Computer Forensics

Chapter 5 - Working with Windows and CLI Systems

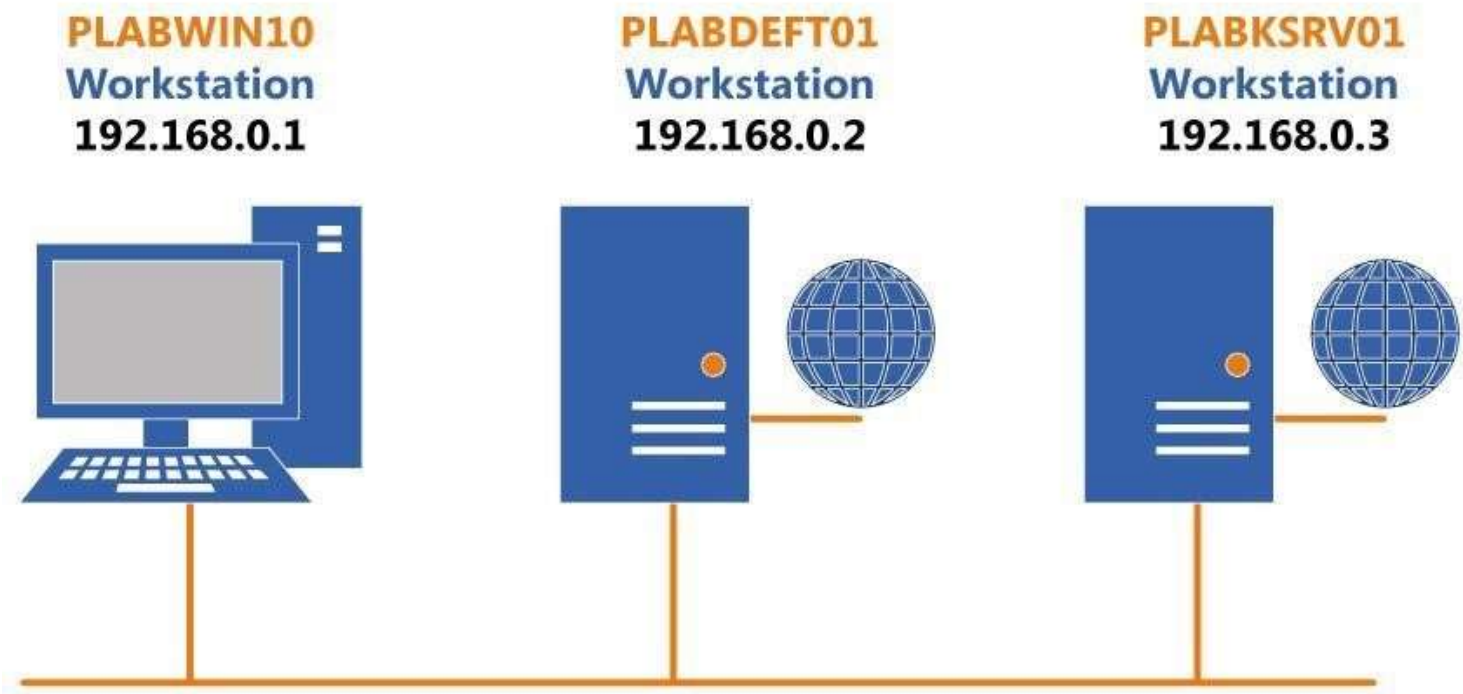
Introduction

The **Working with Windows and CLI Systems** lab provides you with the instructions and devices to develop your hands-on skills in the following topics.

- Exercise 5-1 - Disk Partitions
- Exercise 5-2 - Deleting NTFS Files
- Exercise 5-3 - Examining the Windows Registry
- 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.

Click Next to proceed to the first exercise.

Exercise 5-1 - Disk Partitions

One way to examine a partition's physical level is to use a disk editor, such as Hex Workshop. These tools enable you to view file headers and other critical parts of a file.

Both tasks involve analyzing the key hexadecimal codes the OS uses to identify and maintain the file system. Table 5-1 lists the hexadecimal codes in a partition table and identifies some common file system structures.

Table 5-1 Hexadecimal codes in the partition table

Hexadecimal code	File system
01	DOS 12-bit FAT (floppy disks)
04	DOS 16-bit FAT for partitions smaller than 32 MB
05	Extended partition
06	DOS 16-bit FAT for partitions larger than 32 MB
07	NTFS and exFAT
08	AIX bootable partition
09	AIX data partition
0B	DOS 32-bit FAT
0C	DOS 32-bit FAT for interrupt 13 support
0F	Extended Partition with Logical Block Address (LBA)

17	Hidden NTFS partition (XP and earlier)
1B	Hidden FAT32 partition
1E	Hidden VFAT partition
3C	Partition Magic recovery partition
66–69	Novell partitions
81	Linux
82	Linux swap partition (can also be associated with Solaris partitions)
83	Linux native file systems (Ext2, Ext3, Ext4, Reiser, Xiafs)
86	FAT16 volume/stripe set (Windows NT)
87	High Performance File System (HPFS) fault-tolerant mirrored partition or NTFS volume/stripe set
A5	FreeBSD and BSD/386
A6	OpenBSD
A9	NetBSD
C7	Typical of a corrupted NTFS volume/stripe set
EB	BeOS

In some instances, you might need to identify the OS on an unknown disk. When the operating system has been identified, it will be easier for data forensics to determine the applicable tool to read the data in the disk volume.

Task 1 - Using Hex Workshop

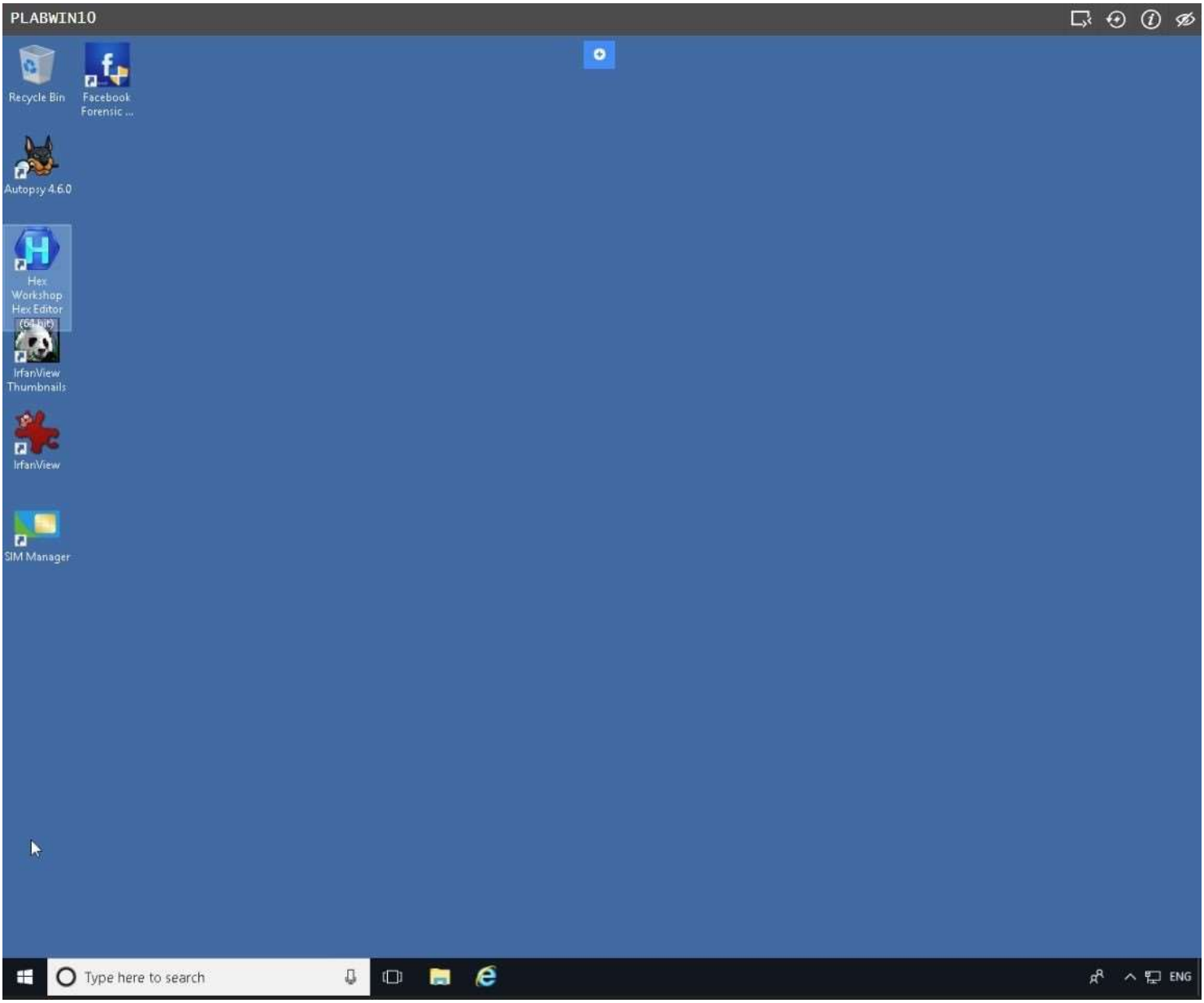
You will use Hex Workshop or another hexadecimal editor, for this task. The following steps show you how to determine a disk's OS by using Hex Workshop:

Step 1

Ensure that you have powered on the required devices indicated in the Introduction.

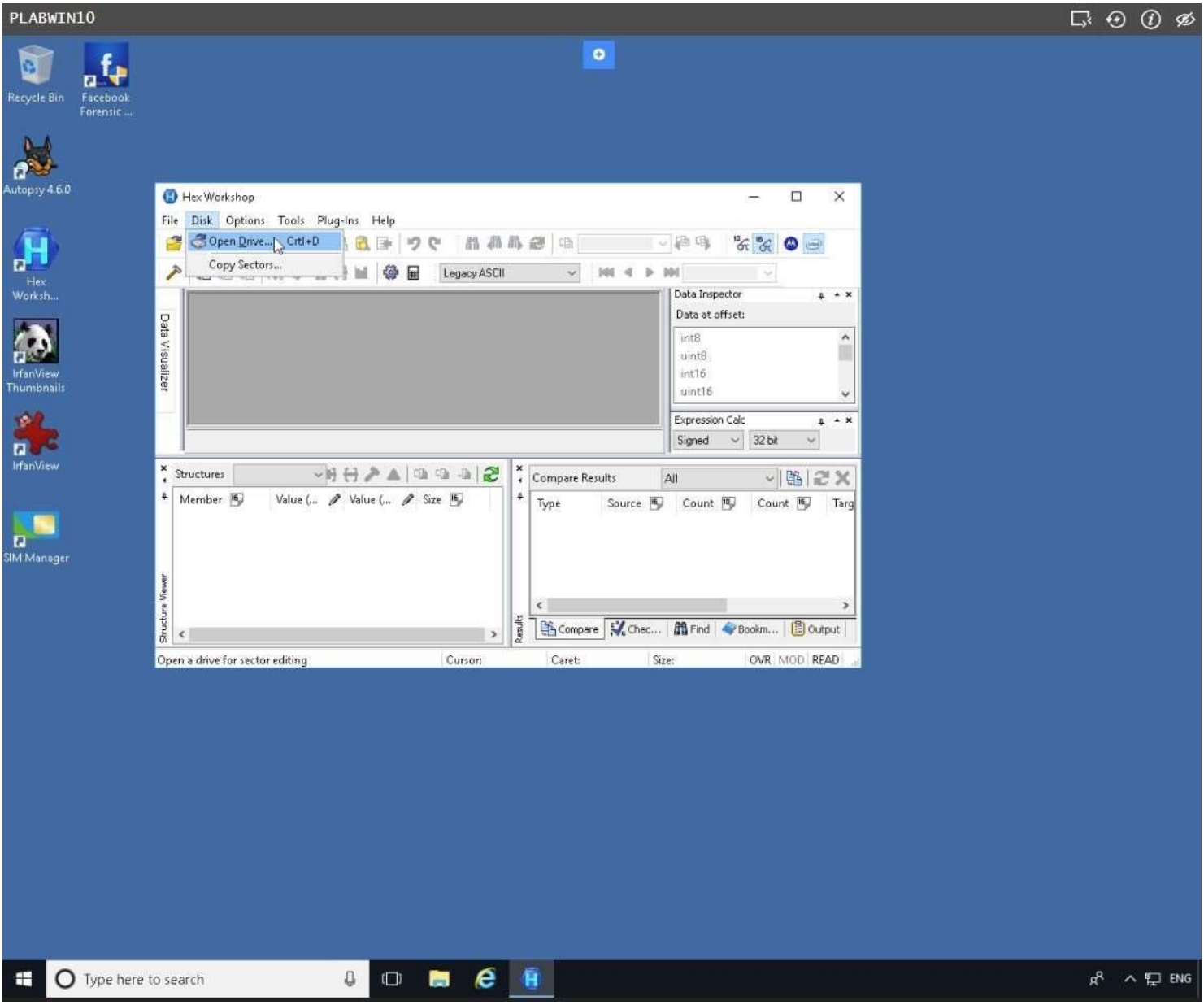
Connect to **PLABWIN10** device.

Once the device has powered back on launch **Hex Workshop** application from desktop.



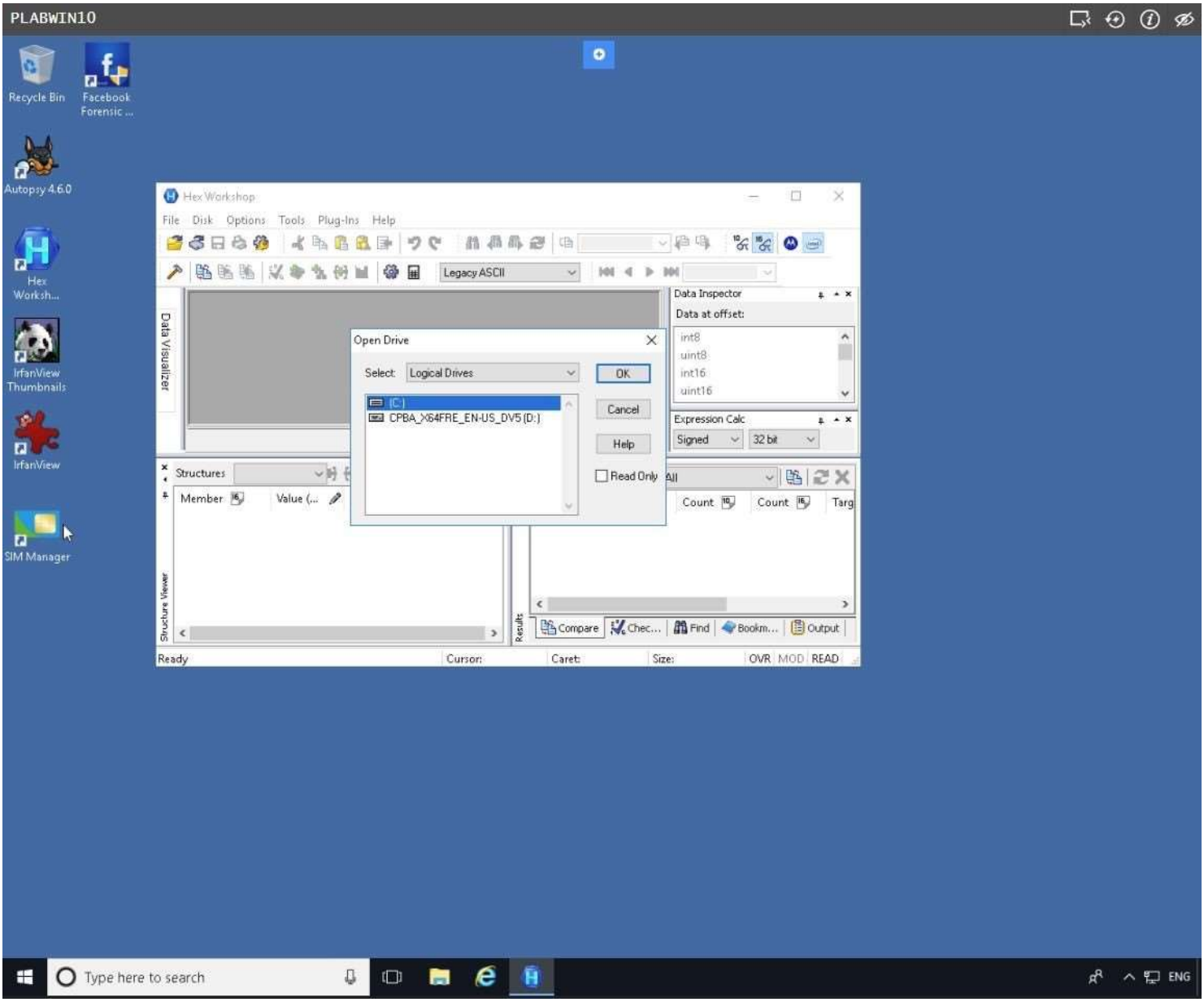
Step 2

When Hex Workshop application opens, click **Disk** from the menu and select **Open Drive**... Click Yes in the UAC.



Step 3

On the Open Drive dialog box, select [C:] drive (or your working drive), and click **OK**.

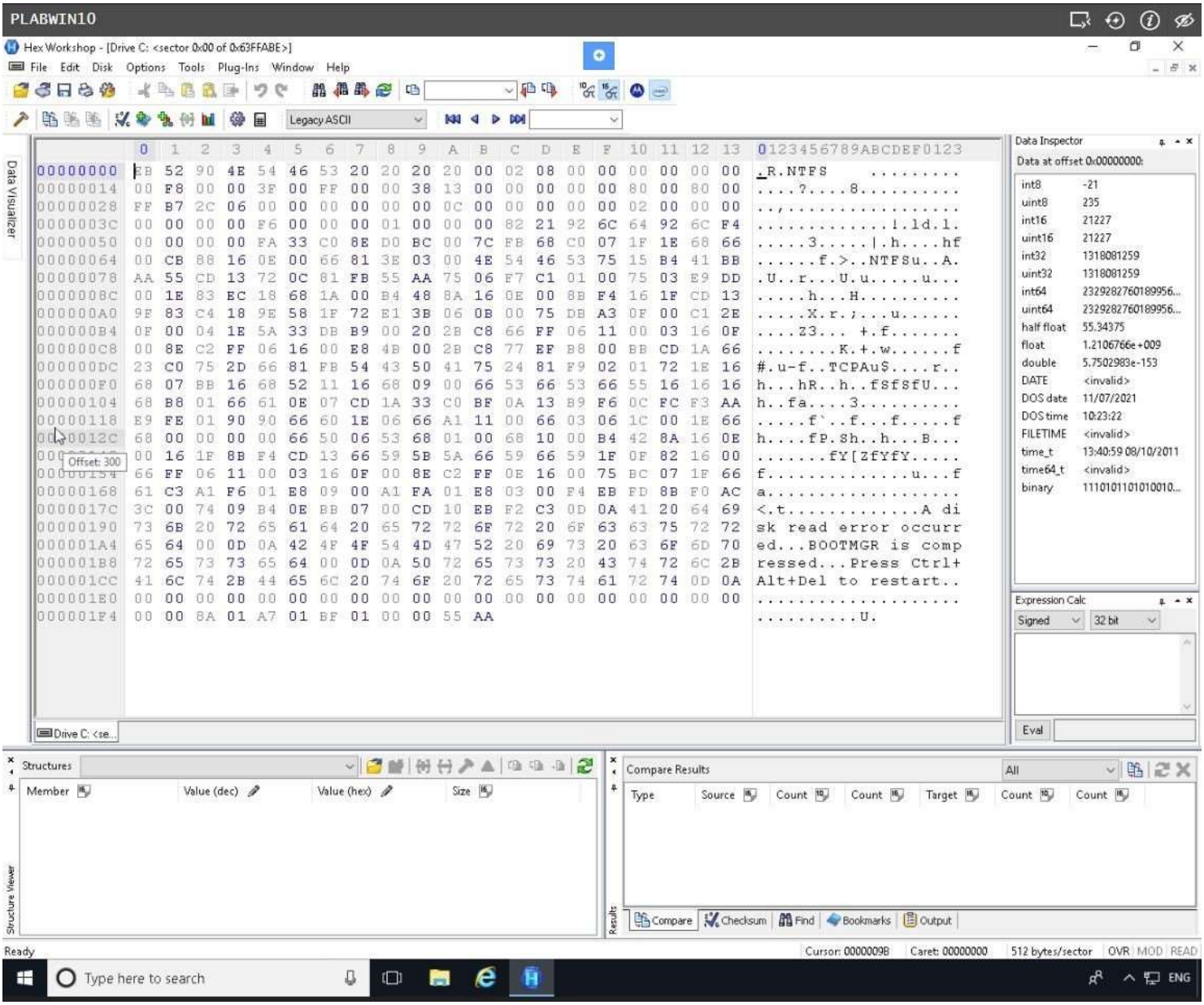


Step 4

Hex Workshop shows a typical hard disk in the Hex Workshop window.

