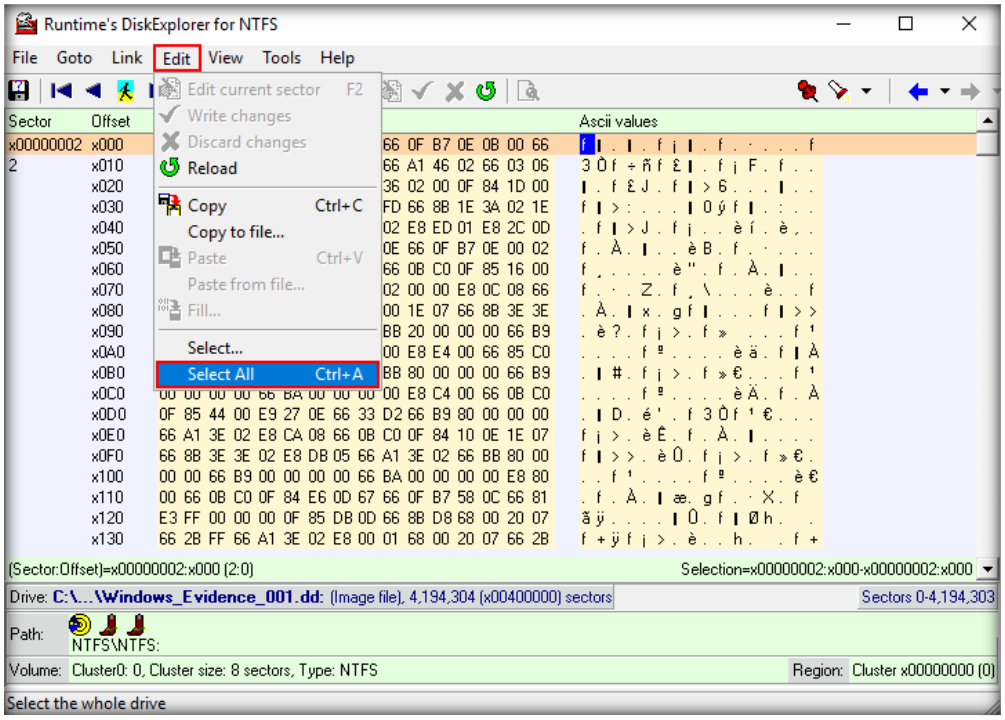


FIGURE 6.11: Go to Edit and click on Select All on DiskExplorer for NTFS Window

15. The entire **Hex** data will be highlighted, as shown in the following screenshot:

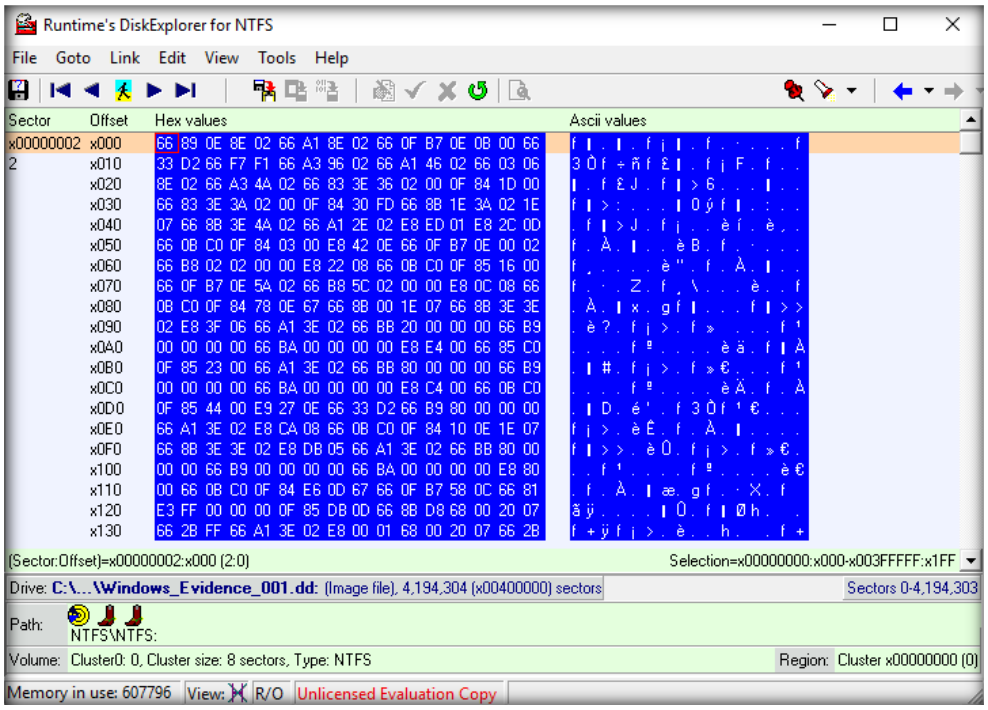


FIGURE 6.12: DiskExplorer for NTFS Window

TASK 5

Copying the Files

16. Navigate to **Edit** and click **Copy to file...** to copy the evidence file for further processing.

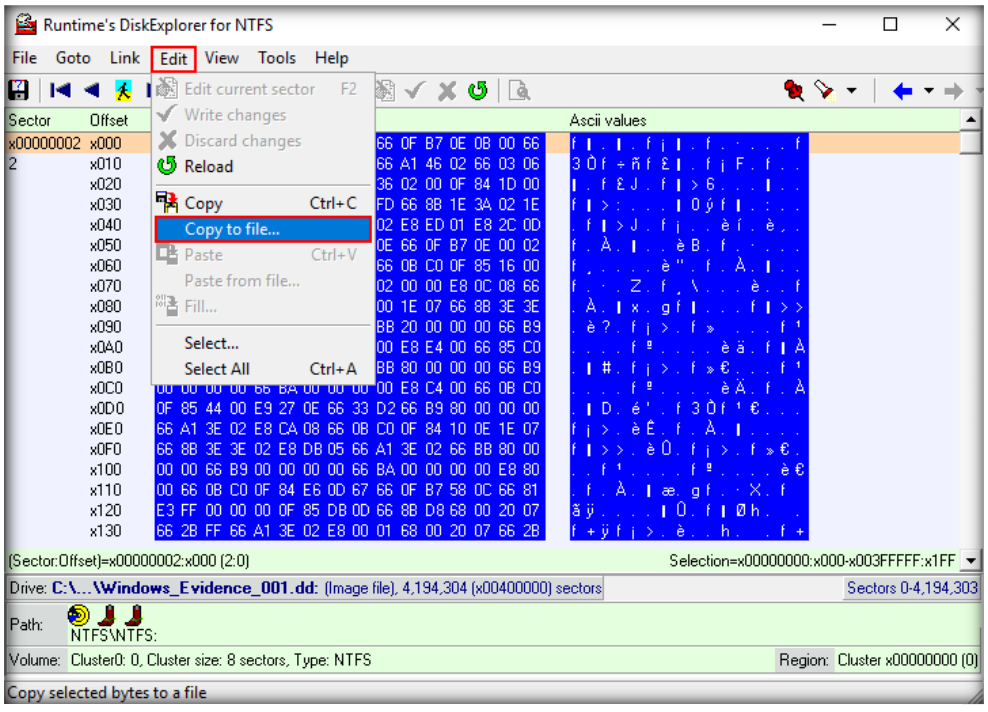


FIGURE 6.13: DiskExplorer for NTFS Copy to File Option

Select the desired drive or file, and the drive/file information—containing e.g., the geometry and the no. of LBA (Logical Block Addressing) sectors—will be displayed in the right window.

17. In the **Copy** pop-up window, select the destination location to save the file, and specify the name for the image file. At the top of the prompt, it will display the size of the image about to be created. Click **Save**.

18. In this lab, we are creating a folder named **Runtime Disk Explorer Image** on the **Desktop**, and saving the file to this location with the name **RDEM.img**.

