Cengage | CEN-CFORENSICS7e: Computer Forensics 7th Edition

Processing Crime and Incident Scenes

Exercises

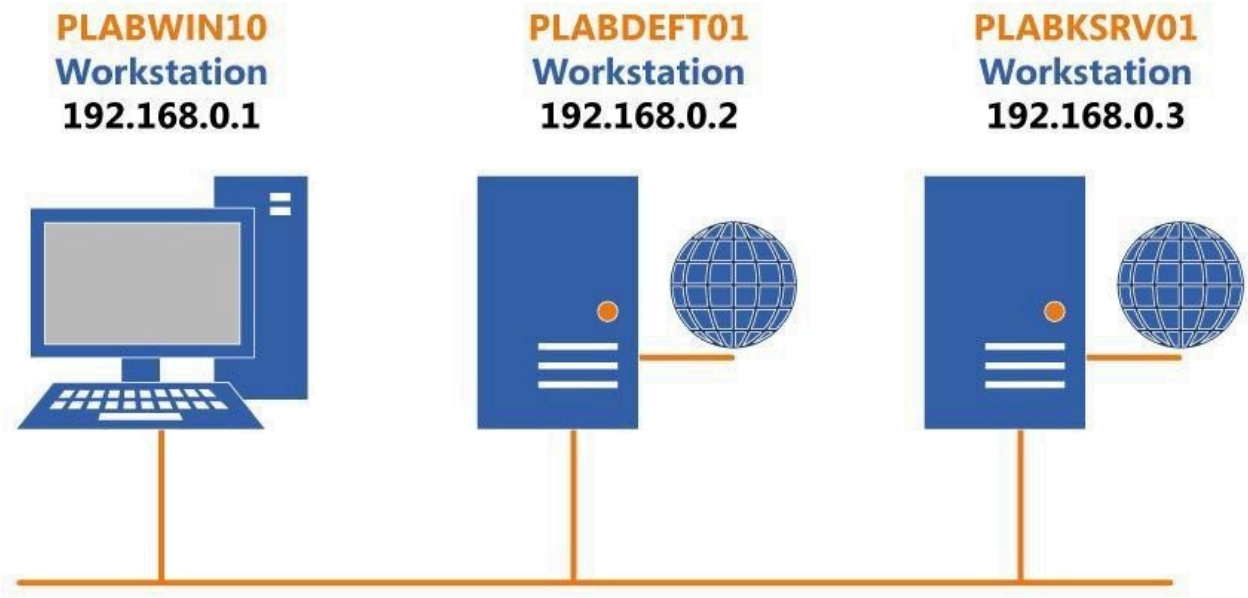
Introduction

The **Processing Crime and Incident Scenes** lab provides you with the instructions and devices to develop your hands-on skills in the following topics.

- Exercise 5-1 Conducting the Investigation: Acquiring Evidence with OSForensics
- Hands-On Project 5-1
- Hands-On Project 5-2
- Hands-On Project 5-3
- Hands-On Project 5-4

Lab Diagram

During your session, you will have access to the following lab configuration. Depending on the exercises, you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.



Connecting to Your Lab

In this module, you will be working on the following equipment to carry out the steps defined in each exercise.

- **PLABWIN10** (Windows 10 - Standalone Workstation)

Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

Lab Assessment

Test your knowledge on the topics covered in this lab by completing the Lab Assessment. Screenshot assessment items can be found at the end of each exercise and review questions are located on the Summary page.

Click Next to proceed to the first exercise.

Exercise 5-1 Conducting the Investigation: Acquiring Evidence with OSForensics

In the following activity, you use OSForensics to analyze an image file.

To get a better understanding of this technology, please refer to your course material or use your preferred search engine to research this topic in more detail.

Task 1 - Extract Evidence Using OSForensics

Step 1

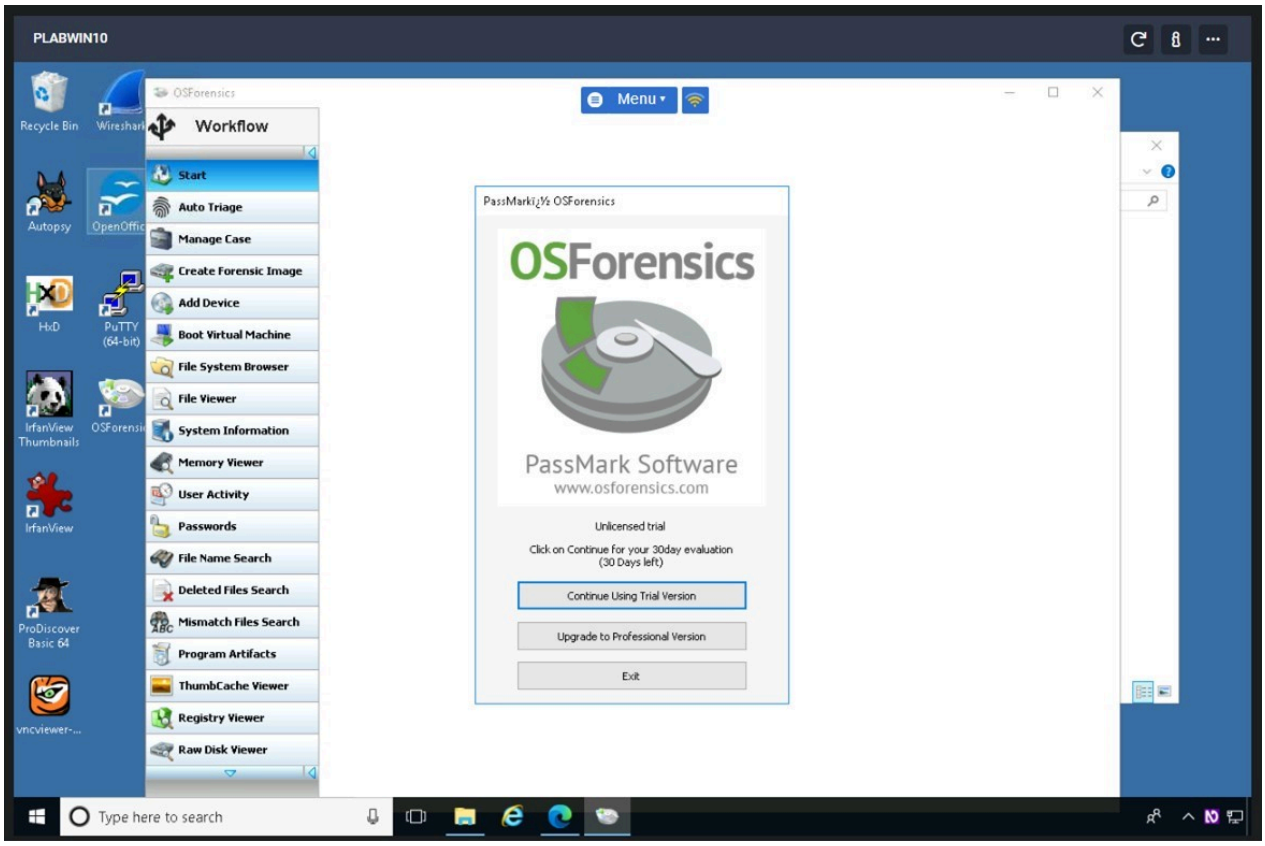
Power on and connect to **PLABWIN10**.

If **OSForensics** is not already installed on **PLABWIN10**, install it by running the **osf.exe** file located in the **Downloads** folder.

Start **OSForensics** from the start menu or using the desktop shortcut.

Step 2

On the **OSForensics** welcome message box, click **Continue Using Trial Version**.



Step 3

Click **Start** in the left pane if necessary. In the right pane, click **Create Case**.

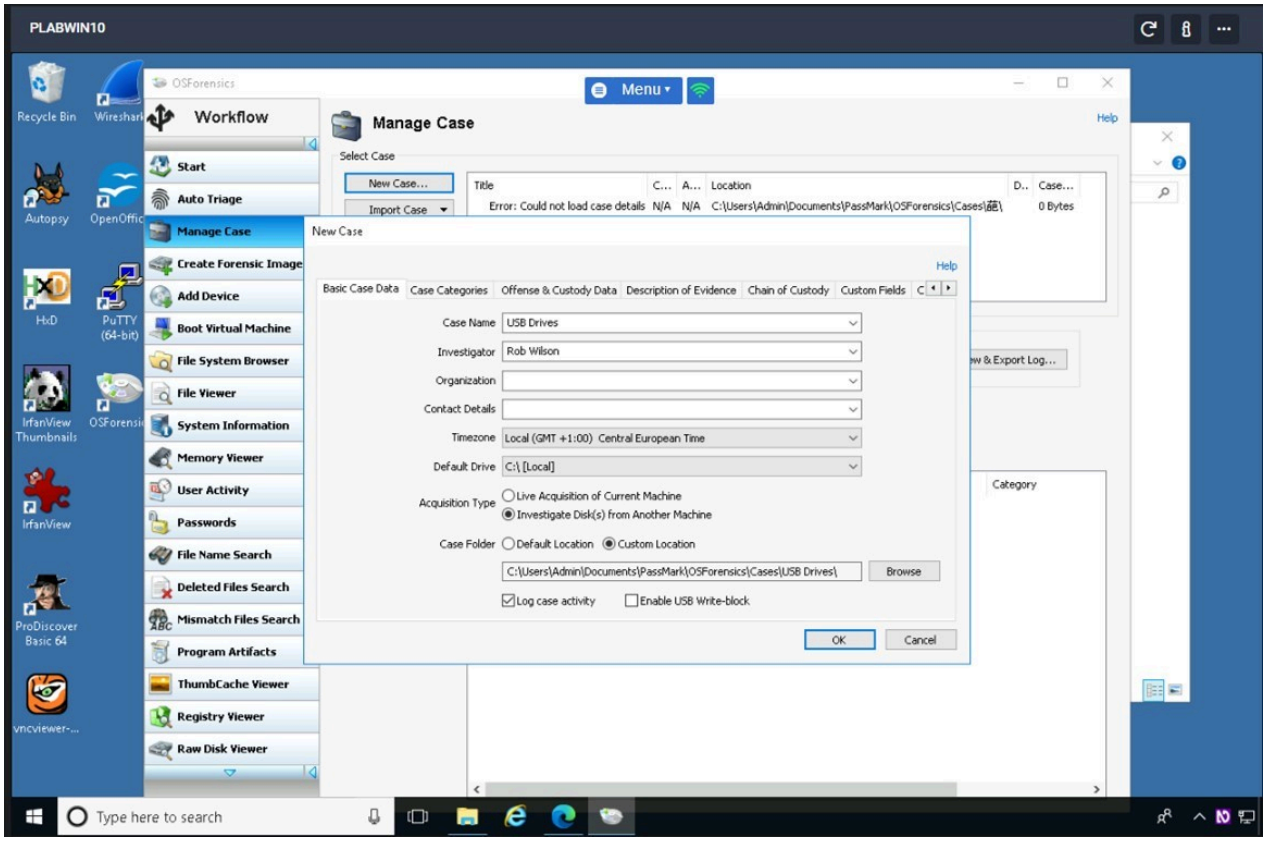
Step 4

In the New Case dialog box, enter your name for Investigator. For the case name, type:

```
USB drives
```

Click **Investigate Disk(s) from Another Machine**.

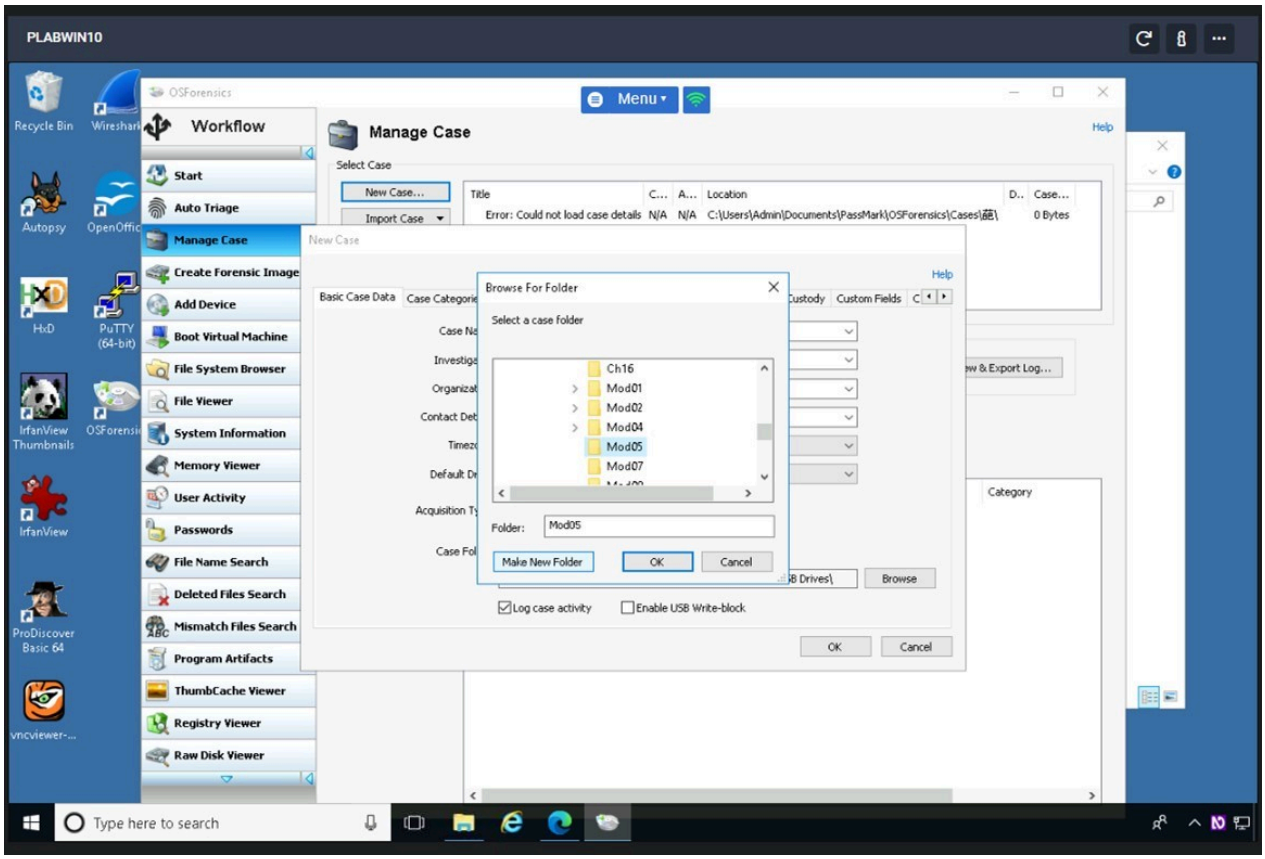
Click **Custom Location** for the case folder. Click the **Browse** button.



Step 5

On the **Browse For Folder** dialog box, navigate to **Local Disk (C:) > Work > Data files** and click **Mod05** folder.

Click **Make New Folder**.

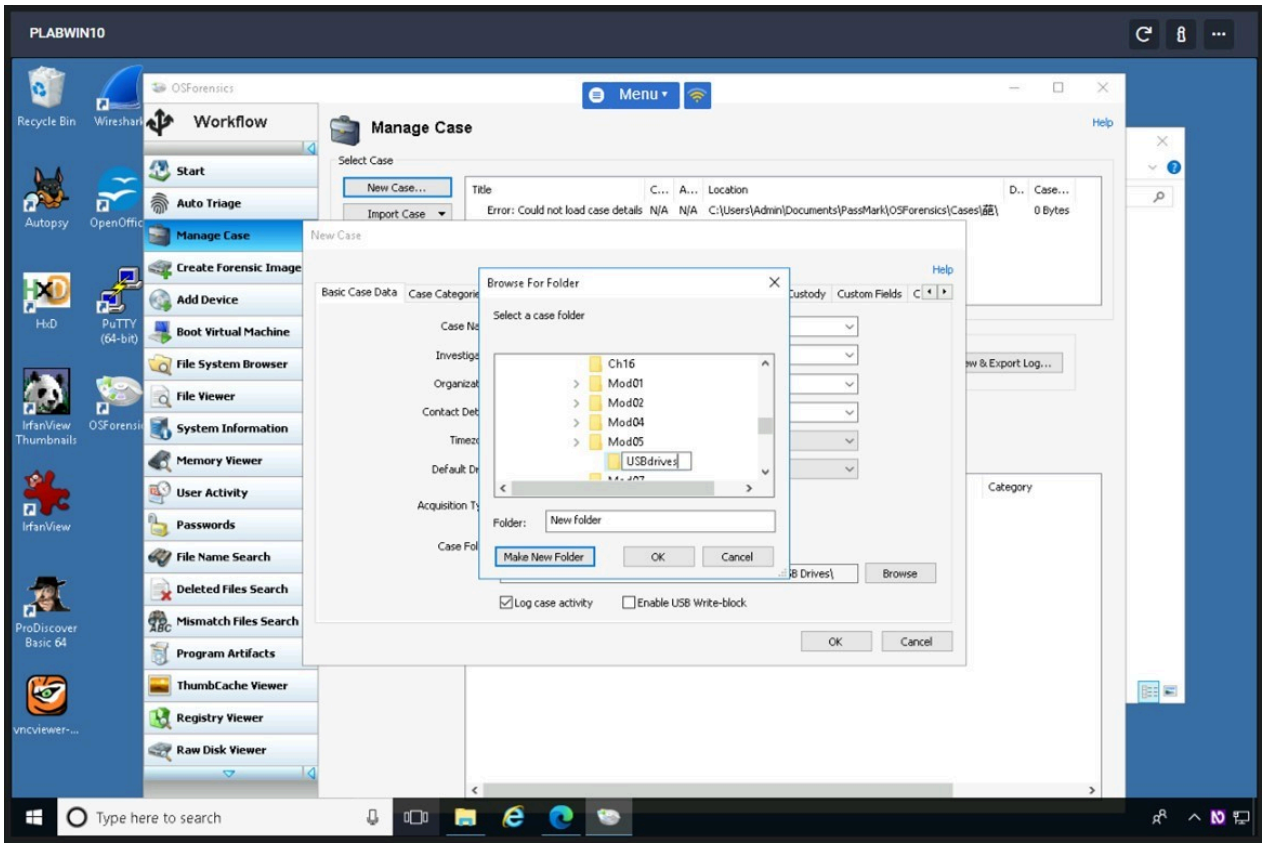


Step 6

Rename the folder as:

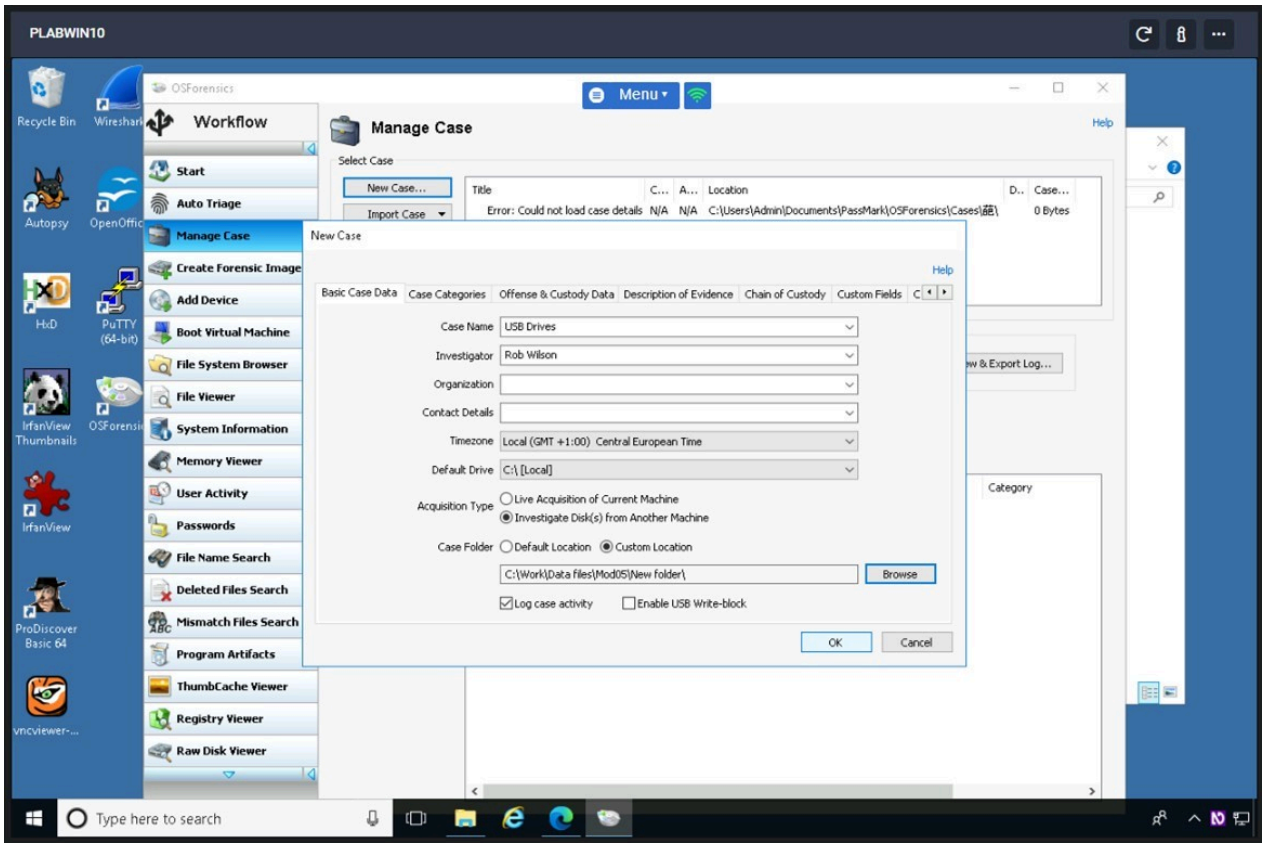
```
USBdrives
```

Click **OK**.



Step 7

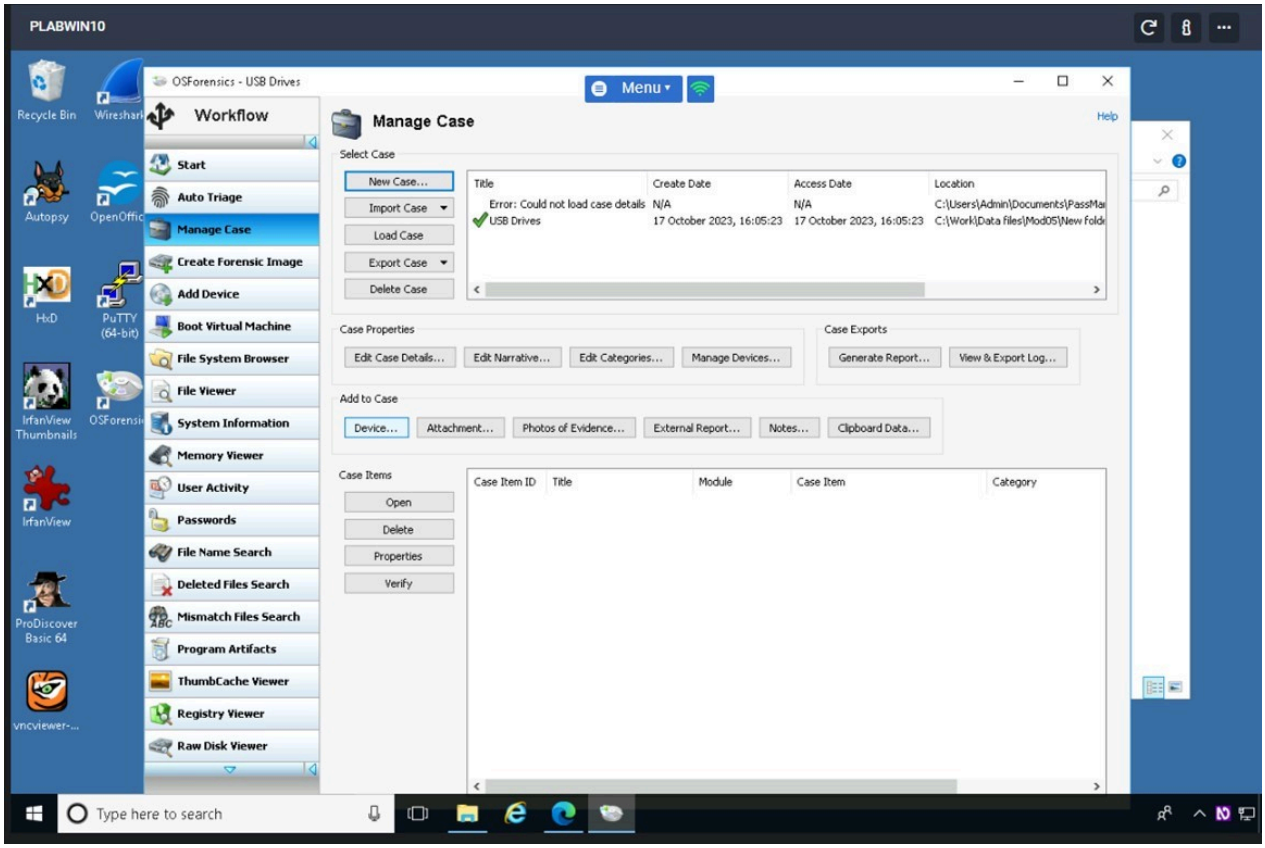
Click **OK** to save changes in the **New Case** dialog box.



Step 8

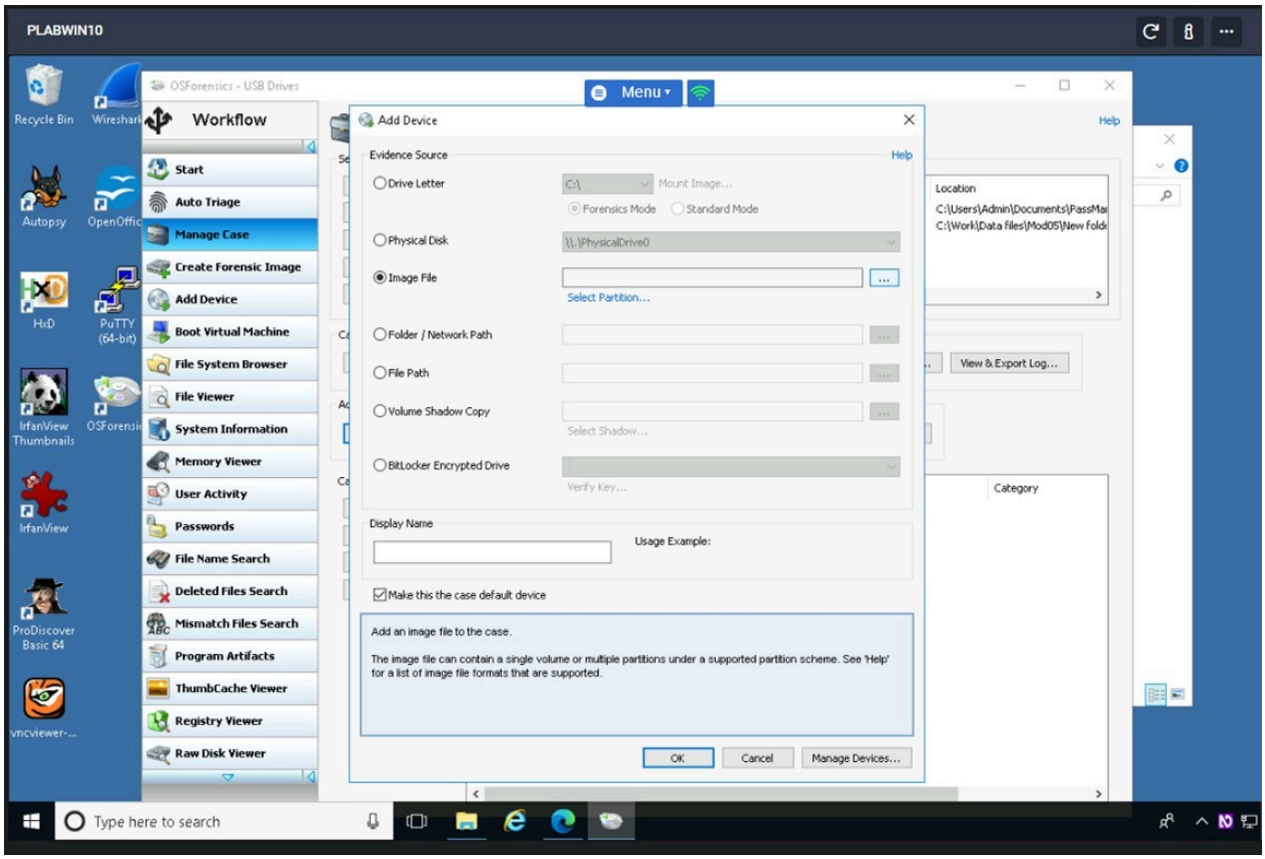
You should see the **Manage Case** window.

Click the **Device** button in the Add to Case section.