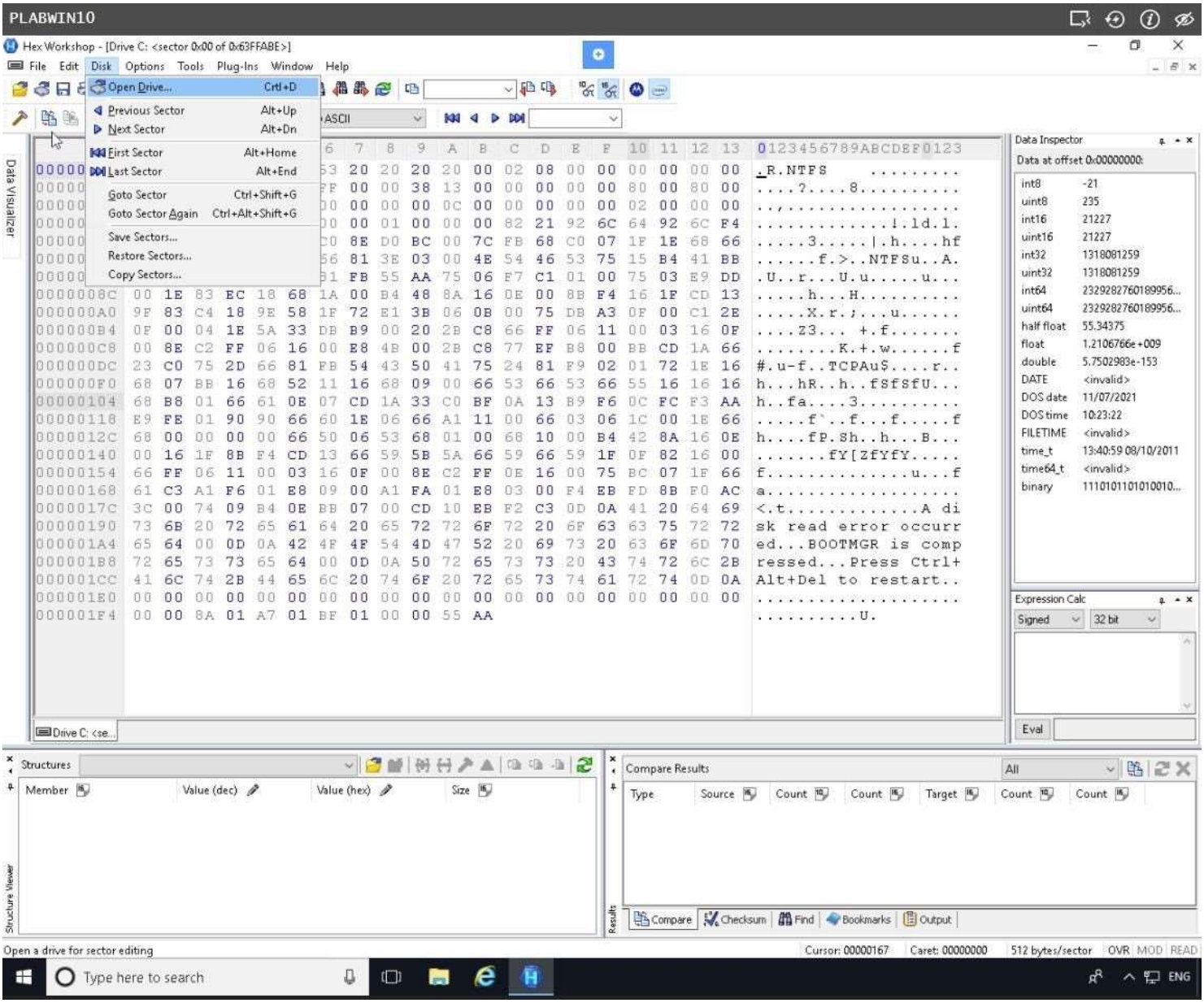
> *Note: If an error message is displayed, you can ignore it because it won't affect your analysis for this activity.*

The C drive displays "**.R.NTFS**" if the partition is formatted as an NTFS drive. If it's a FAT drive, it displays MSDOS5.0 or MSWIN4.1 in the first logical sector, which is sector 0 of the partition. Note that the physical drive's sector 0 is the drive's boot sector and is not associated with the partition's sector 0 location.



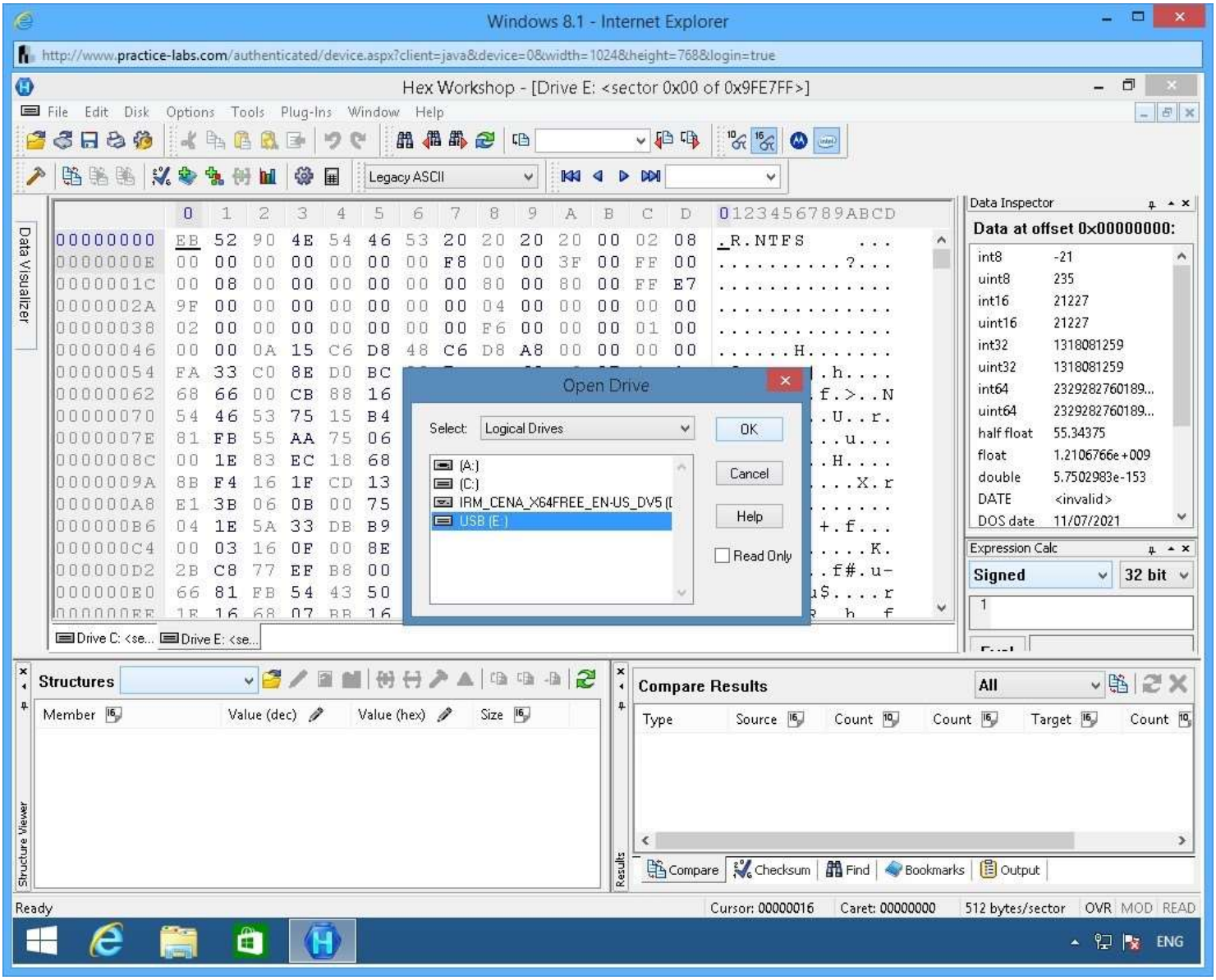
Step 5

Click **Disk** menu and select **Open Drive**.



Step 6

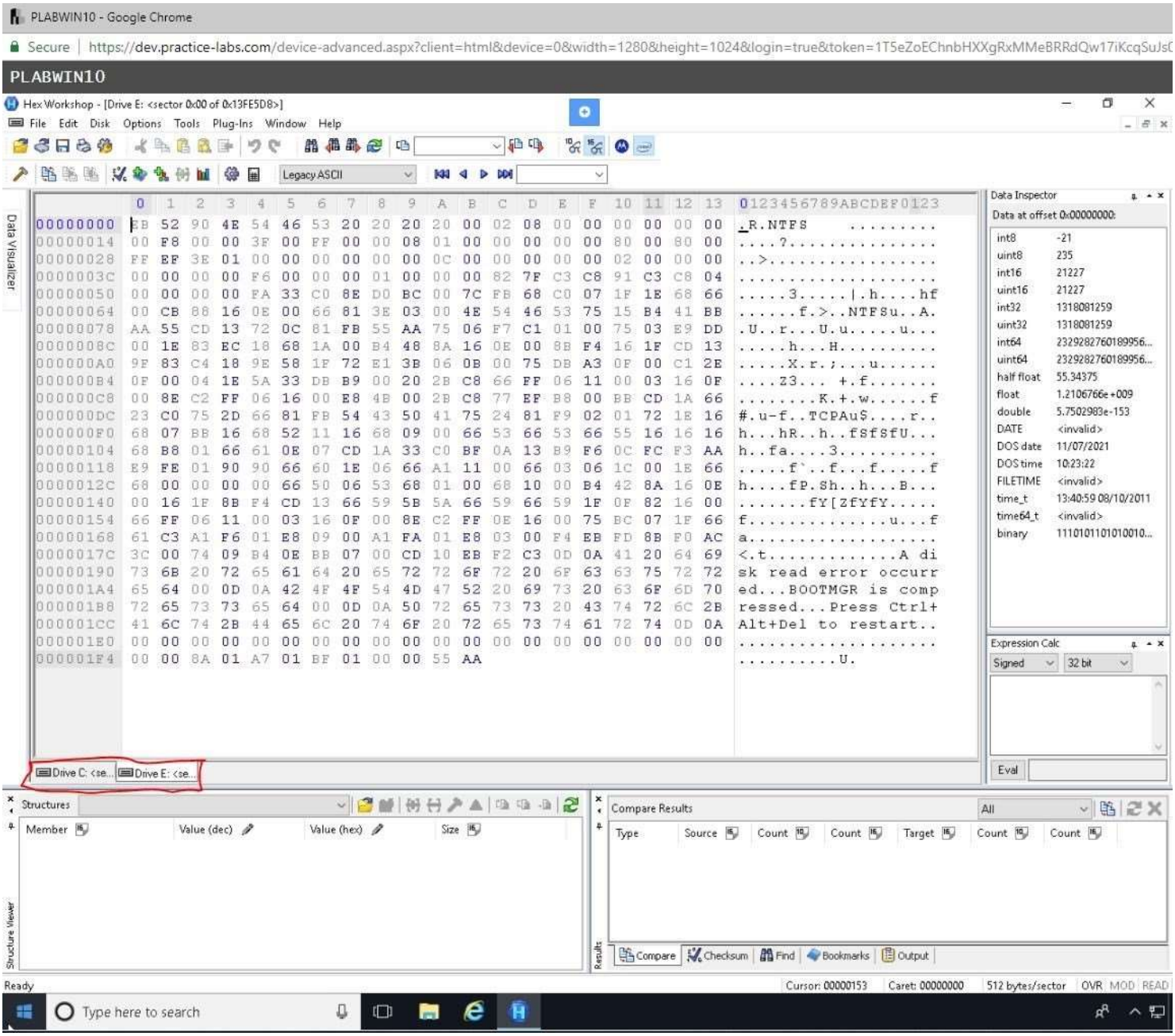
On the **Open Drive** dialog box, click **USB [E:]** drive and click **OK**.



Step 7

Using the folders tab in the middle, compare drives **C** and **E**.

Leave **Hex Workshop** open for the next activity.



Task 2 - Inspect another drive

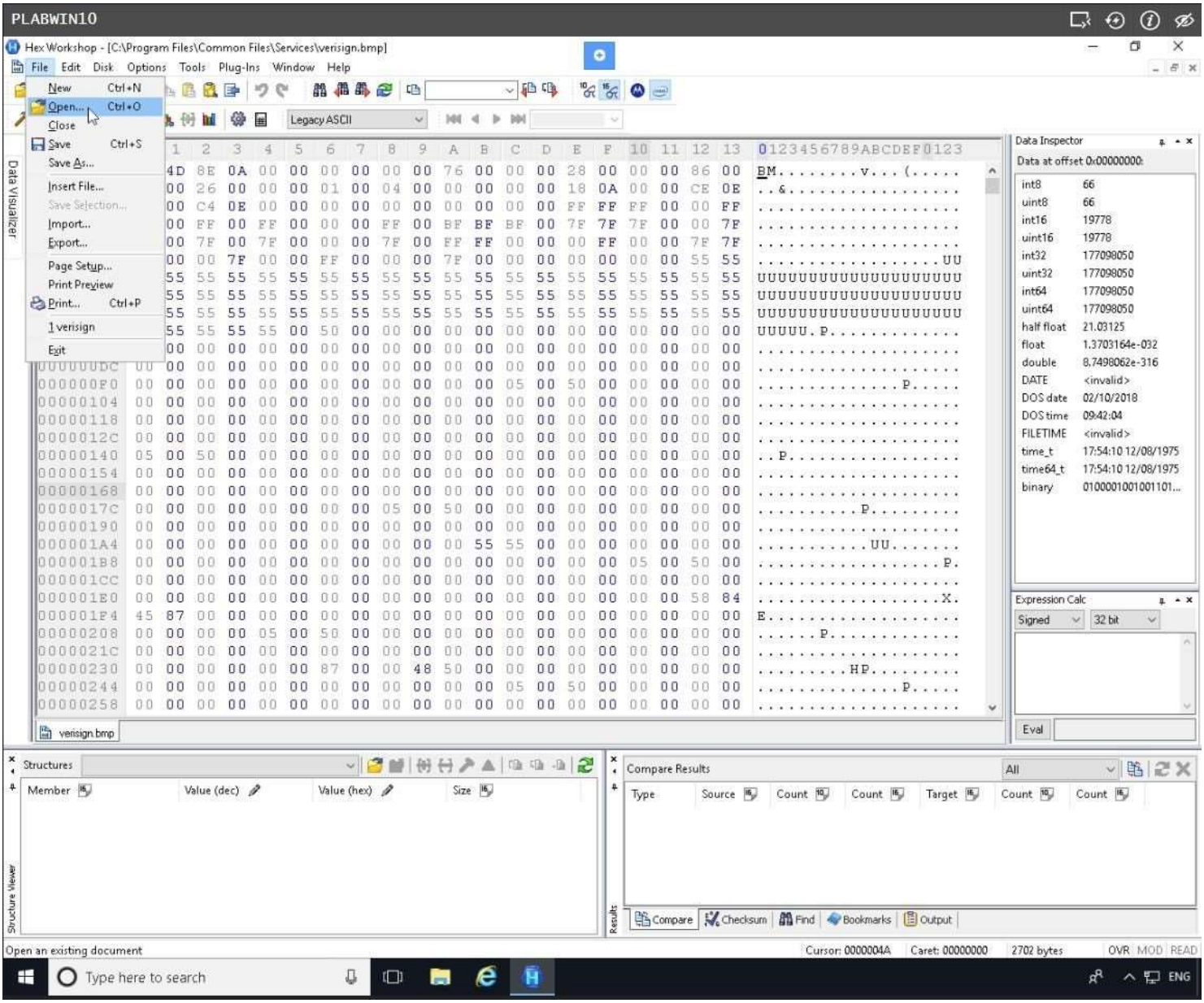
With tools such as Hex Workshop, you can also identify file headers to determine the file types, with or without an extension.

In this task, you will browse for a bitmap file in File Explorer and a Word document (.doc). (In the Hands-On Projects, you apply these techniques to other file types.) Then follow these steps:

Step 1

On **PLABWIN10**, **Hex Workshop** application is open.

Click **File** and select **Open**.

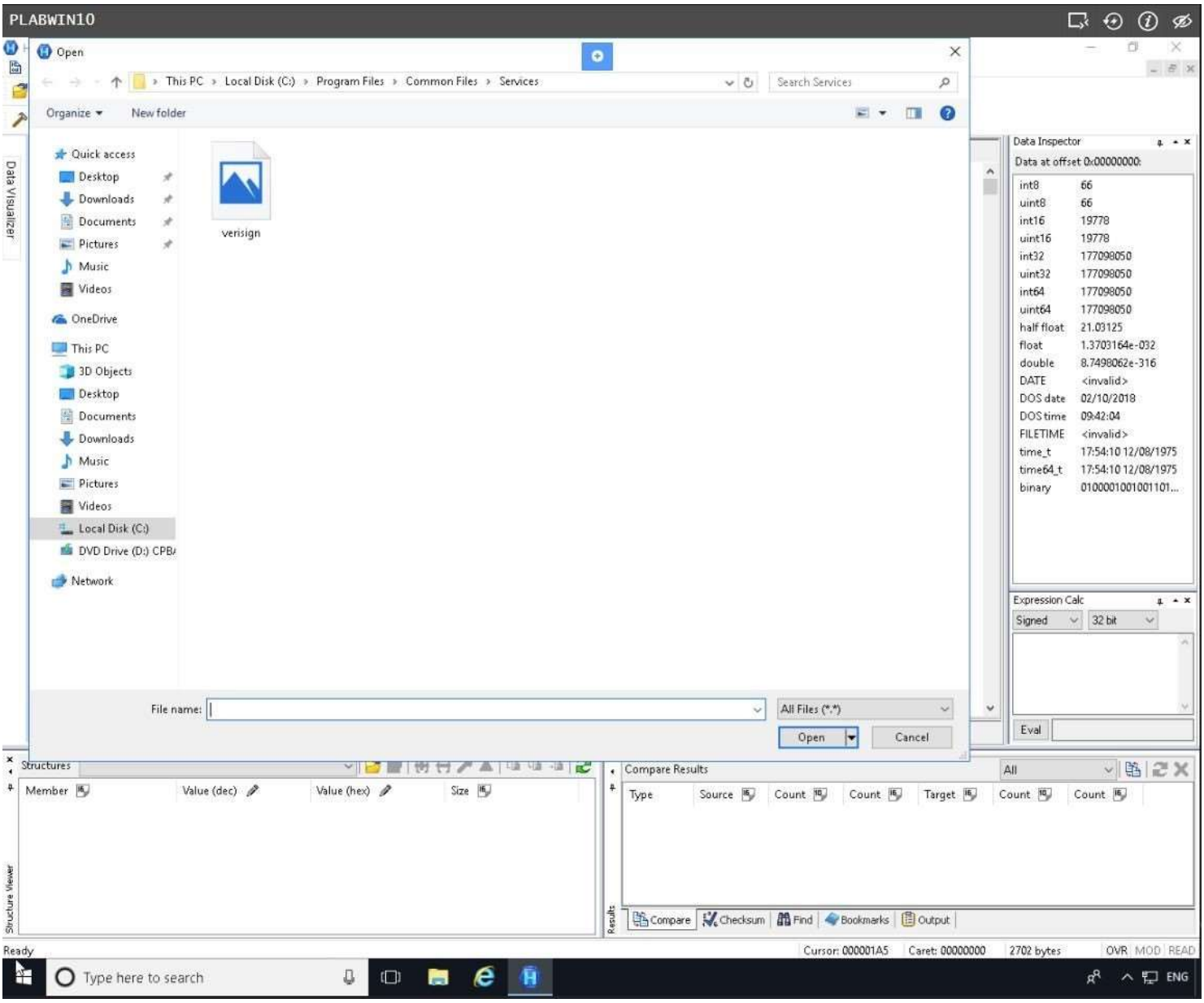


Step 2

On the **Open** dialog box, expand **Local Disk (C:) > Program Files > Common Files** then click **Services** folder.

Select **verisign** bitmap and click **Open**.