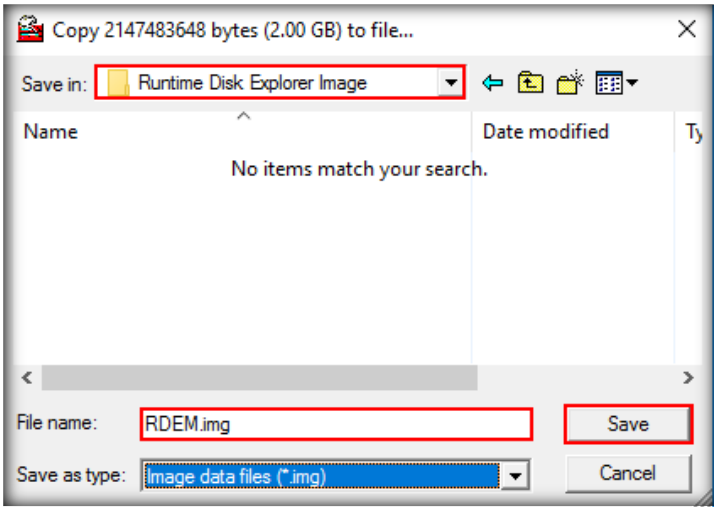


FIGURE 6.14: DiskExplorer for NTFS Save Option

19. In the **Confirm** pop-up, click **No** to save the image to a single file.

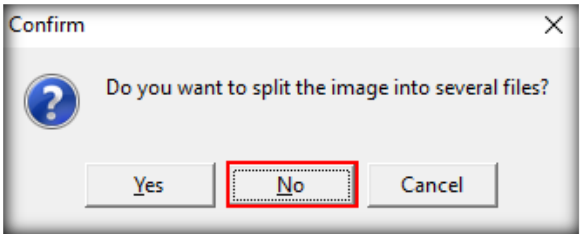


FIGURE 6.15: DiskExplorer for NTFS Confirm

20. The application will start copying the image file. The progress of this process will reflect as shown in the screenshot below:

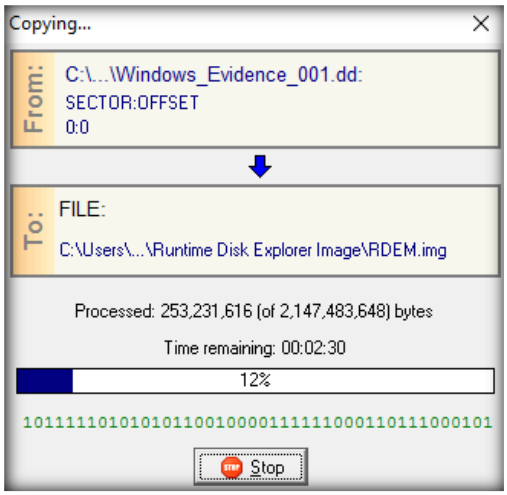


FIGURE 6.16: DiskExplorer for NTFS Copying window

Mounting a volume is the process of making the DiskExplorer know a certain file system structure. This is required by some navigation features, such as jumping to a cluster or jumping to a directory, and by the advanced recovery features, such as recover file and view file.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Lab

7

Viewing Contents of Forensic Image File

After acquiring the forensic image of the hard disk, the forensic investigator needs to preview the contents of the image file to see if it contains any evidence useful for investigation or any additional analysis is required.

ICON KEY

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

Lab Scenario

As part of investigation in an information theft case, senior investigator Alex has concluded scanning all the systems using the AccessData FTK Imager tool to know if the deleted files on the systems contain any information of evidentiary value. The tool saves the investigator's time as it eliminates the hectic process of recovering every deleted file from the system.

To be an expert forensic investigator, you must understand how to assess forensic images and collect the evidentiary data from those images.

Lab Objectives

The objective of this lab is to help students learn how to use **AccessData FTK Imager** for viewing forensics images.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication

To carry out the lab, you need:

- A computer running **Windows Server 2016** virtual machine
- Administrative privileges to execute the commands
- A web browser with internet access
- **AccessData FTK Imager 4.3.1** installer located at **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\AccessData FTK Imager**

Note: You can also download the latest version of **AccessData FTK Imager tool** from https://accessdata.com/product-download

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

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

Lab Duration

Time: 15 minutes

Overview of the Lab

This lab familiarizes you with the **AccessData FTK Imager** tool and helps you learn how to investigate forensic images of computer data without subjecting the original evidence to modification. It also helps you understand how to assess electronic evidence to determine whether further analysis of the evidence with a forensic tool is necessary.

Lab Tasks

TASK 1

Install the Application

1. Login to the **Windows Server 2016** virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv10 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\AccessData FTK Imager**, double-click **AccessData_FTK_Imager_4.3.1.exe** to launch the setup, and follow the wizard-driven installation instructions to install the application.