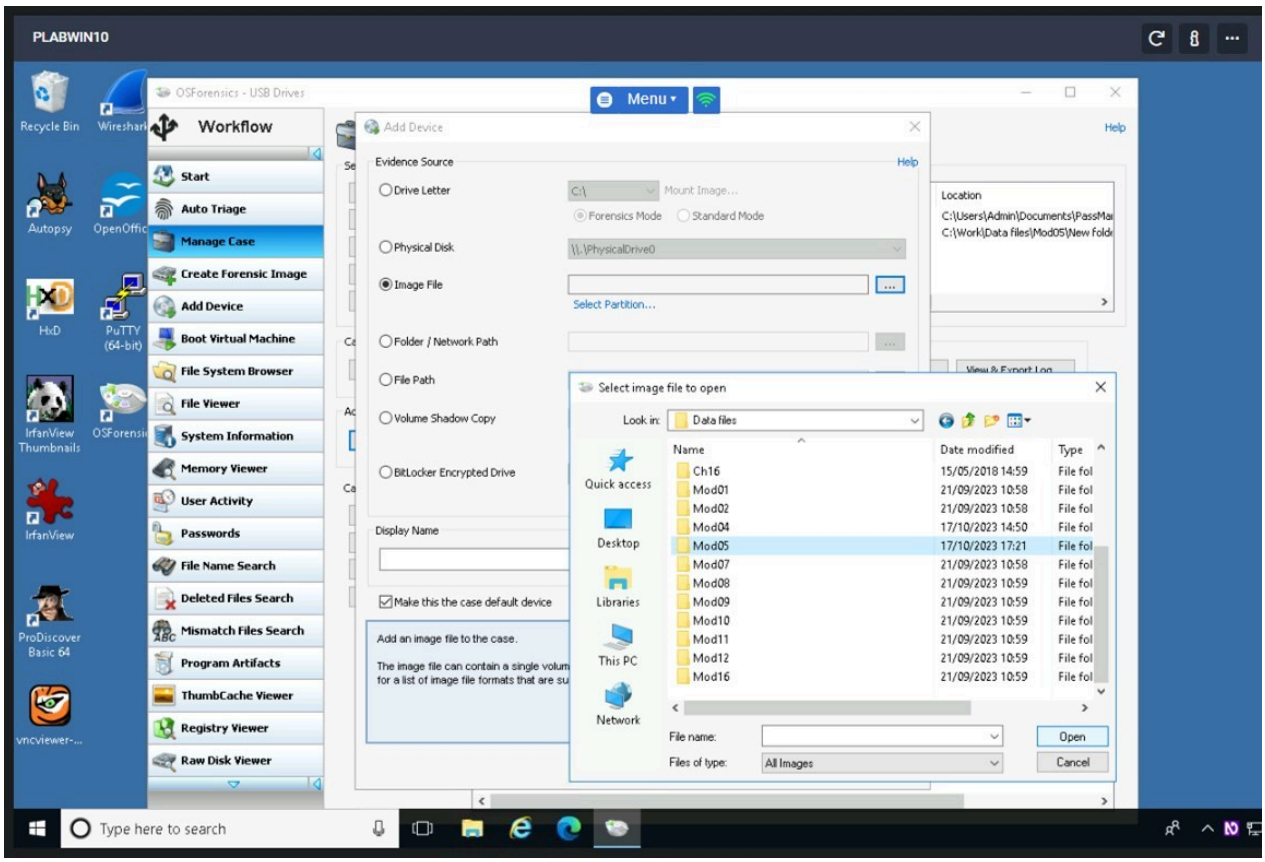
Step 9

On the **Add Device** dialog box, click the **Image File** option and select **[...]** button.



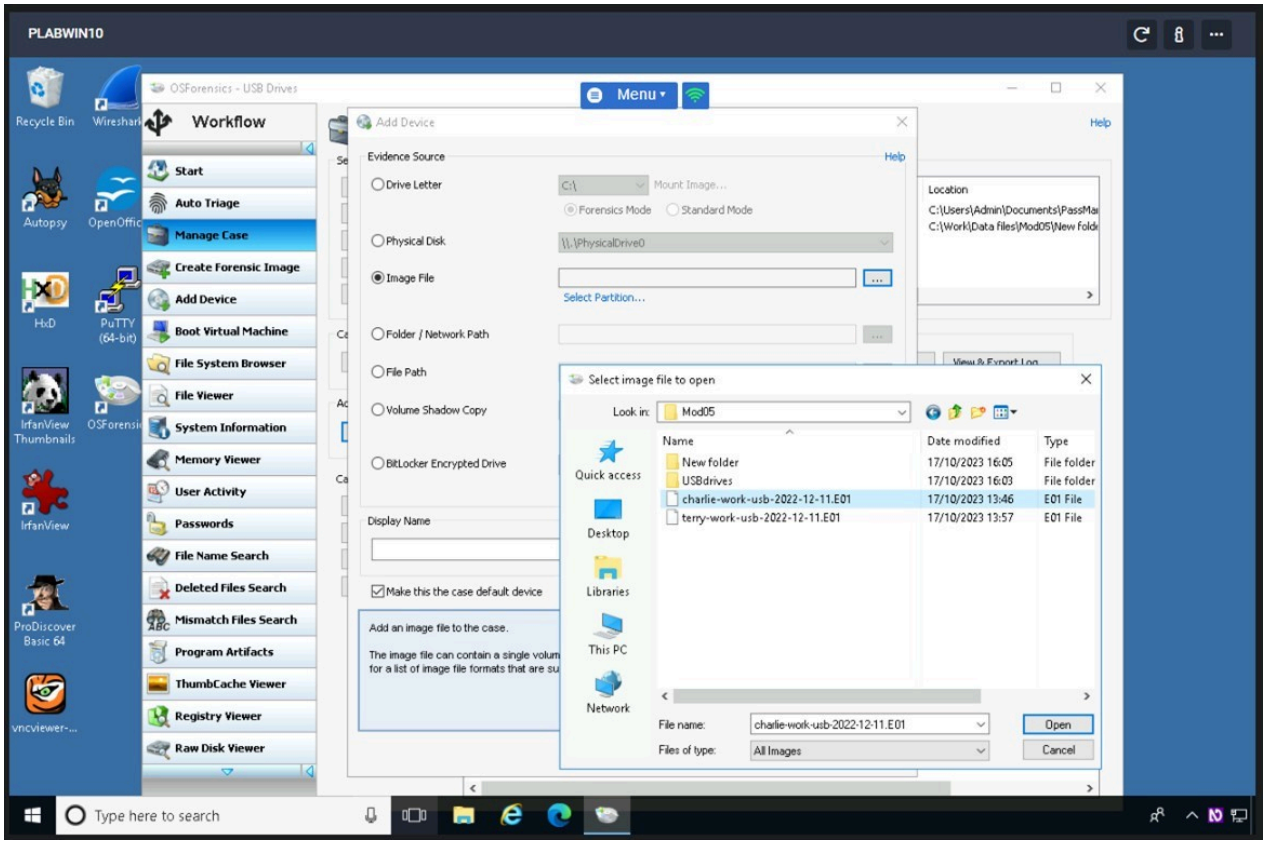
Step 10

On the **Select image file to open** dialog box, access the **Look in** drop-down list and navigate to **This PC > Local Disk (C:) > Work > Data files > Mod05** path.



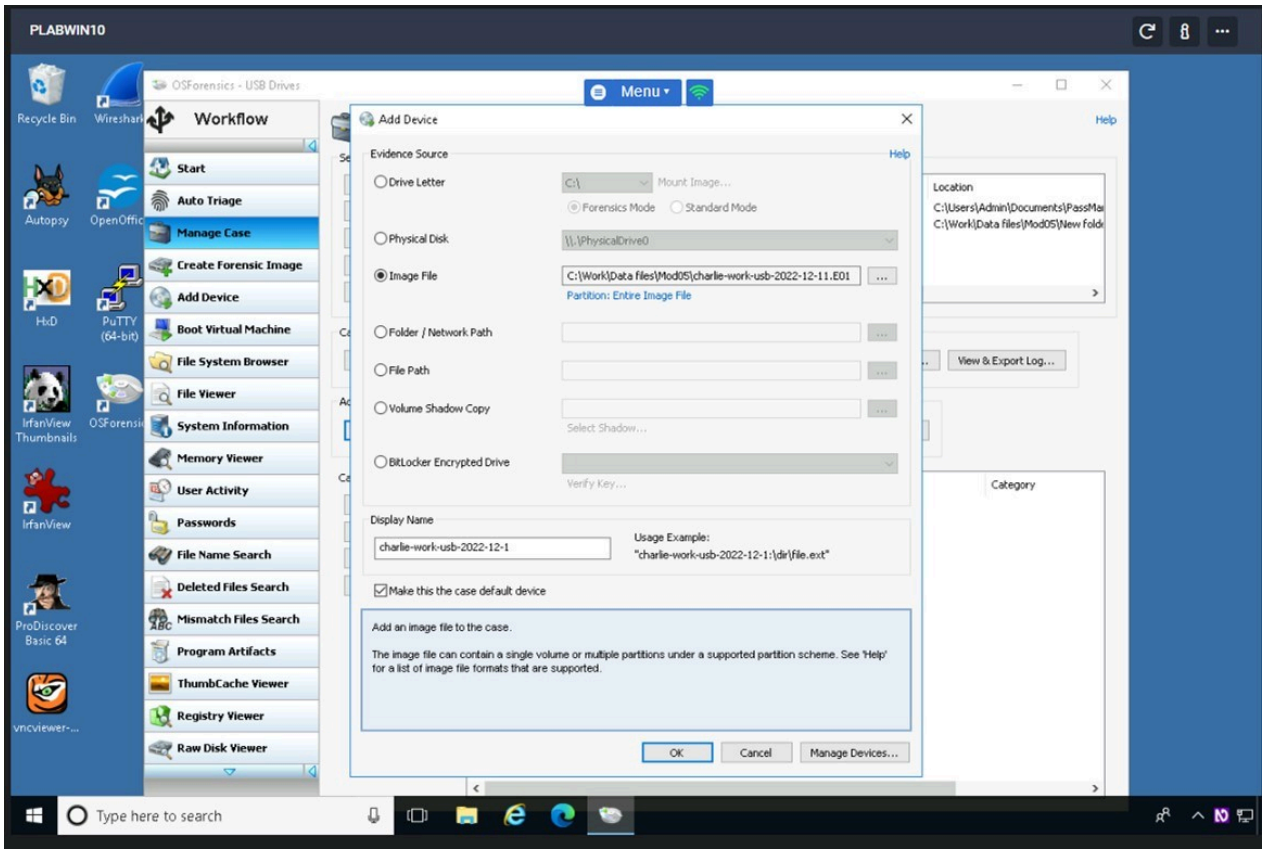
Step 11

Still, on the **Select image file to open the** dialog box, click **charlie-work-usb-2022-12-11.E01**, and click **Open**.



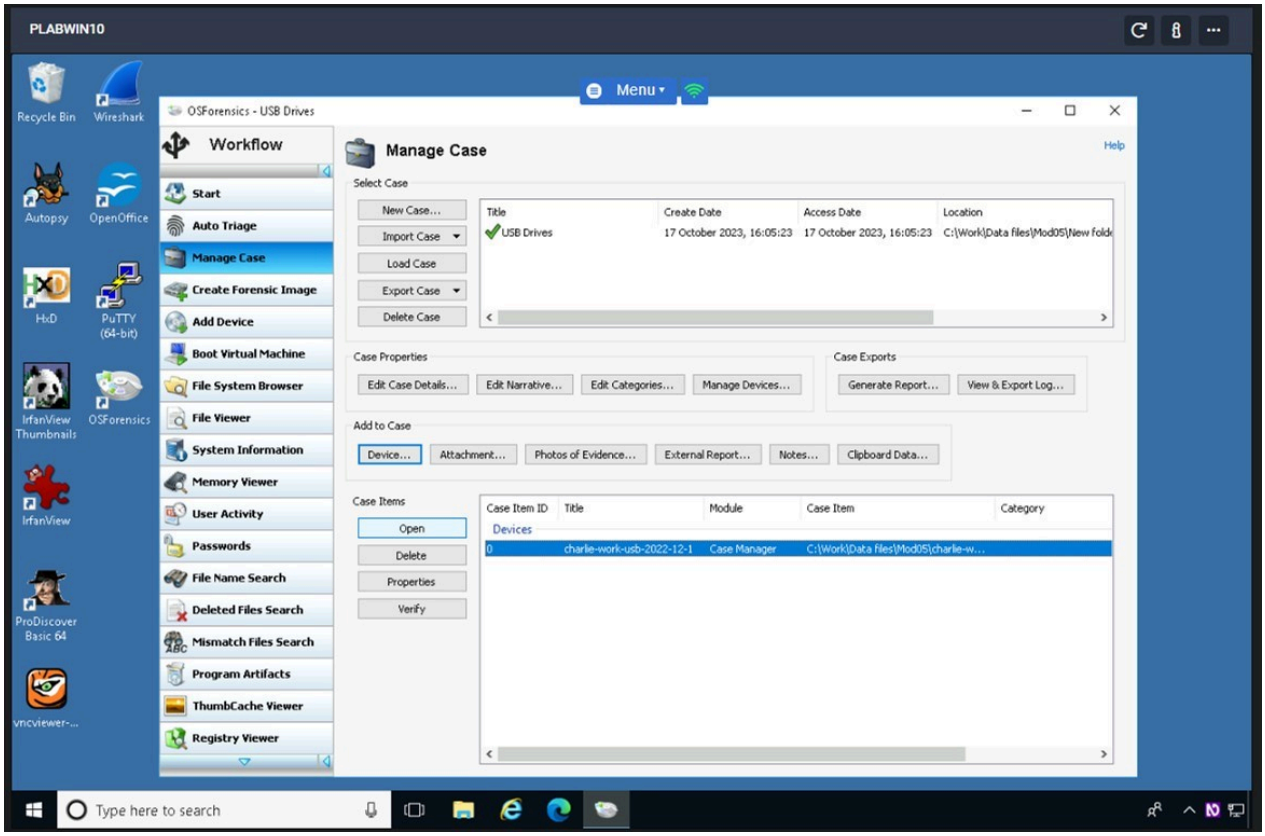
Step 12

In the Add Device window, click **OK**.



Step 13

Click the **charlie-work-usb-2022-12-11.E01** filename in the bottom pane on the right, and then click the **Open** button to the left.

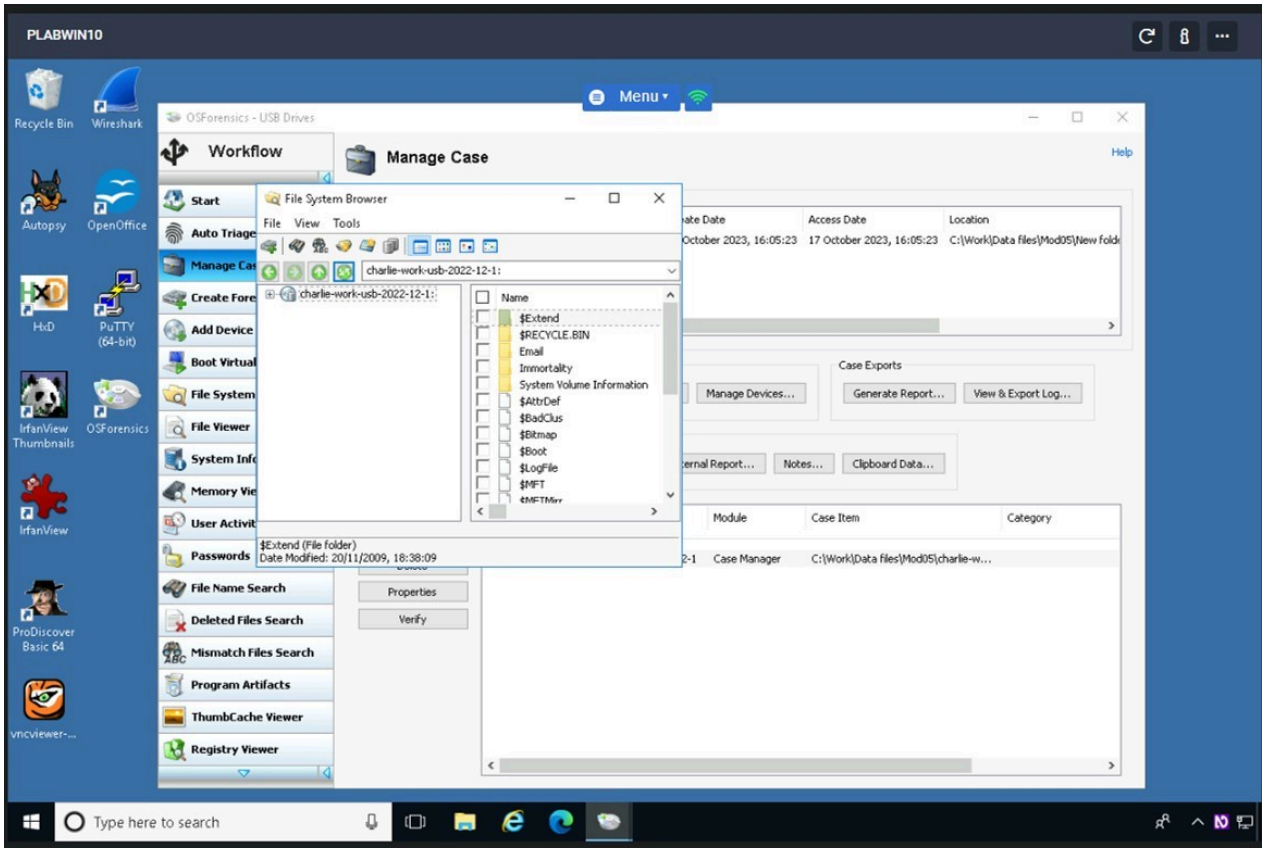


Step 14

The **File System Browser** window displays the files on a USB drive.

This window is fairly easy to use as a tool to search for specific files.

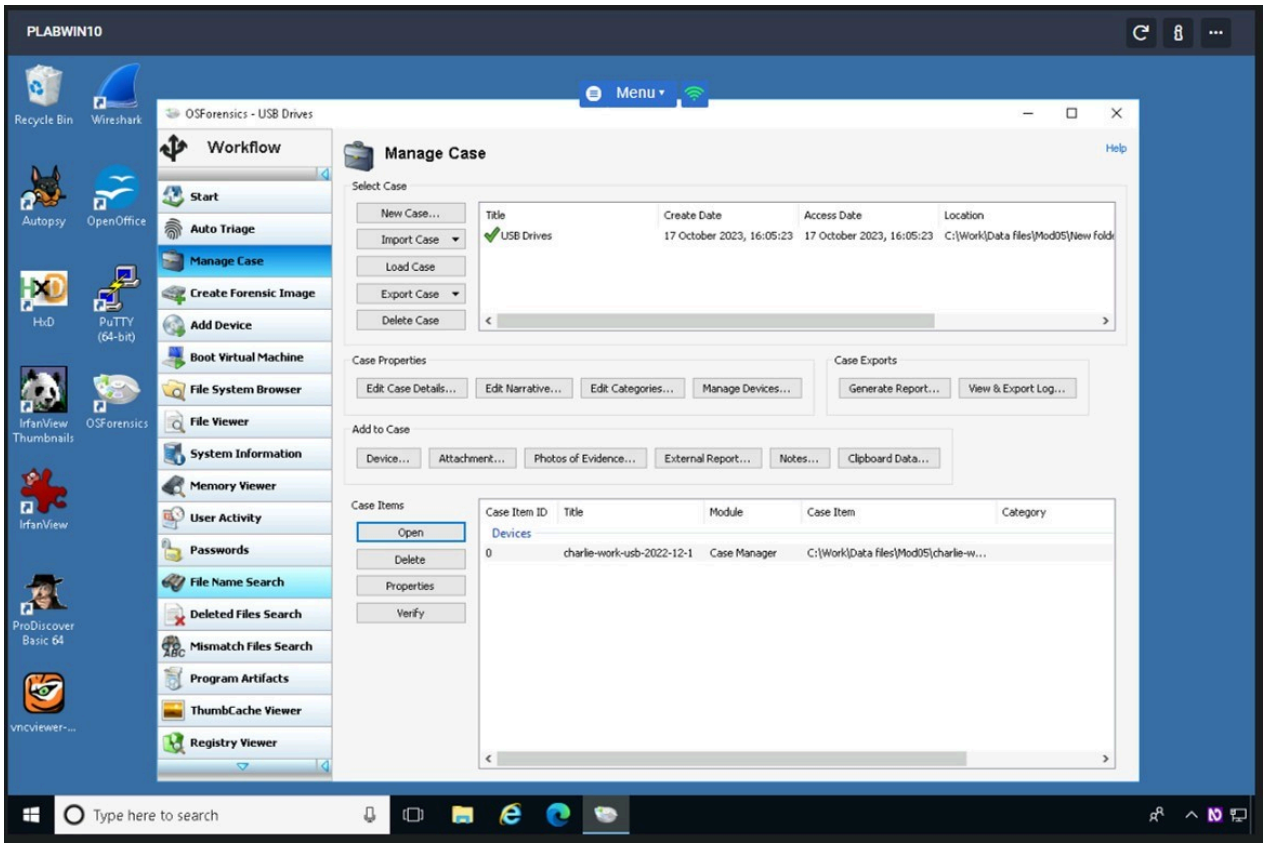
Close the window.



Step 15

You are back on the **OSForensics - USB drives - Manage Case** window.

Click the **File Name Search** button in the left pane of the main window.

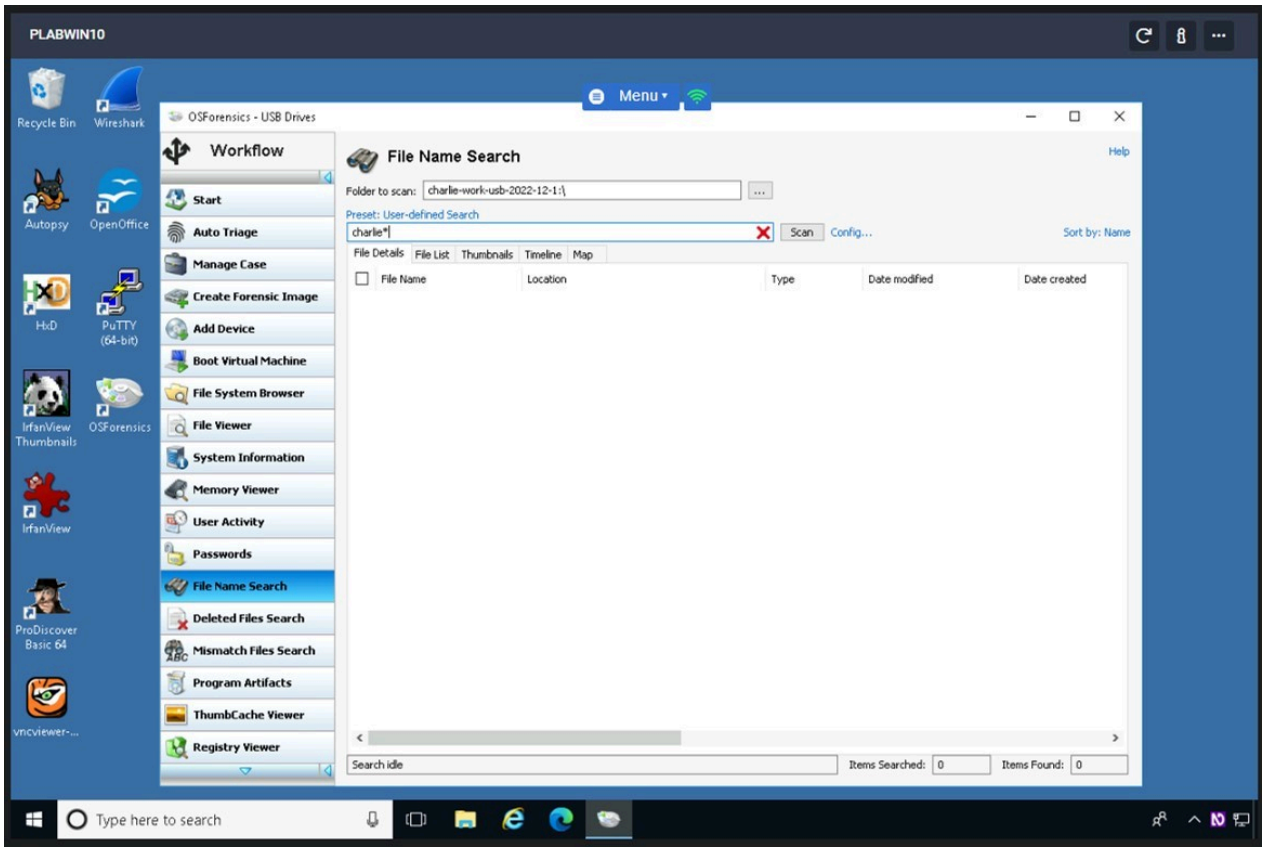


Step 16

In the **Search Pattern** text box, type:

```
charlie*
```

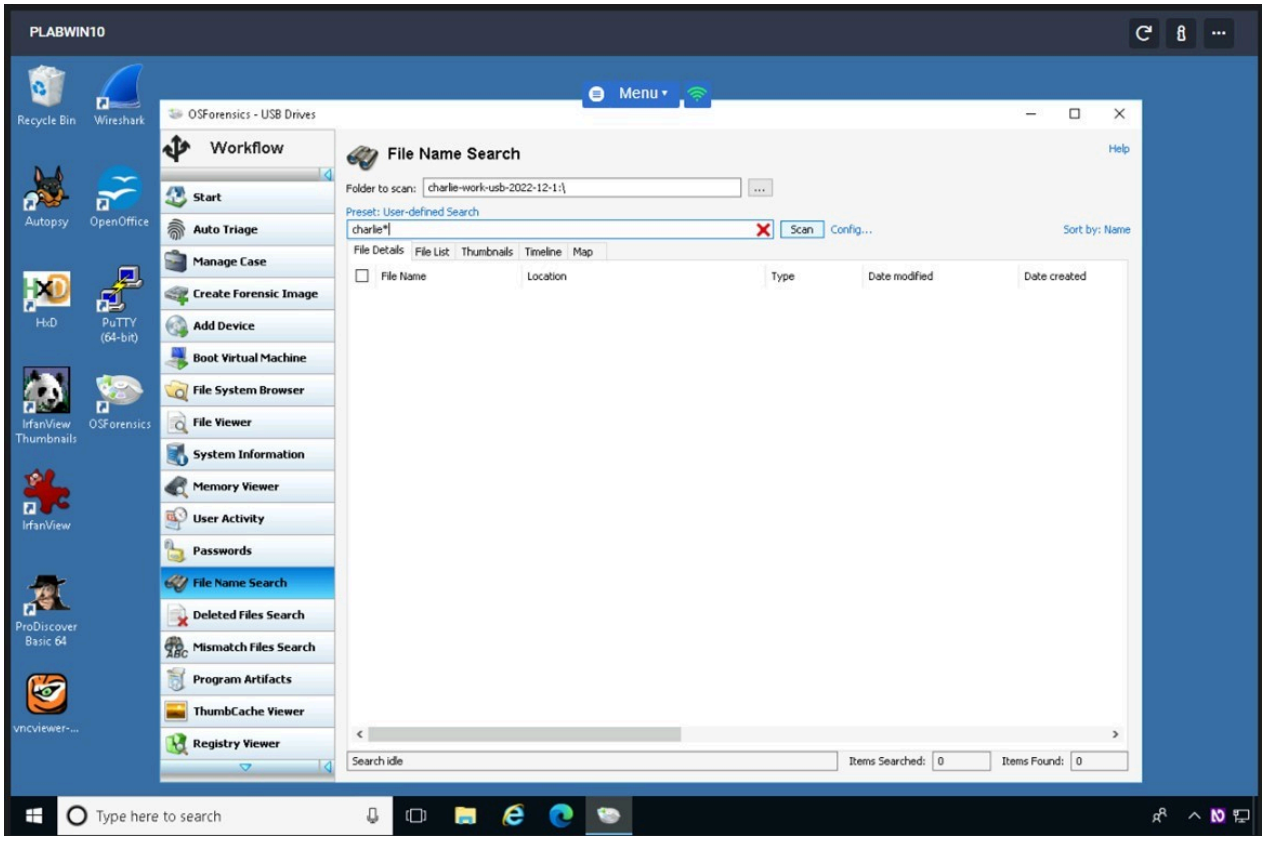
Beside the **Start Folder** field, click [...].



Step 17

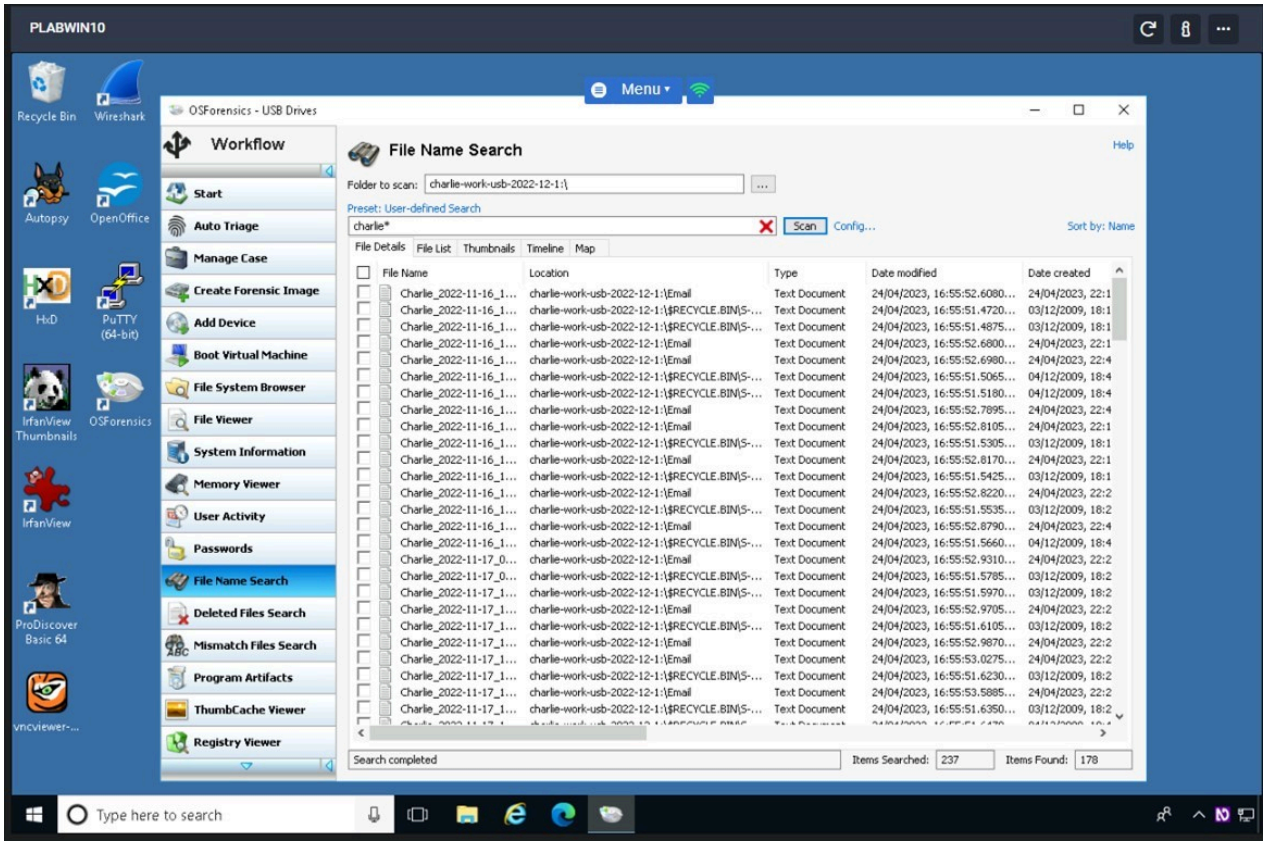
Make sure the **Folder** to scan box contains **charlie-work-usb-2022-12-1**:\.