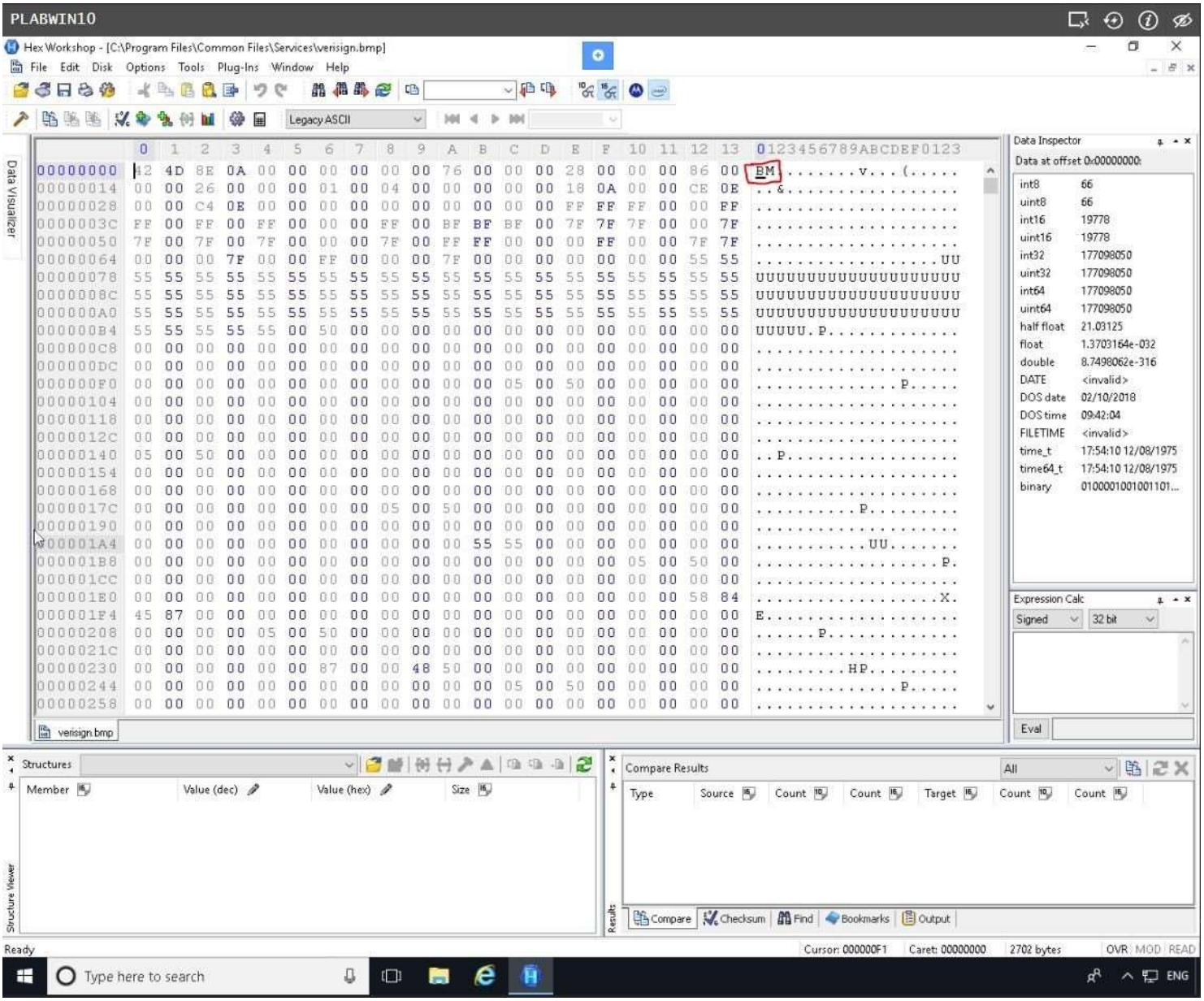
> *Note: If you get a Hex Workshop evaluation warning message, click OK to continue.*



Step 3

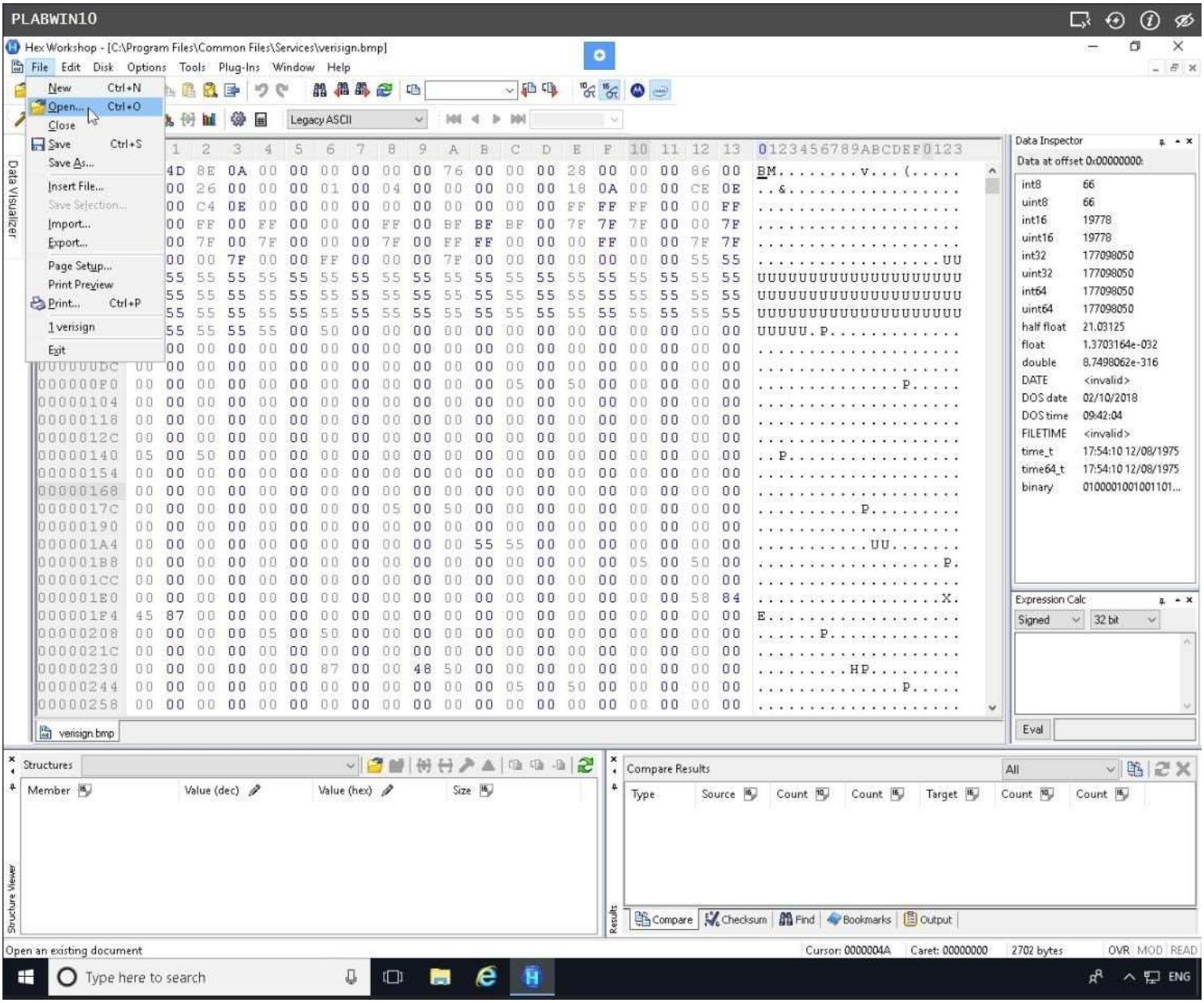
The Hex Workshop window identifies the file type for the graphic.

For .bmp files, it shows “**BM6**,” “**BM**,” or “**BMF**” as shown in the screenshot to indicate a BM file signature.



Step 4

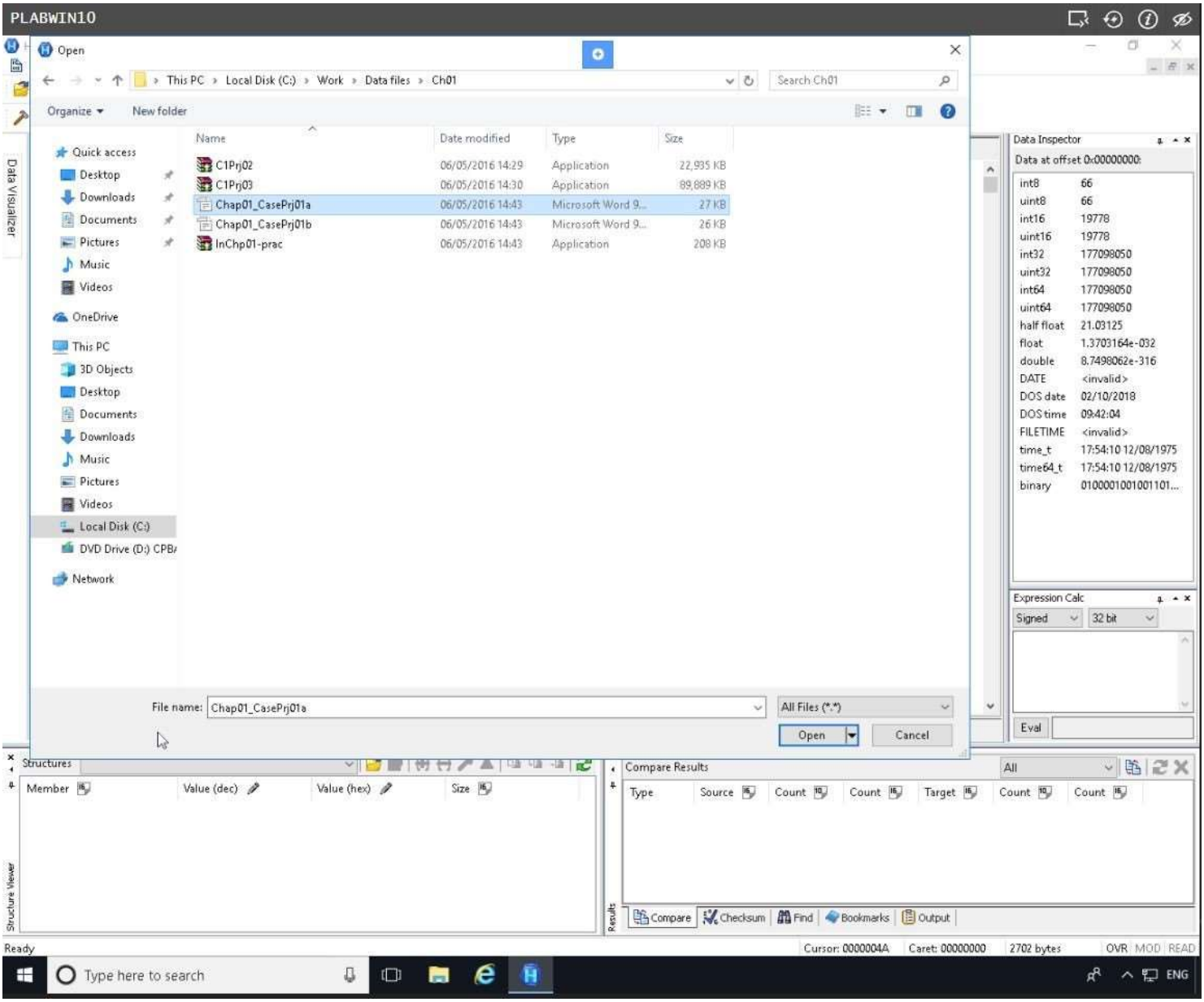
To open an Office 2003 or later Word document, click **File**, select **Open** from the menu.



Step 5

On the **Open** dialog box, expand **Local Disk C > Work > Data files** and click **Ch01** folder.

Select **Chap01_CasePrj01a** document file and click **Open**.

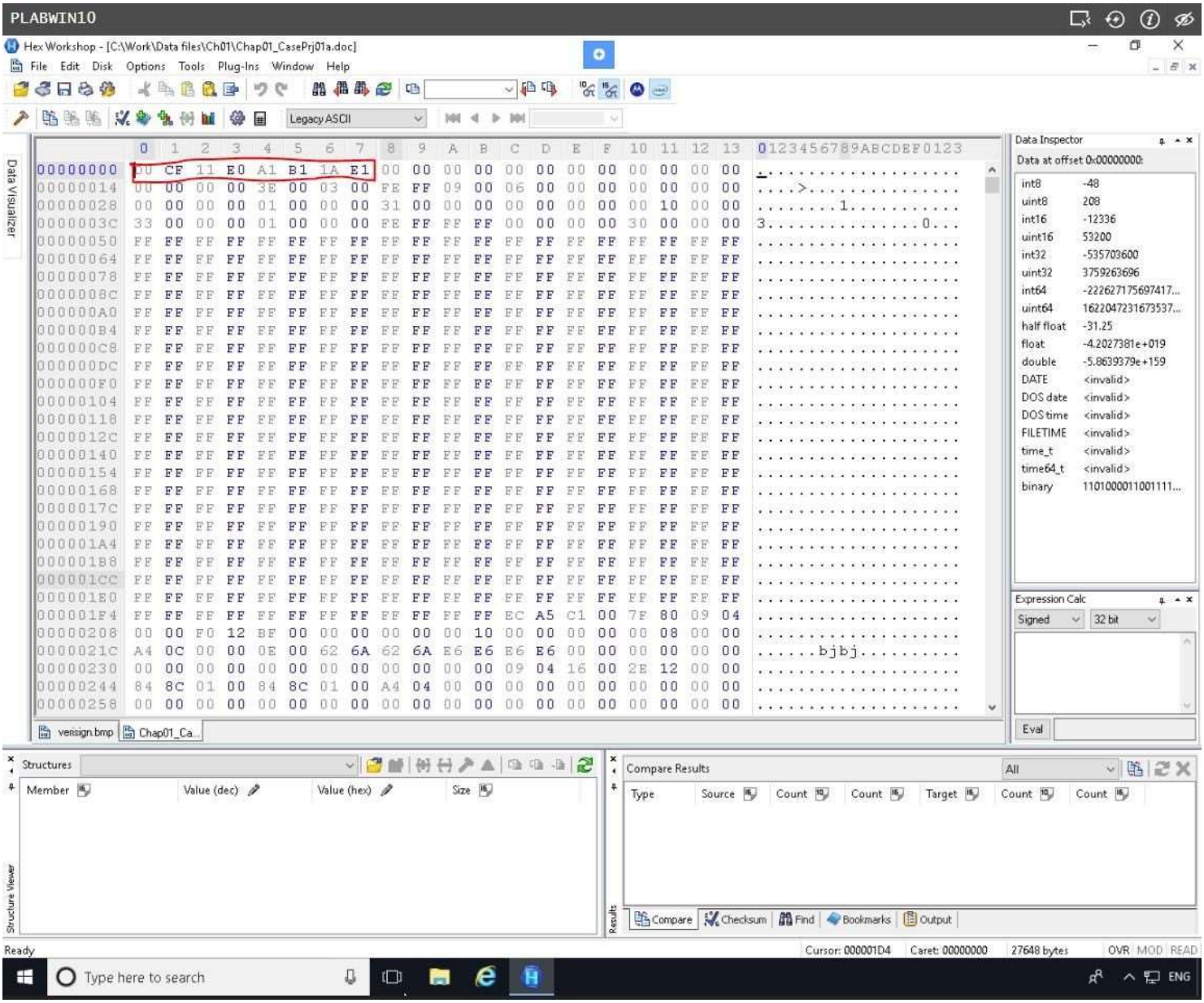


Step 6

As shown in screenshot, the first line contains a row of 0s followed by "**D0 CF 11 E0 A1 B1 1A E1**," which identifies the file as a Microsoft Office (before Office 2007) document.

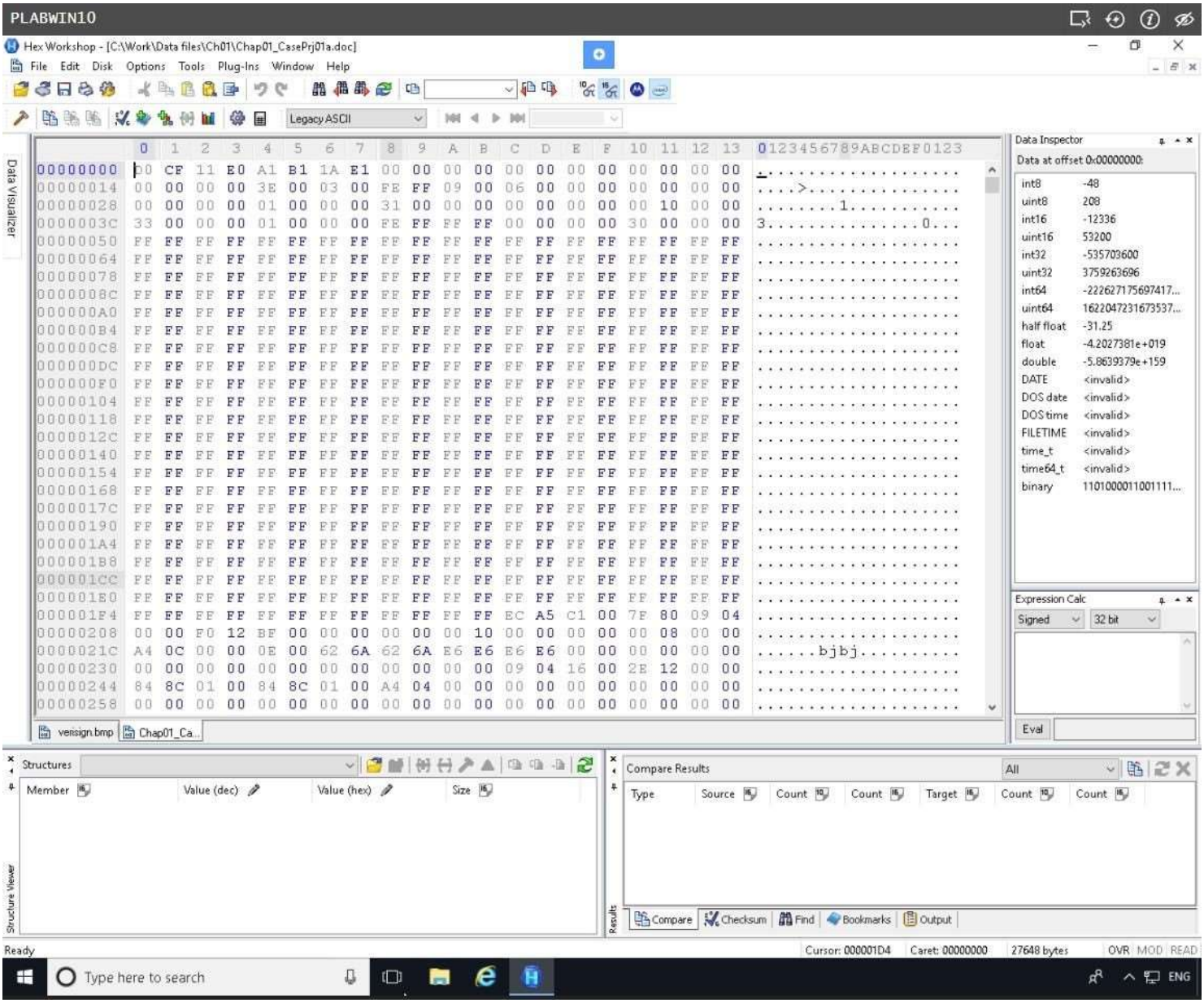
The same file header is displayed for an Excel or a PowerPoint file but doesn't apply to Access databases. For Microsoft Office 2007 and later, the first two characters are "PK" or "OOXML," which represent a compressed file.

> *Note: Depending on the hexadecimal editor being used, hex values can be grouped in sets of two or four digits.*



Step 7

Exit **Hex Workshop** application by clicking the [X] button.



Keep the device powered on in their current state and proceed to the next exercise.

Exercise 5-2 - Deleting NTFS Files

Typically, you use Windows or File Explorer to delete files from a disk. When a file is deleted in Windows NT and later, the OS renames it and moves it to the Recycle Bin. Another method is using the del (delete) MS-DOS command. This method doesn't rename and move the file to the Recycle Bin, but it eliminates the file from the Master File Table - MFT listing in the same way FAT does.

When you delete a file in Windows or File Explorer, you can restore it from the Recycle Bin.

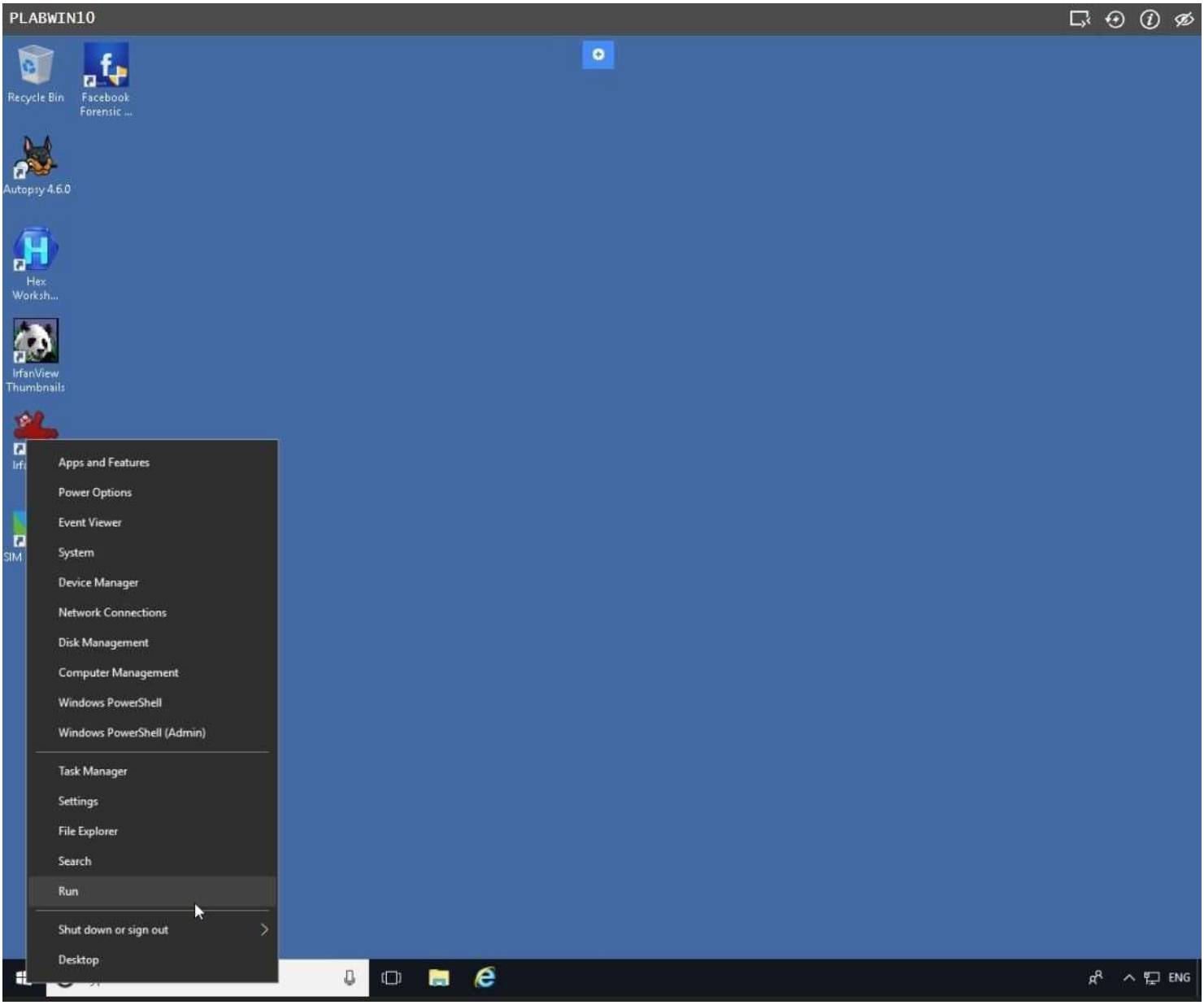
Task 1 - Collect User SID

Within the Windows operating system, a user and group account are uniquely identified with a string called security identifier (SID). Whenever a user or group is created in Windows, an SID is assigned to the account. If the account is deleted, the SID is retired and never reused. Therefore, all privileges and permissions granted to the deleted account are permanently revoked and will have to be re-assigned should the account be re-created. An SID is assigned to built-in user account like administrator and guest.