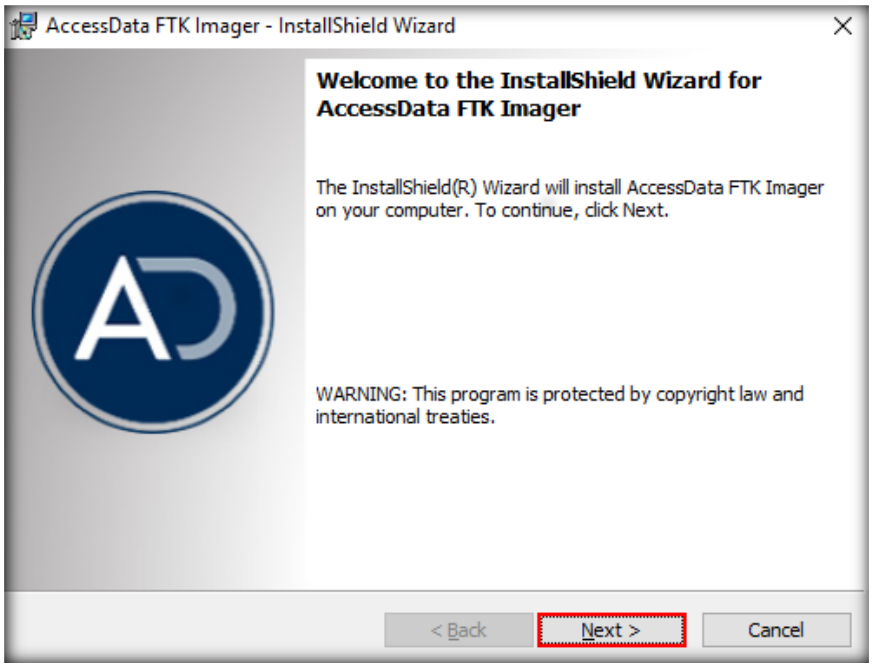


FIGURE 7.1: AccessData FTK Imager Installation Wizard

Note: At the end of the installation process, ensure that the **Launch AccessData FTK Imager** option is checked in the setup wizard and then click **Finish**.

3. The main window of **AccessData FTK Imager** appears, as shown in the following screenshot:

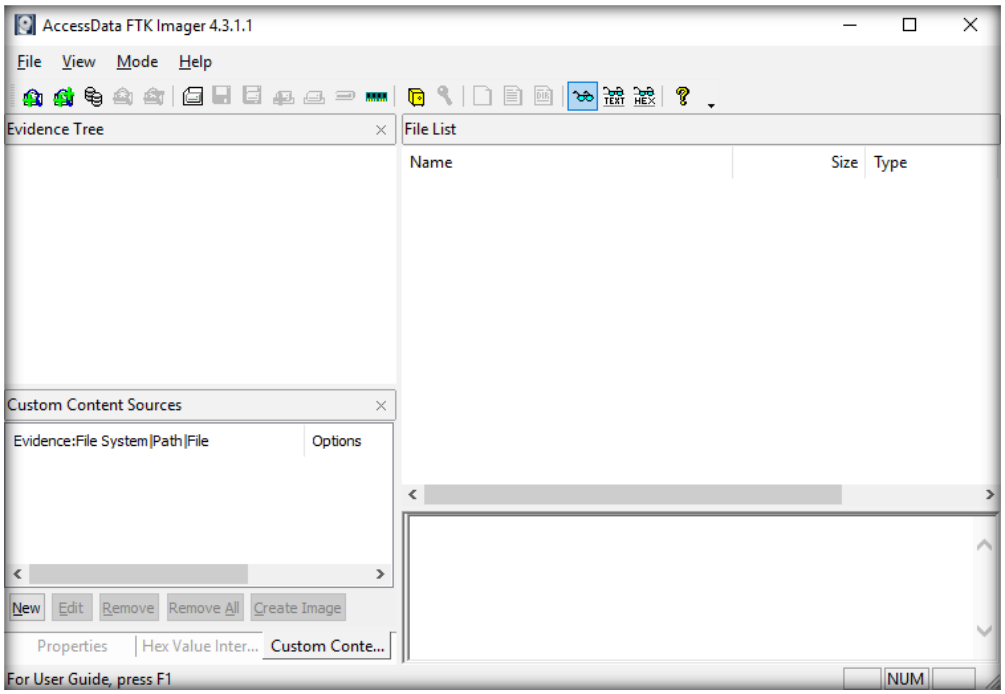
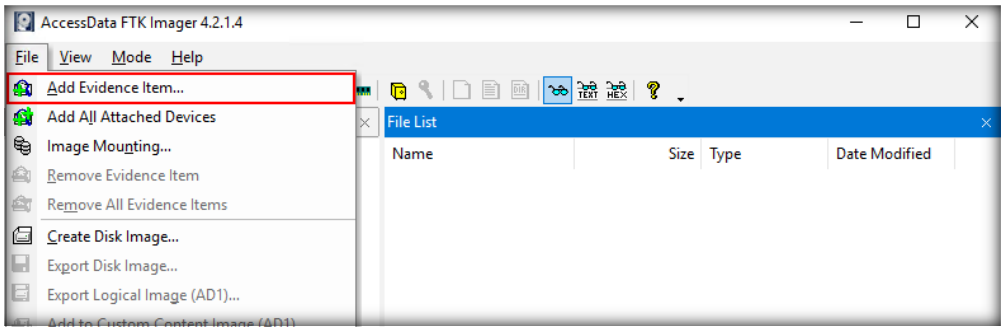


FIGURE 7.2: AccessData FTK Imager

4. Click **File → Add Evidence Item...** to add evidence.



Preview files and folders on local hard drives, network drives, floppy diskettes, zip disks, CDs, and DVDs.