Click **Scan**.



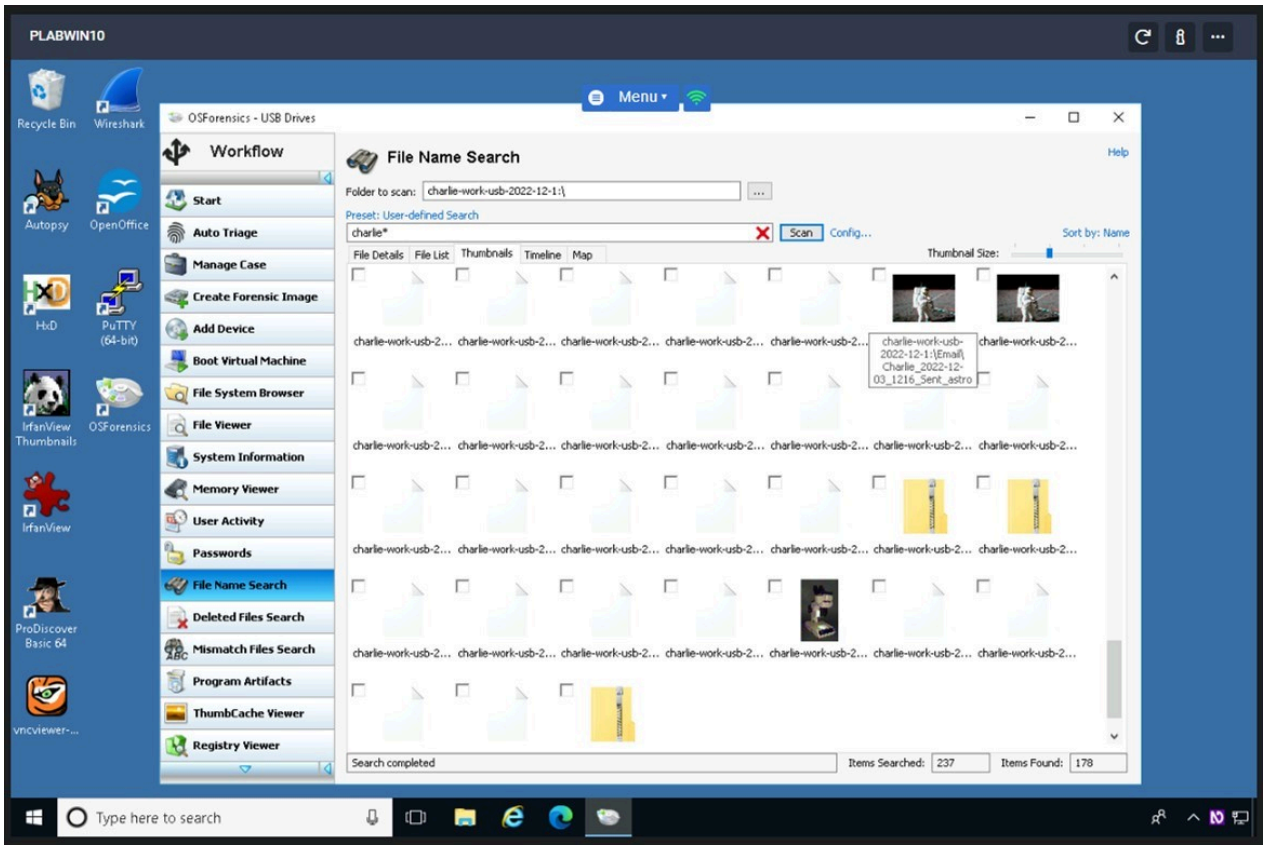
Step 18

After a few moments, a list of files found in Charlie's USB drive is displayed.



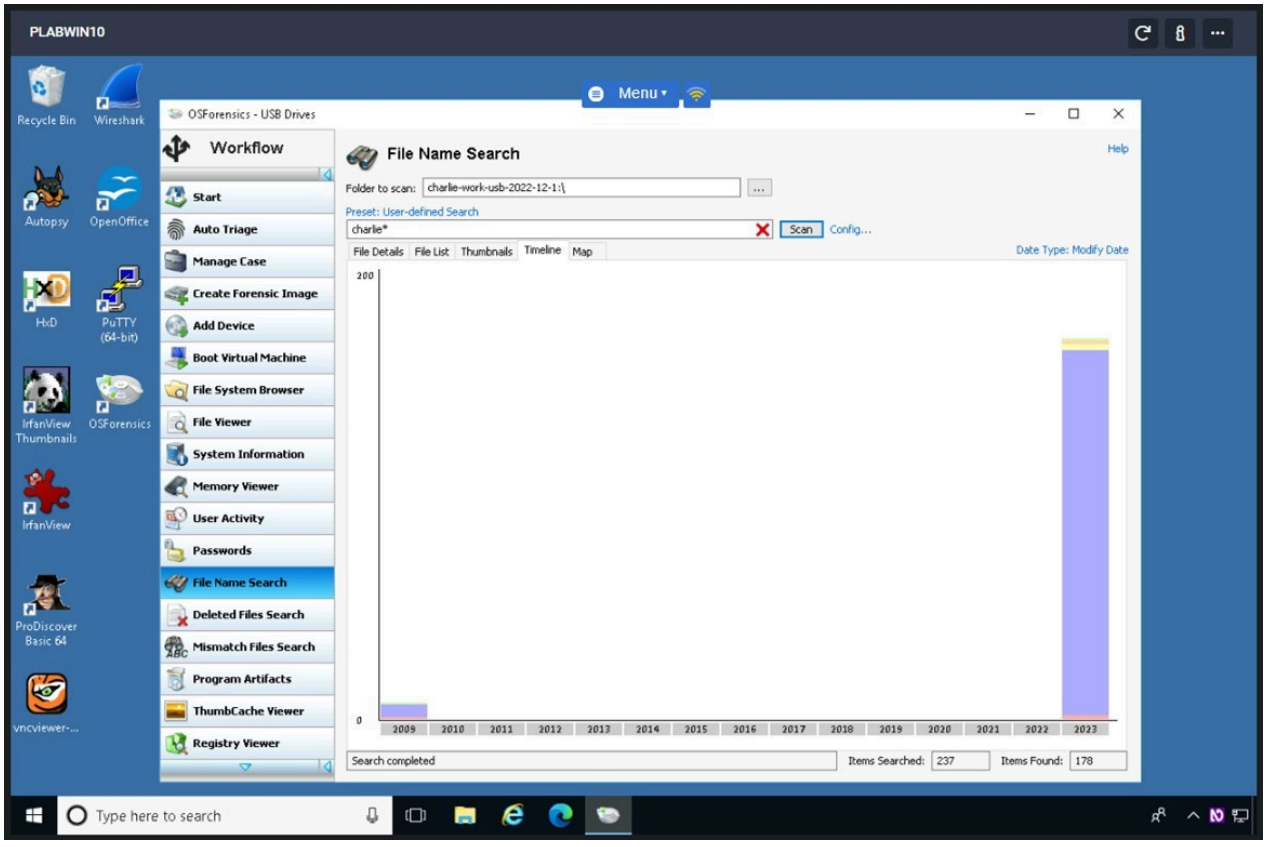
Step 19

You can use the tabs at the top of the search results to see the **Thumbnails** of files on the device. **Click** the **Thumbnails** tab. The files are displayed in the Thumbnails view.



Step 20

Click the **Timeline** tab. A timeline of the items is displayed.



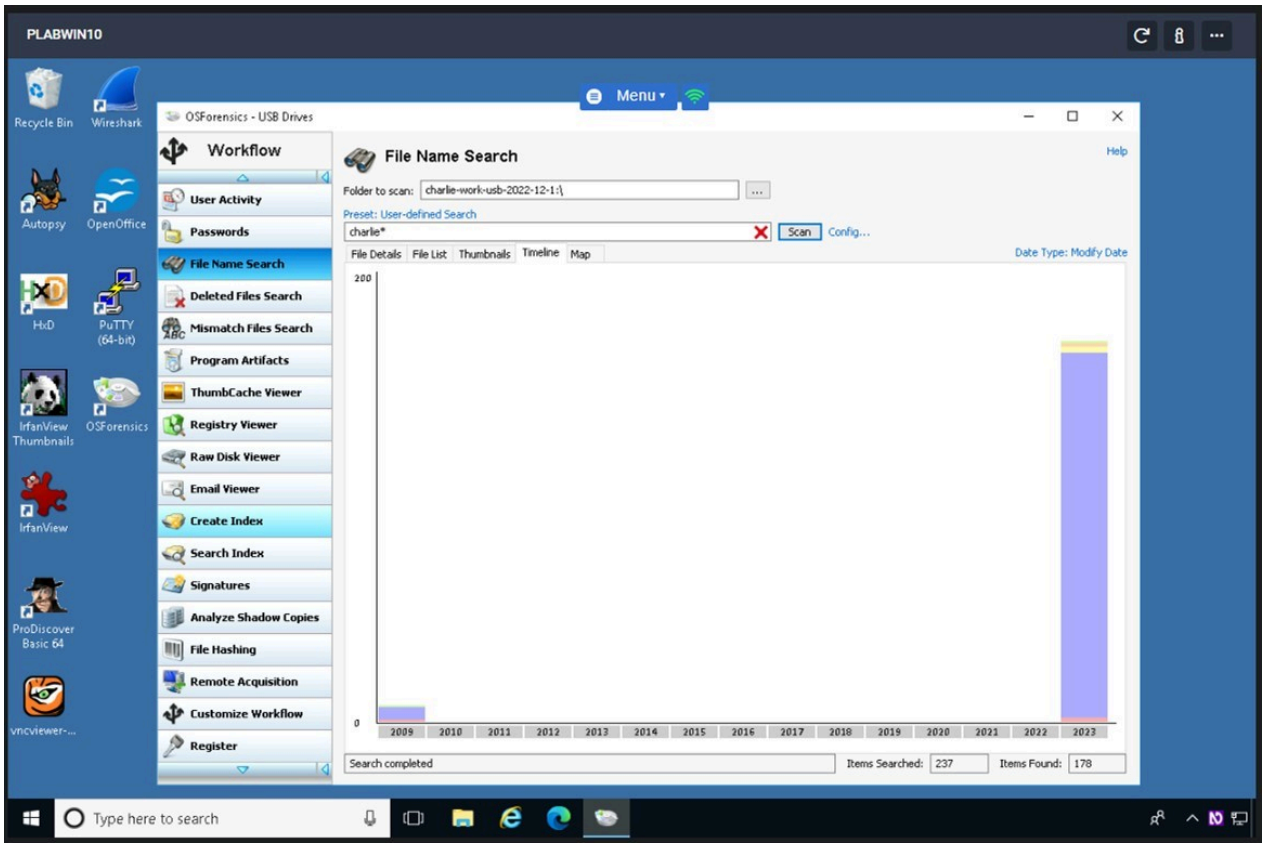
Task 2 - Create Index

To create an index of files found in the user's USB drive image, perform the following steps:

Step 1

On the **PLABWIN10** device, make sure the **OSForensics -USB drives** window is open.

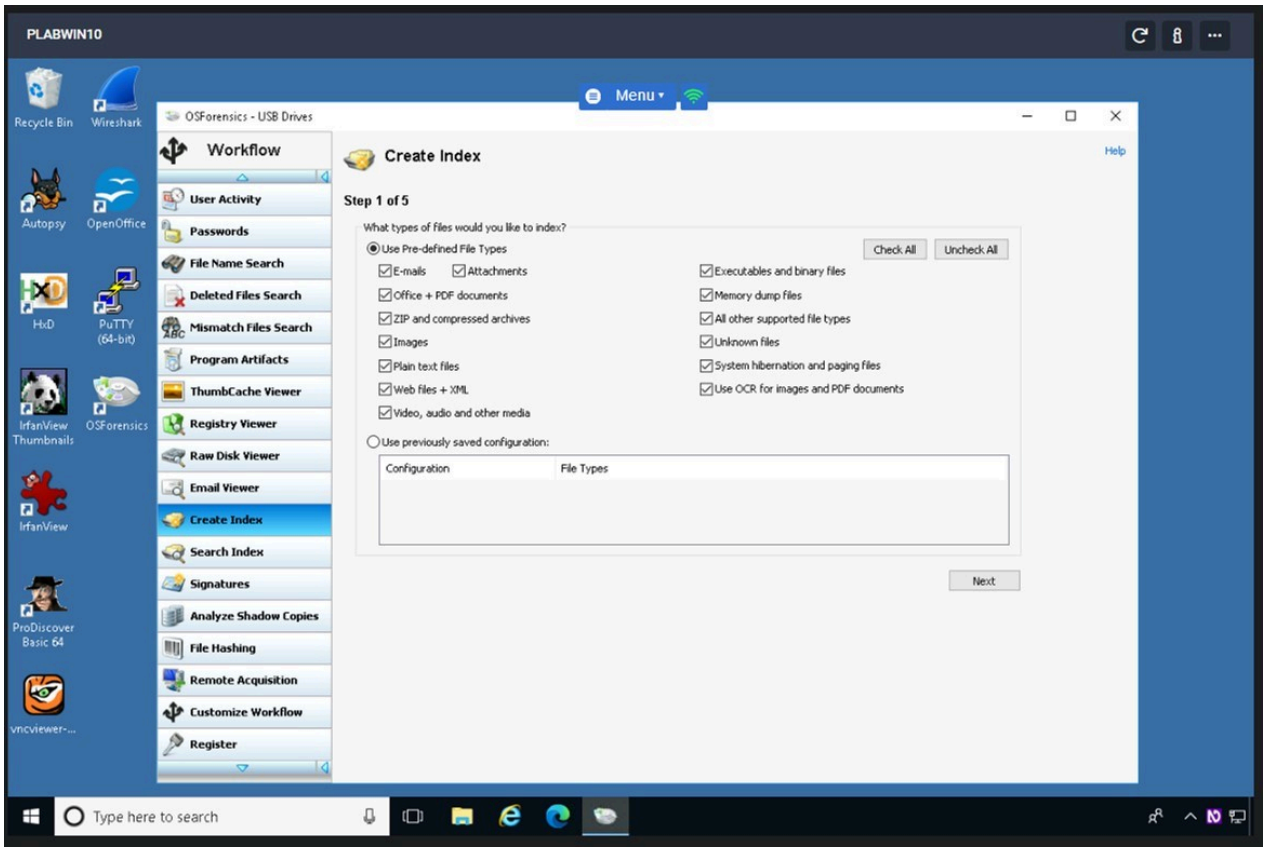
Next, click the **Create Index** button in the left pane to start the **Create Index Wizard**.



Step 2

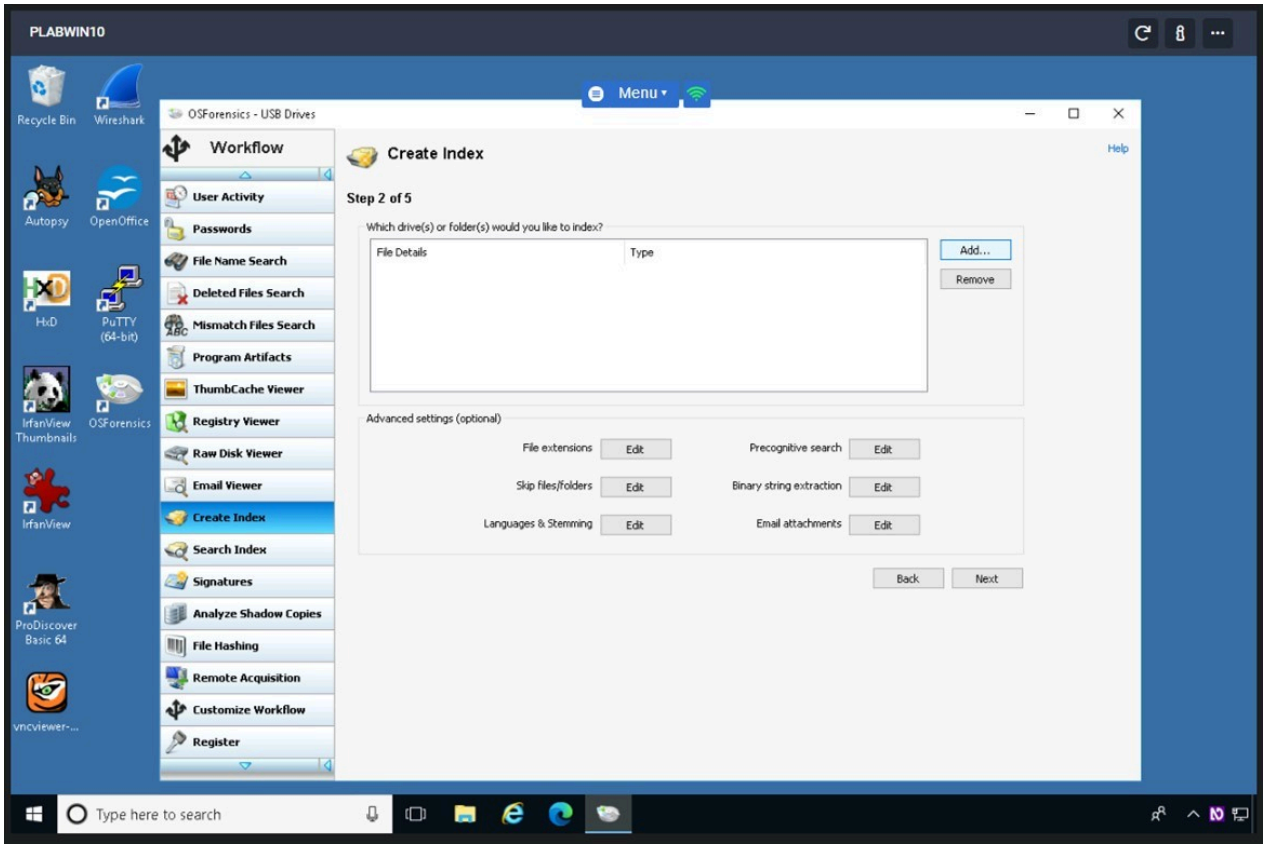
In the **Create Index Step 1 of 5** window, click the **Use Pre-defined File Types** option button, if necessary.

Click all the file types listed and then click **Next**.



Step 3

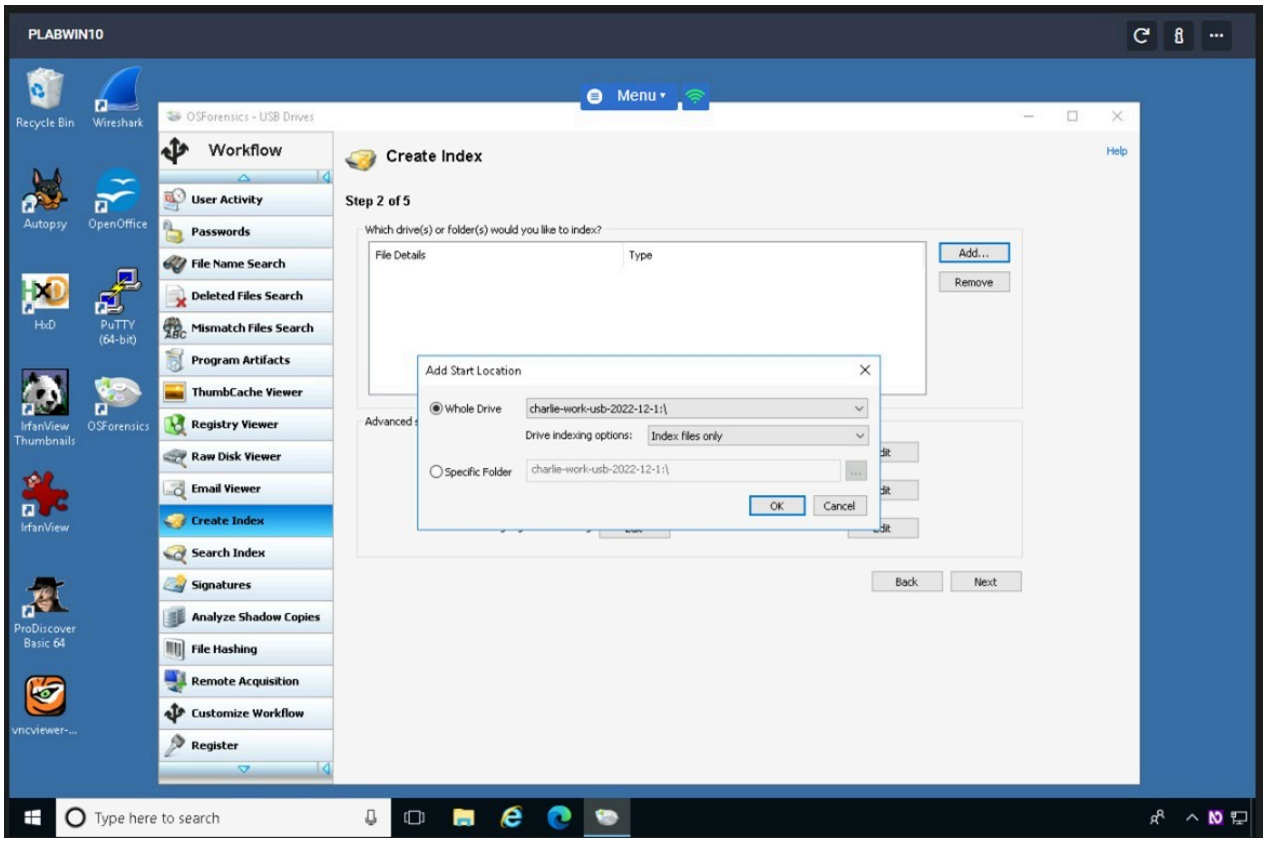
In the **Step 2 of 5** window, click the **Add** button.



Step 4

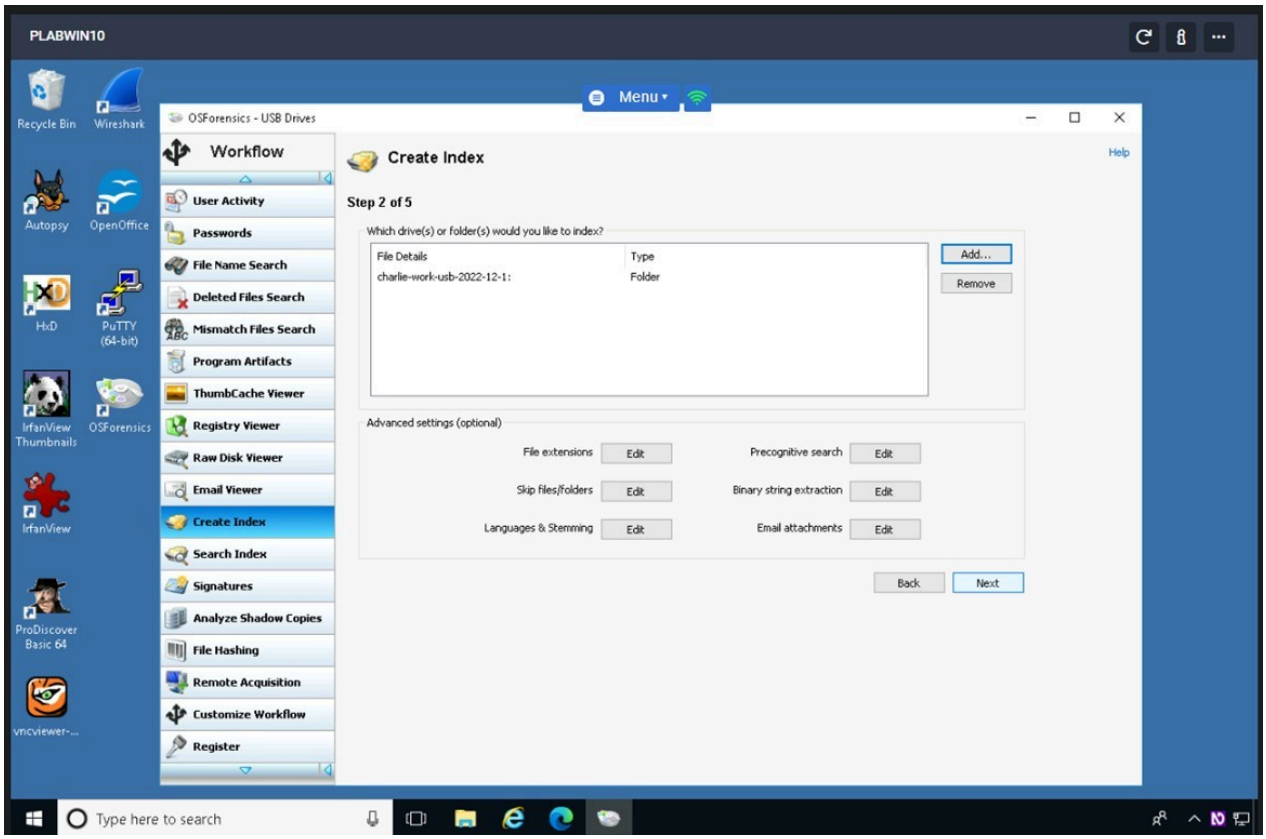
On the **Add Start Location** dialog box, verify that the **Whole Drive** option is selected and **charlie-work-usb-2022-12-1:** is listed.

Click **OK**.



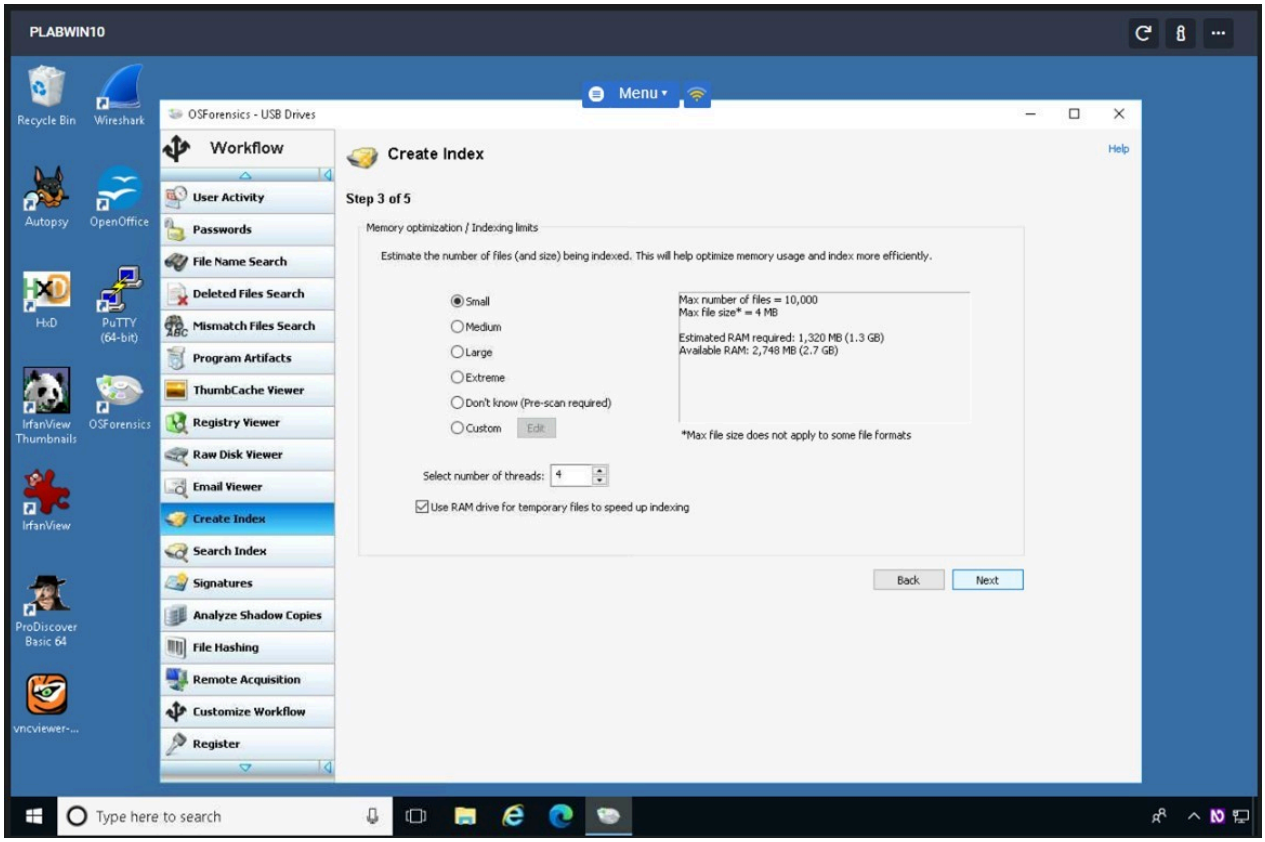
Step 5

Back on **Step 2 of 5** page, click **Next**.