In this task, you will use the SID of the local administrator account.

Step 1

On **PLABWIN10** device, right-click **Start** and select **Run**.

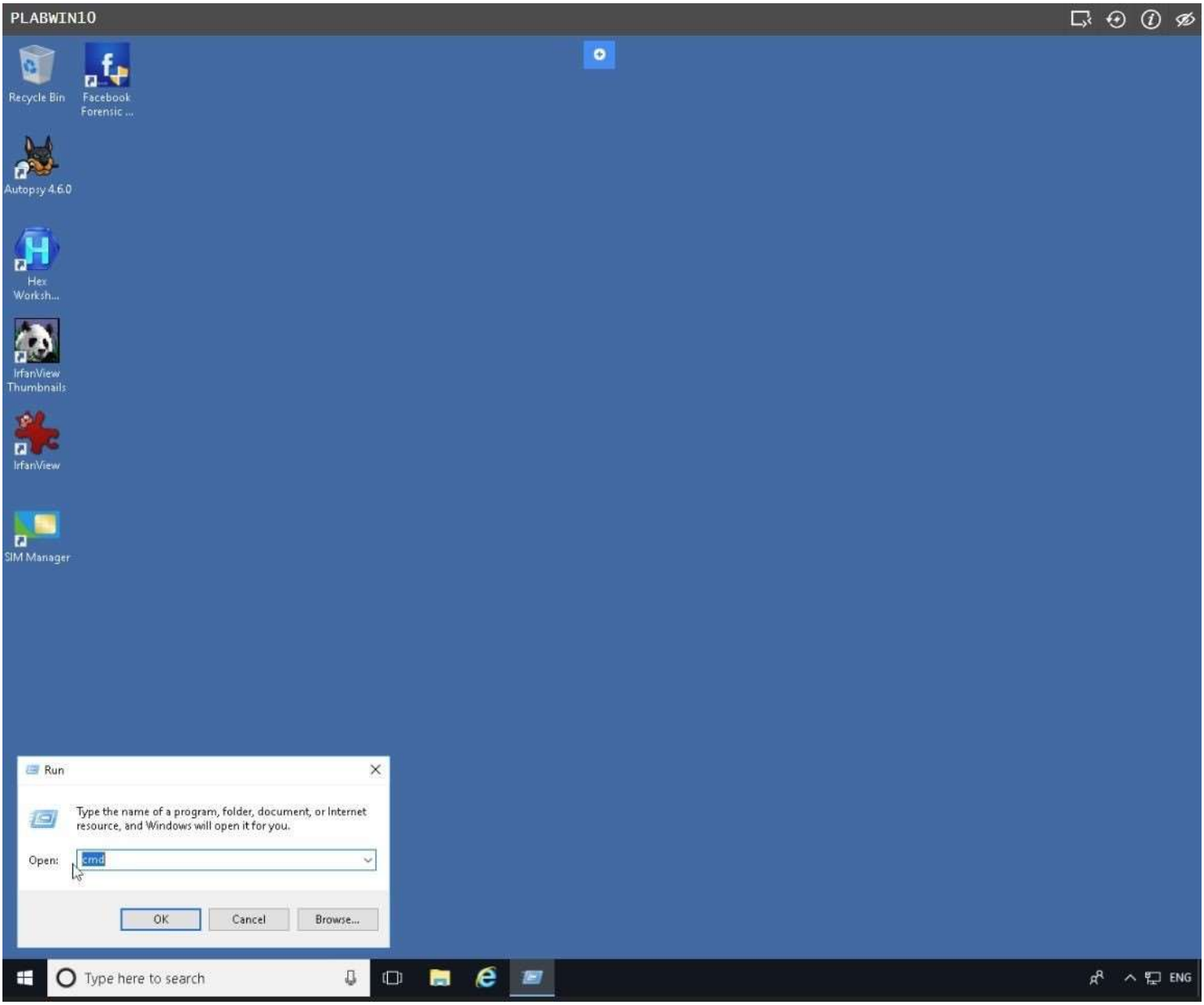


Step 2

On the **Run** dialog box, type:

```
Cmd
```

Press **Enter**.

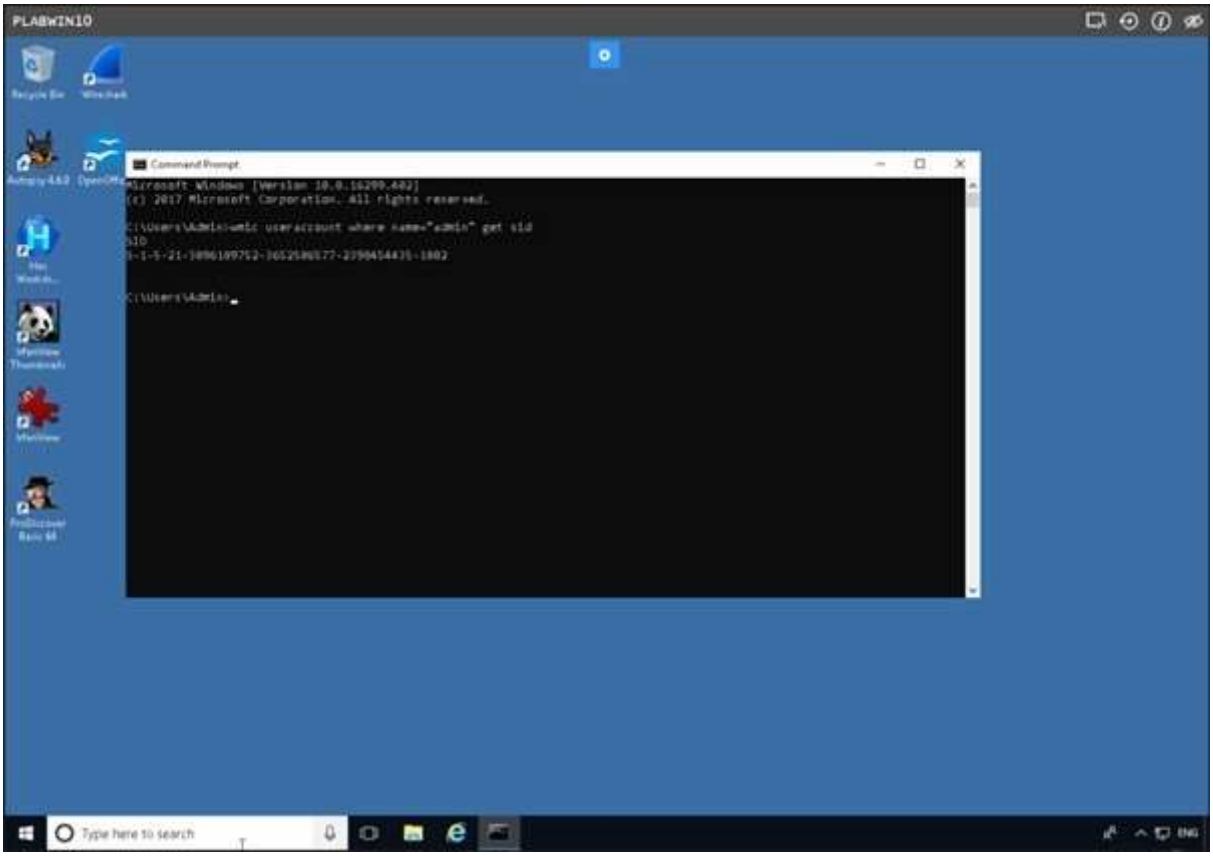


Step 3

On the command prompt, type:

```
wmic useraccount where name=”admin” get sid
```

Press **Enter**.

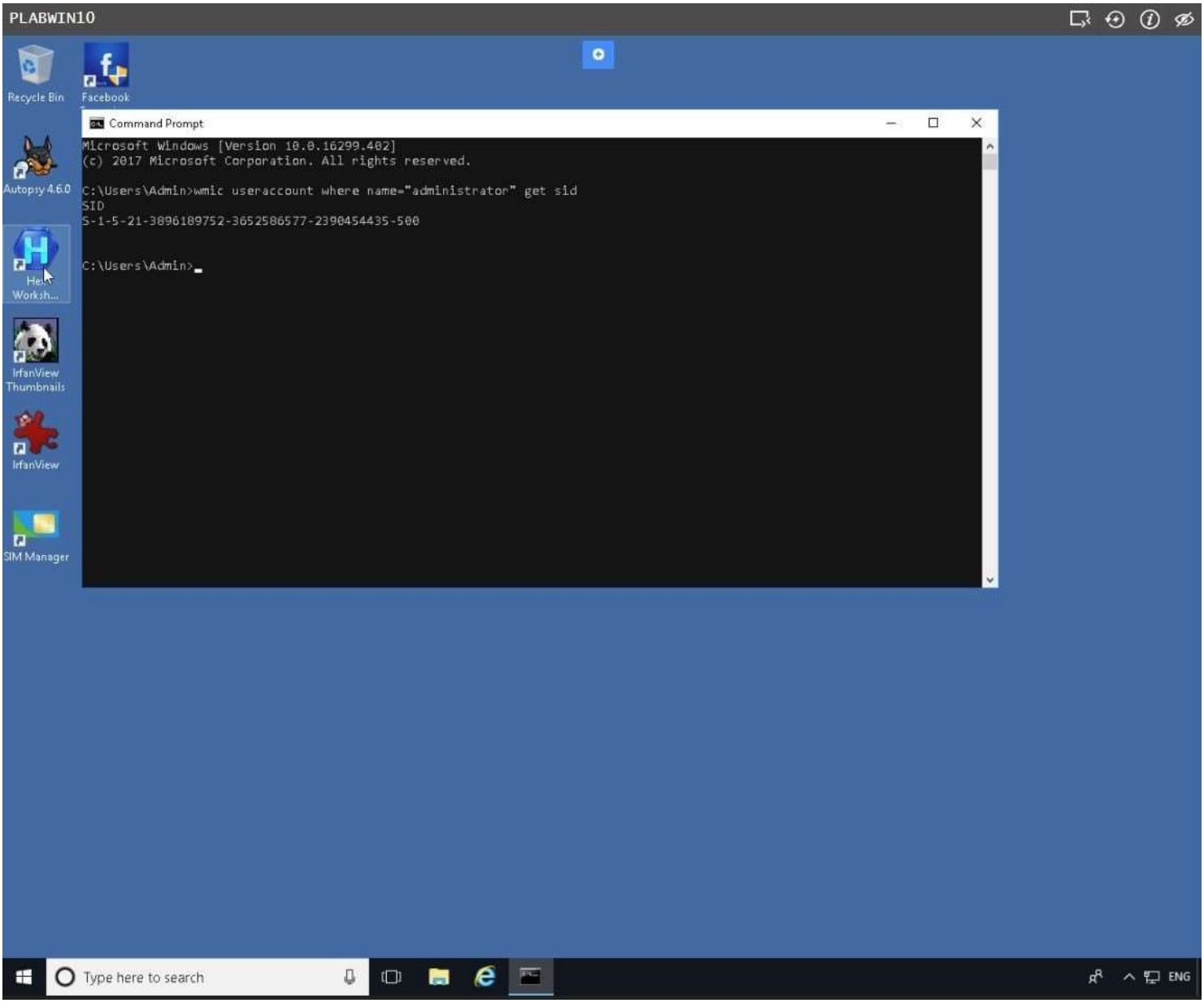


Step 4

The SID of the local administrator is displayed. Observe the returned SID.

Please note that in your lab the SID value may slightly differ. The administrator SID ends with the number **1002**.

Minimize **command line** window.



Task 2 - Viewing Deleted Files

There are a number of ways to view deleted files in Windows. In this task, you will delete some files and view them using a computer forensics tool like OSForensics.

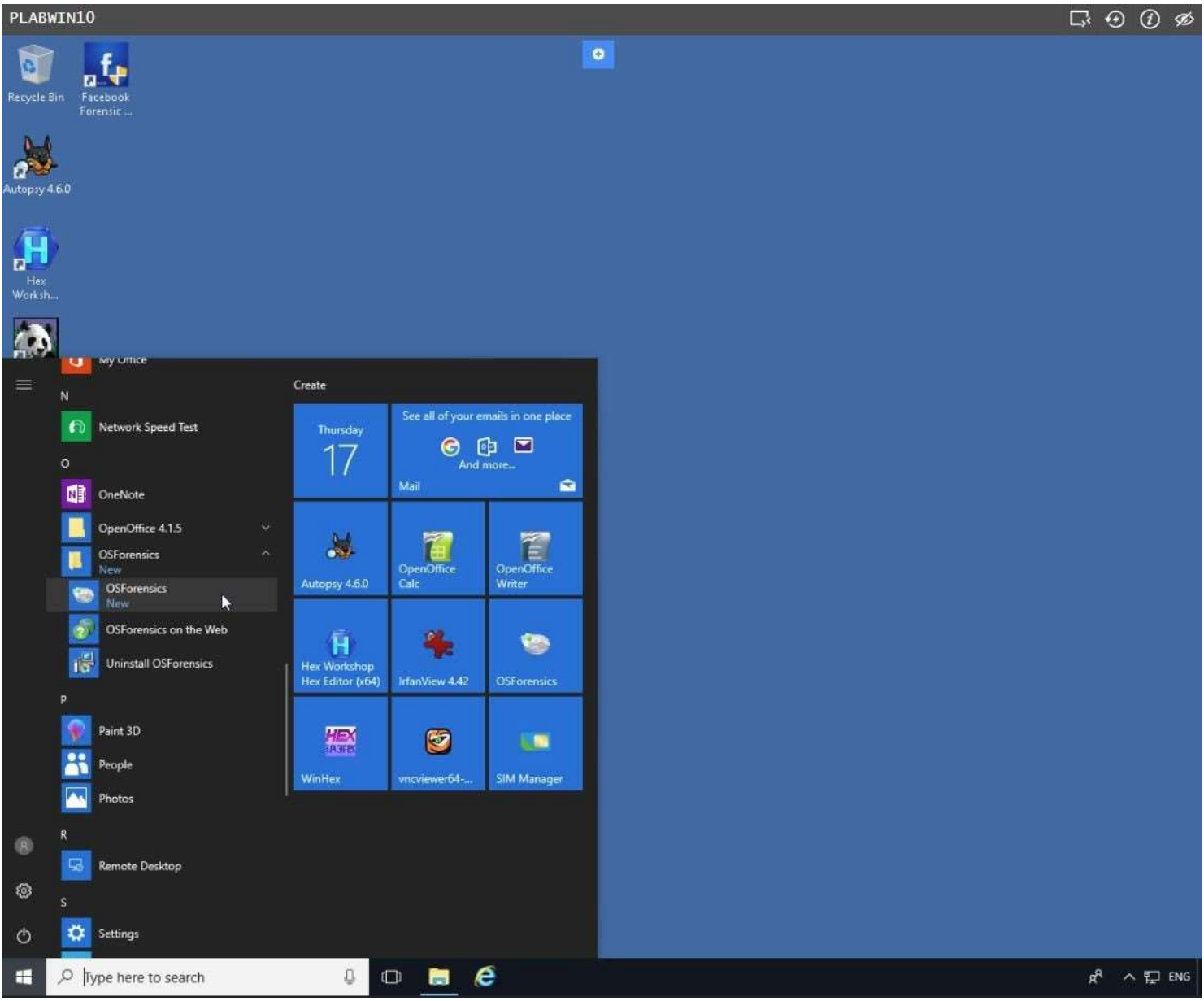
To view deleted files, perform the following steps:

Step 1

Ensure that you have powered on the required devices in the Introduction.

Connect to **PLABWIN10** and install **OSForensics** from **Tools and resources** on the intranet.

Click **Start**, scroll down to **OSForensics**, then click **OSForensics**.

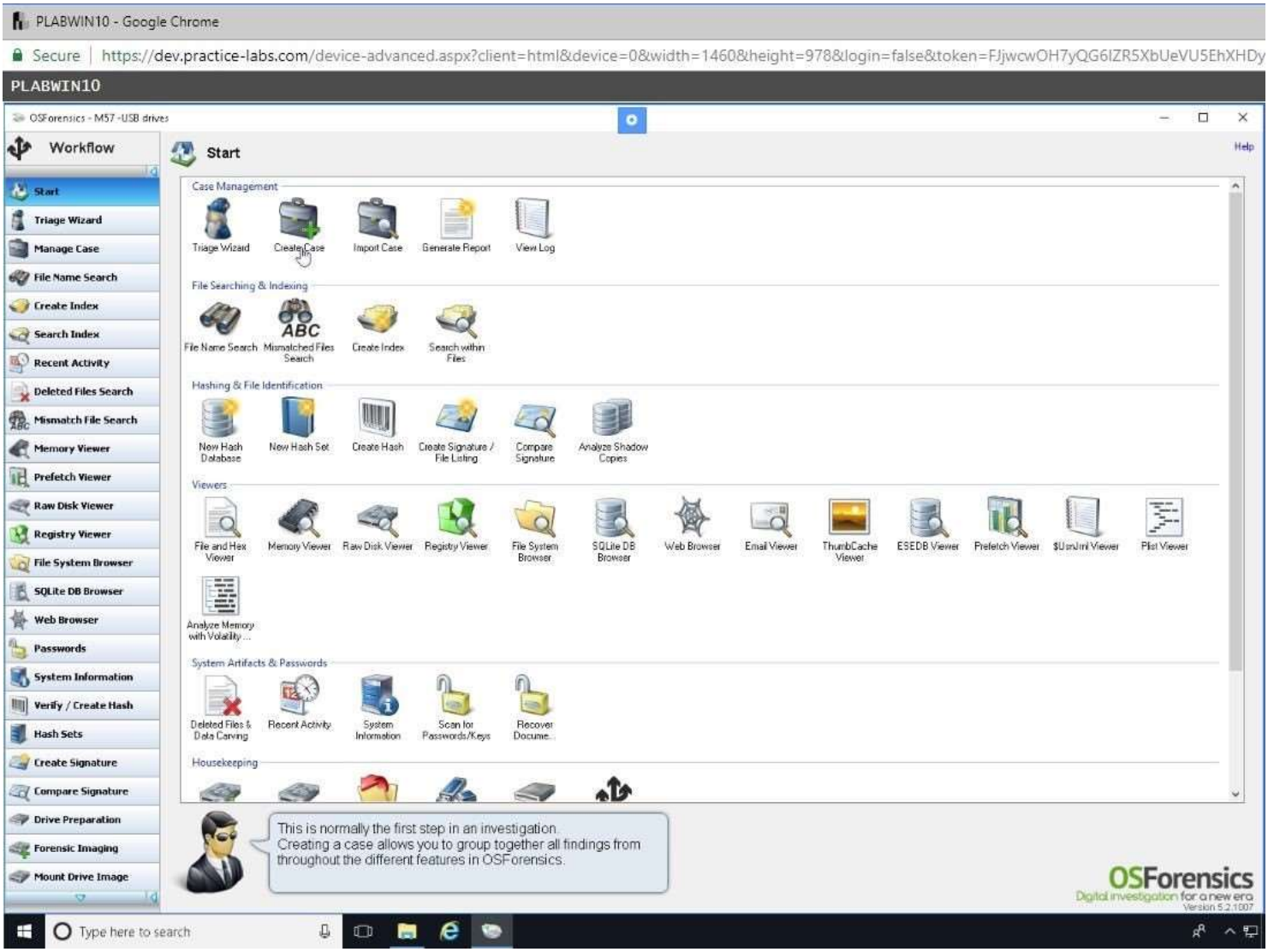


Step 2

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

Step 3

On the **OSForensics** window, under the **Start > Case Management** section click **Create Case**.