FIGURE 7.3: Adding an Evidence

Note: Alternatively, you may also click on the **Add Evidence** icon from the toolbar to add evidence. The **Add Evidence** icon is highlighted in the screenshot below:

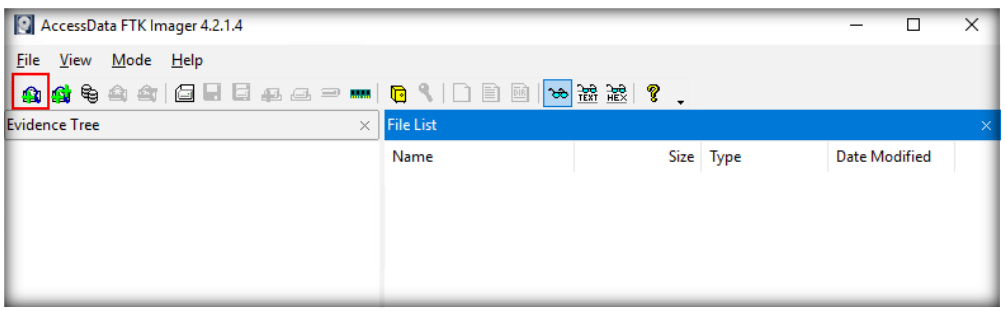


FIGURE 7.4: Adding an Evidence

5. A **Select Source** window opens. Select the **Image File** option and click **Next**.

Note: In this lab, we will be examining a **dd** image; therefore, select the **Image File** radio button.

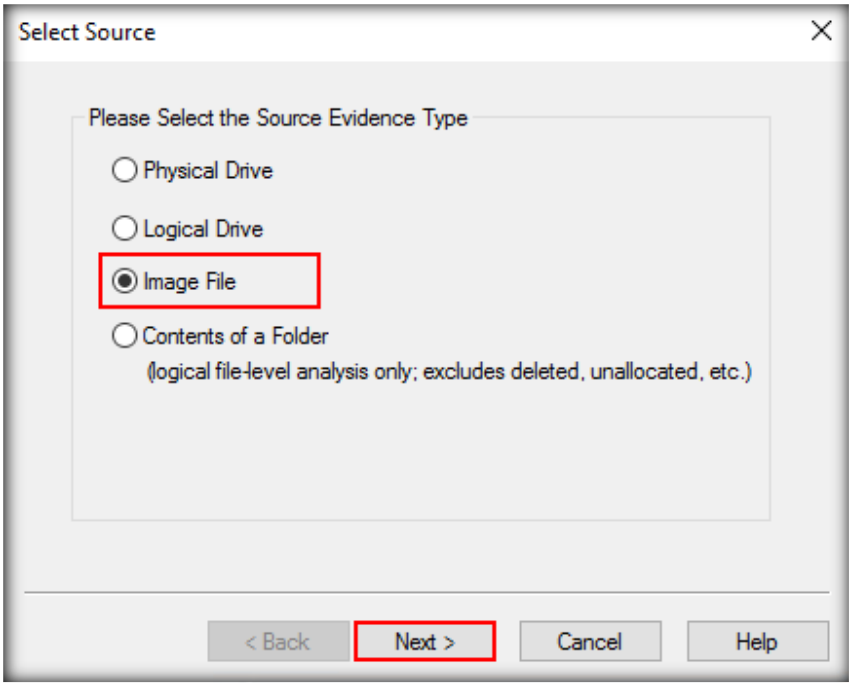


FIGURE 7.5: AccessData FTK Imager Selecting Source

Preview the contents of forensic images stored on the local machine or on a network drive.

6. Click the **Browse** button to specify the image file path **(C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd)** and then click **Finish**.