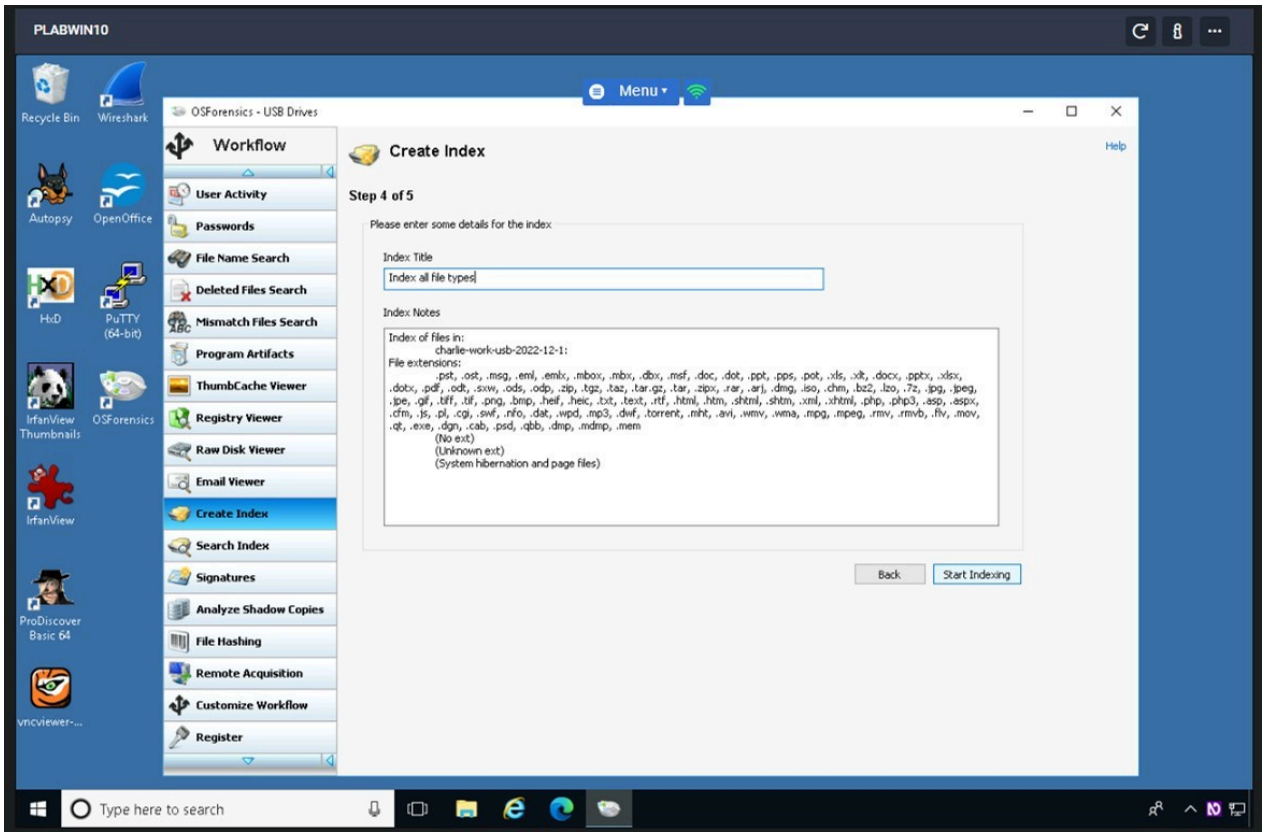
Step 6

In the **Step 3 of 5** window, choose **Small** for the Estimated number of files, and then click **Next.**

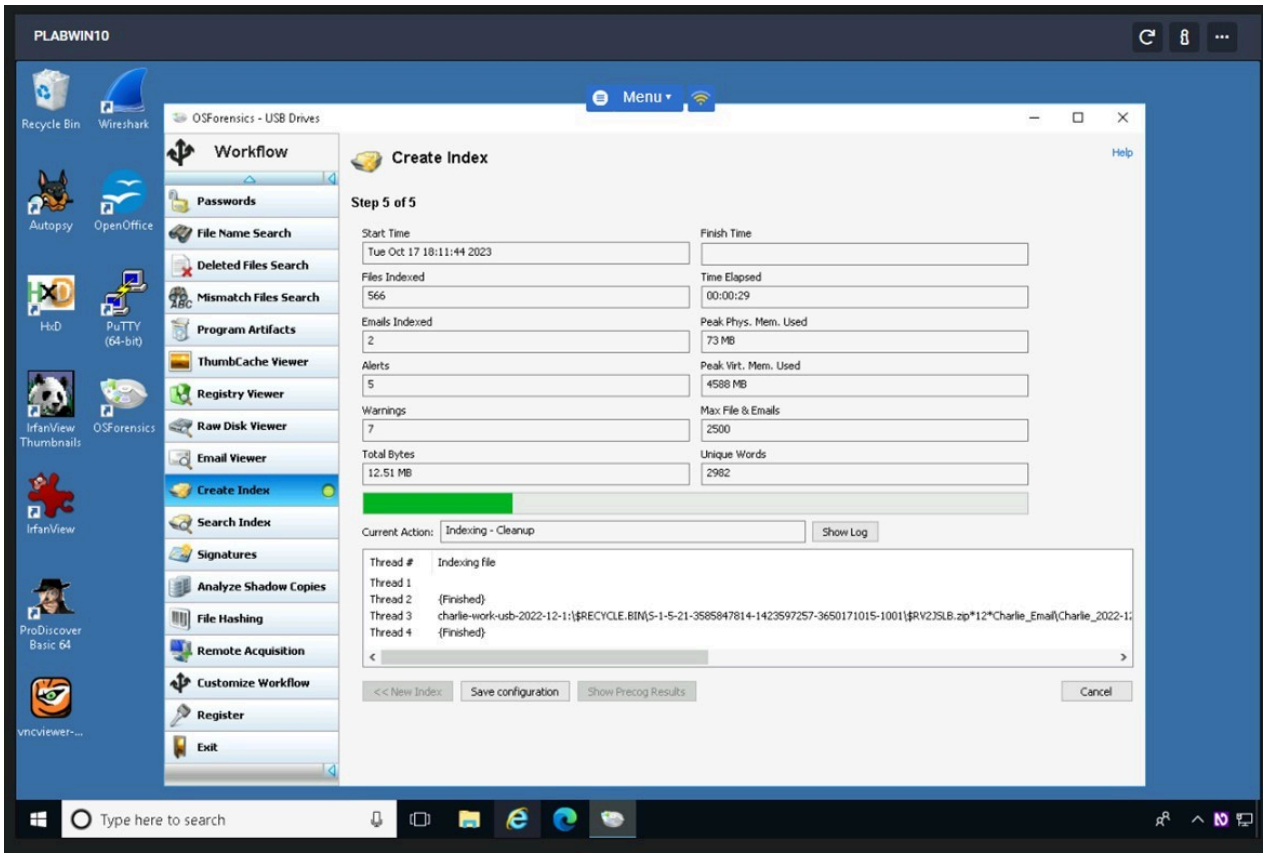


Step 7

The **Step 4 of 5** window, change the **Index Title** to Index all file types, and then click **Start Indexing**.

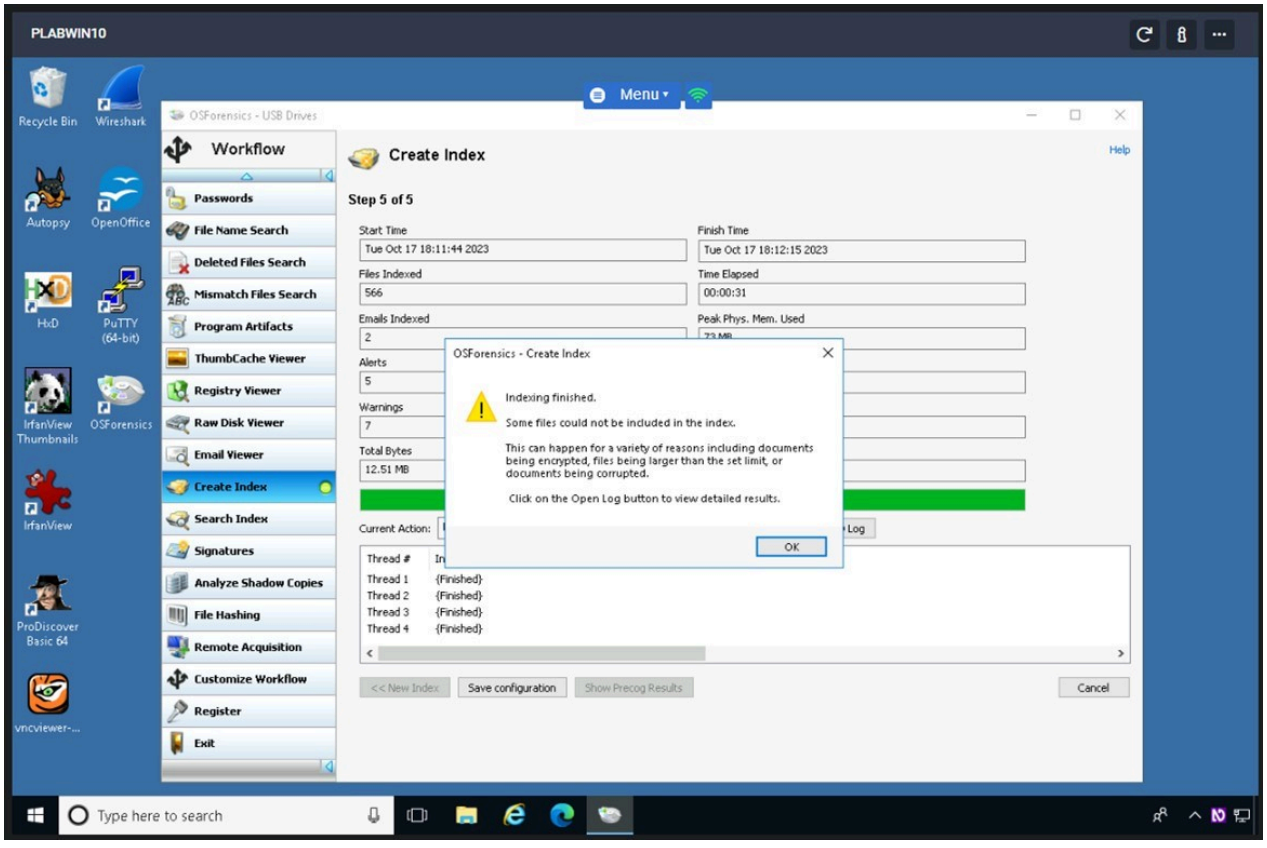


Step 5 of 5 window shows the files being processed for indexing.



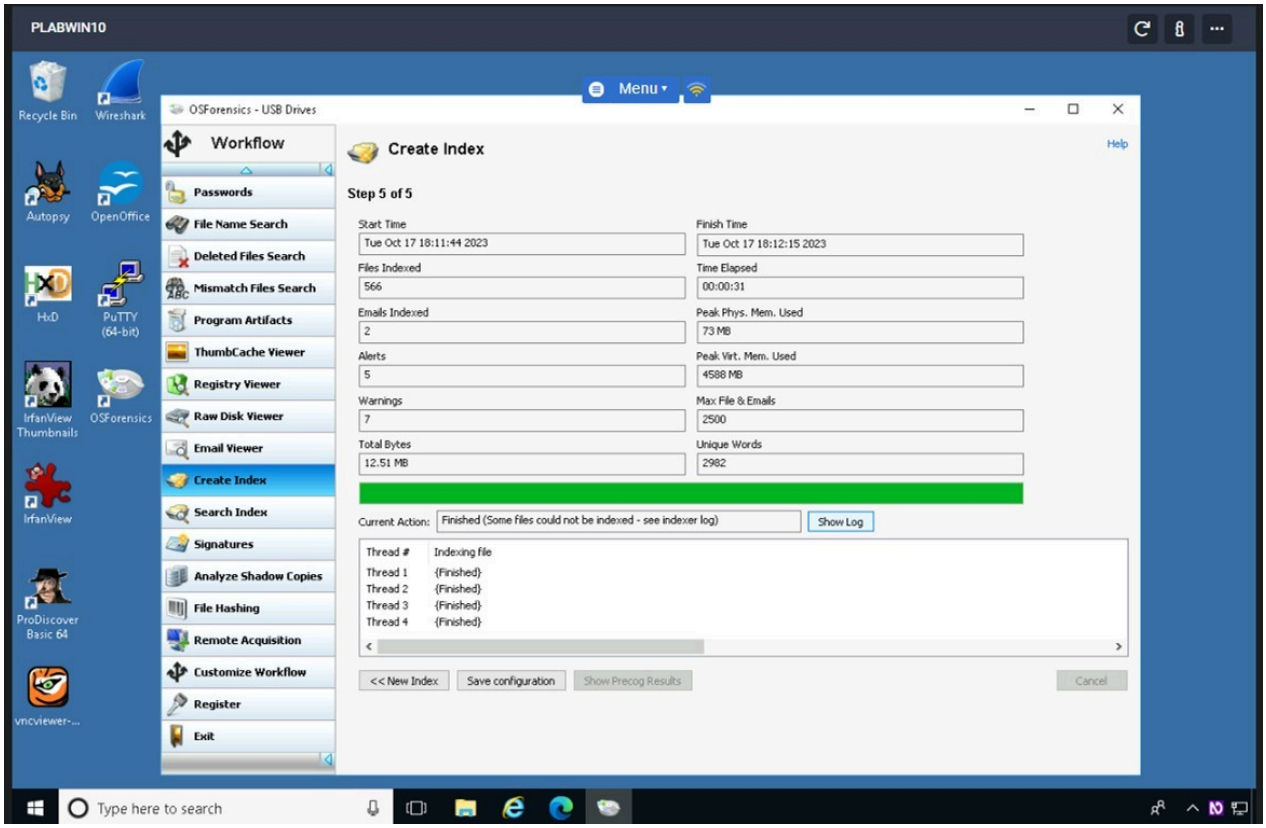
Step 8

When the indexing is finished, if necessary, click **OK** in the message box informing you that some files cannot be included in the index.



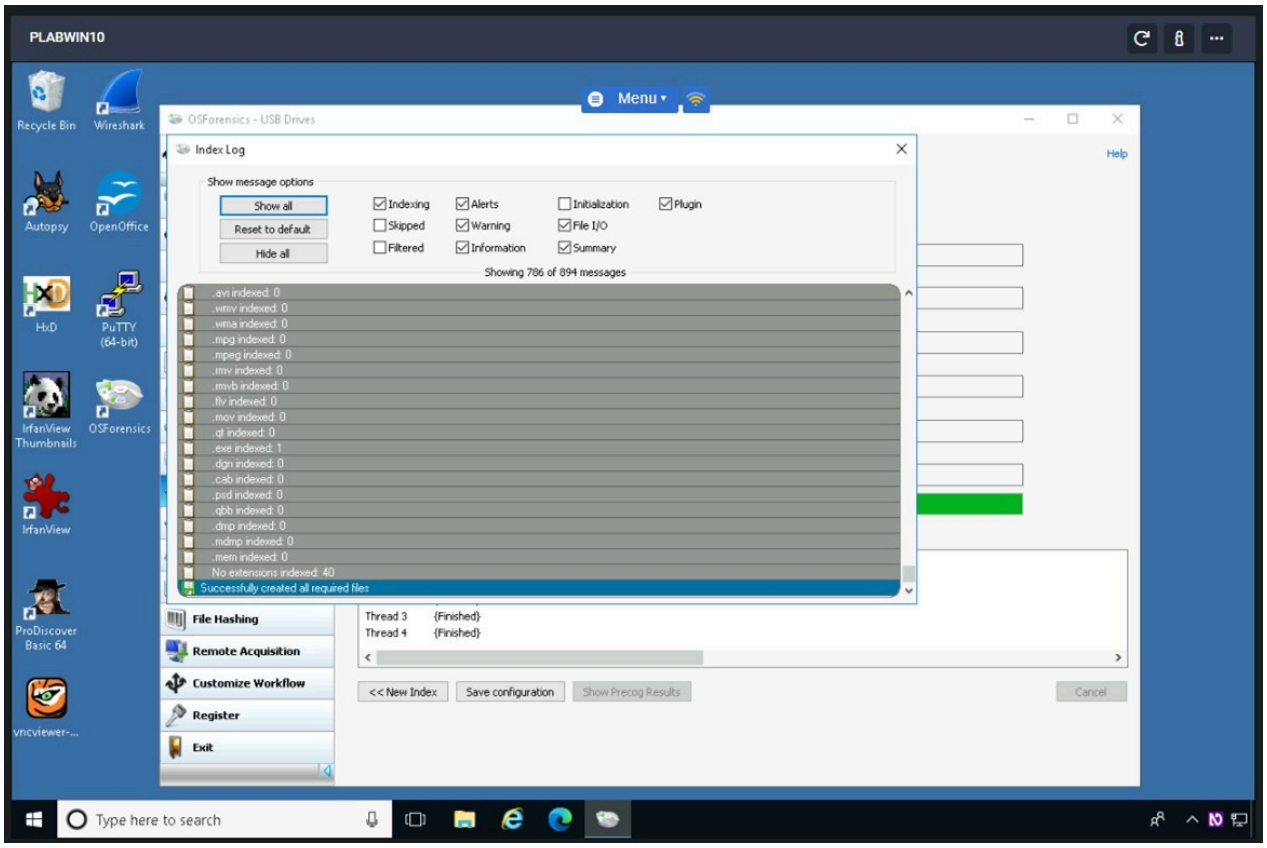
Step 9

Click the **Show Log** button just below the green progress bar in the **Step 5 of 5** window.



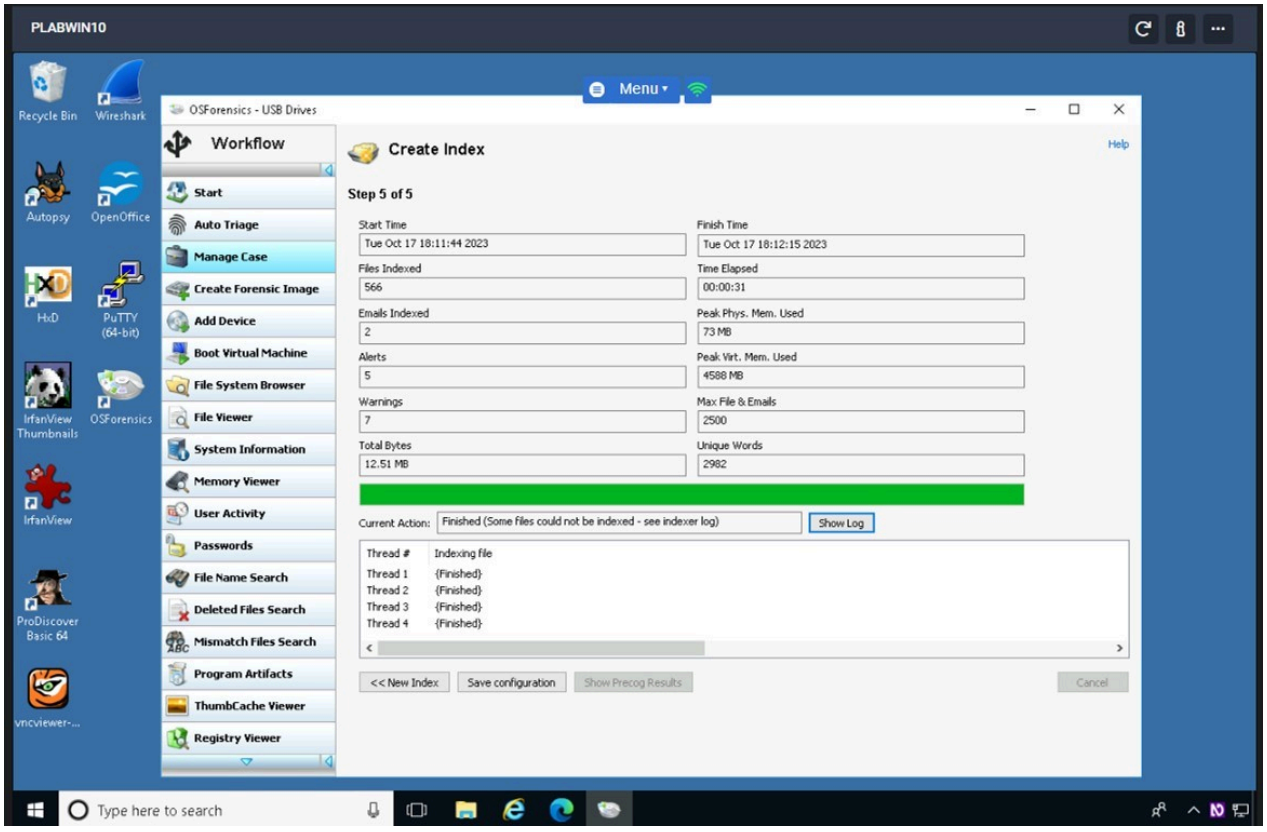
Step 10

The window that opens shows you the files that were indexed, any errors that occurred, and a summary of what was done. After examining the summary, close the window.



Step 11

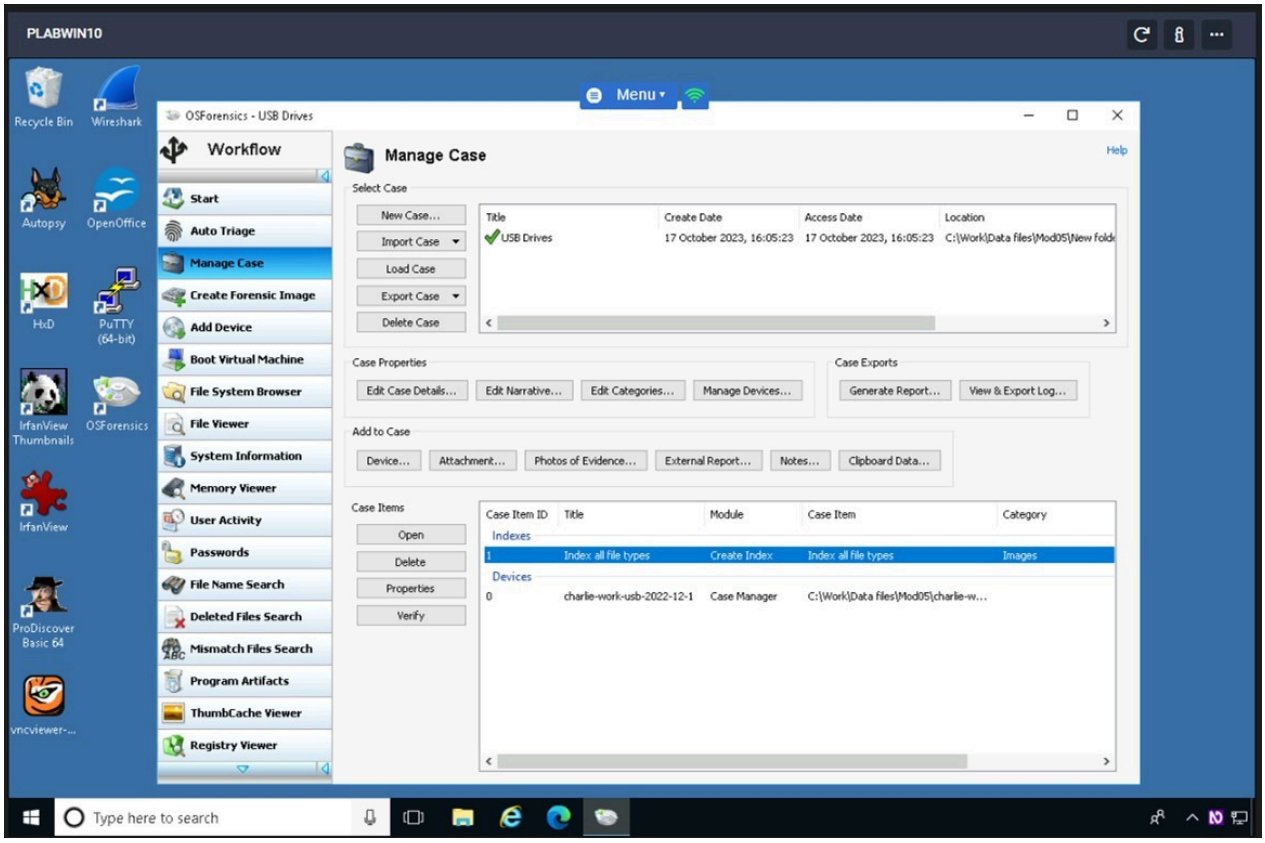
Back on the **Create Index, Step 5 of 5** window, click the **Manage Case** button in the left pane.



Step 12

Notice that the index is now listed in the bottom pane on the right. Scroll to the bottom of the left pane and click the **Close [X]** button.

This activity has given you a chance to see how indexing is done in the OSForensics tool you use throughout the book. You should now be able to create a case, add it to your inventory, scan the files, and perform indexing, which will be useful later for searching.



Screenshot

1 of 9

Click the button to take a screenshot of PLABWIN10

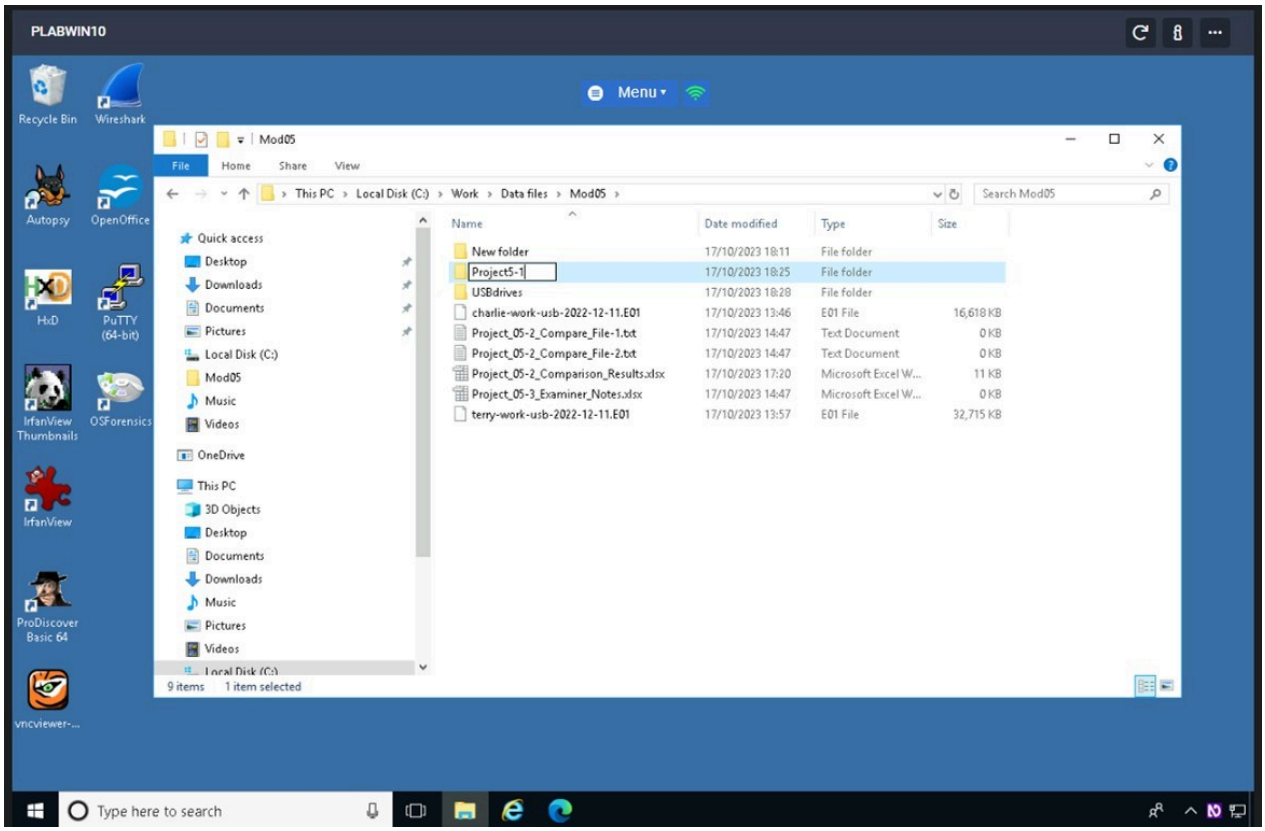
Leave the devices you have powered on in their current state and proceed to the next exercise.

Hands-On Project 5-1

The data for this module came from the M57 Patents case, which is a hypothetical case created for new investigators to practice on real data. In this project, you examine the USB drive of Terry, the IT person. Your job is to ascertain whether Terry is involved in anything illicit or against company policy.

Step 1

Open **File Explorer** and create a new folder called **Project5-1** in your **C:\Work\Data files\Mod05 folder**.



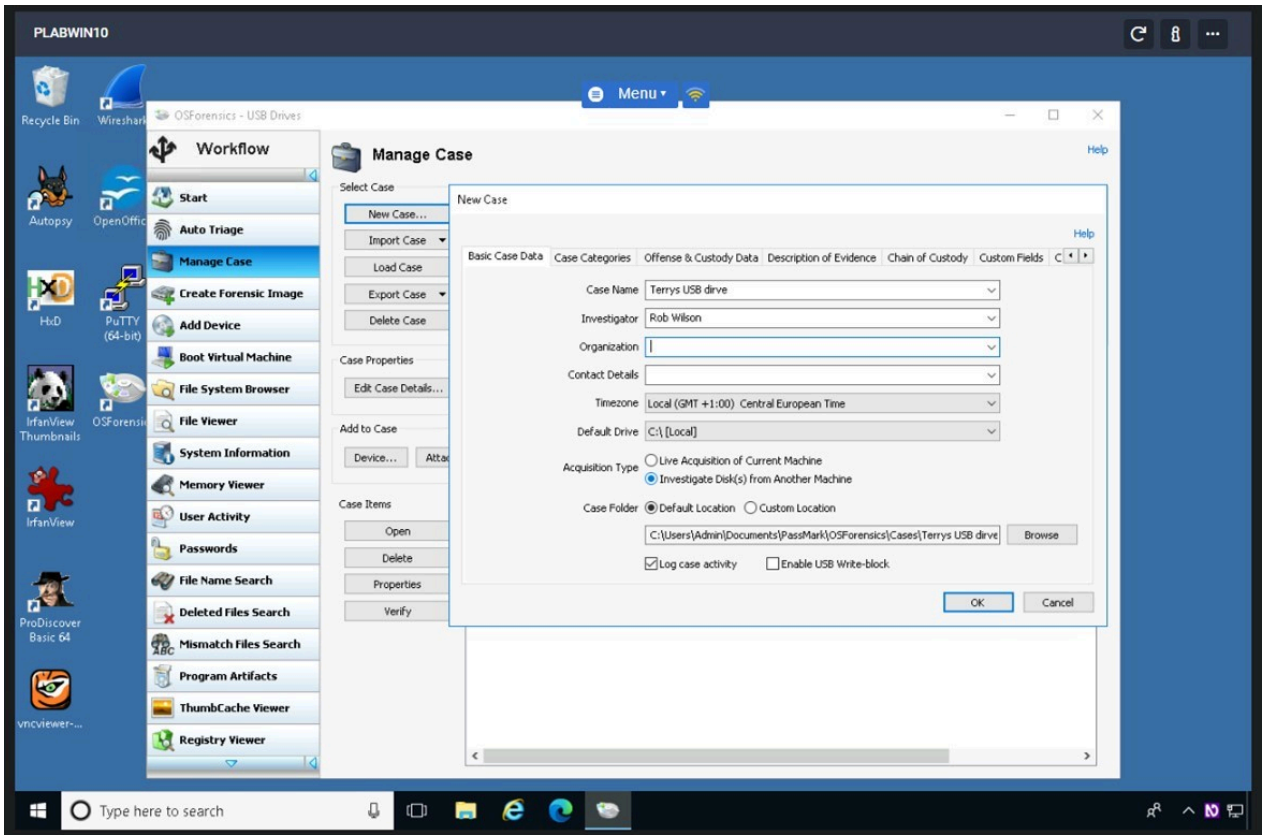
Start **OSForensics**. If prompted to allow the program to make changes to your computer, click **OK** or **Yes**. In the **OSForensics** message box, click **Continue Using Trial Version**.

Step 2

Click **Start** in the left pane if necessary. In the right pane, click **Create Case**.