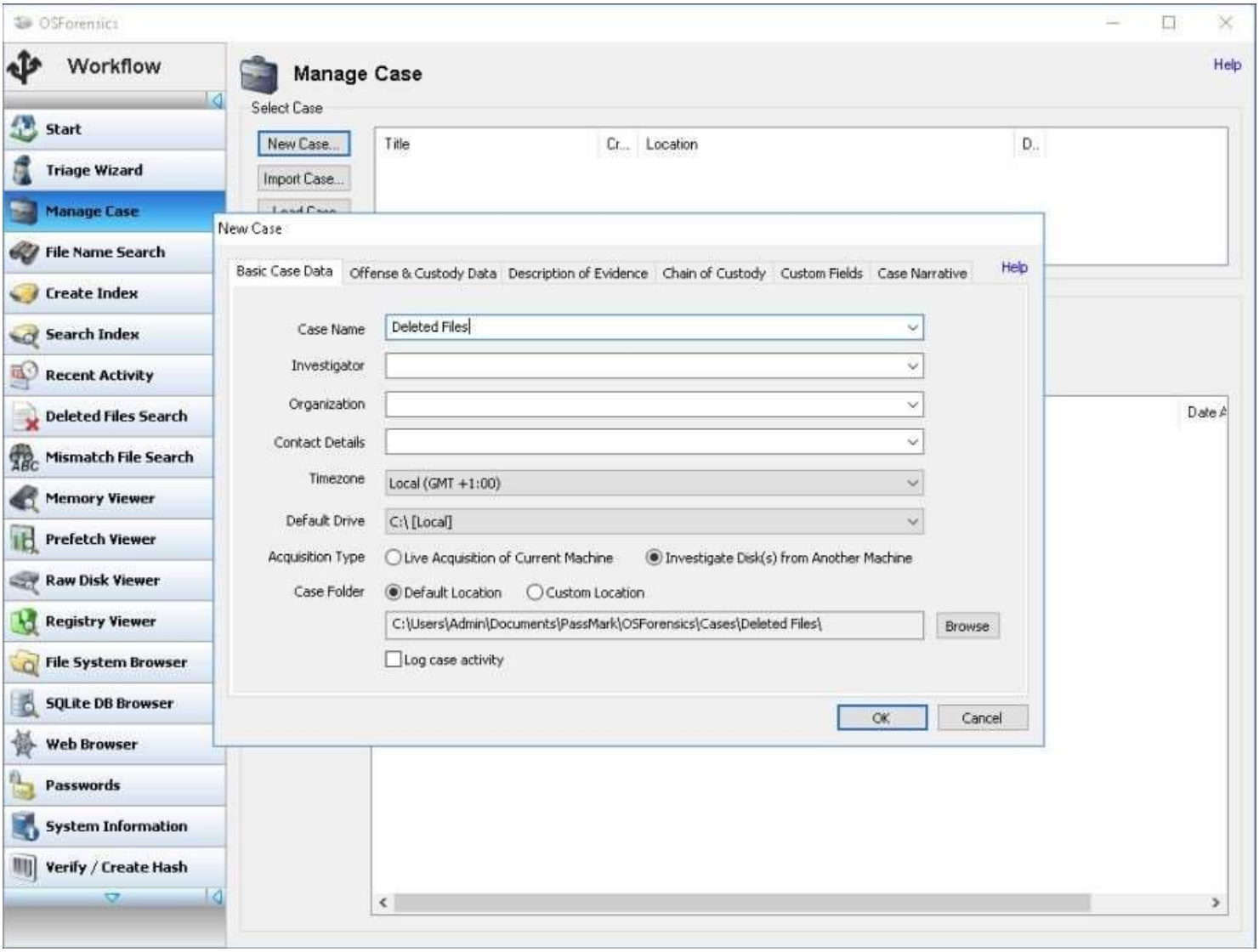


Step 4

The **New Case** dialog box is displayed. In the **Case Name** text box, type:

```
Deleted Files
```

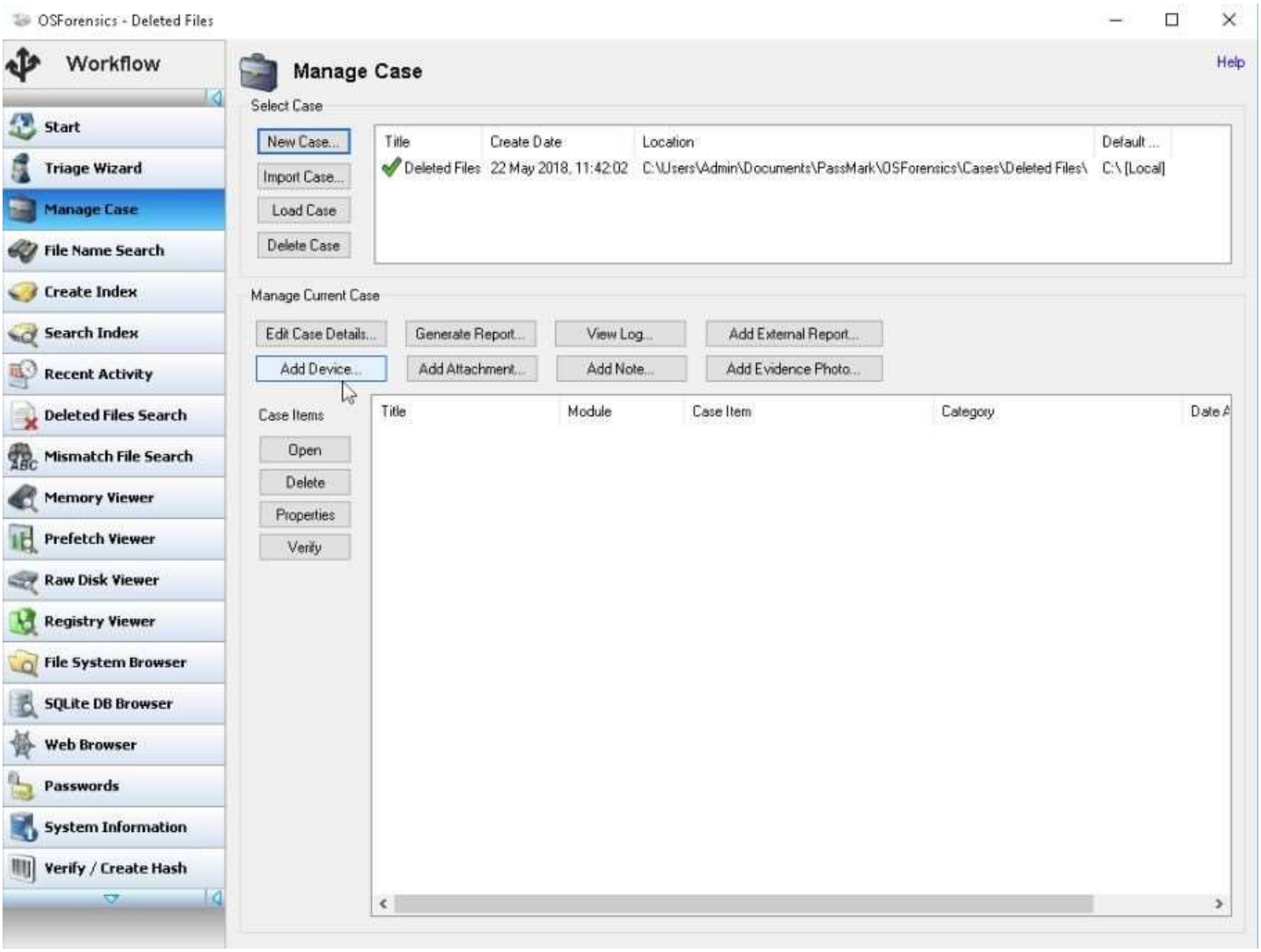
Keep the other fields blank and click **OK**.



Step 5

The **Manage Case** is now selected.

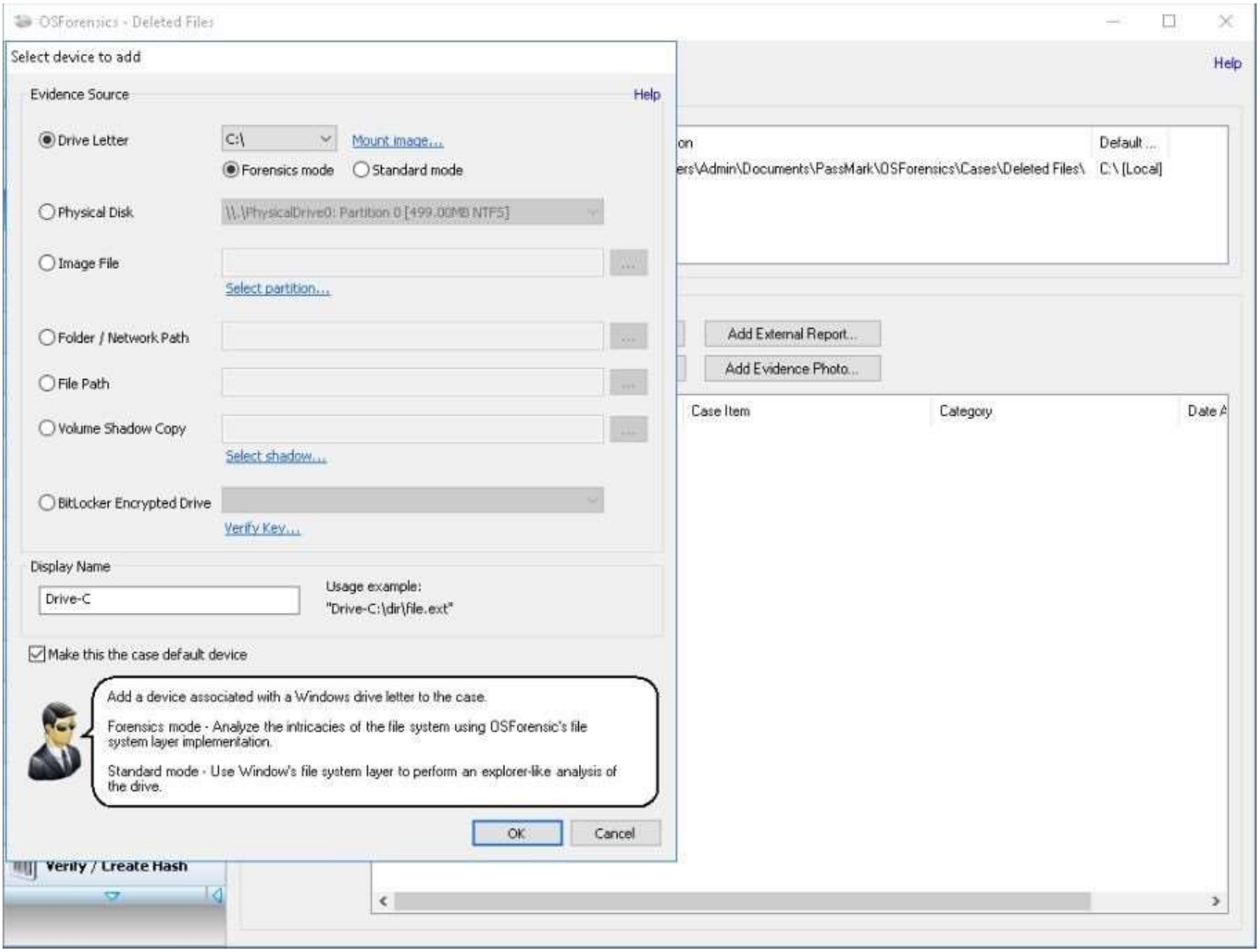
Under the **Manage Current Case** section, click **Add Device**...



Step 6

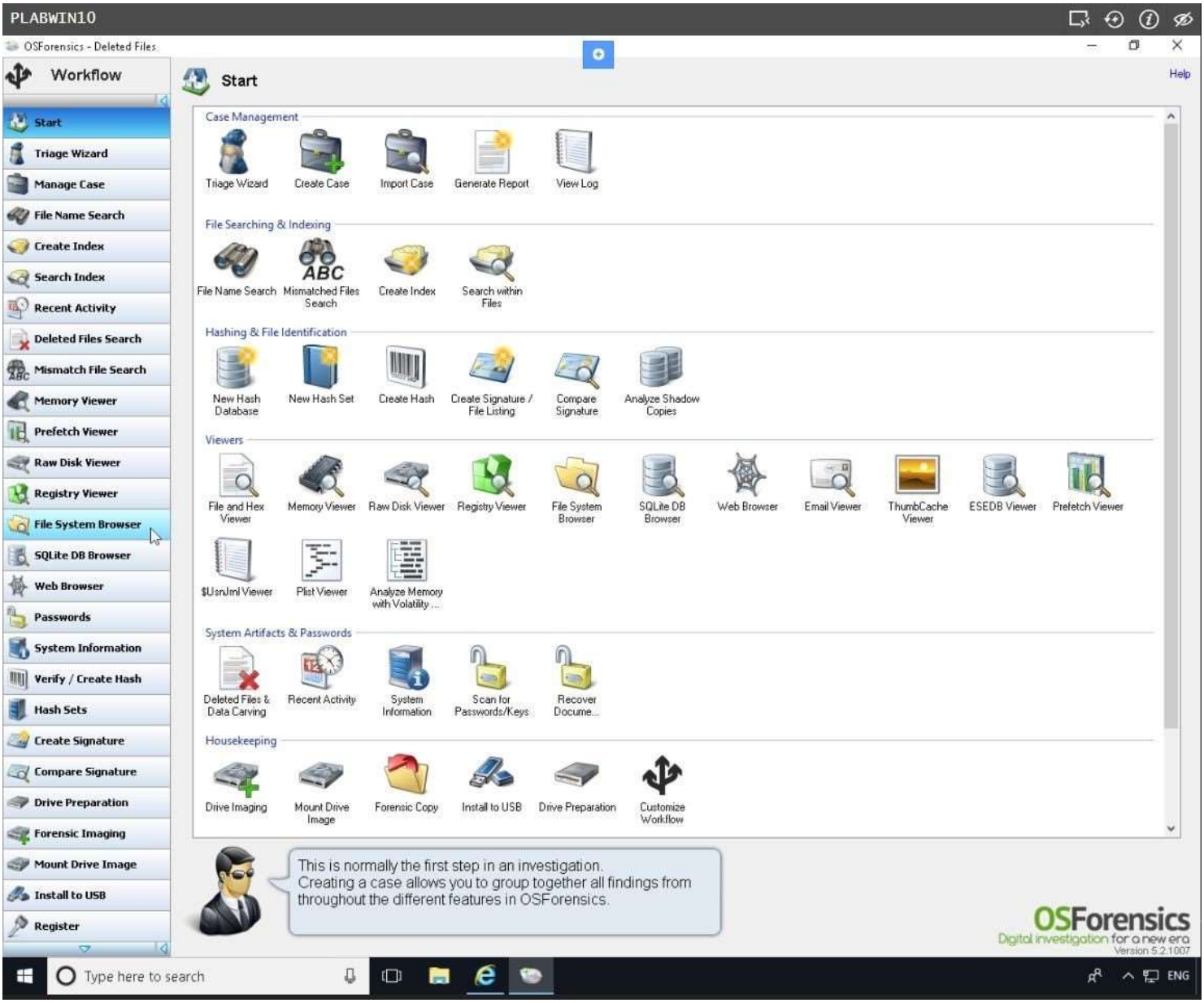
On the **Select device to add** dialog box, ensure that **Drive Letter** option button is selected and **C:** is displayed in the drop-down list.

Click **OK**.



Step 7

Back on the **Manage Case** window, locate the left panel and click **File System Browser**.



Step 8

The **File System Browser** window opens.

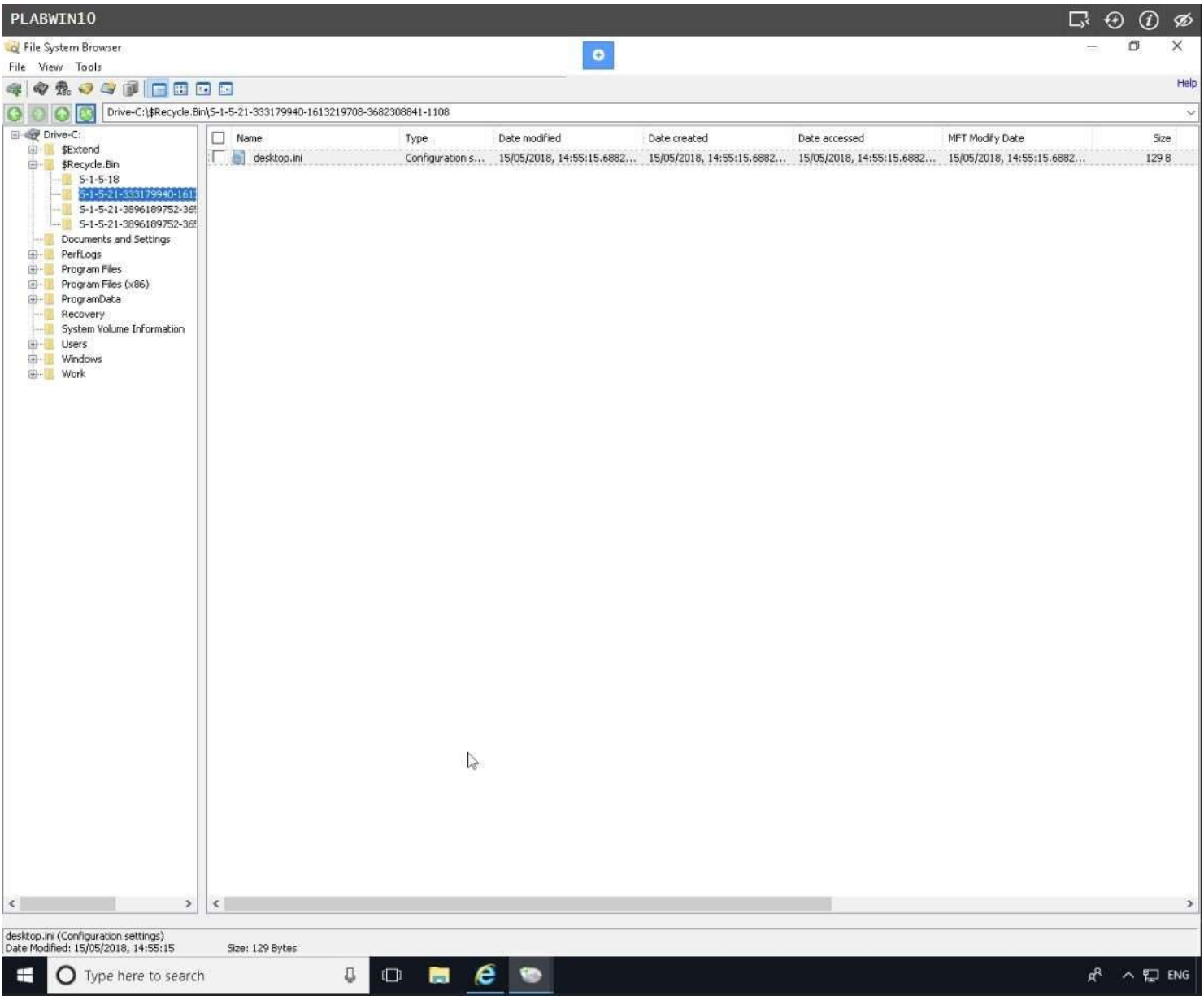
Expand **Drive-C:** node.

Then click **$Recycle.Bin** > **S-1-5-21-xxx...** Move the line at the center to be able to see the SID.

Where **S-1-5-21-xxx** the SID value of the administrator that was displayed in a task you performed earlier, refer to **Task 1**.

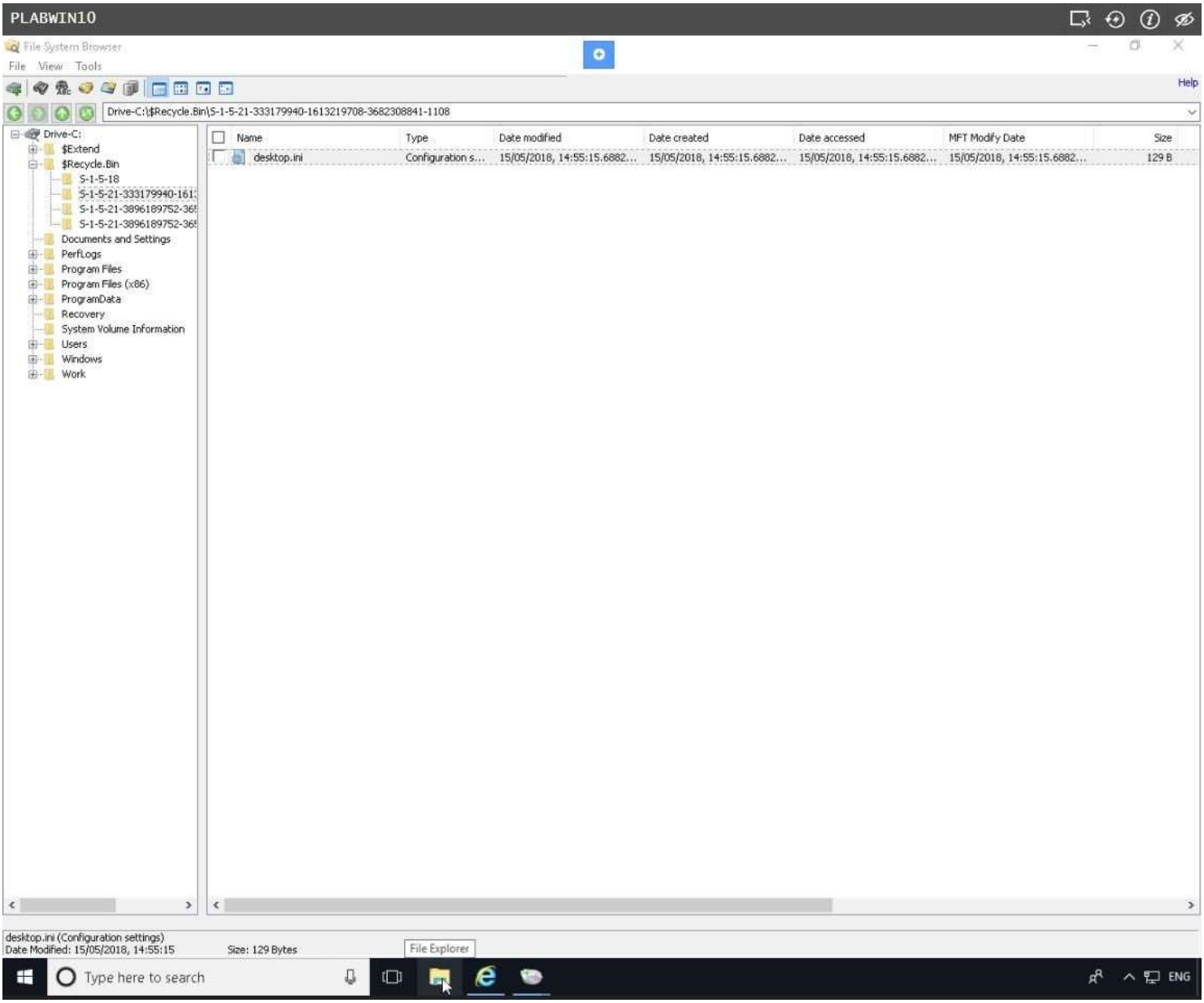
Notice that it contains only one hidden file called **desktop.ini**.