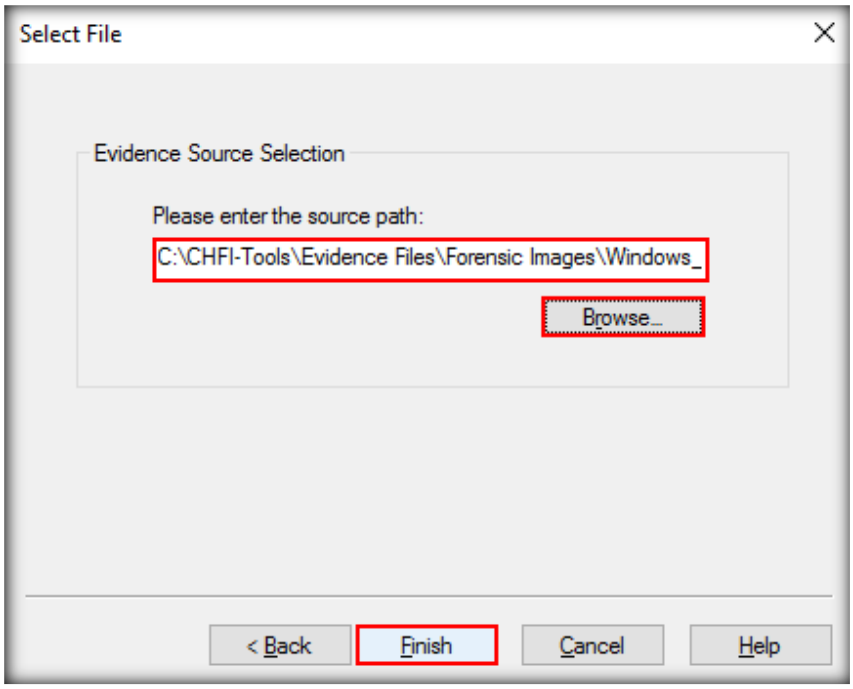


FIGURE 7.6: AccessData FTK Imager Giving Path of Image File

Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive.

7. The evidence file (**Windows_Evidence_001.dd**) appears in the left pane of the main window under the **Evidence Tree** section. **Expand** the evidence file and its contents so that it appears in the form of a tree, as shown in the following screenshot:

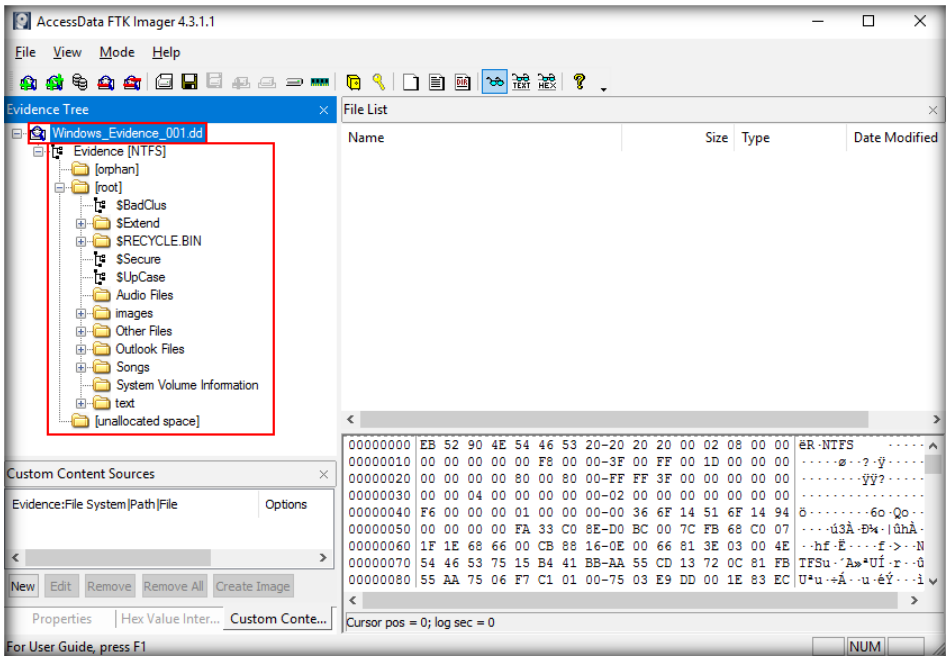


FIGURE 7.7: AccessData FTK Imager giving Evidence Tree

See and recover files that have been deleted from the Recycle Bin but have not yet been overwritten the drive.