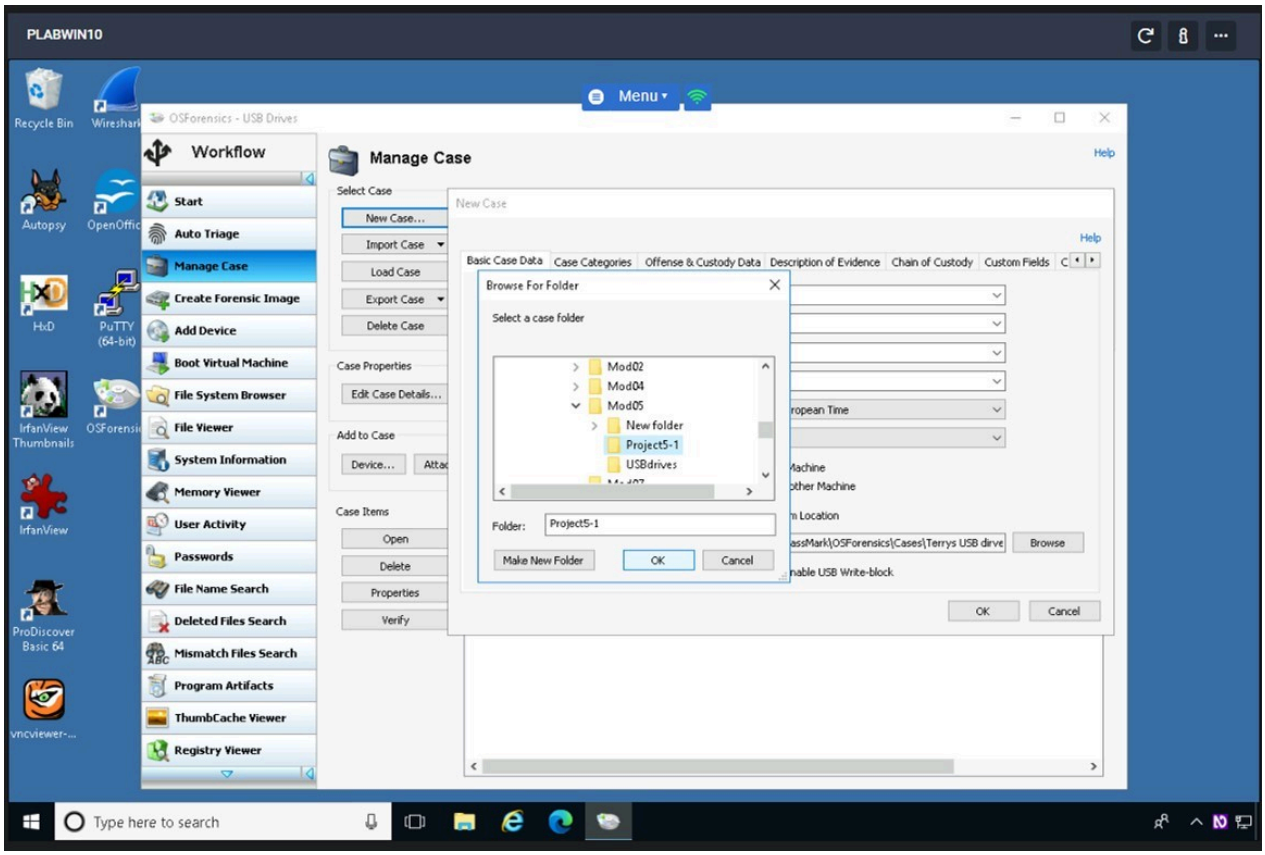
Step 3

In the New Case dialog box, enter your name in the Investigator text box. In the Case Name text box, type **Terrys USB drive**, and then click **Investigate Disk(s) from Another Machine**.

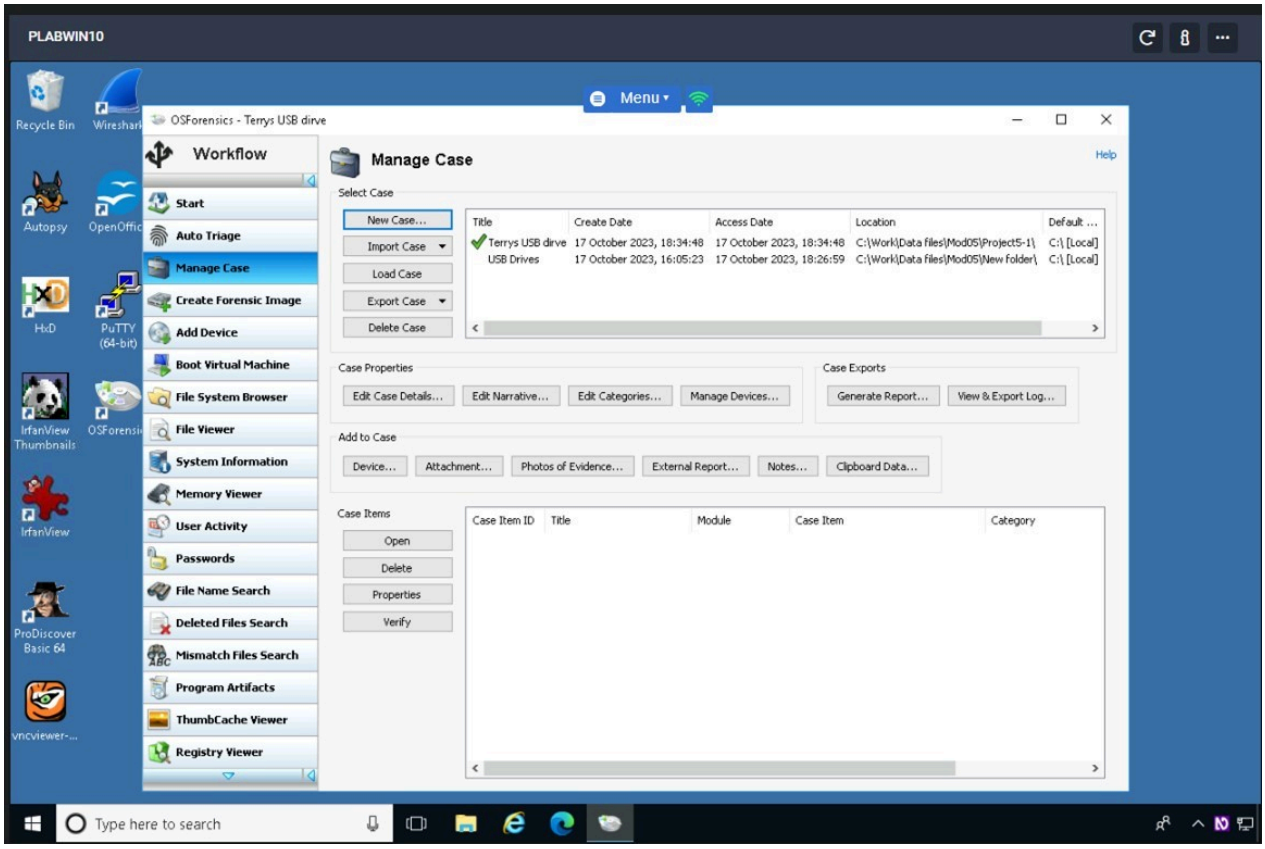


Step 4

Click **Custom Location** for the case folder. Click the **Browse** button on the lower right, navigate to and click your **Project5-1** folder, and then click **OK** twice.

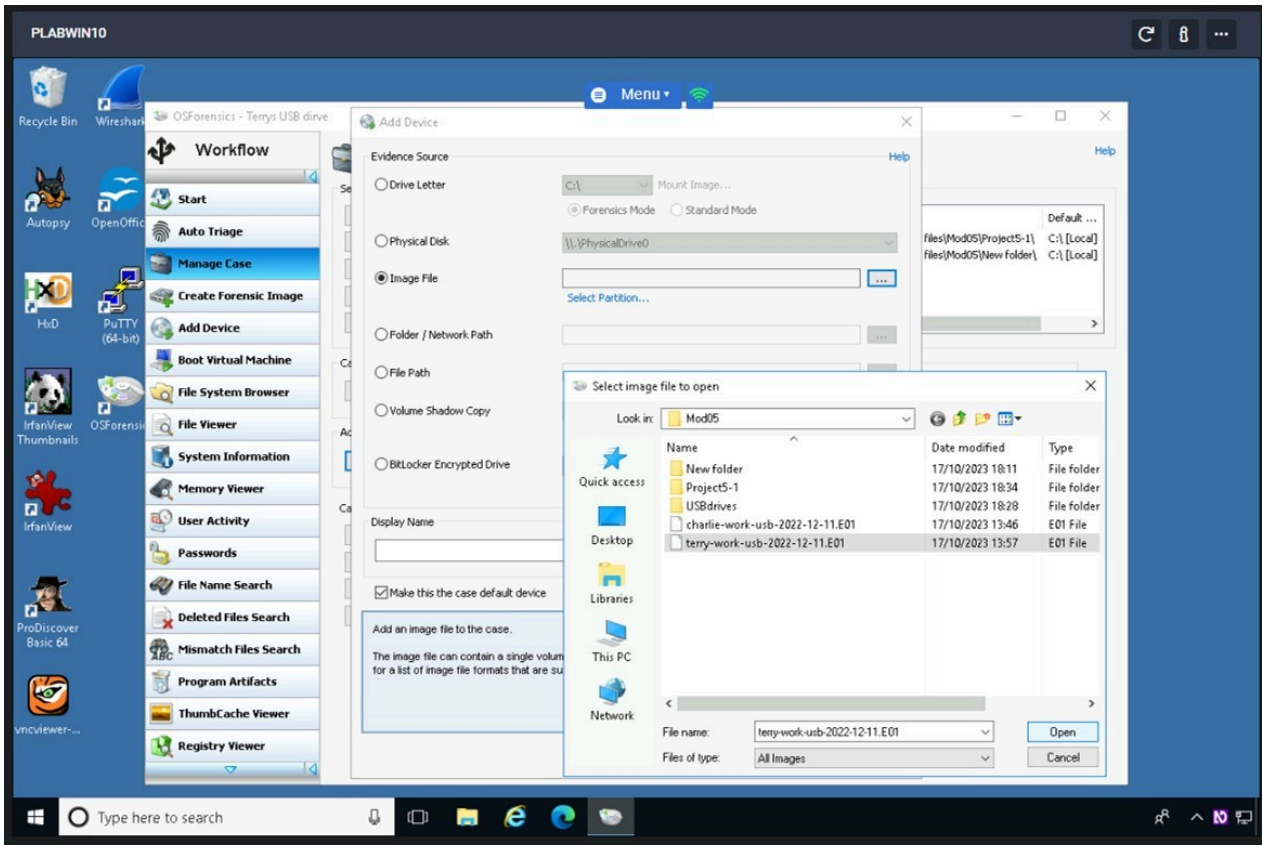


You should see the **Manage Case** window.



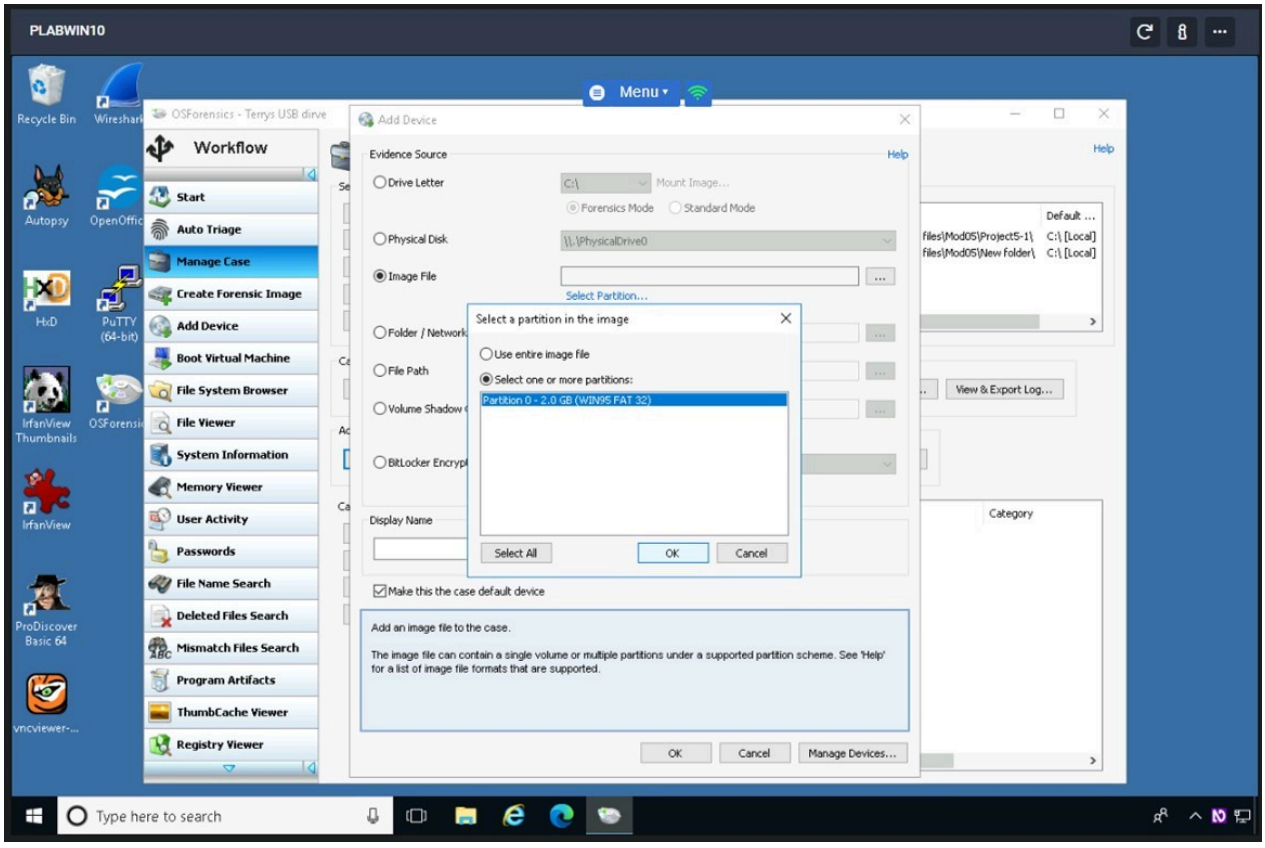
Step 5

Click the **Device** button in the **Add to case** section to open the "**Select device to add**" dialog box, and then click the **Image File** option button. Click the **Browse** button, navigate to the c:\work\datafiles\mod05 folder, and click **terry-work-usb-2022-12-11.E01**. Click **Open**.

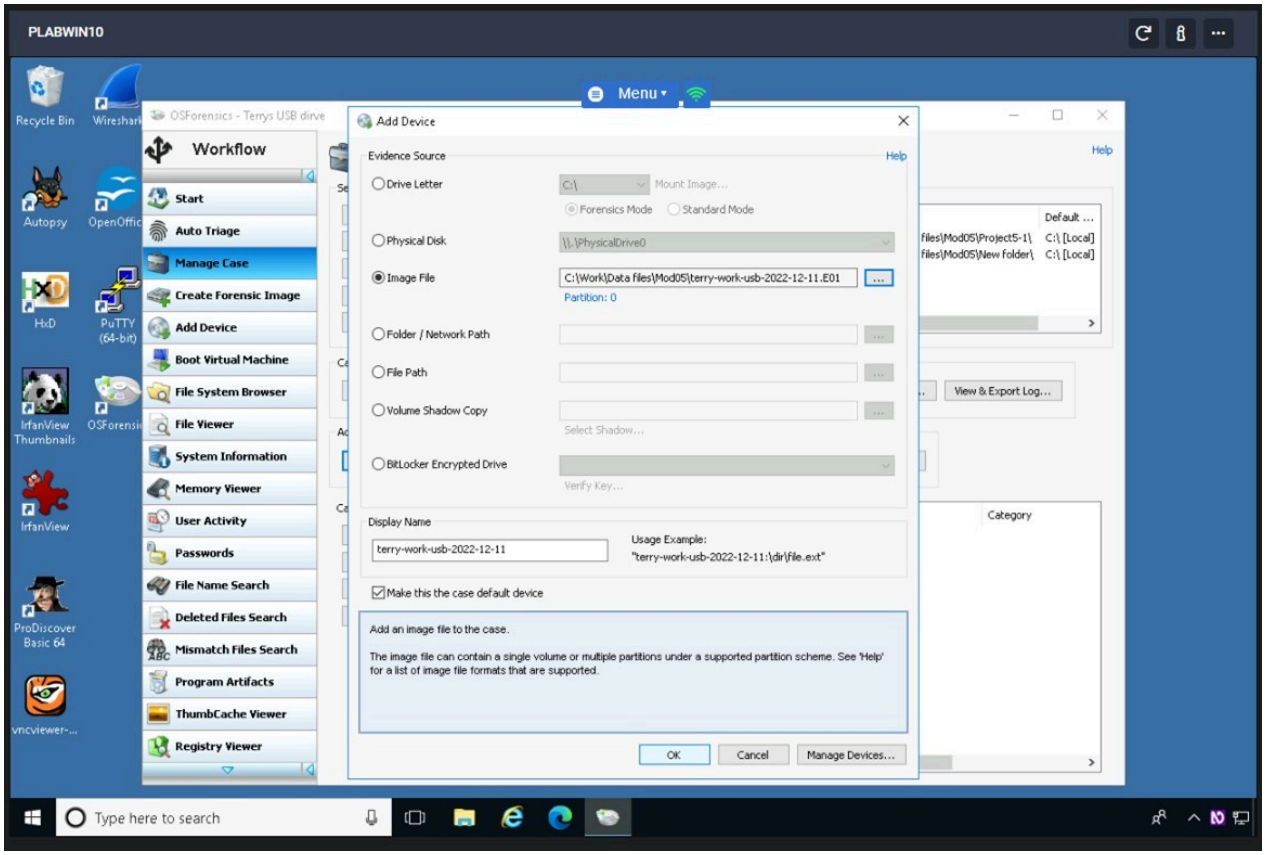


Step 6

In the message box asking which partition to use, leave the default setting Partition 0 - 2.0 GB (WIN95 FAT 32), and then click **OK**.

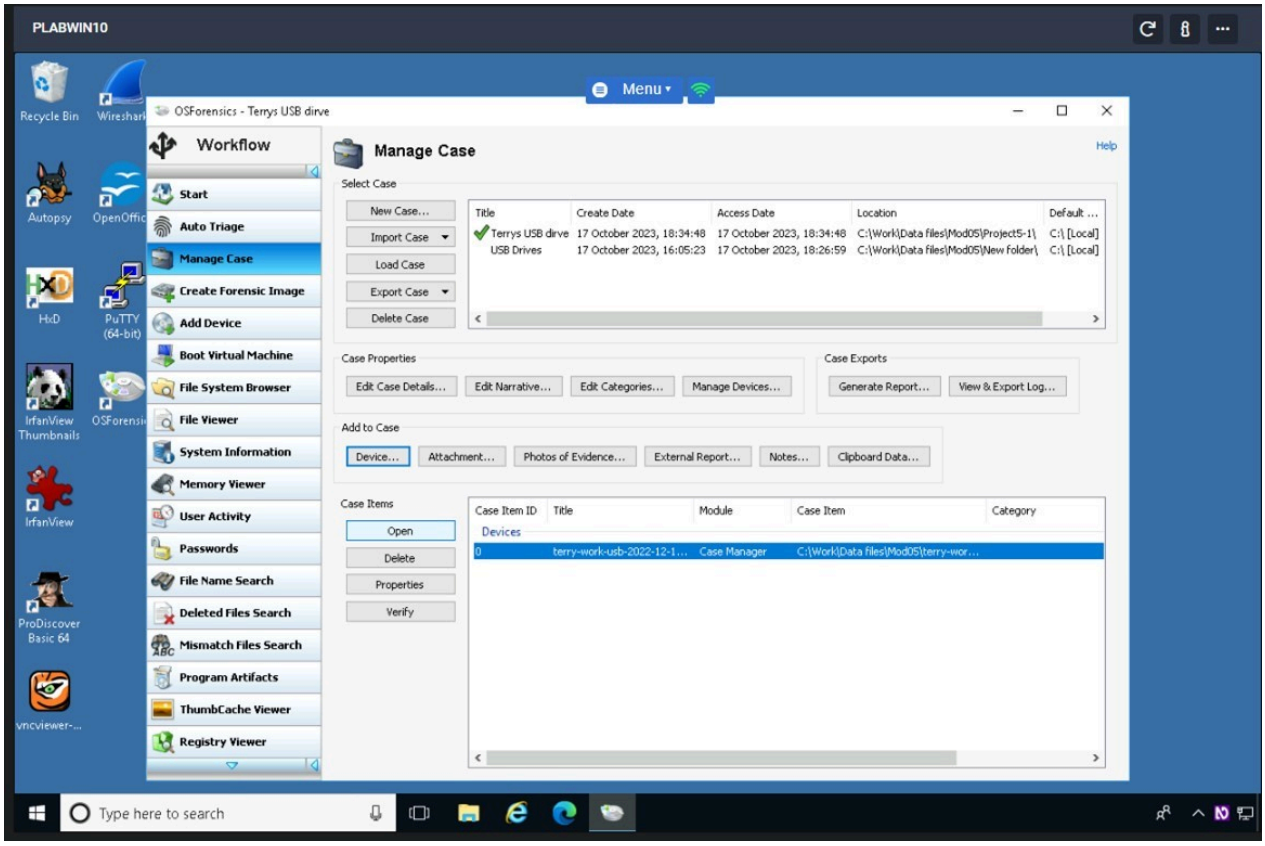


Click **OK** to close the “Add Device” dialog box.



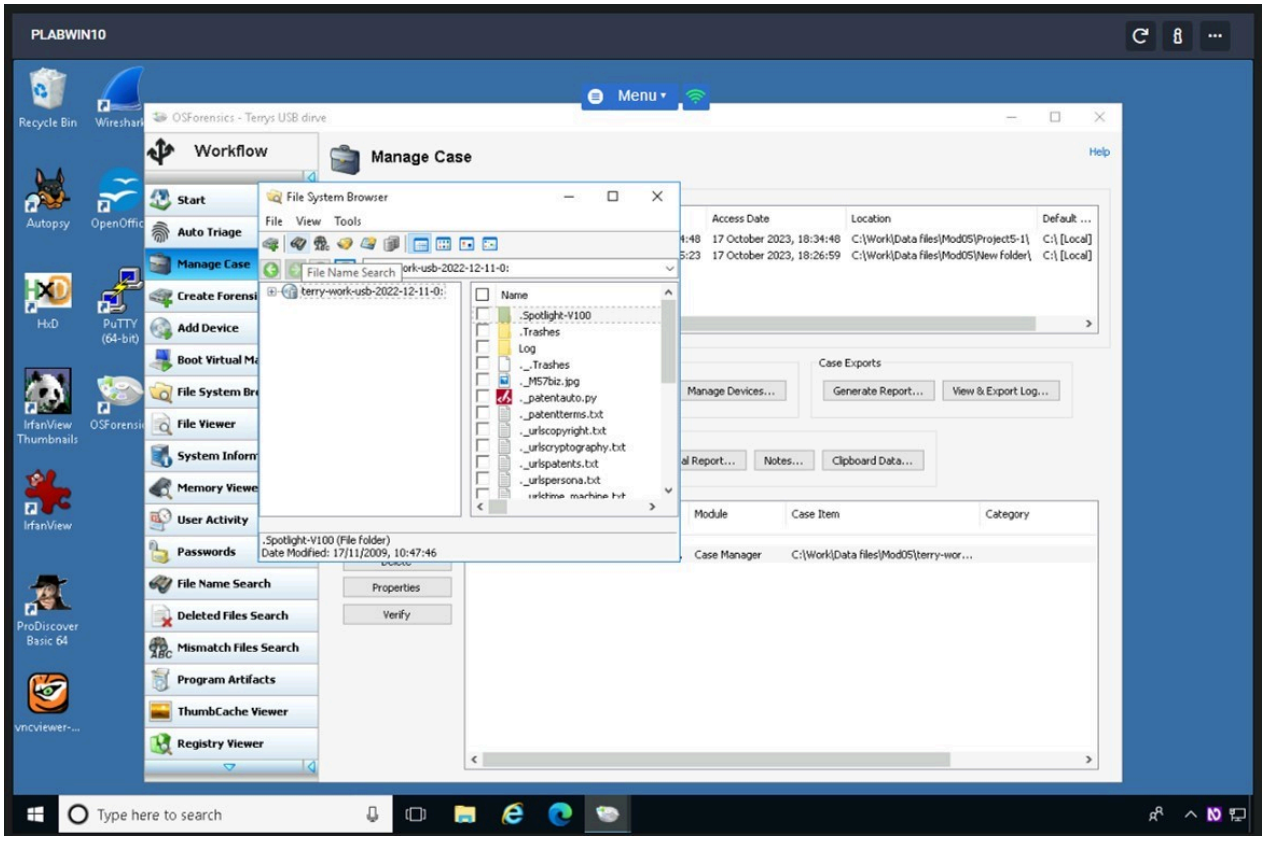
Step 7

Click the **terry-work-usb-2022-12-11.E01** filename at the lower right, and then click the **Open** button to the left to open the File System Browser window.

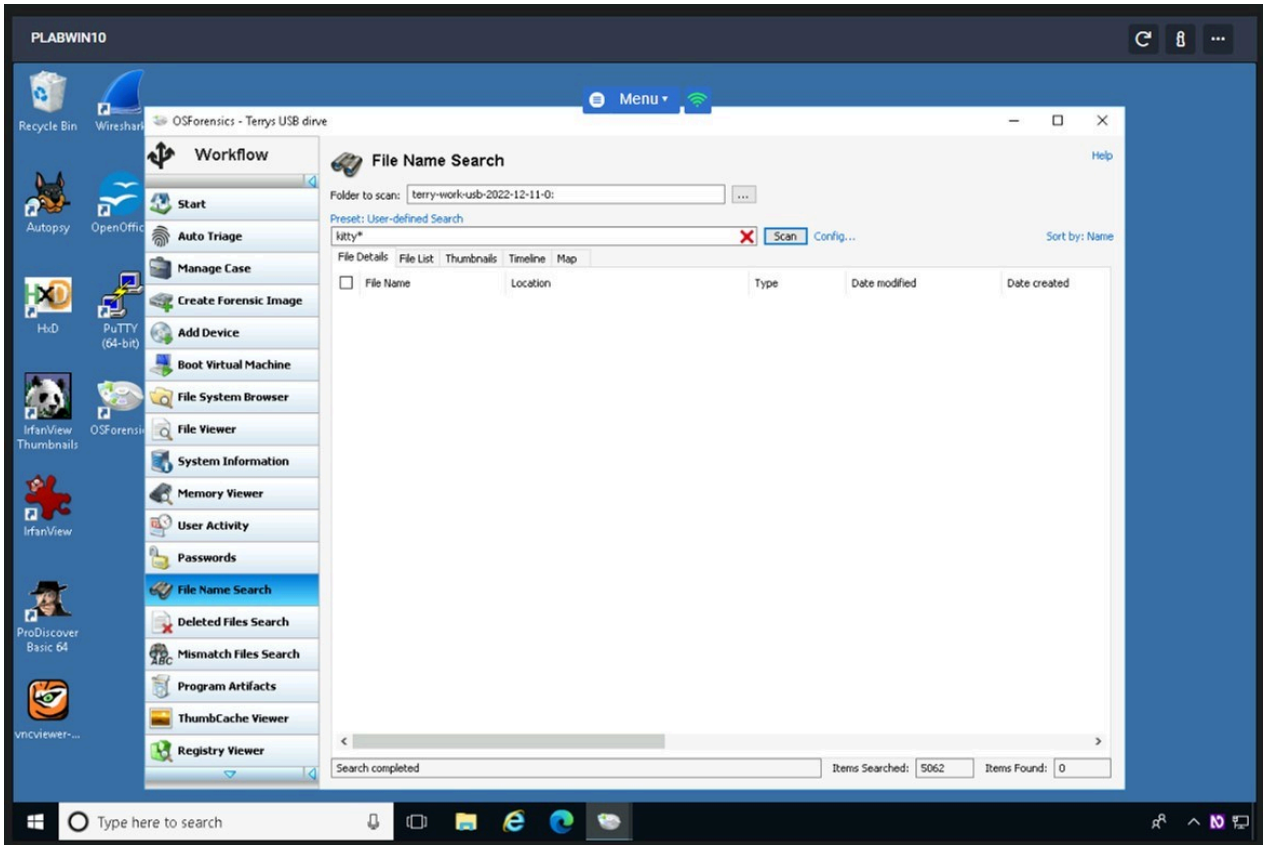


Step 8

Click the **File Name Search** icon in the File System Browser window or the left pane of the main window.