Keep the **File System Browser** window open.



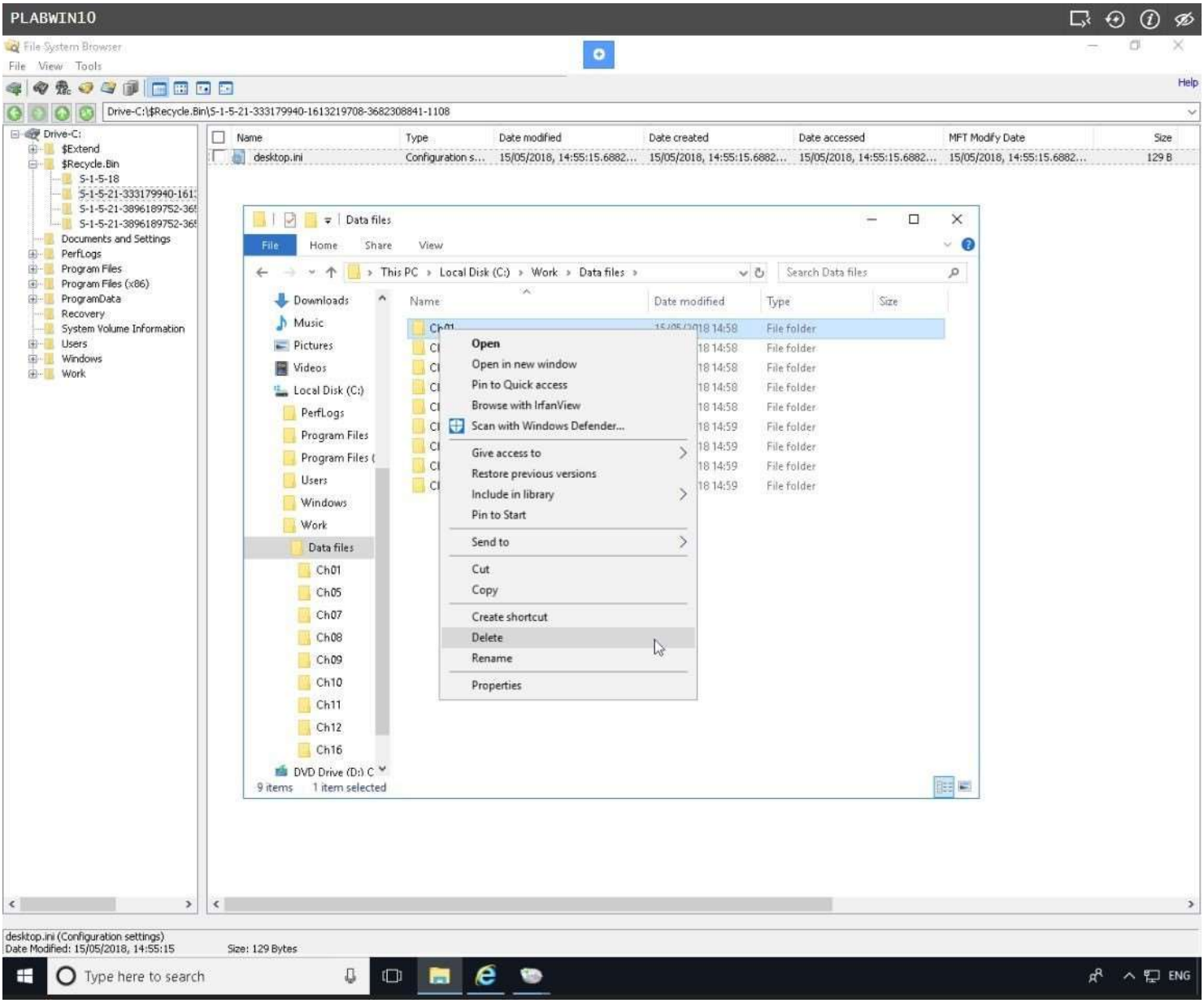
Step 9

Click **File Explorer** icon on taskbar.



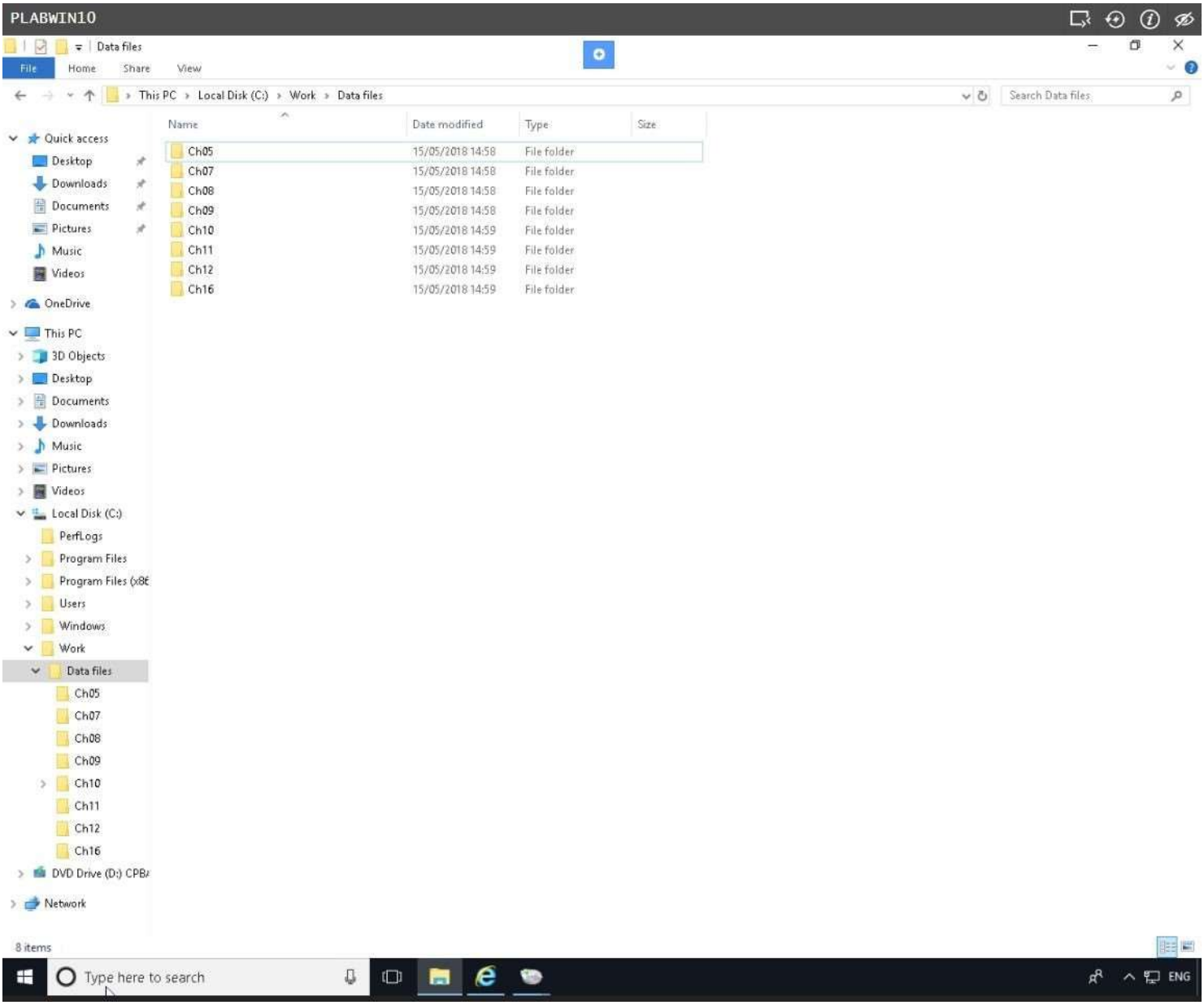
Step 10

On **File Explorer** window, expand **Local Disk C** then click the **Work** folder > **Data Files** and right-click **Ch01** and click **Delete.** If necessary, click **Continue** on the popup.



Step 11

Close **File Explorer** after deleting **Ch01** folder.



Step 12

You are back on the **File System Browser** window.

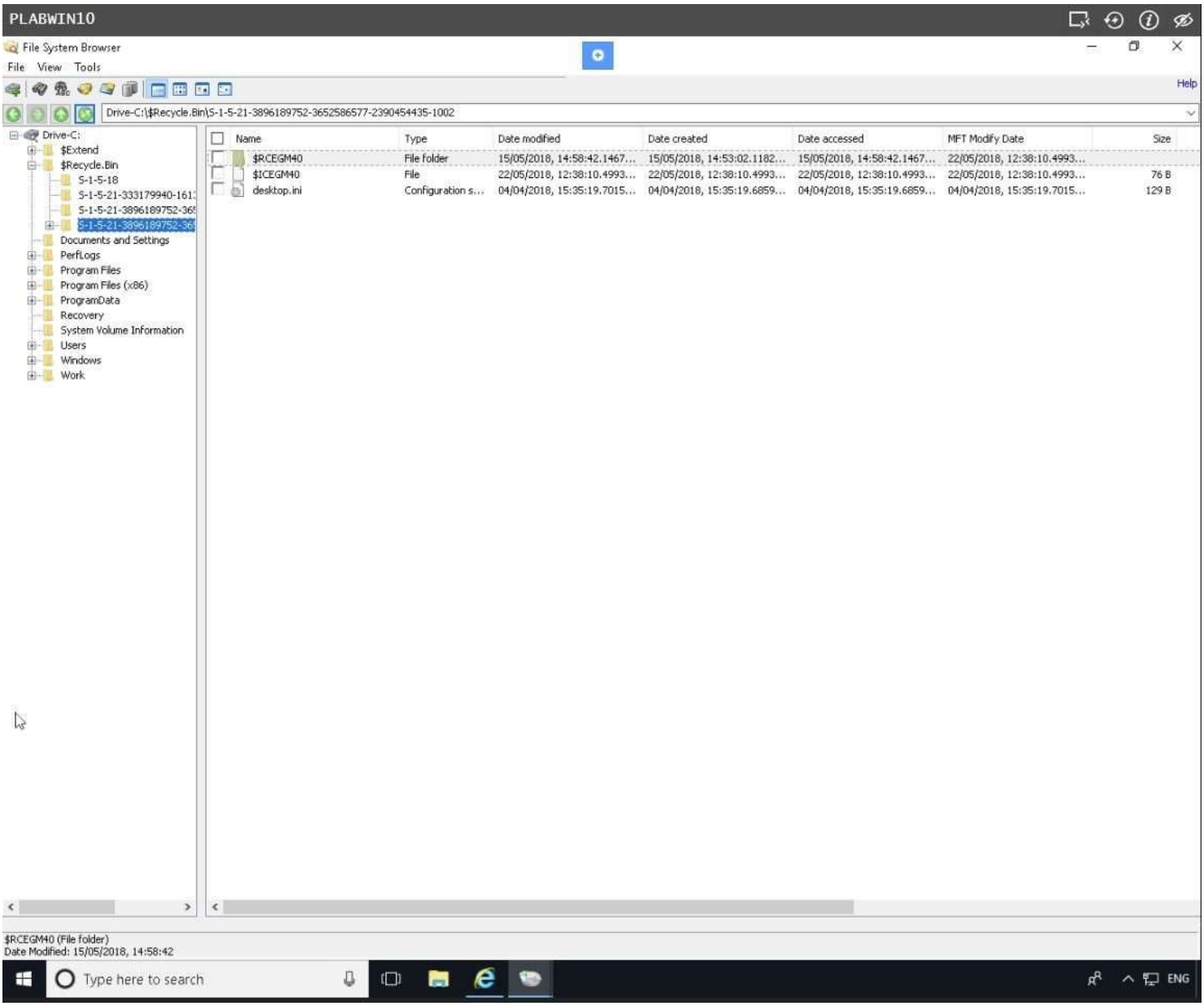
Click again on **$Recycle.Bin** and click on the SID **S-1-5-21-xxx** that was collected in an earlier step to refresh the display.

Notice that the folder called "**Work**" was renamed. Windows changes the filename with a unique identity in the Recycle Bin.

> **Important**: The unique name on the screenshot may differ from your actual lab.

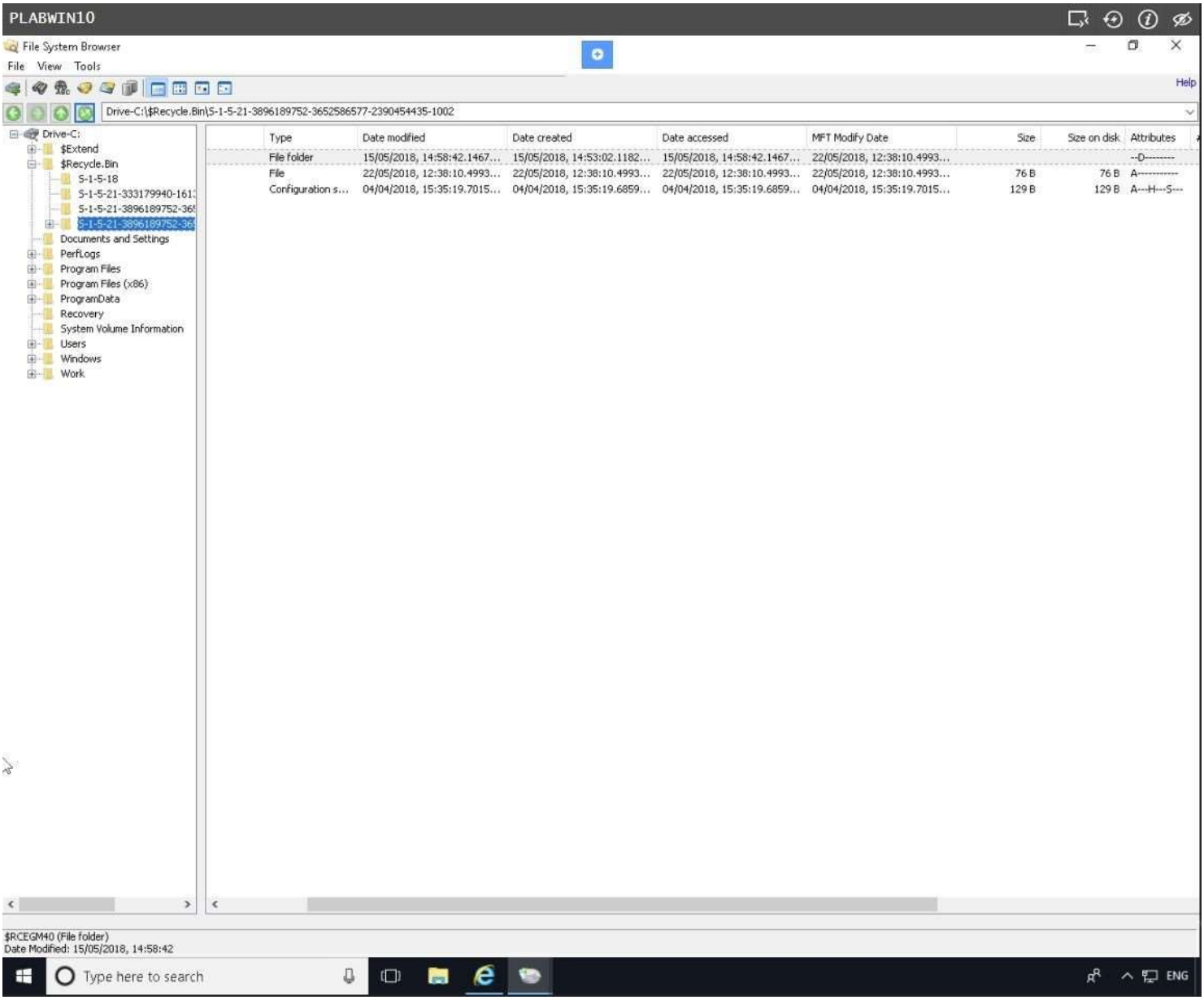
In addition, a new file was added, the name of which resembles the deleted folder.

> **Note:** If the file does not show up, please close OSForensics and reopen the program. Then navigate back to the **File System Browser**.



Step 13

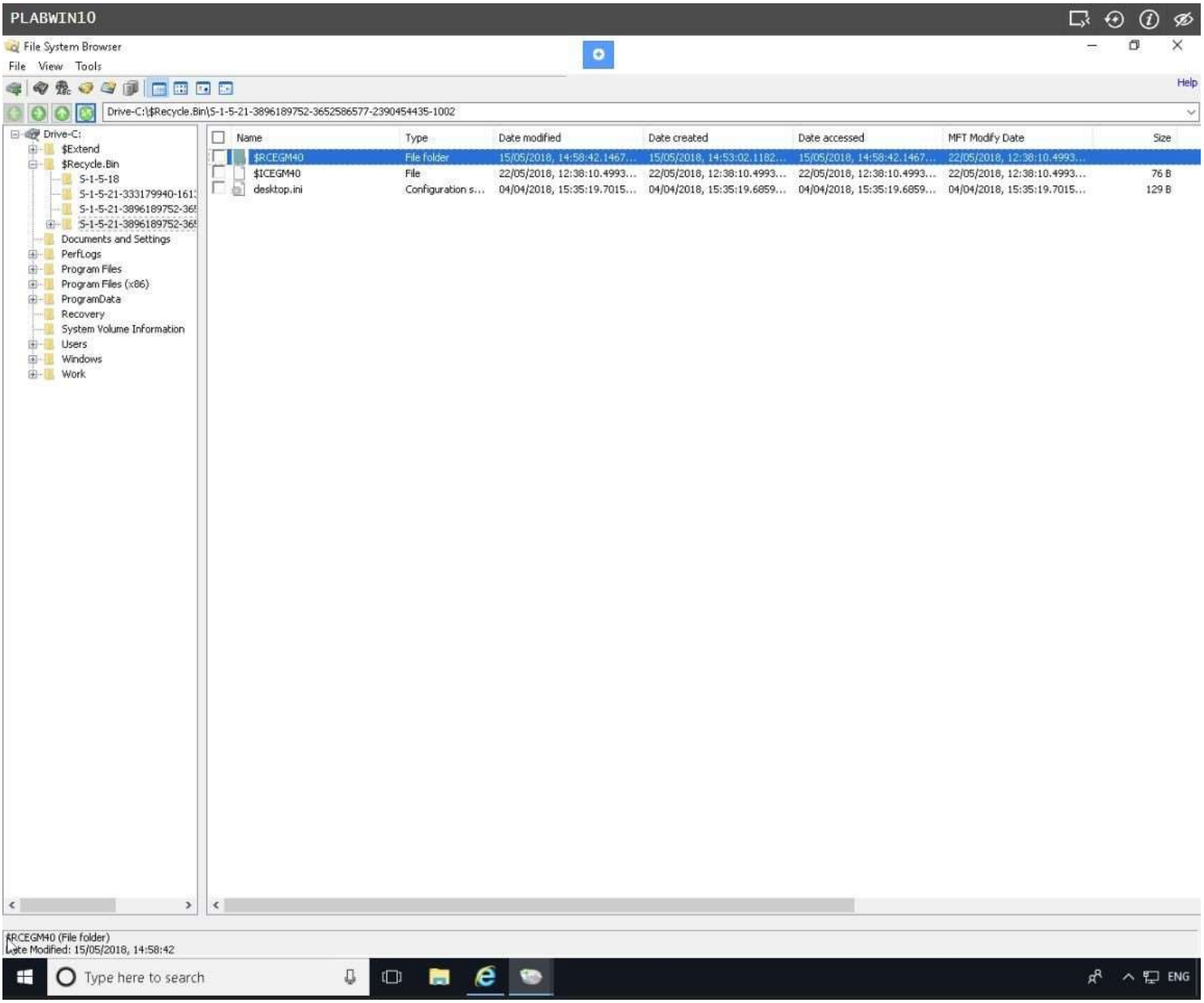
On the details pane, scroll horizontally to view the other details about the deleted folder.



Step 14

To see other details about the deleted files, you will need to open the folders.

Double-click on the deleted folder.