TASK 2

Viewing the Content of a Forensics Image

8. Select any file or folder from the **Evidence Tree** to view the file list in the **Right** pane under **File List**.

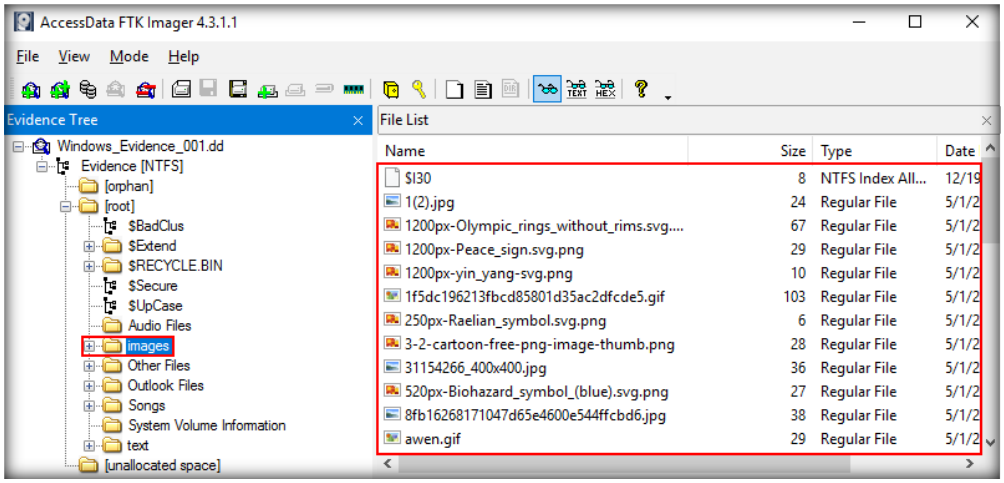


FIGURE 7.8: AccessData FTK Imager File List

Generate hash reports for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case evidence.

9. Apart from viewing the contents of a file or folder, **AccessData FTK Imager** also lets you view the hex values of files. Hex values help determine the raw and exact contents of a file even if it has been deleted or overwritten. Hex values thus help you identify and retrieve information that normally cannot be accessed by the OS.

10. To view the **Hex** value of a file, select a file from the **File List** and click the **Hex** icon on the toolbar.

11. Hex values of the selected file will be displayed in the **bottom-right** pane.

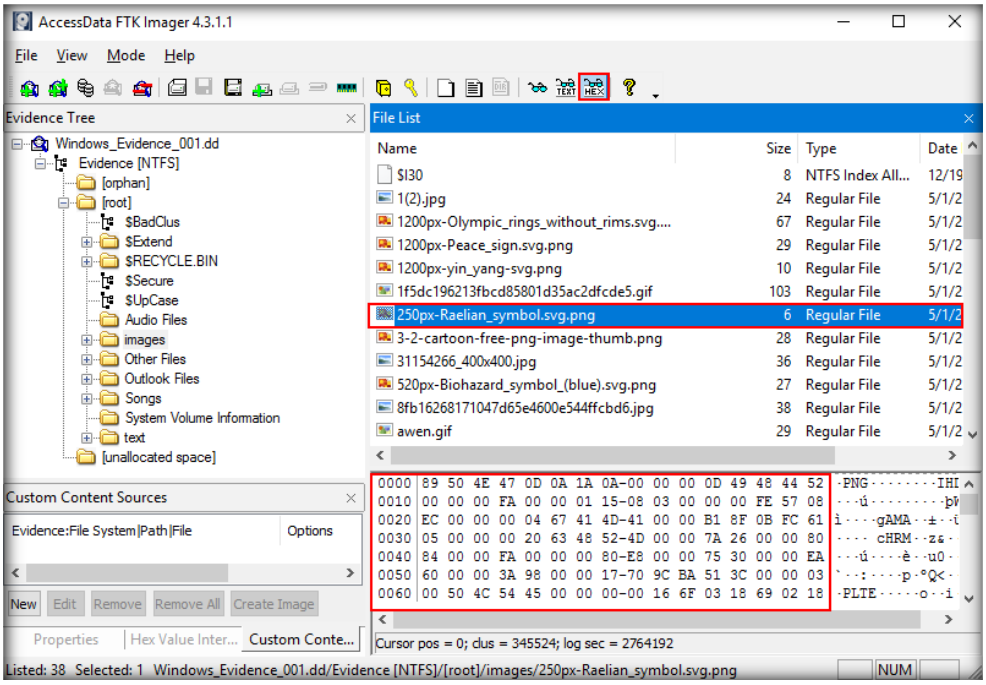


FIGURE 7.9: AccessData FTK Imager Hex View

12. Click the **Properties** tab in the **lower-left** pane to view the properties such as file class, size, date, start cluster, etc. of the selected file.