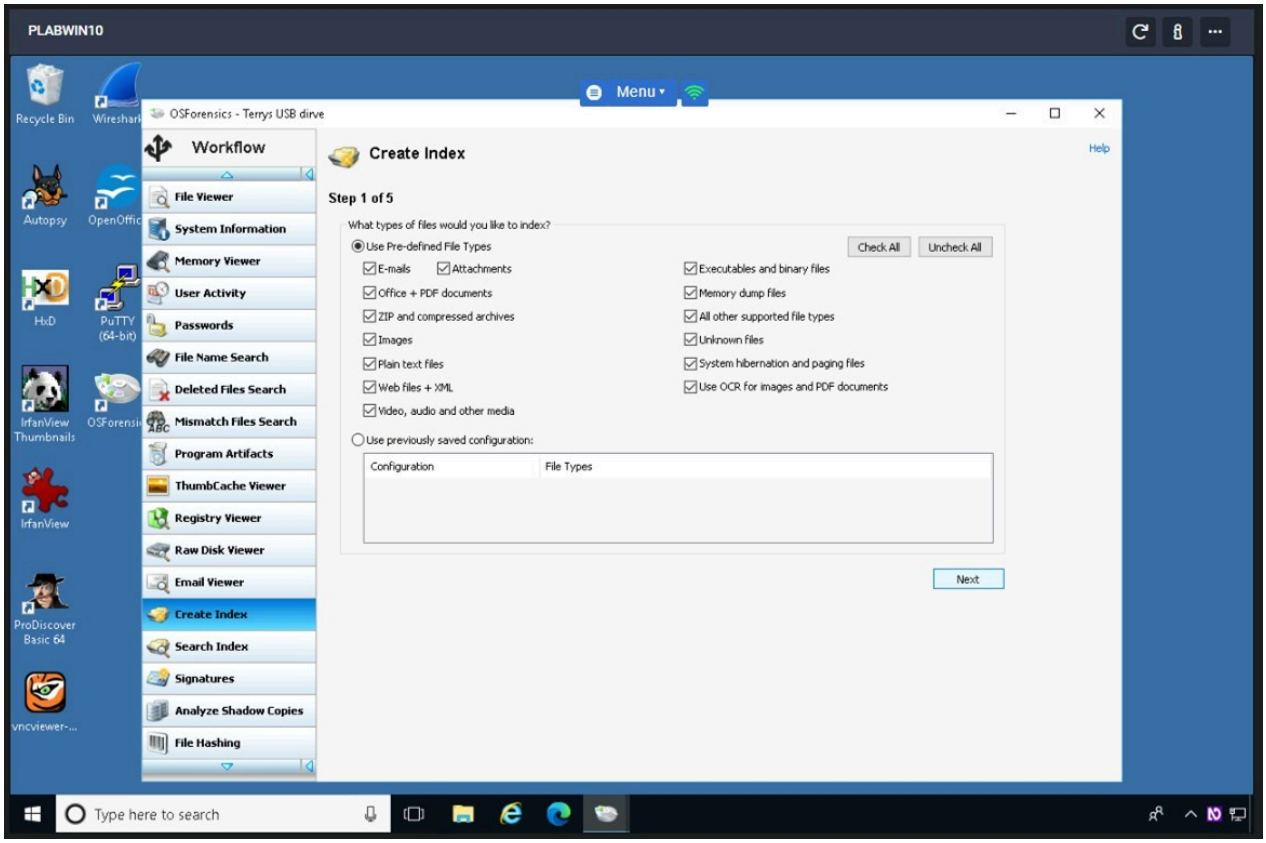


In the Search Pattern text box, type **kitty***. On the far right, click the **Scan** button. Notice that no files containing the word “kitty” were found on his USB drive.



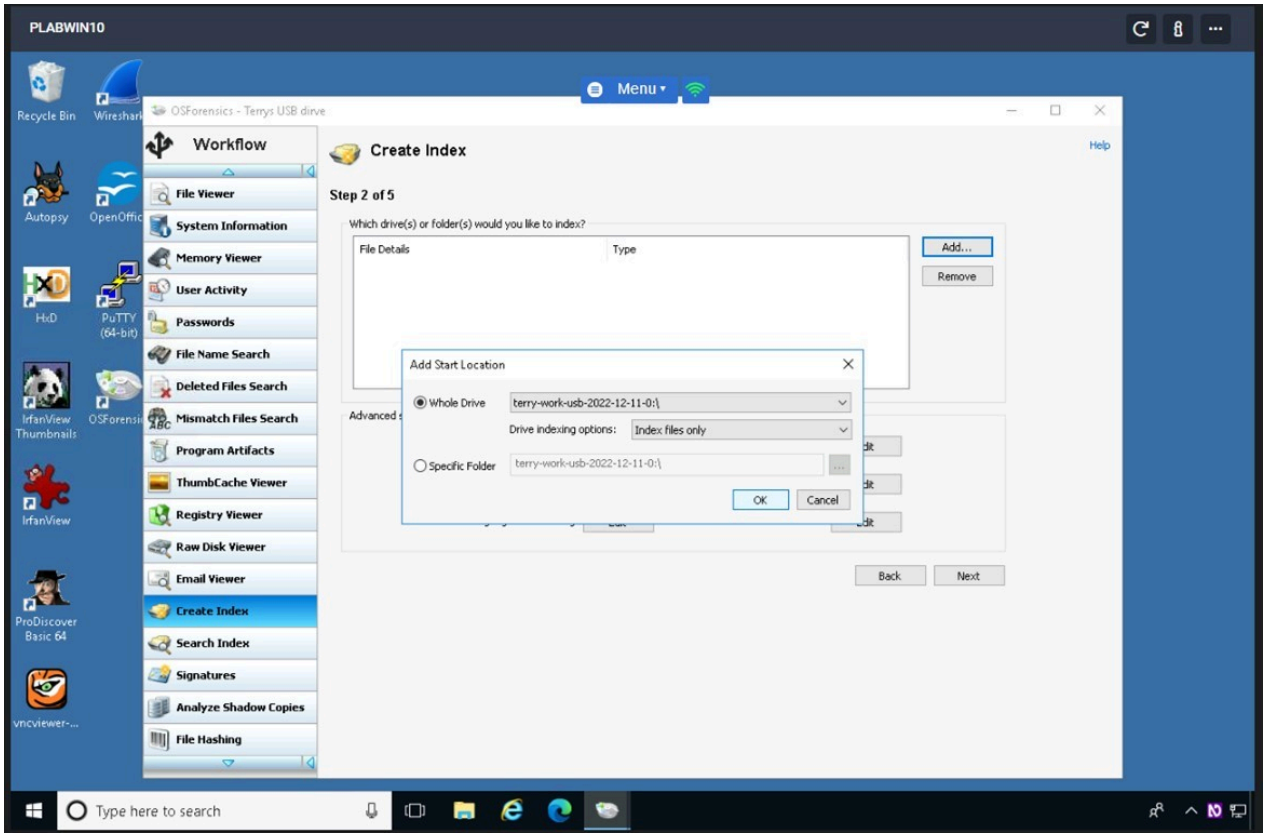
Step 9

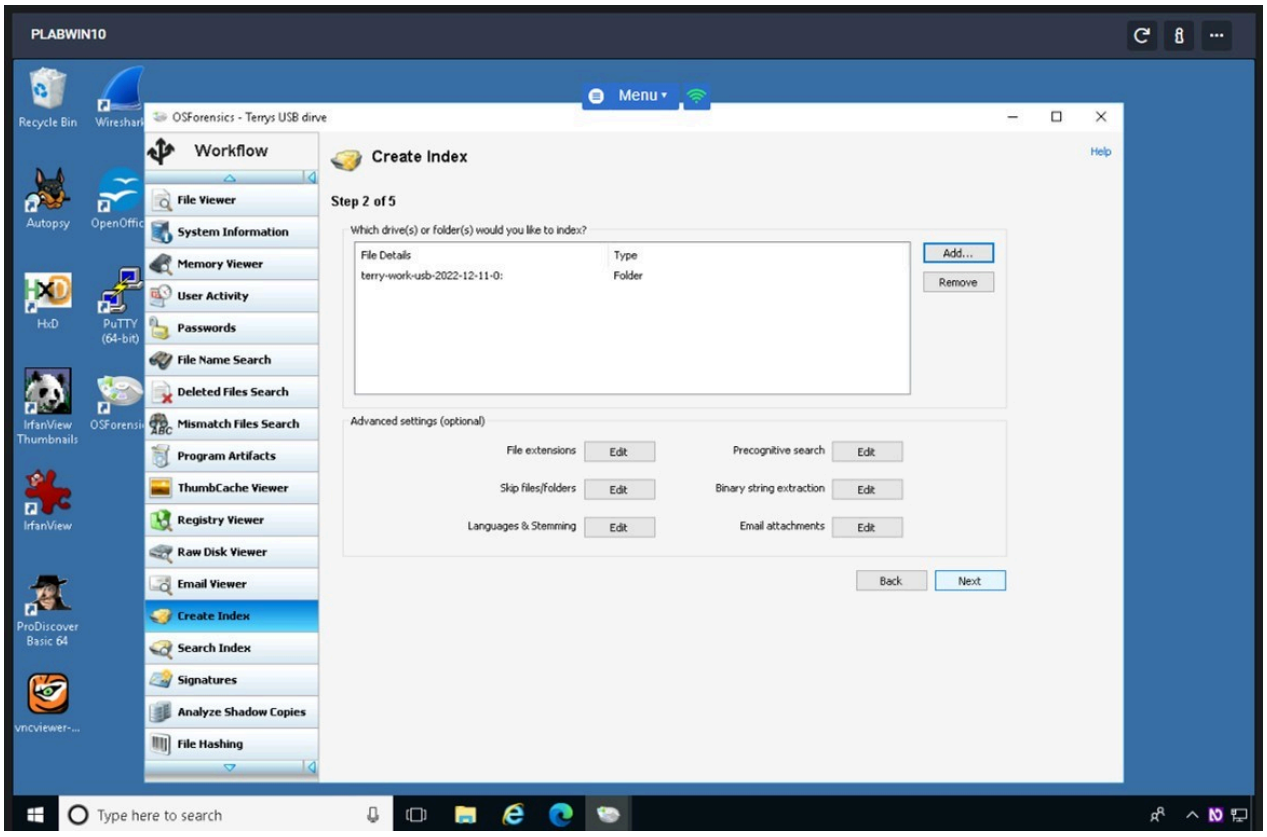
Click the **Create Index** button in the left pane. (Note: You might have to click New Index if the window is showing the results from the index of Charlie’s USB drive.) In the **Step 1 of 5** window, click the **Use Pre-determined File Types** option button, click all the file types listed, and then click **Next**.



Step 10

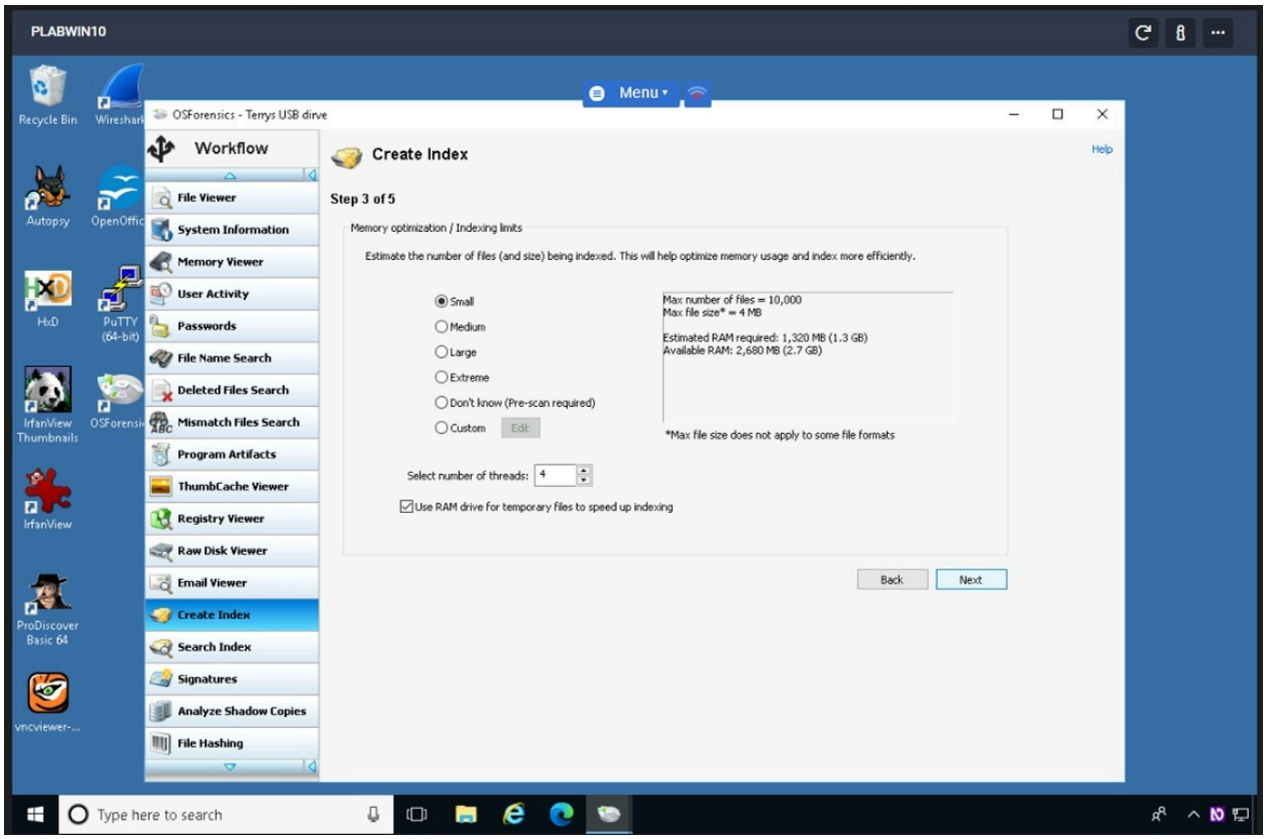
In **Step 2 of 5** window, click Charlie's USB image and click **Remove** to delete it from the list box, if necessary. Click **Add**. In the Whole Drive box, make sure **terry-workusb-2022-12-11-0:** is selected. If not click the down arrow and select it, click **OK**, and then click **Next**.





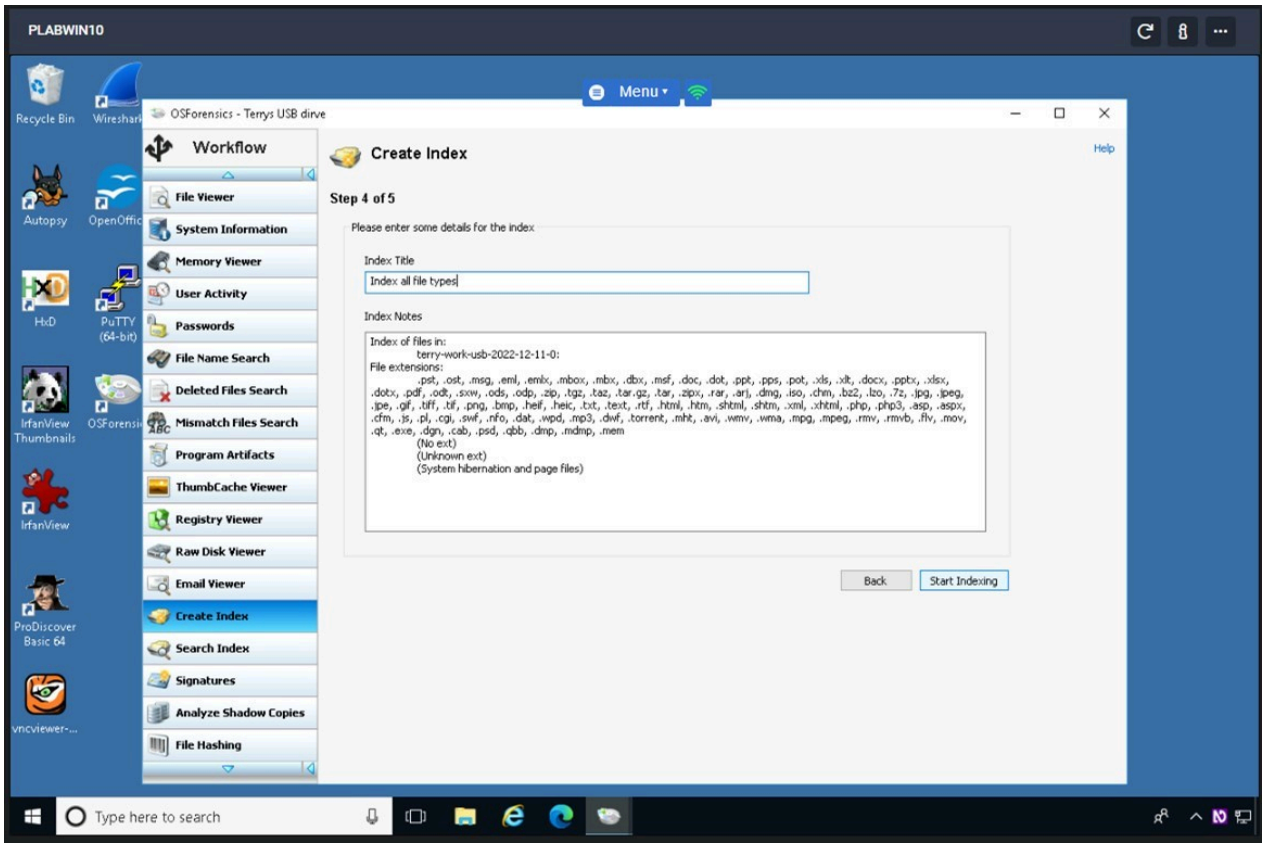
Step 11

In the **Step 3 of 5** window, select **Small** for the Estimate of the number of files, and then click **Next**.

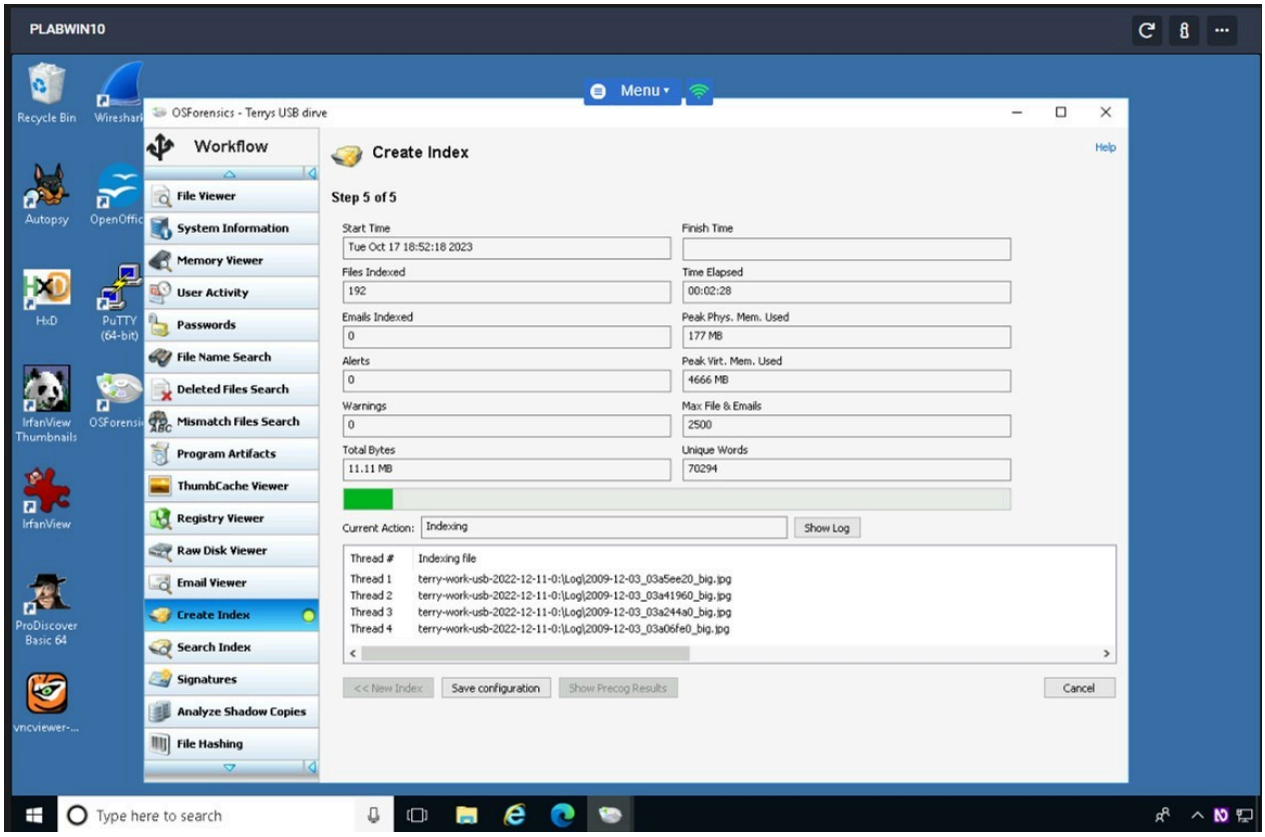


Step 12

Type Index all file types in the **Index Title** text box, and then click **Start Indexing**.

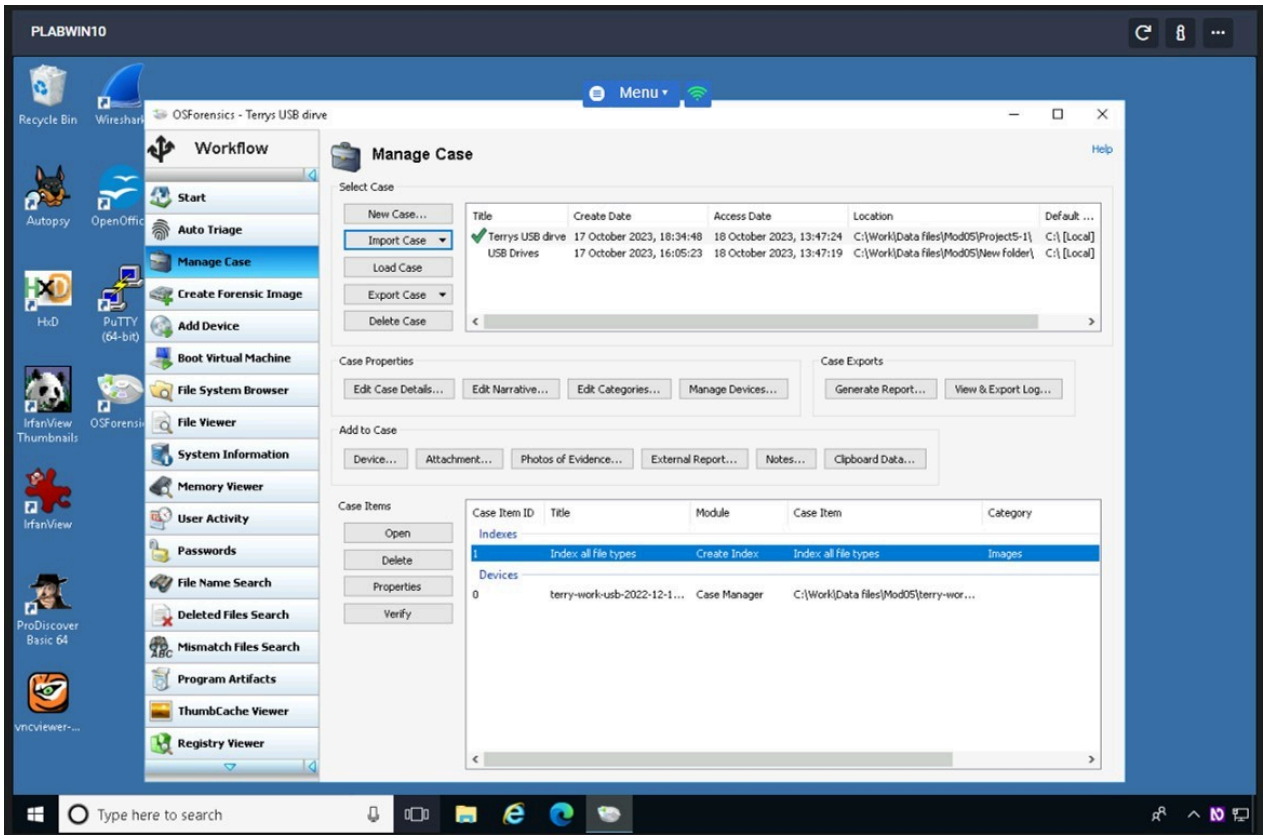


When the indexing is finished, which might take a while (enough time to get a coffee), click **OK** in the message box.



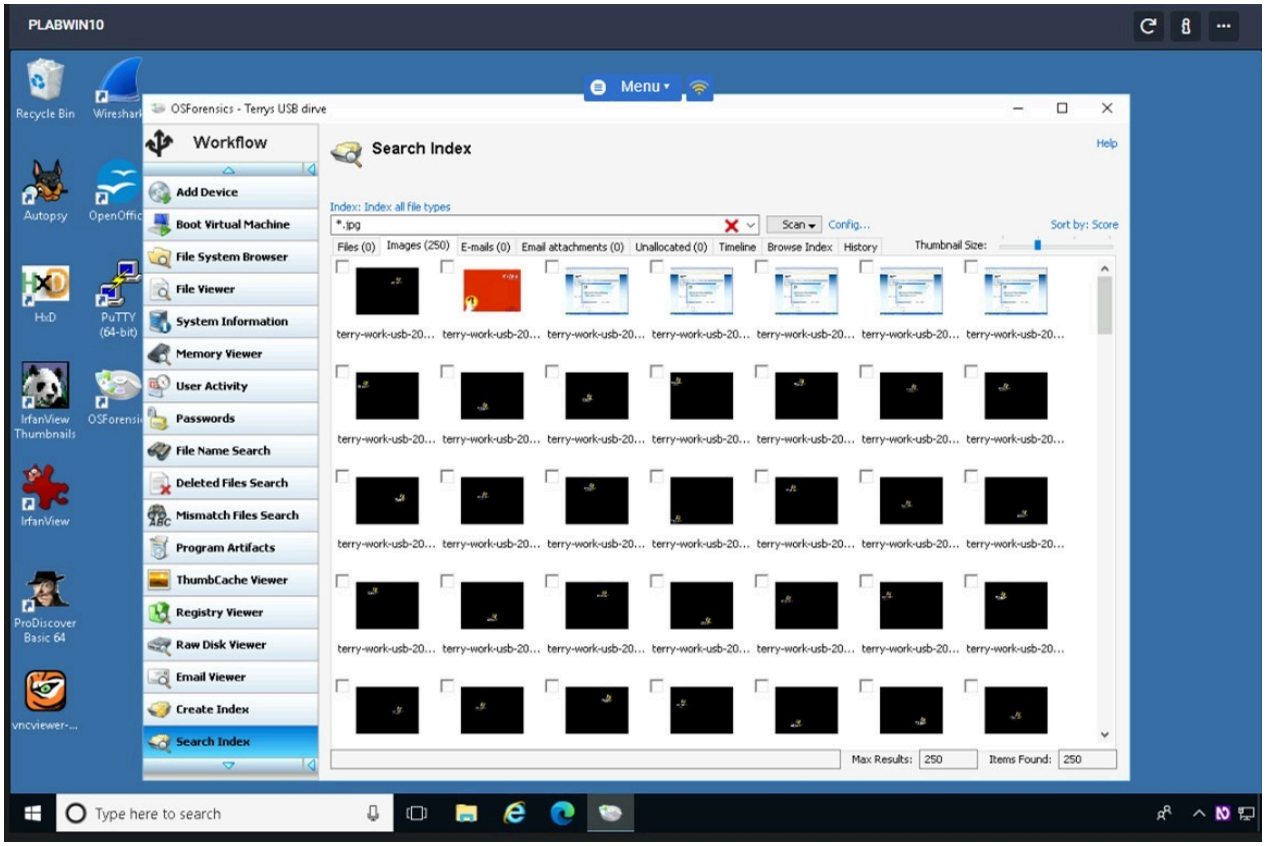
Step 13

Click the **Manage Case** button in the left pane. In the lower right pane, double-click **Index all file types** under **Indexes** in the **Case Items** area, open any text or picture files and examine them.



Step 14

In the Search Index window, enter *.jpg in the search box and click **Scan**. 250 images should be found. Close the pop-up window that alerts you that the trial version is restricted to 250 files.



Step 15

Scroll to the bottom of the left pane and click the **Exit** button. Write a 1-2 page paper explaining the importance of the files you examined. How might they affect a patent case?

There are no screenshot items for this exercise.

Leave the devices you have powered on in their current state and proceed to the next exercise.

Hands-On Project 5-2

In this project, you will create a file on a USB E: drive present in the **PLABWIN10** device. You will then calculate its hash value in **FTK Imager**. Then, you change the file and calculate the hash value again to compare the files. You need a Windows computer and a USB drive.

Step 1

Create a folder called **M5Prj5-2** on your **USB E:** drive, and then start **Notepad**.