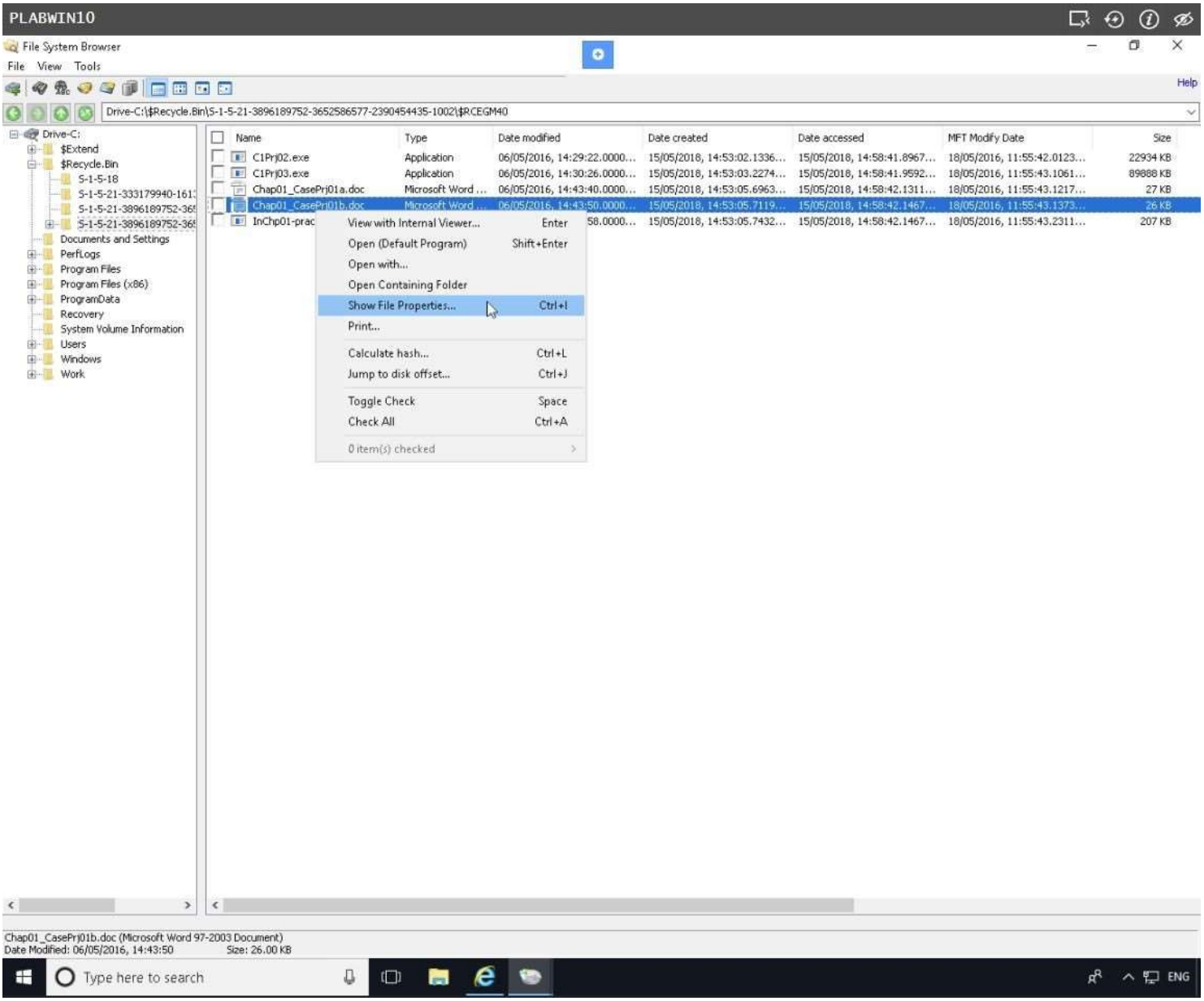


Step 15

Details about the deleted files are displayed.

Examine the different properties about the deleted files as displayed in the column headers by scrolling horizontally.

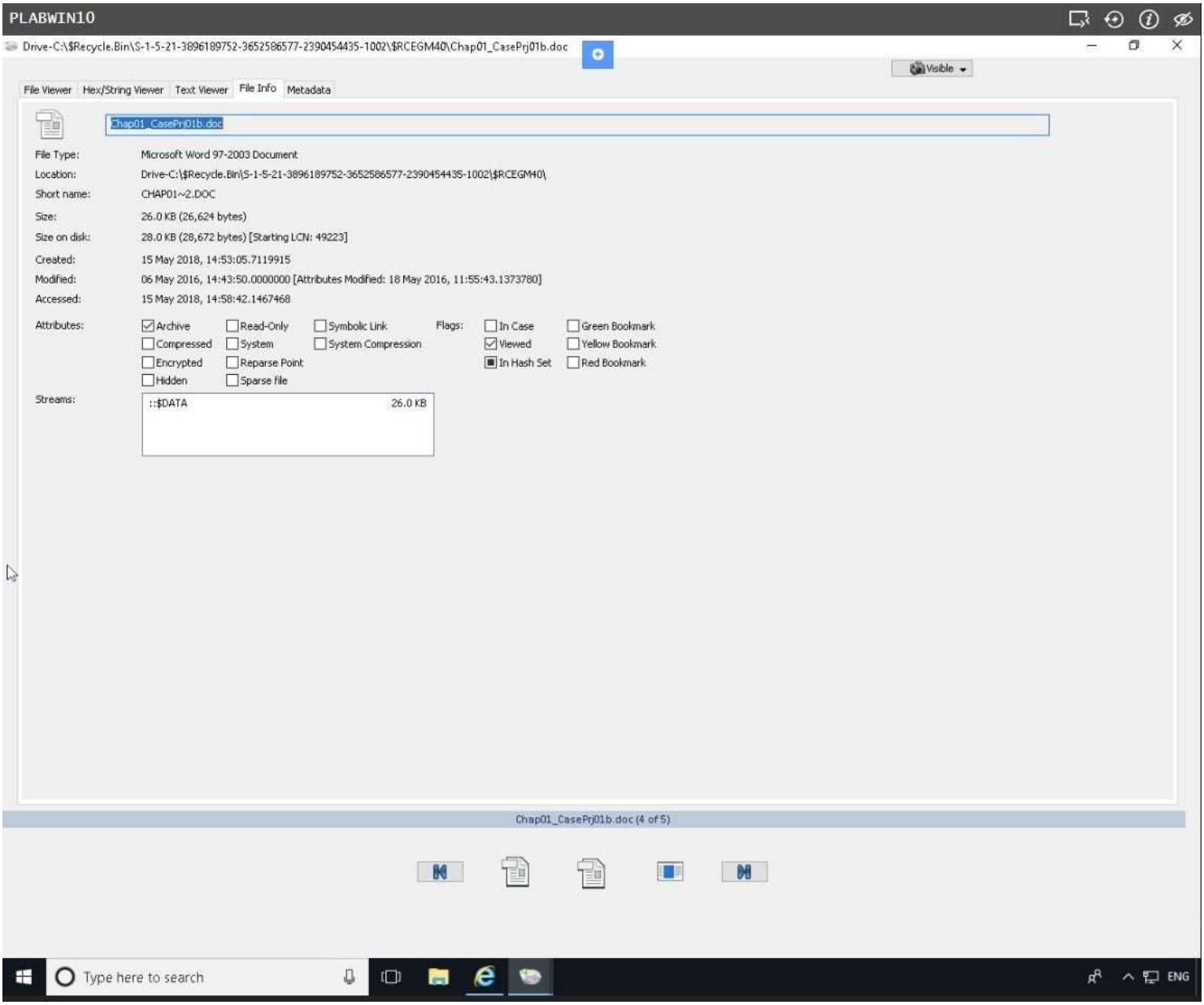
Now right-click **Chap01_CasePrj01b.doc** and select **Show File Properties**...



Step 16

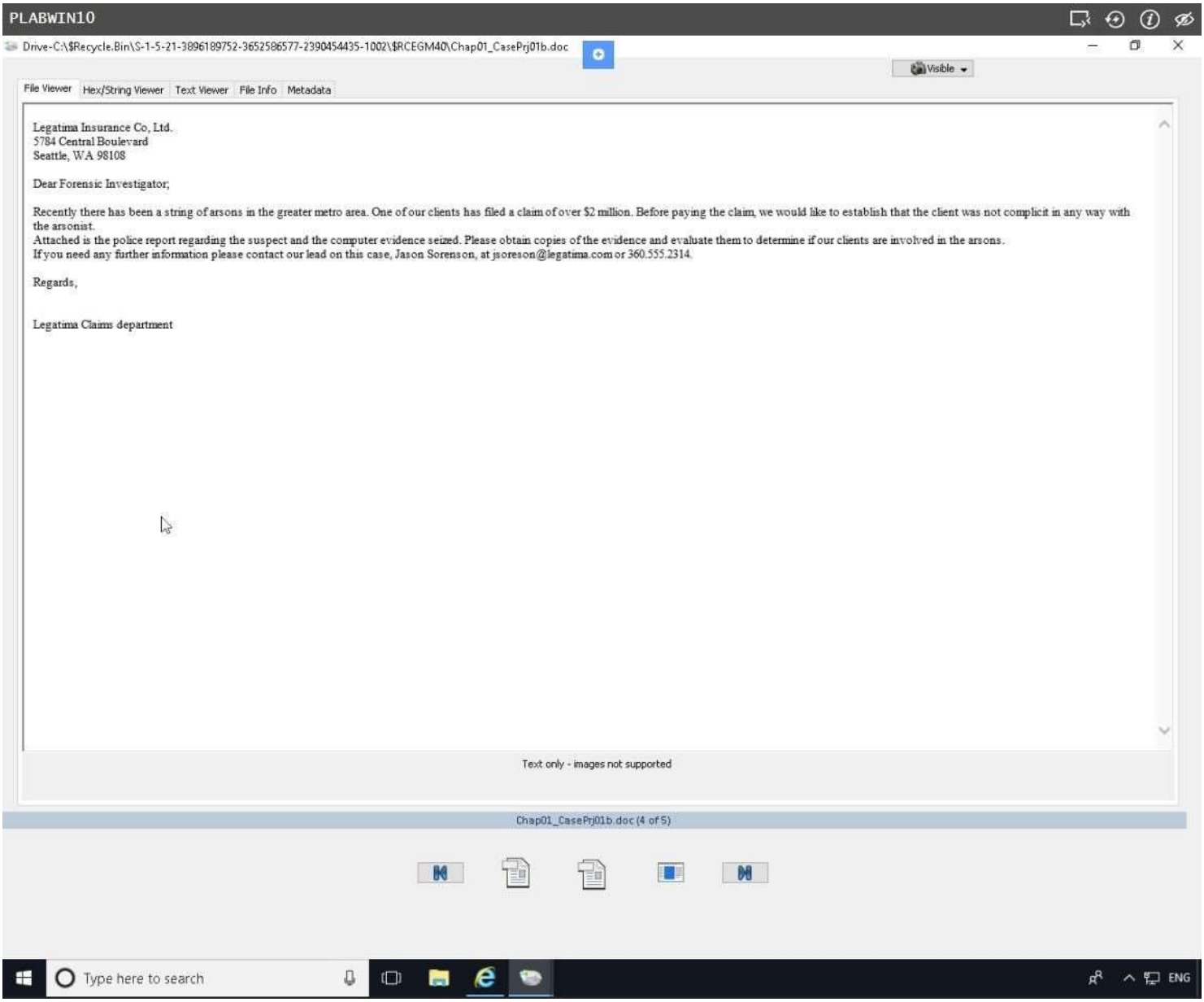
The **Drive C:\Recycle.Bin\S-1-5-21-xxx\Data files\Ch01\Chap01_CasePrj01b.doc** dialog box is displayed.

On the **File Info** tab information about this deleted file is presented. Observe the different properties pertaining to this document file.



Step 17

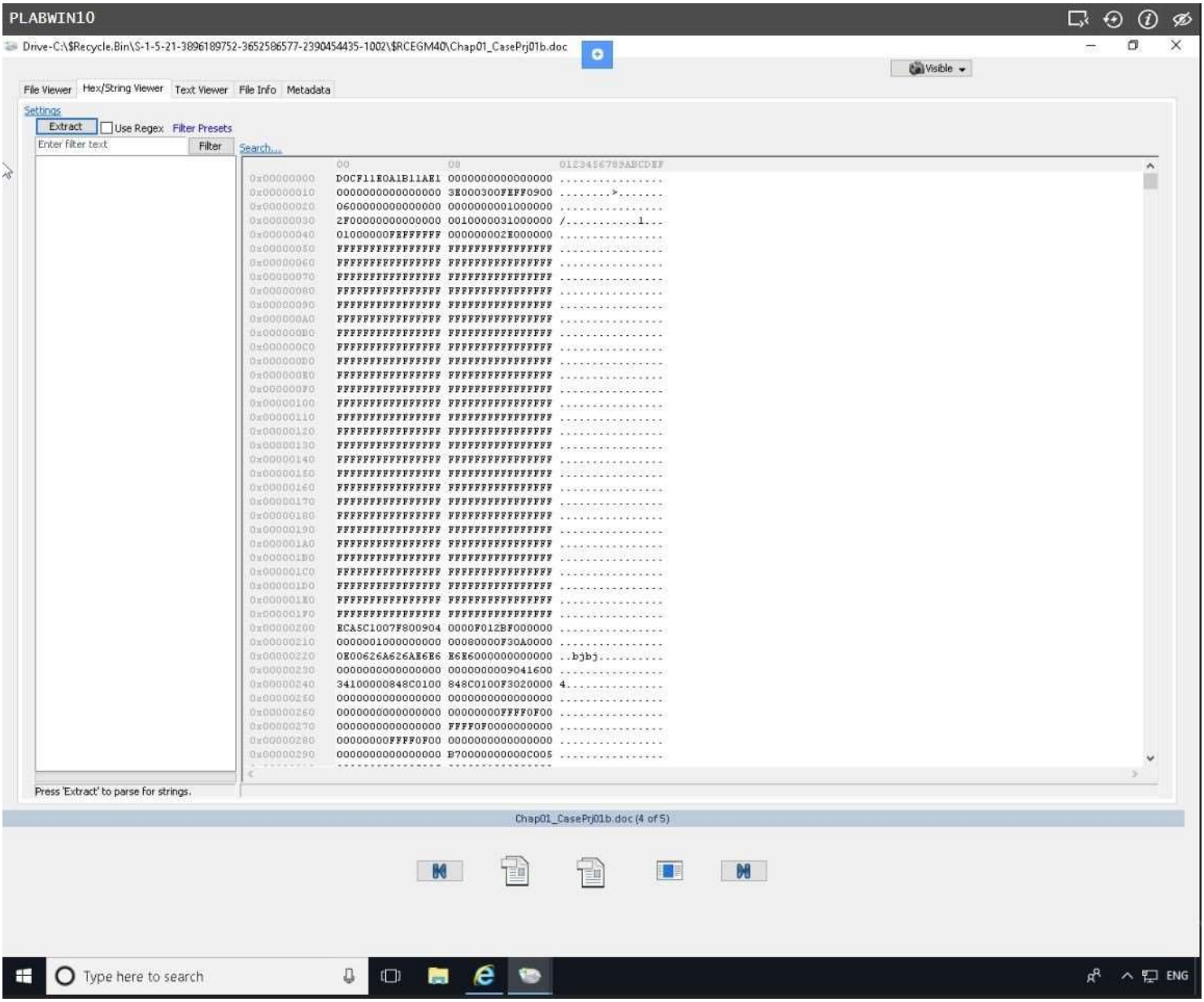
Click **File Viewer** tab.



Step 18

The **File Viewer** tab displays the content of this file, since it contains text information.

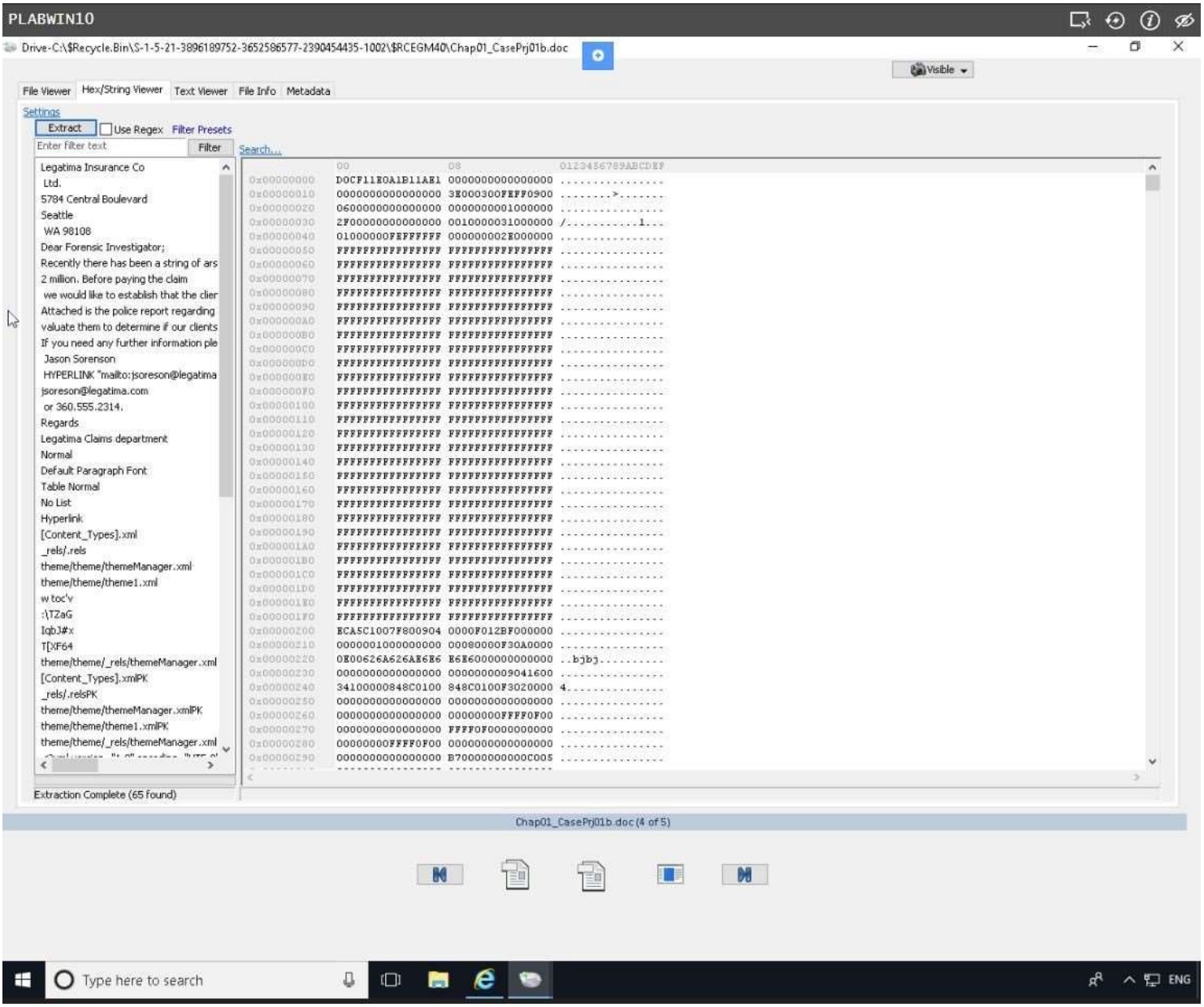
Click **Hex/String Viewer** tab.



Step 19

On the **Hex/String Viewer** tab, Hex and ASCII patterns are displayed.

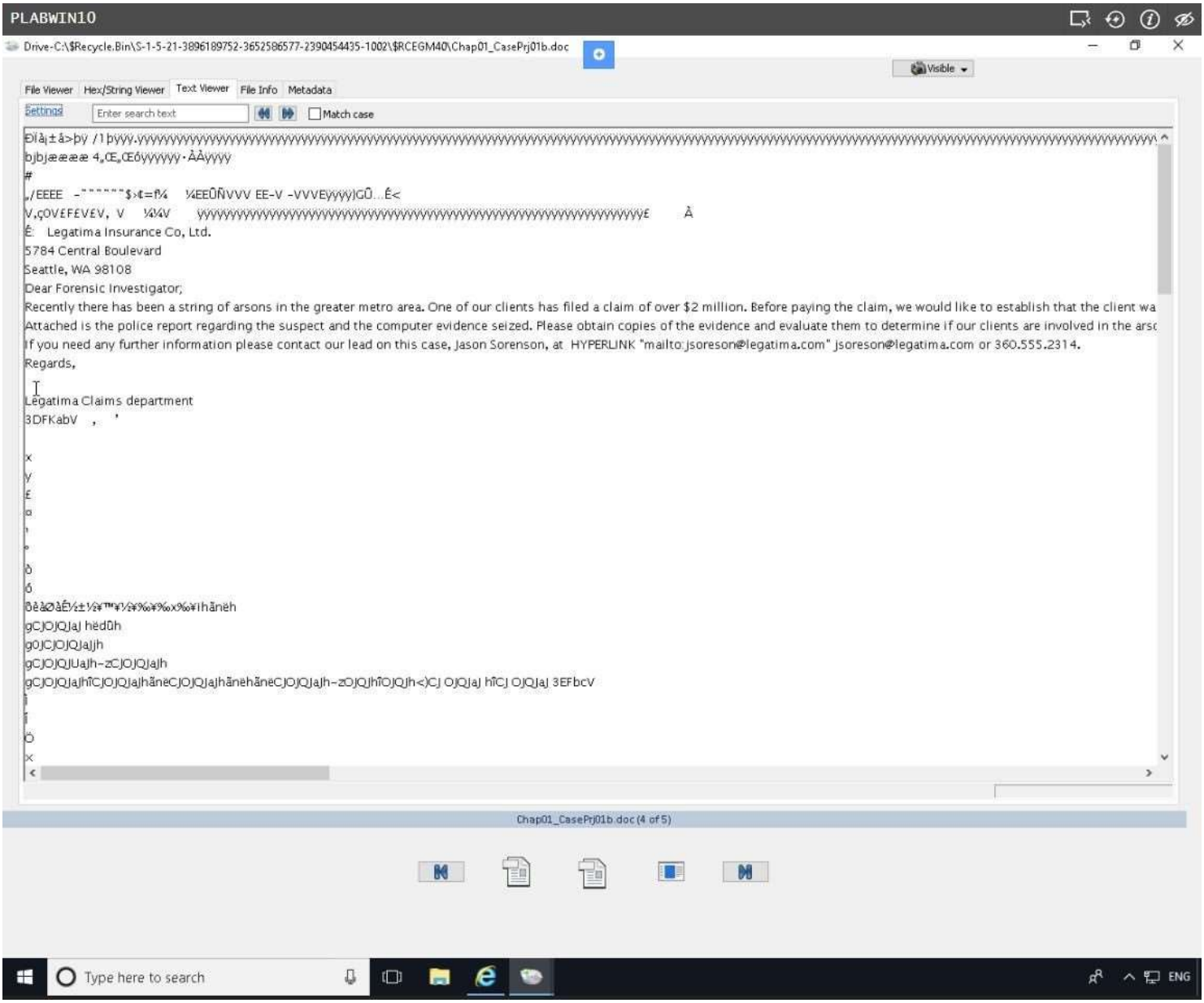
Click **Extract** on the left pane to get information about the hex data.