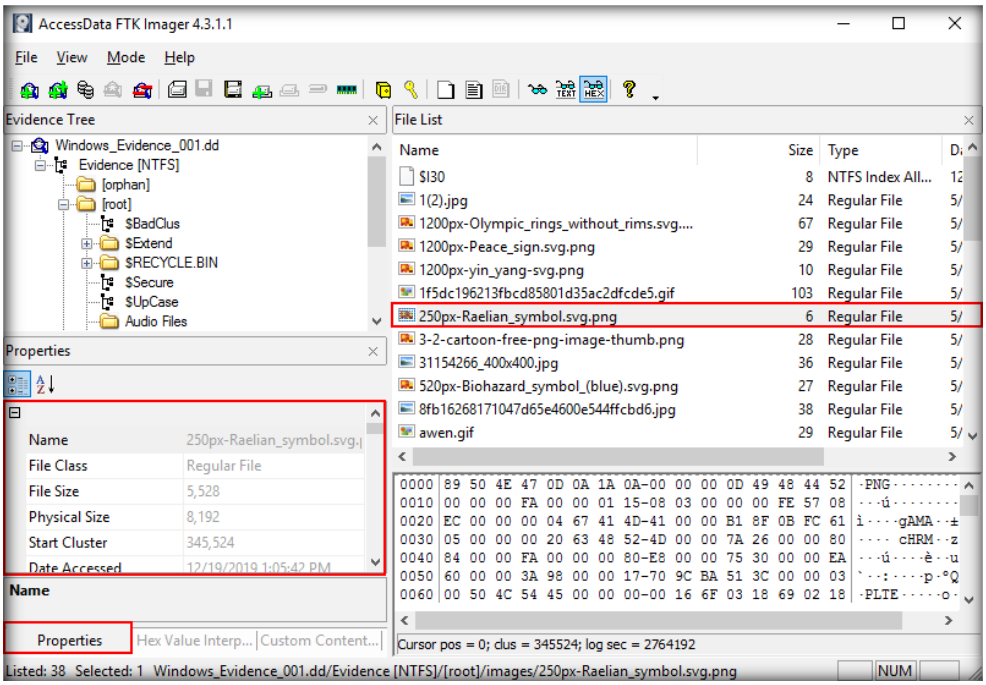


FIGURE 7.10: AccessData FTK Imager Properties Window

13. Click the **Hex Value Interpreter** tab in the **lower-left** pane to view the properties such as signed integer, DOS date, etc. of the selected file.

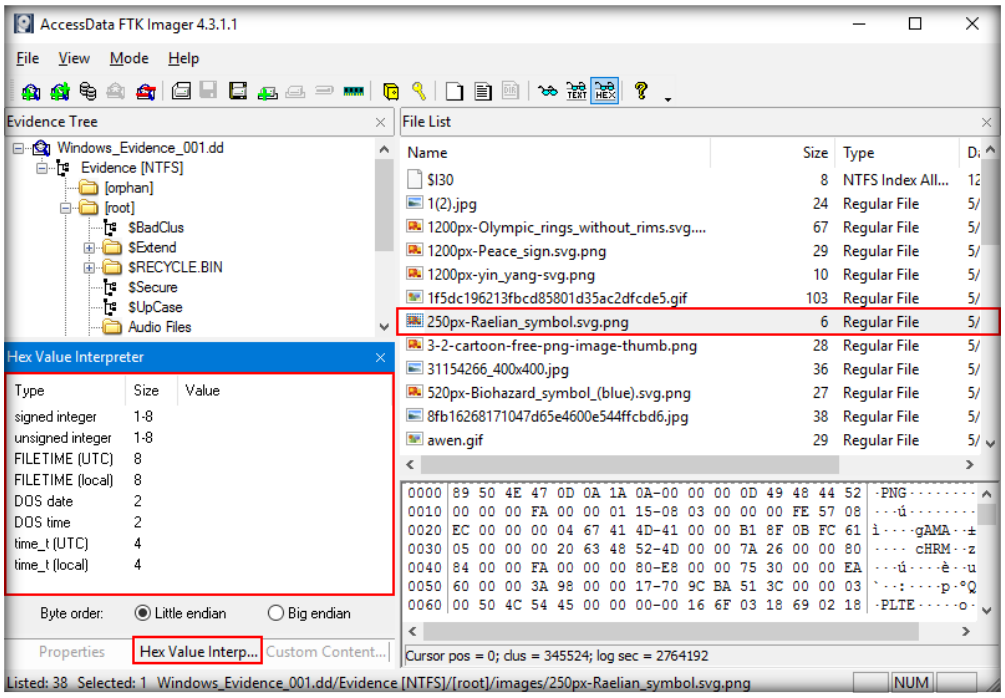


FIGURE 7.11: AccessData FTK Imager Hex Value Interpreter Window

14. This way you can examine the contents of the forensic image file using **AccessData FTK Imager** tool.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

This page is intentionally left blank.