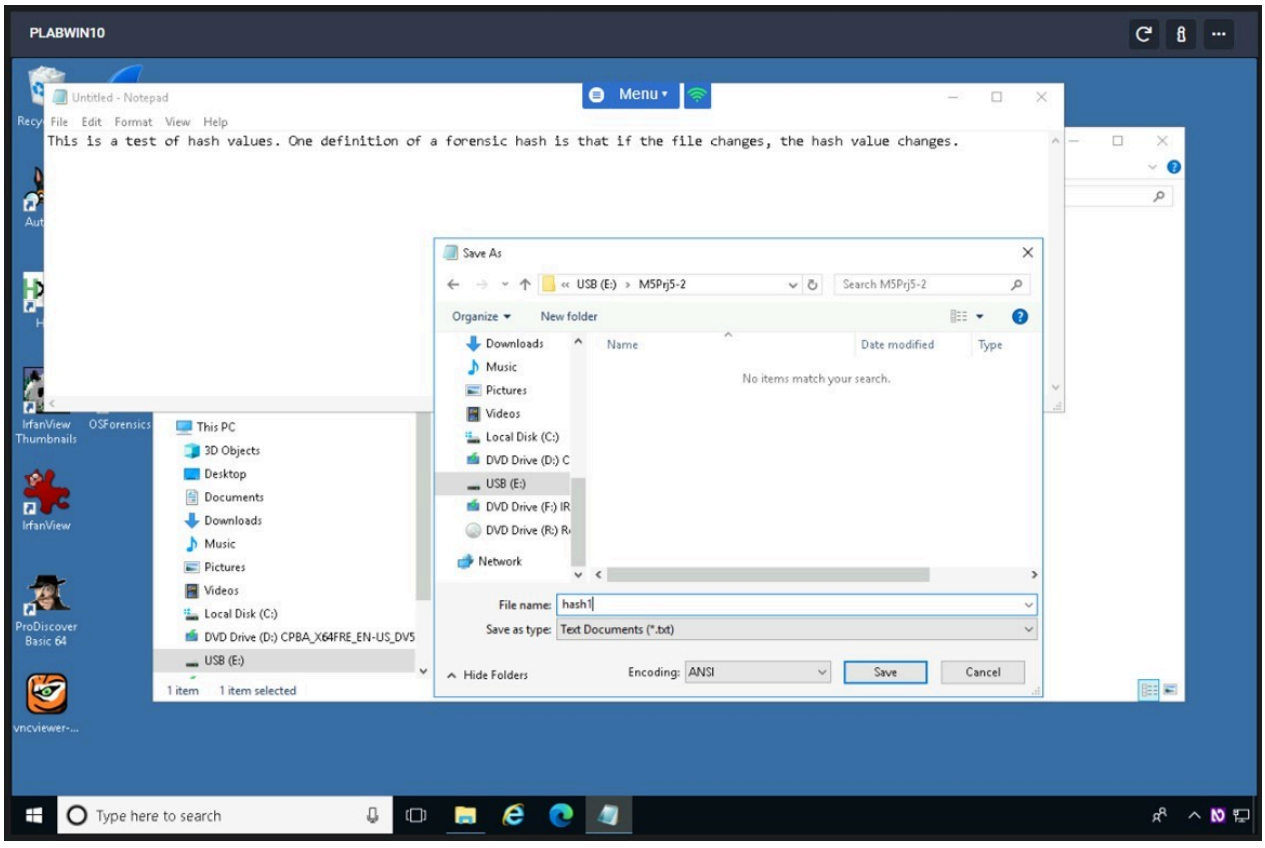
Step 2

In a new text file, type:

```
This is a test of hash values. One definition of a forensic hash is
that if the file changes, the hash value changes.
```

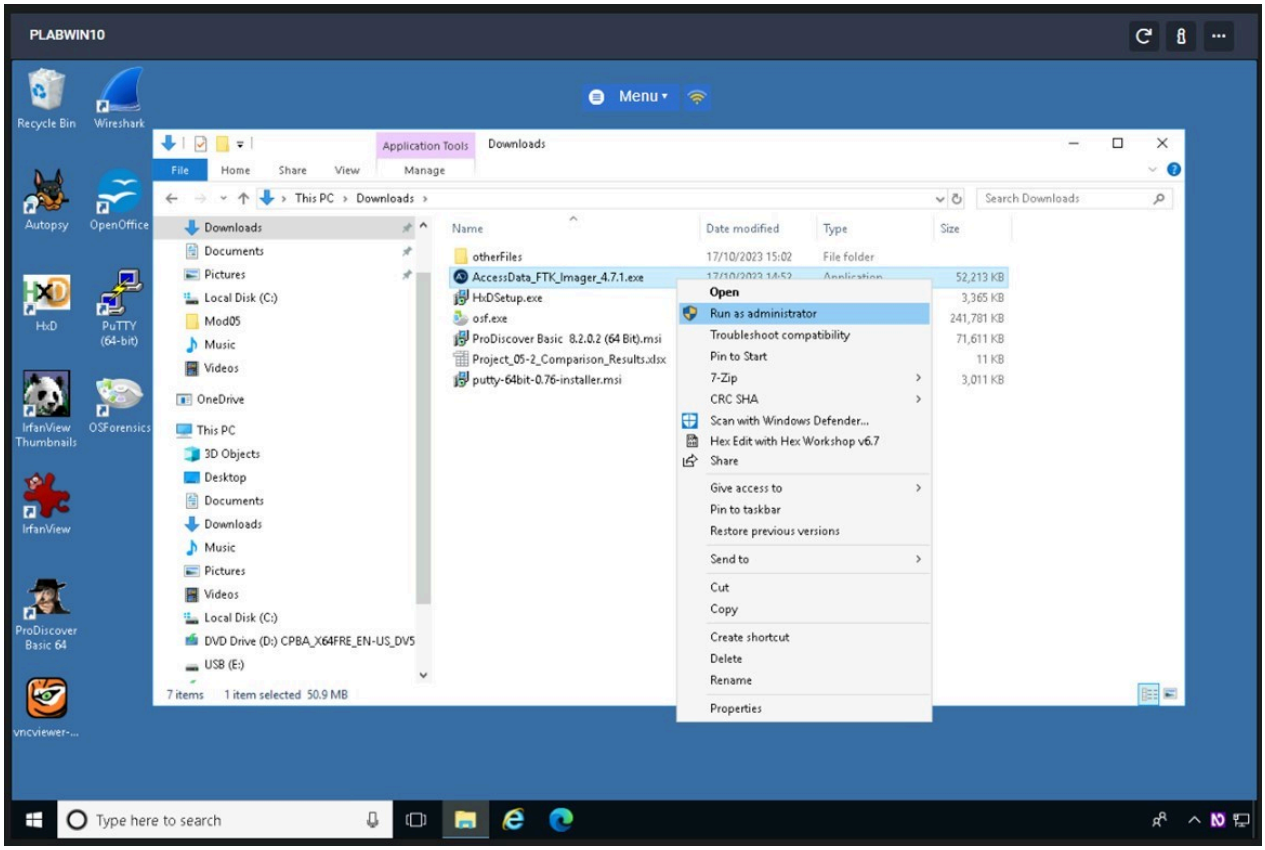
Step 3

Save the file as **hash1** in the **M5Prj5-2** folder on your **USB E:** drive, and then exit **Notepad**.



Step 4

Launch **File Explorer**. Navigate to the Downloads folder and right-click the AccessData_FTK_Imager install executable, and choose Run as administrator.

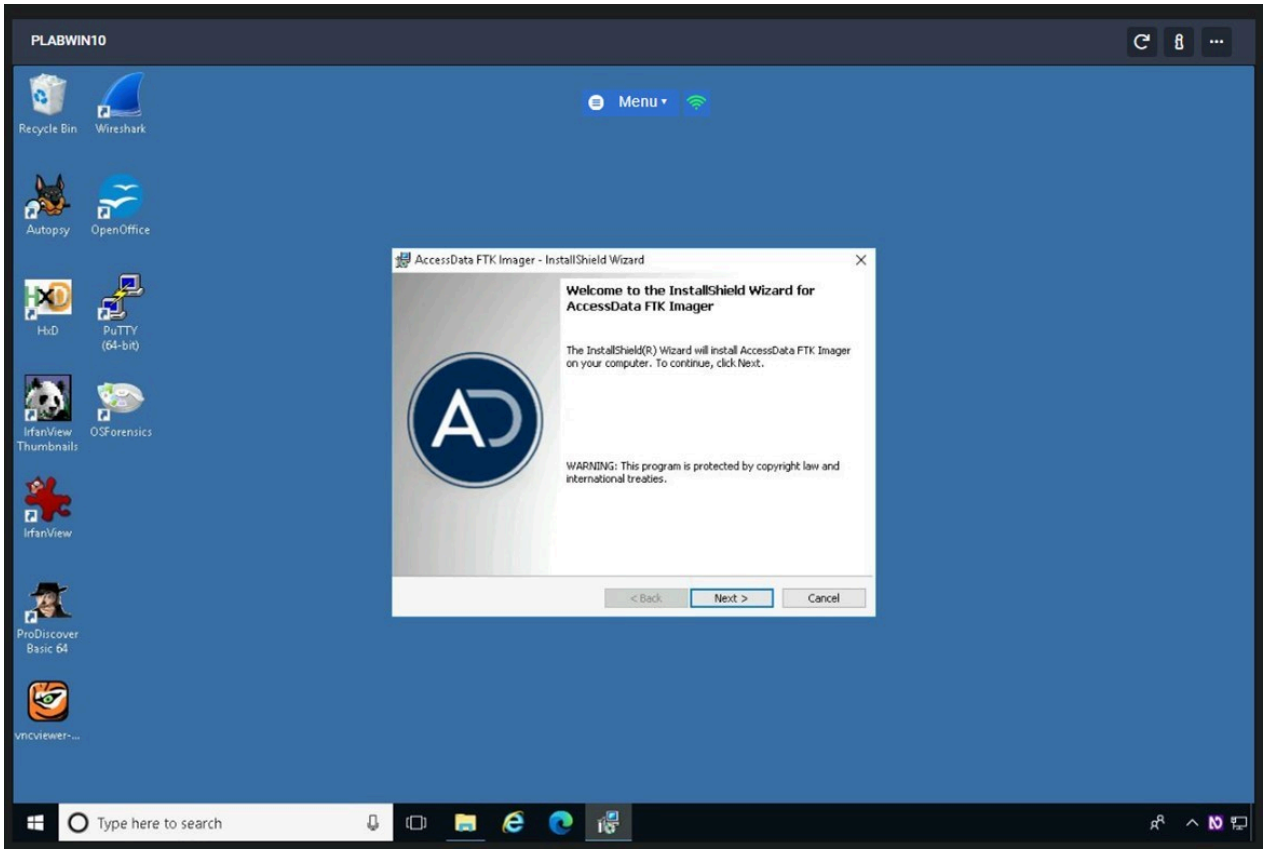


If a UAC prompt appears, click **Yes** in the UAC to continue.

Step 5

The **Welcome to the InstallShield Wizard for AccessData FTK Imager** screen is displayed.

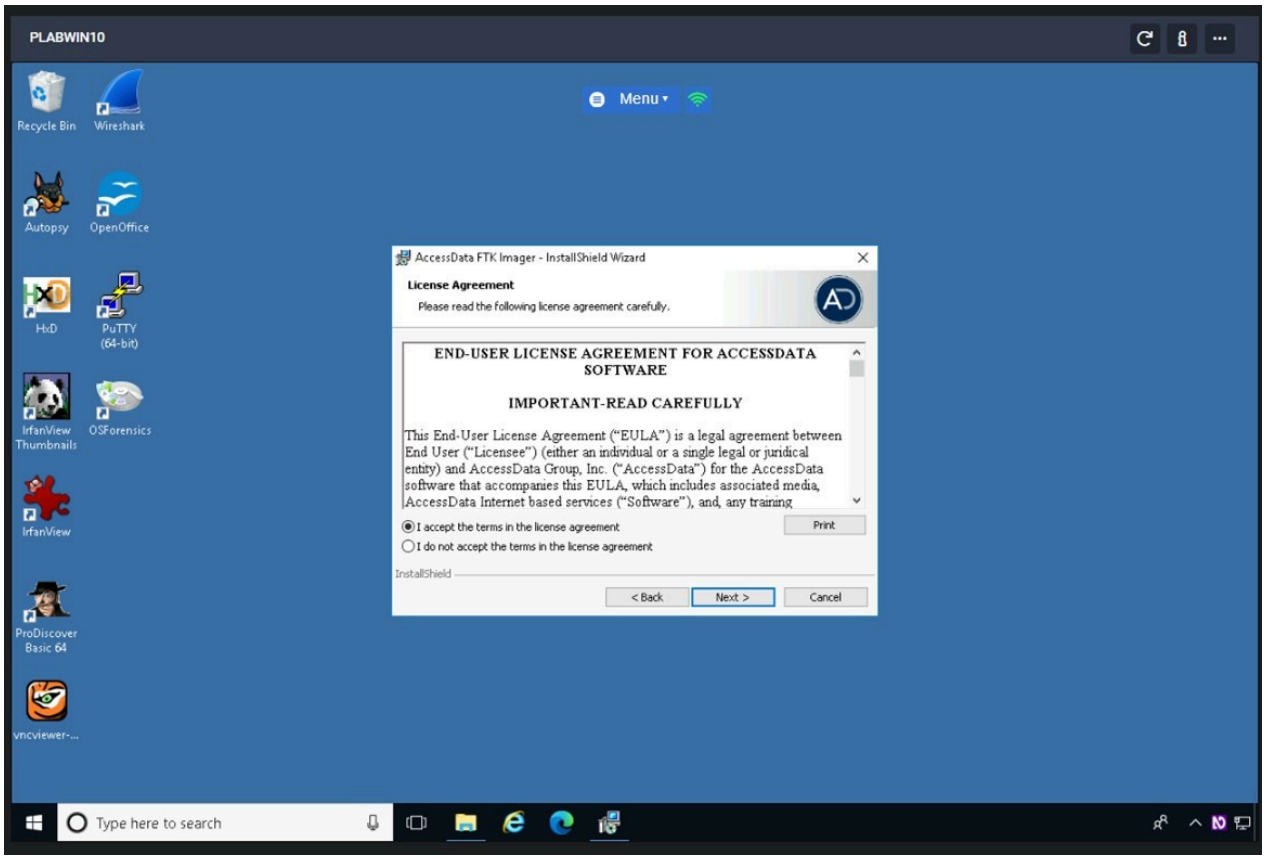
Click **Next**.



Step 6

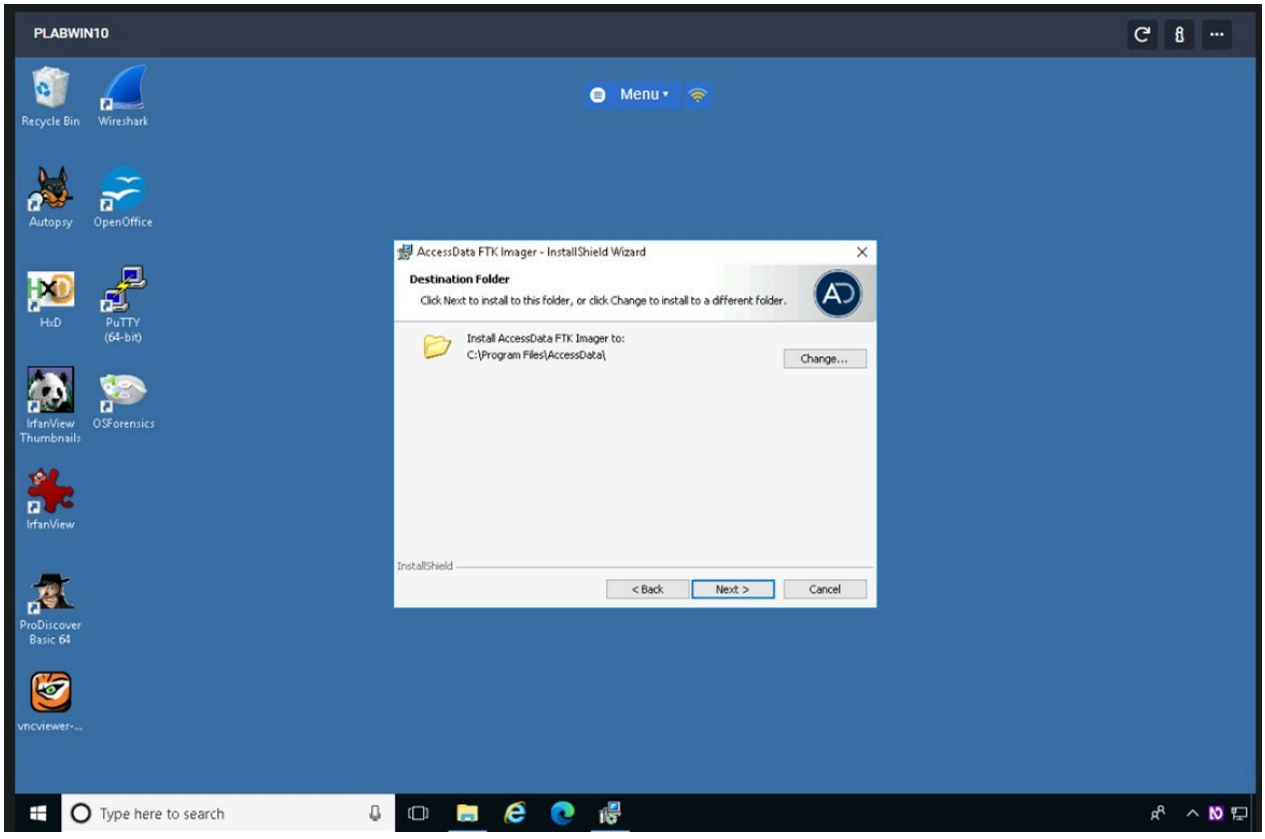
On the **License Agreement** page, click **I accept the terms in the license agreement** option.

Click **Next**.



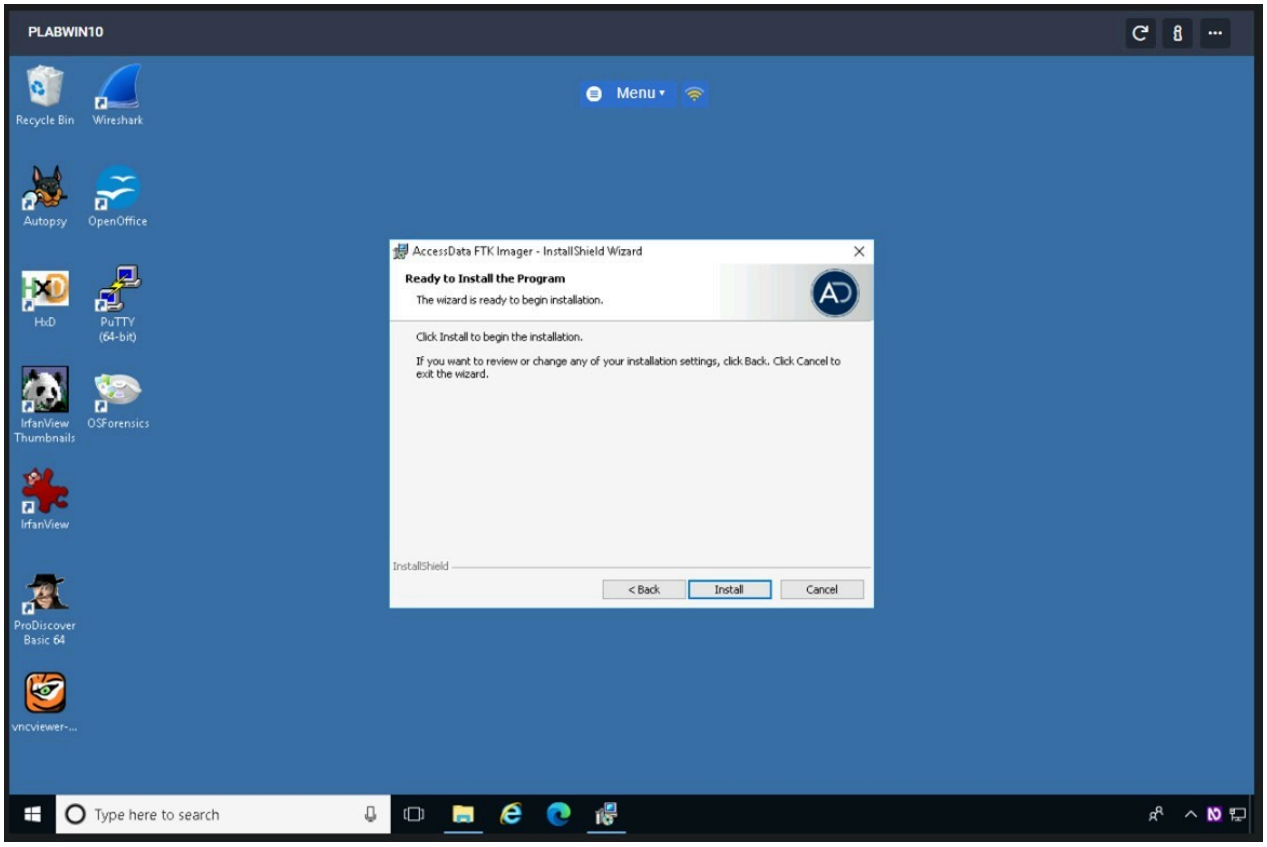
Step 7

Accept the default folder path in the **Destination Folder** page by clicking **Next**.



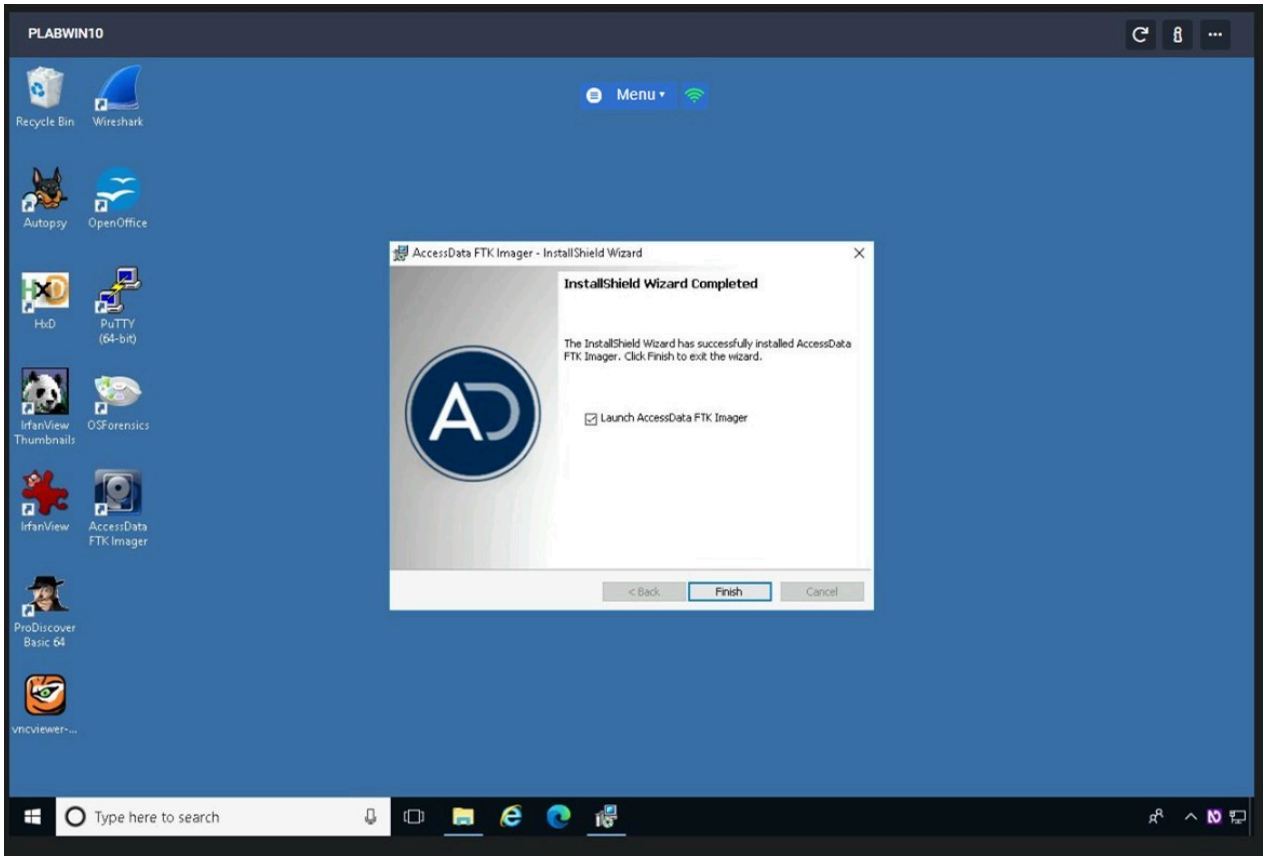
Step 8

Click **Install** when **Ready to Install the Program** page is displayed.



Step 9

Click **Finish** when a successful installation is successfully completed.



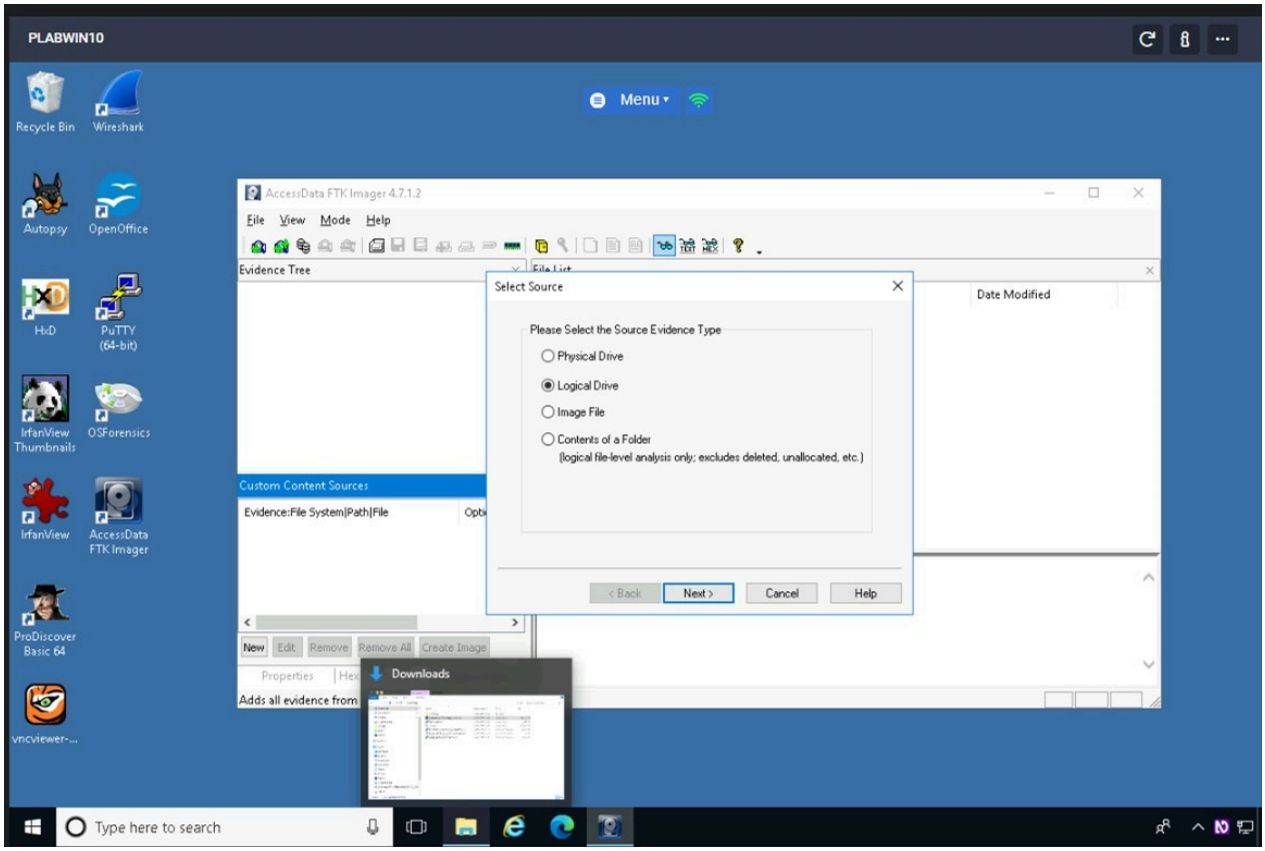
Step 10

The **FTK Imager** application opens.

Click **File**, **Add Evidence Item** from the menu.

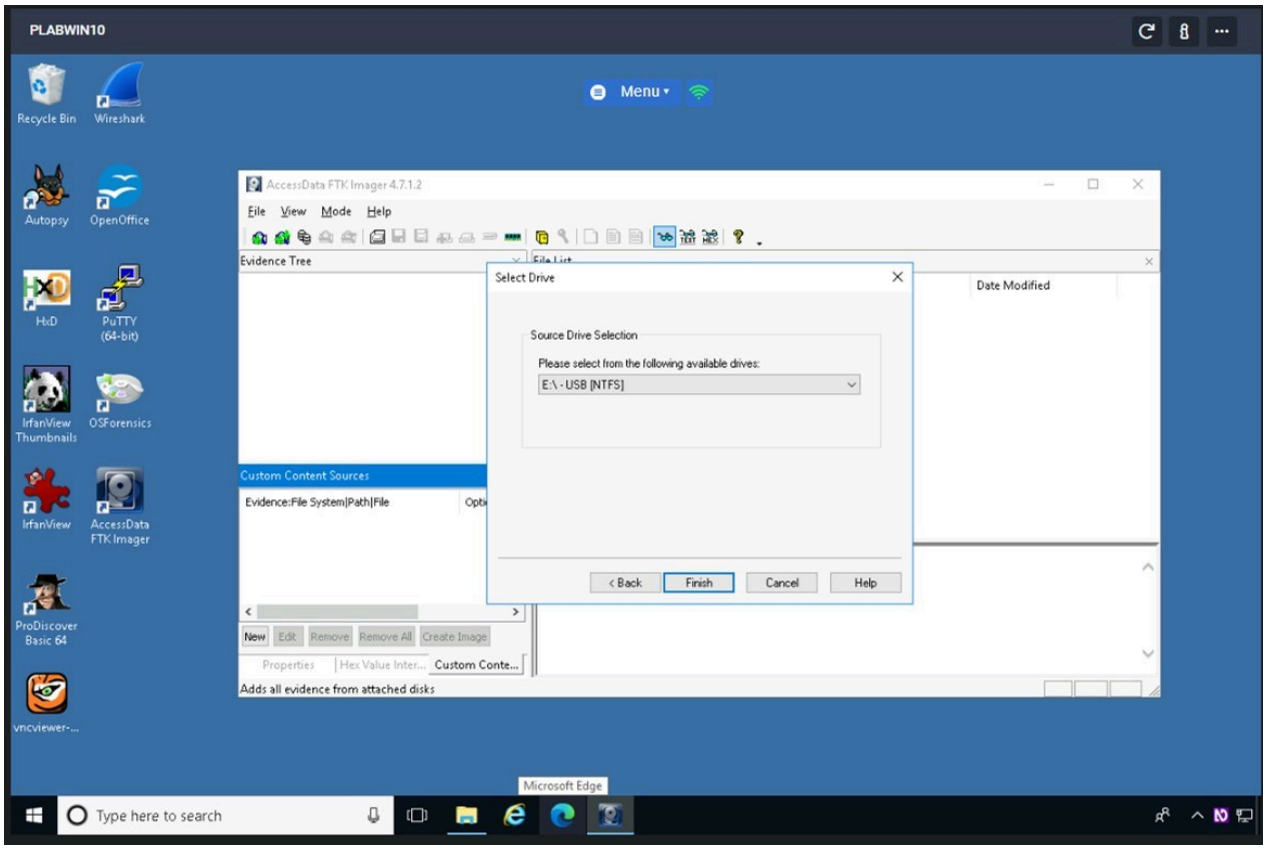
Step 11

In the **Select Source** dialog box, click the **Logical Drive** option button, and then click **Next**.



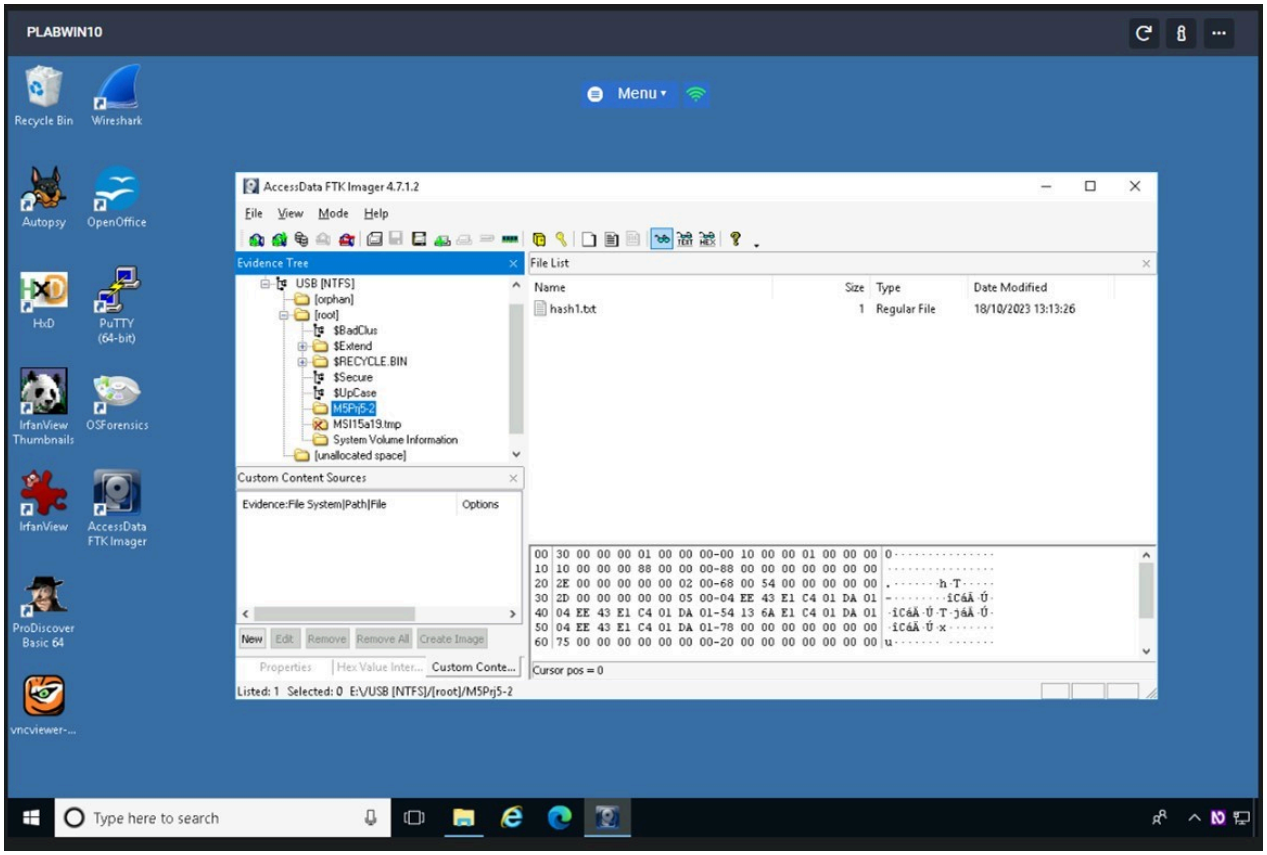
Step 12

In the **Select Drive** dialog box, click the **Source Drive Selection** drop-down list, click to select your **E:\ - USB [NTFS]** drive, and then click **Finish**.



Step 13

In the upper-left pane, click to expand your **E:\ > USB [NTFS] > [root]** drive and continue expanding until you can click the **M5Prj5-2** folder. In the upper-right pane, you should see the **hash1.txt** file you created.

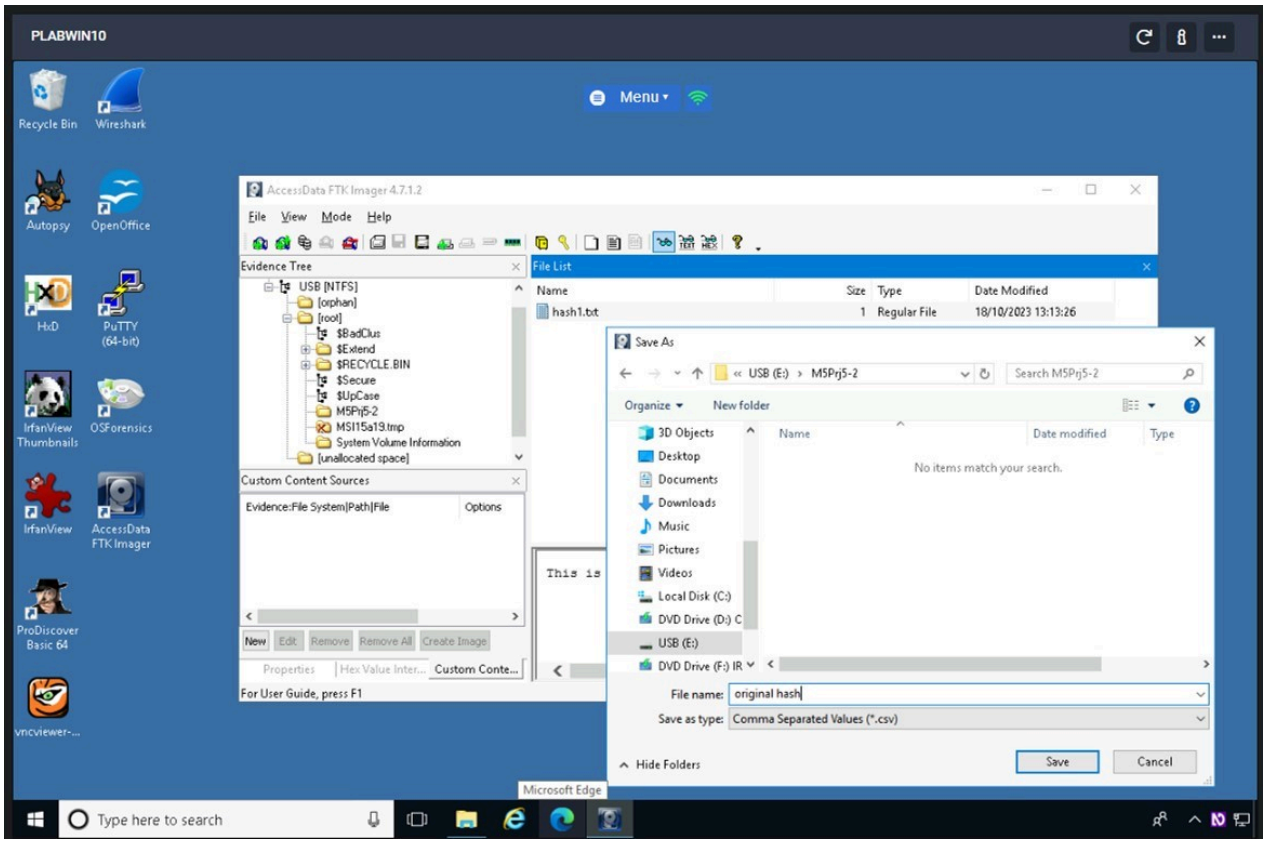


Step 14

Right-click the **hash1.txt** file and click **Export File Hash List.**

Save the file as **original hash** in the **M5Prj5-2** folder on your **USB E:** drive.

FTK Imager saves it as a **.csv** file.



Step 15

Exit **FTK Imager** and start **Notepad**.

Step 16

Open **hash1.txt** in Notepad. Add one letter to the end of the file, save it, and exit Notepad.

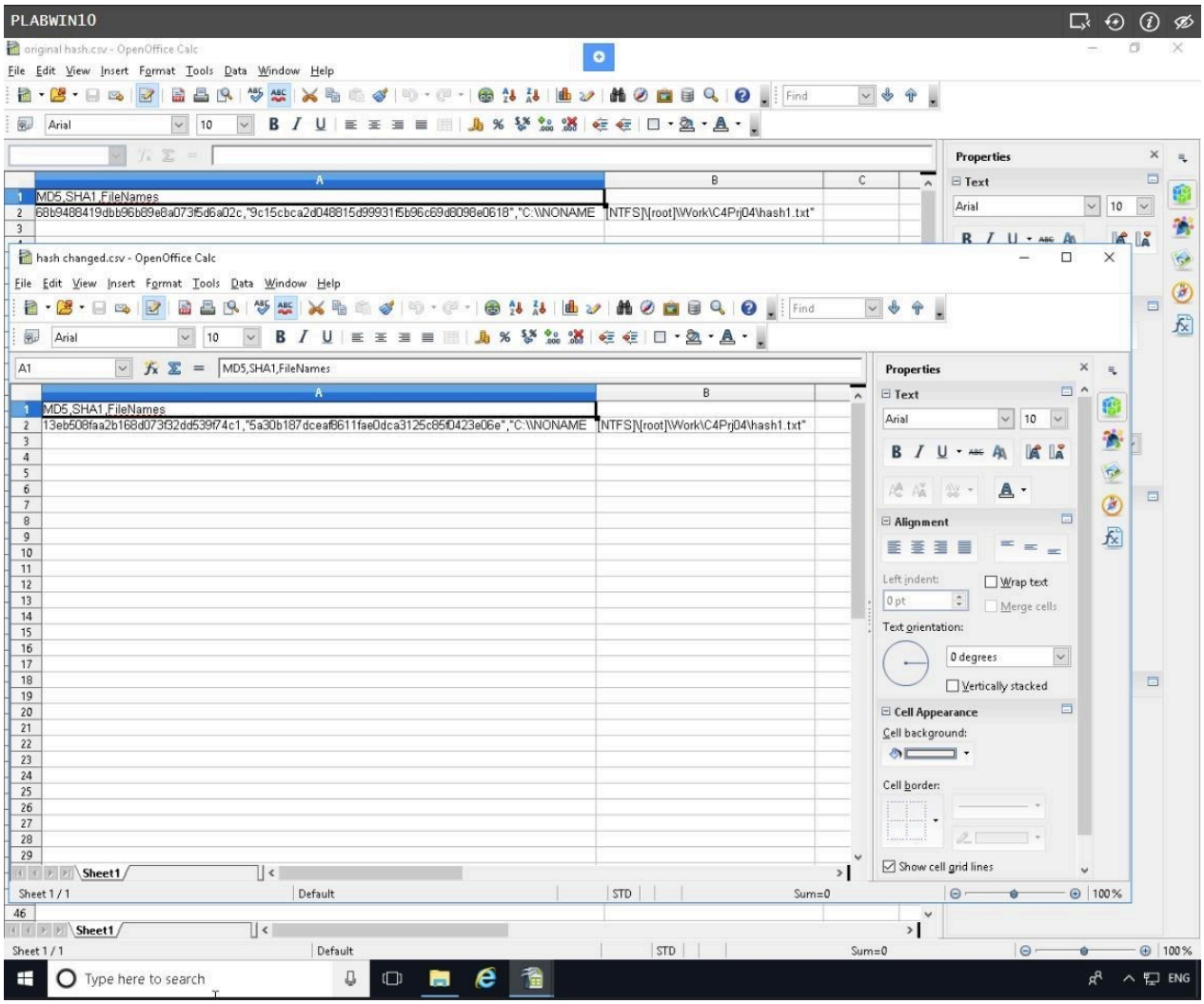
Step 17

Open the **original hash** and **changed hash** files on your USB E: drive using **OpenOffice Calc** (or another spreadsheet program).

On the **Text Import - [filename.csv]** dialog box, click **OK**.

Compare the hash values in both files to see whether they are different, and then exit **OpenOffice Calc**.

Exit **OpenOffice Calc** when finished.



Screenshot

2 of 9

Click the button to take a screenshot of PLABWIN10

Leave the devices you have powered on in their current state and proceed to the next exercise.

Hands-On Project 5-3

In this project, you create a file on your USB E: drive and calculate its hash values in FTK Imager. Then, you change the filename and extension and calculate the hash values again to compare them. You will use the PLABWIN10 computer and the USB E: drive.

Step 1

Create a folder called **C4Prj05** on your **USB E:** drive, and then start **Notepad**.

Step 2

In a new text file, type:

```
This project shows that the file, not the filename, has to change
for the hash value to change.
```

Step 3

Click **File**, **Save As** from the menu, and save the file as **testhash** in the **C4Prj05** folder on your **USB E:** drive. Exit **Notepad** and start **FTK Imager** (clicking **Yes** in the UAC message box, if necessary).

Step 4

Click **File**, **Add Evidence Item** from the menu. In the **Select Source** dialog box, click the **Logical Drive** option button, and then click **Next**.

Step 5

In the **Select Drive** dialog box, click the **Source Drive Selection** list arrow, click to select your **USB E:** drive, and then click **Finish**.

Step 6

In the upper-left pane, click to expand your **E:\ > USB [NTFS] > root** drive and continue expanding until you can click the **C4Prj05** folder. In the upper-right pane, you should see the **testhash** file you created.

Step 7

Right-click the **testhash** file and click **Export File Hash List**. Save the file as **original hash value** in the **C4Prj05** folder on your **USB E:** drive. FTK Imager saves it as a .csv file.

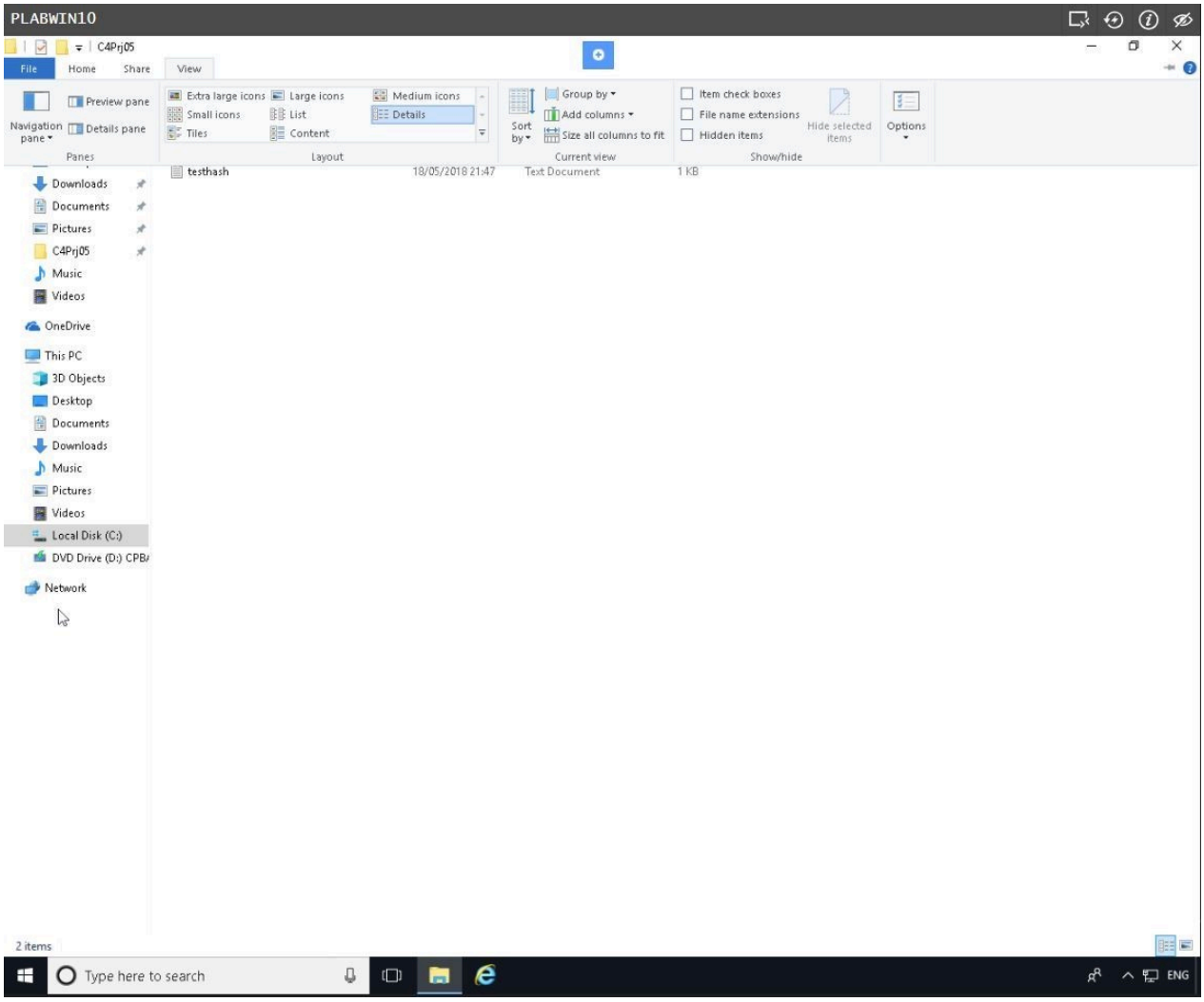
Step 8

Click to select your **E:** drive in the upper-left pane, if necessary, and then click **File**, **Remove Evidence Item** from the menu. Exit **FTK Imager**.

Step 9

Open **File Explorer**. Click the **View** menu.

On the ribbon that appears, click **Options** and then select **Change folder and search options**.



Step 10

On the **Folder Options** dialog box, click the **View** tab.

Under the **View** tab in the **Advanced settings** section, clear the **Hide extensions for known file types** checkbox.

Click **OK**. Close the **File Explorer** window.

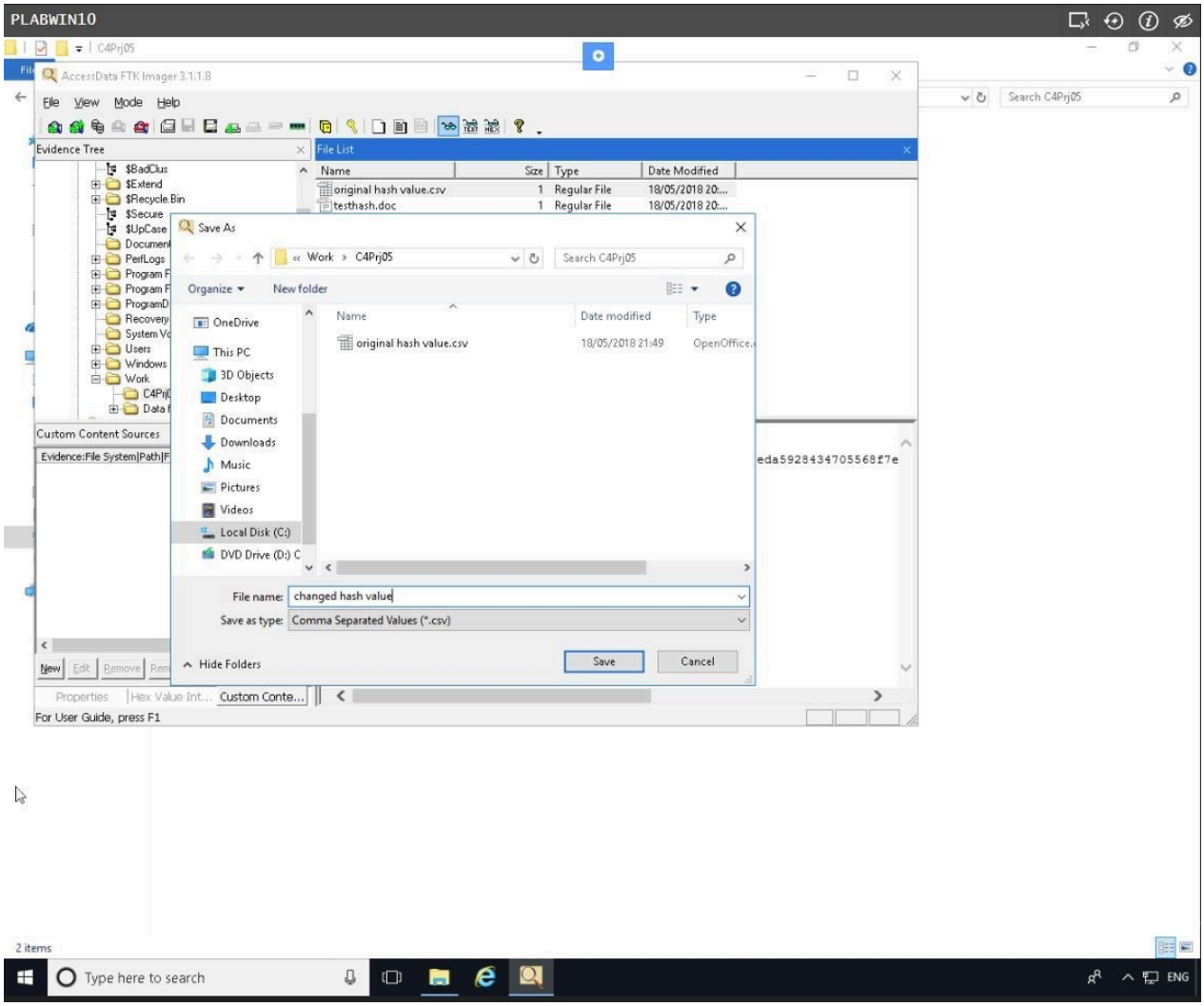
Step 11

Navigate to **USB (E:) > C4Prj05** folder.

Right-click the **testhash.txt** file on your **USB E:** drive and rename it as **testhash.doc**. In the warning message about the change in extension, click **Yes**.

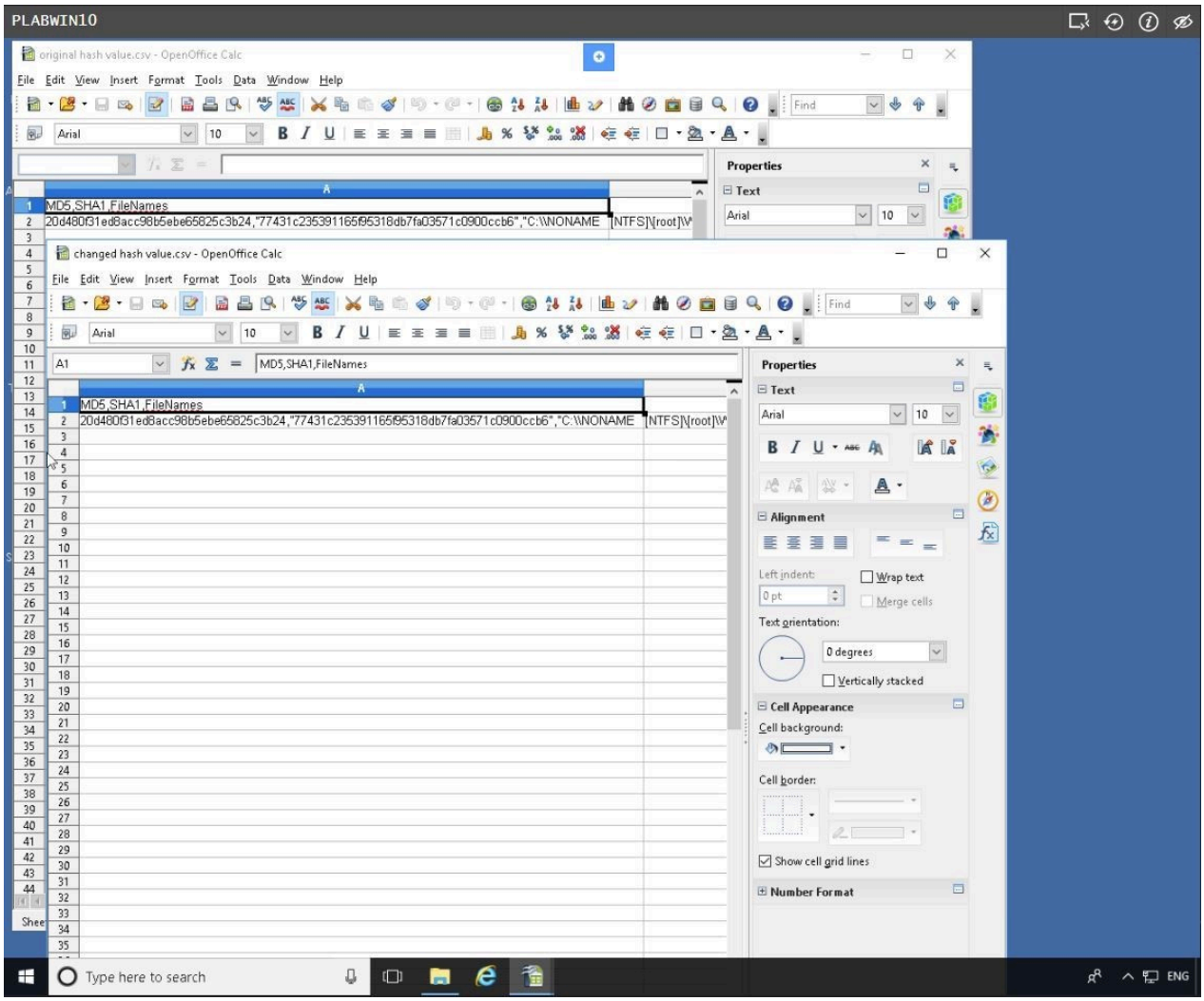
Step 12

Start **FTK Imager**. Follow Steps 4 to 8, but this time, when you export the file hash list, save the file as **changed hash value**. Exit **FTK Imager**.



Step 13

Open the **original hash value** and **changed hash value** in **OpenOffice Calc** (or another spreadsheet program). Compare the hash values in both files to see whether they are different, and then exit **OpenOffice Calc**.



Screenshot

3 of 9

Click the button to take a screenshot of PLABWIN10

Hands-On Project 5-4

As part of a digital forensics investigation, it may be necessary to determine what the differences are between two files that appear to be identical. For this project, you will examine the contents of two files to identify their differences using the hexadecimal editor HxD.

Step 1

From File Explorer, double-click the file *Project_05-2_Comparison_Results.xlsx* ***to open it in your spreadsheet*** program. Type your name in the Examiner's Name field in cell C3.

Step 2

Start **HxD**, and then click **Analysis**, then **Data comparison**, and then **Compare**.

Step 3

In the Window arrangement pane of the Compare Window, click the **Tile horizontally** button, and then in the Scope pane, click **All**.

Step 4

In the Compare window, click the **1. Data source** ellipse button and, in the Open window, navigate to your Work folder, click **Project_05-2_Compare_File-1.docx**, and then click **Open**.

Step 5

In the Compare Window, click the **2. Data source** ellipse button and, in the Open window, navigate to your Work folder, click **Project_05-2_Compare_File-2.docx**, click **Open**, and then click **OK**.

Step 6

Examine the differences between the two files by clicking **Analysis**, **Data comparison**, and then **Next difference**. For each difference located, record the offset byte position (the offset is displayed in the lower left corner of the HxD window) and the character values between the two files in **Project_05-2_Comparison_Results.xlsx**.

Screenshot

Click the button to take a screenshot of PLABWIN10

Step 7

When finished, close HxD and submit to your instructor the following file:

Project_05-2_Comparison_Results.xlsx

Lab Assessment

Did you complete all the lab steps? Don't forget to complete the review questions on the next page.

Summary

- Digital evidence is anything stored or transmitted on electronic or optical media. It's extremely fragile and easily altered.
- In the private sector, an incident scene is often a place of work, such as a contained office or manufacturing area. Because everything from the computers used to violate a company policy to the surrounding facility is under a controlled authority, investigating and controlling the scene is easier than at a crime scene.
- Companies should publish policies stating that they reserve the right to inspect digital assets at will; otherwise, employees' expectation of privacy prevents an employer from legally conducting an intrusive investigation or covert surveillance. A well-defined company policy states that an employer has the right to examine, inspect, or access any company-owned digital asset.
- Approved procedures must be followed, even in private-sector investigations, because civil cases can easily become criminal cases. If an internal corporate case is turned over to law enforcement because of criminal activity, the corporate investigator must avoid becoming an agent of law enforcement.
- Criminal cases require a correctly executed and well-defined search warrant. A specific crime and location must be spelled out in the warrant. For all criminal investigations in the United States, the Fourth Amendment specifies that a law enforcement officer can search for and seize criminal evidence only with probable cause, which is facts or circumstances that lead a reasonable person to believe a crime has been committed or is about to be committed.
- The plain view doctrine applies when investigators find evidentiary items that aren't specified in a warrant or under probable cause.
- When preparing for a case, describe the nature of the case, identify the type of OS, determine whether you can seize the computer or digital device, and obtain a description of the location.
- Preparing for the search and seizure of computers or digital devices is probably the most important step in a digital investigation.

- If you deal with situations involving hazardous materials often, you might need to get HAZMAT certification or have someone else with this certification collect the evidence.
- Always take pictures or use a video camera to document the scene. Prevent professional curiosity from contaminating evidence by limiting who enters the scene.
- As you collect digital evidence, guard against physically destroying or contaminating it. Take precautions to prevent static electricity discharge to electronic devices. If possible, bag or box digital evidence and any hardware you collect from the scene. As you collect hardware, sketch the equipment, including exact markings of where components are located. Tag and number each cable, port, and other connection and record its number and description in a log.
- Selecting a medium for storing digital evidence usually depends on how long you need to keep the evidence. The ideal storage media are CDs, DVD-Rs, DVD-RWs, or offsite storage. You can also use magnetic tapes, such as 4-mm DAT and DLT magnetic tapes.
- Forensic hash values are used to verify that data or storage media haven't been altered. The two most common hashing algorithms for forensics purposes are currently MD5 and SHA-1. A forensic hash can't be predicted; each file produces a unique hash value, and if the file changes, the hash value must change.
- You must handle all evidence the same way every time you handle it. Apply the same security and accountability controls for evidence in a civil lawsuit as for evidence from a crime scene to comply with state or federal rules of evidence.
- After you determine that an incident scene has digital data or devices, identify the information or artifacts that can be used as evidence. Next, catalog or document the evidence you find. Your goal is to preserve evidence integrity, which means you must not modify the evidence as you collect and catalog it. An incident scene should be photographed and sketched, and then each item should be labeled and put in an evidence bag. Collect, preserve, document, analyze, identify, and organize the evidence. Then, rebuild evidence or repeat a situation to verify that you get the same results every time.

- Employee compliance investigations require that an organization have policies in place that inform employees that they do not expect privacy.

Lab Assessment

Test your knowledge on the topics covered in this lab by completing the review questions below.

Question

5 of 9

What is the best approach to handling the expectation of privacy by employees in the event an investigation needs to be carried out on company-owned digital assets?

- No approach or planning is necessary – there is no right to privacy in the corporate environment.
- A well-defined published policy that clearly states that an employer has the right to examine, inspect or access company-owned assets.
- If an investigation needs to be carried out, simply have the employee sign a waiver form before it begins.
- Every employee has the right to privacy in the corporate environment, so no policies can be forced upon them.

Question

6 of 9

When investigators find evidentiary items that aren't specified in a warrant or under probable cause, what type of doctrine applies?

- Probable cause doctrine
- Clear view doctrine
- Plain view doctrine
- Fourth amendment doctrine

Question

7 of 9

Hashing algorithms are used on evidence files to uphold the chain of custody in an investigation. Which of the following is NOT a hashing algorithm?

- SHA-256
- MD5
- DAT-1
- SHA-1

Question

8 of 9

Which of the following are ideal examples of storage media? Choose two.

- [ ] Floppy Disks
- [ ] CDs
- [ ] VCRs
- [ ] Magnetic Tape

Question

9 of 9

If you face an investigation where dangerous substances might be around, you may need to obtain which of the following?

- DANMAT certificate
- HAZMAT certificate
- DANSUB certificate
- CHEMMAT certificate

Summary

Please ensure you have completed all items before submitting your report,

submitting will log you out.

Screenshot ⊖

Screenshot ⊖

Screenshot ⊖

Screenshot ⊖

Question ⊖

Question ⊖

Question ⊖

Question ⊖

Question ⊖