Step 20

Scroll through the information given on the left pane.

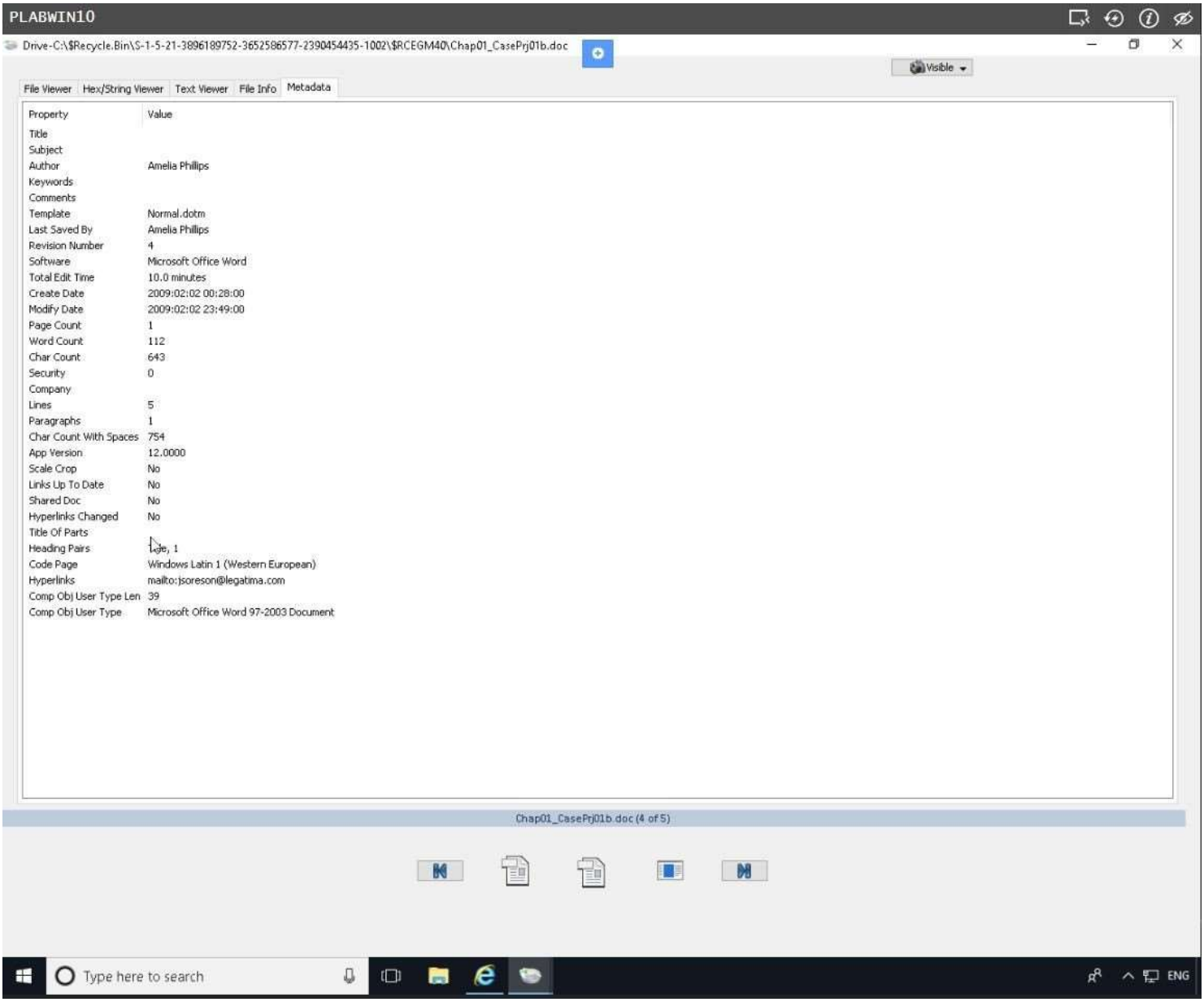
When finished, access **Text Viewer** tab.



Step 21

The **Text Viewer** tab displays text and other formatting codes. Scroll through the information as desired.

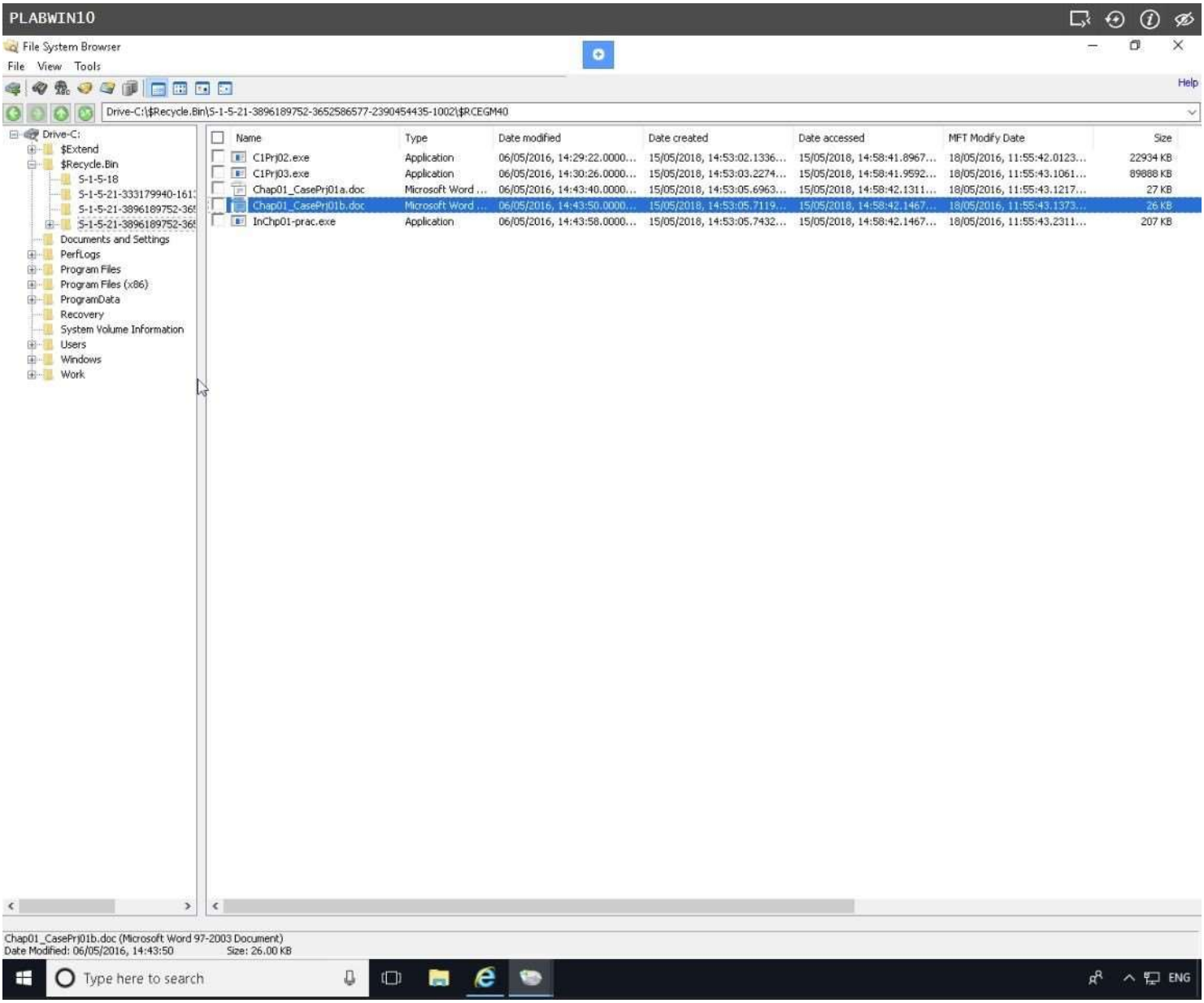
Click **Metadata** tab when done.



Step 22

The **Metadata** tab displays other important information about the document file.

When finished viewing the details, click **[X]** to close the window.

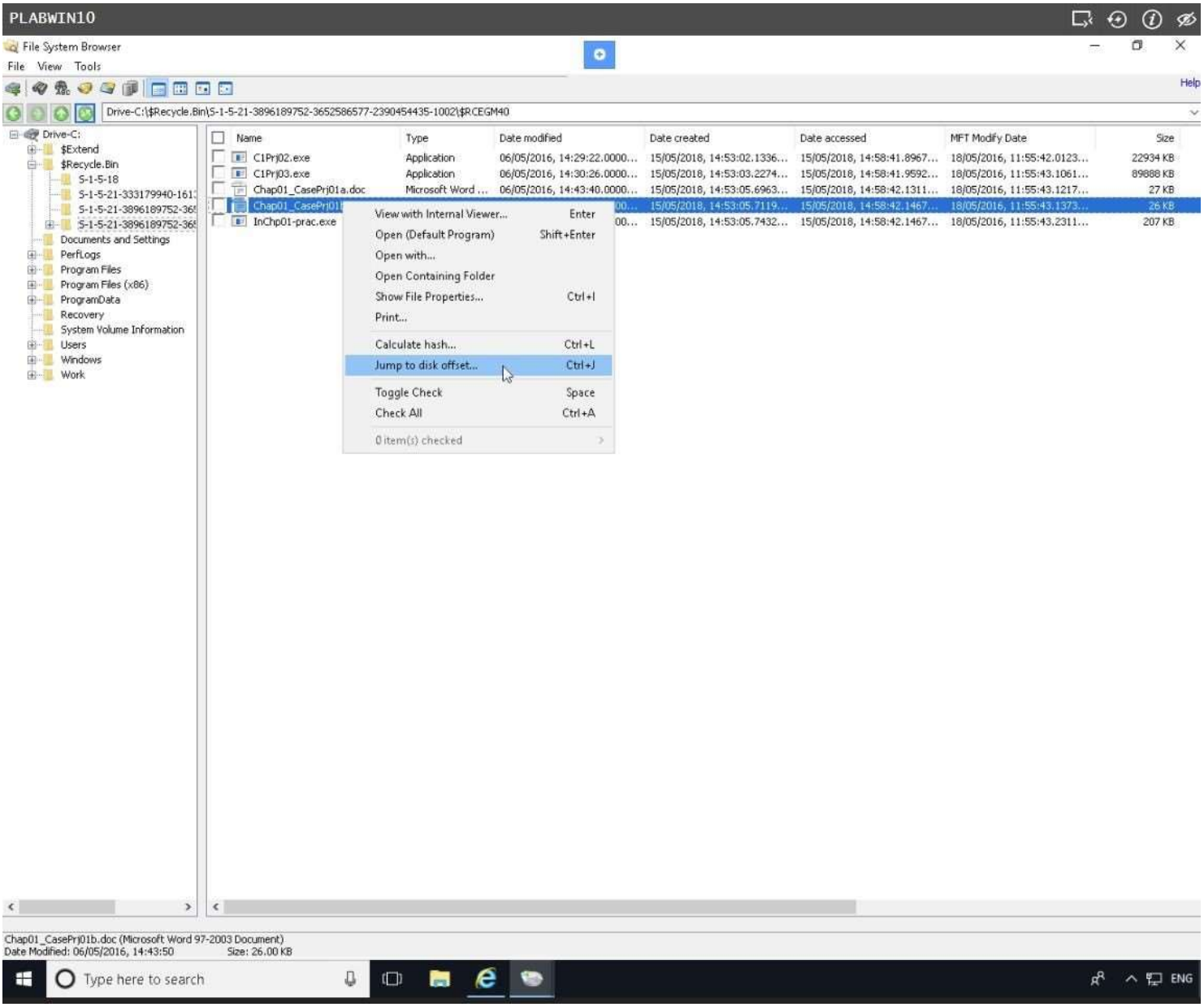


Step 23

Back on **File System Browser** window, the file **Chap01_CasePrj01b.doc** is selected.

You will now view location of this file in the disk.

Right-click **Chap01_CasePrj01b.doc** file and select **Jump to disk offset**...

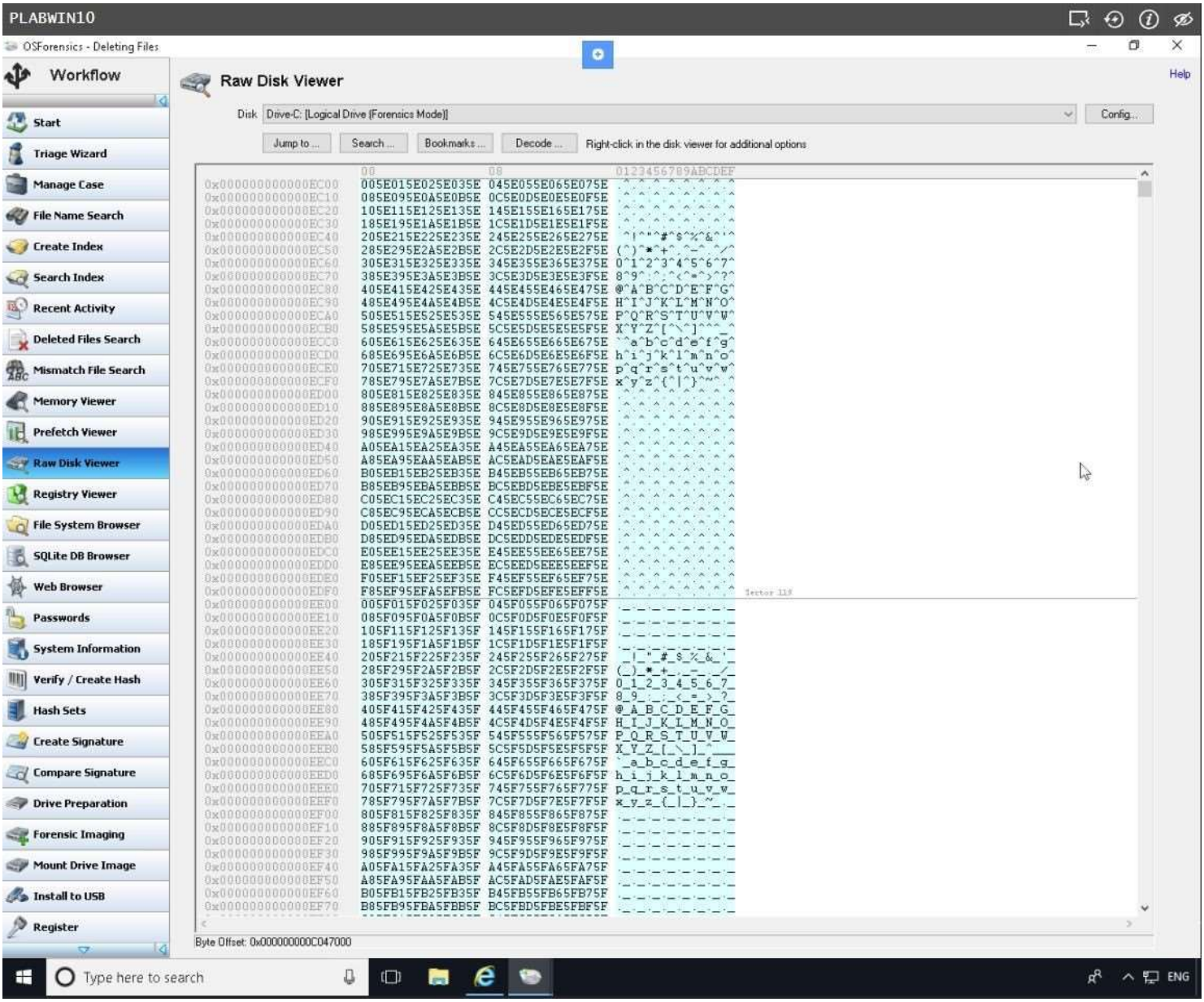


Step 24

The **Raw Disk Viewer** window opens.

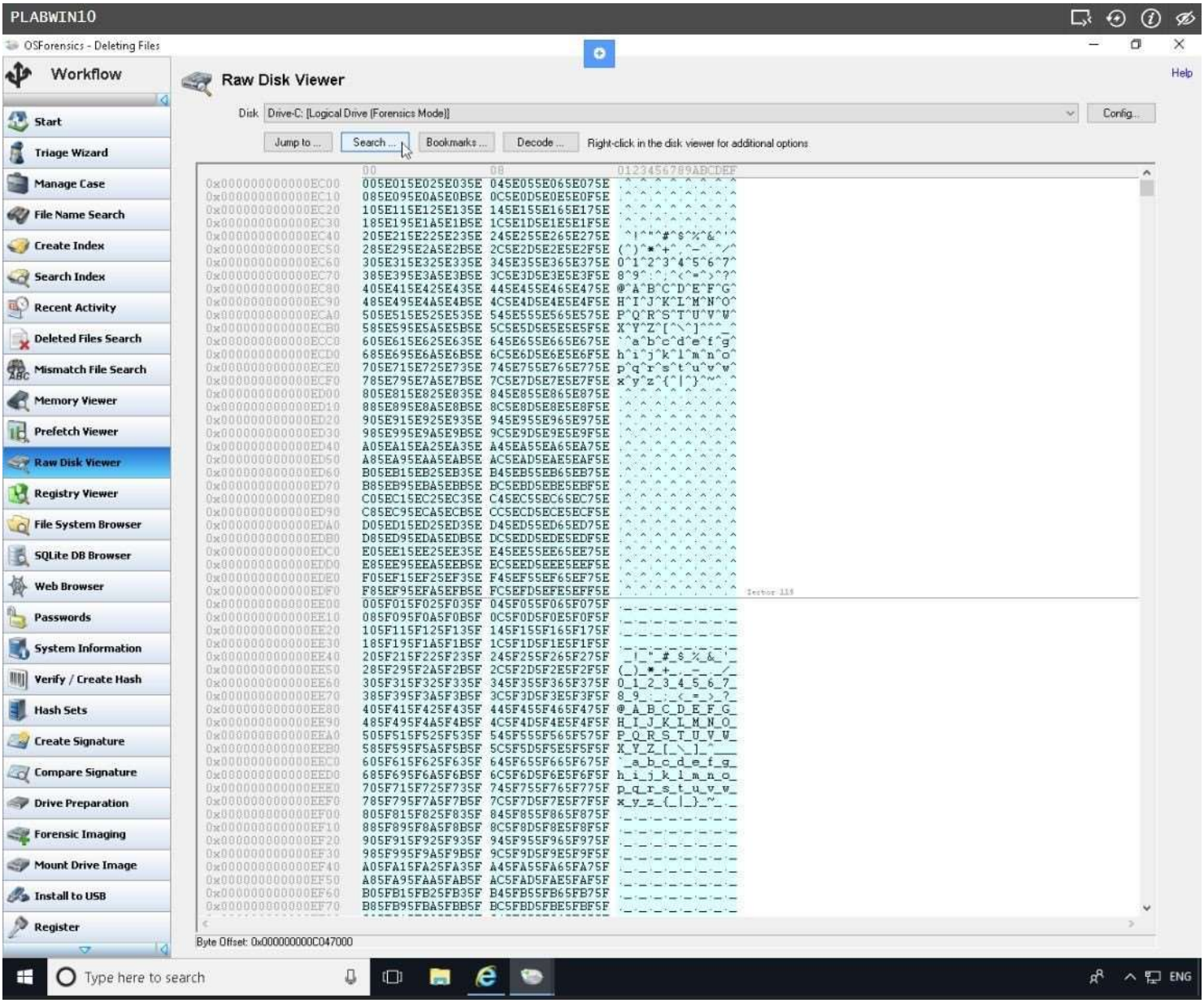
Notice that it jumped directly to the disk sectors (highlighted in green color) where the file **Chap01_CasePrj01b.doc** is located in the disk.

Scroll down a bit to see the clusters that are marked free.



Step 25

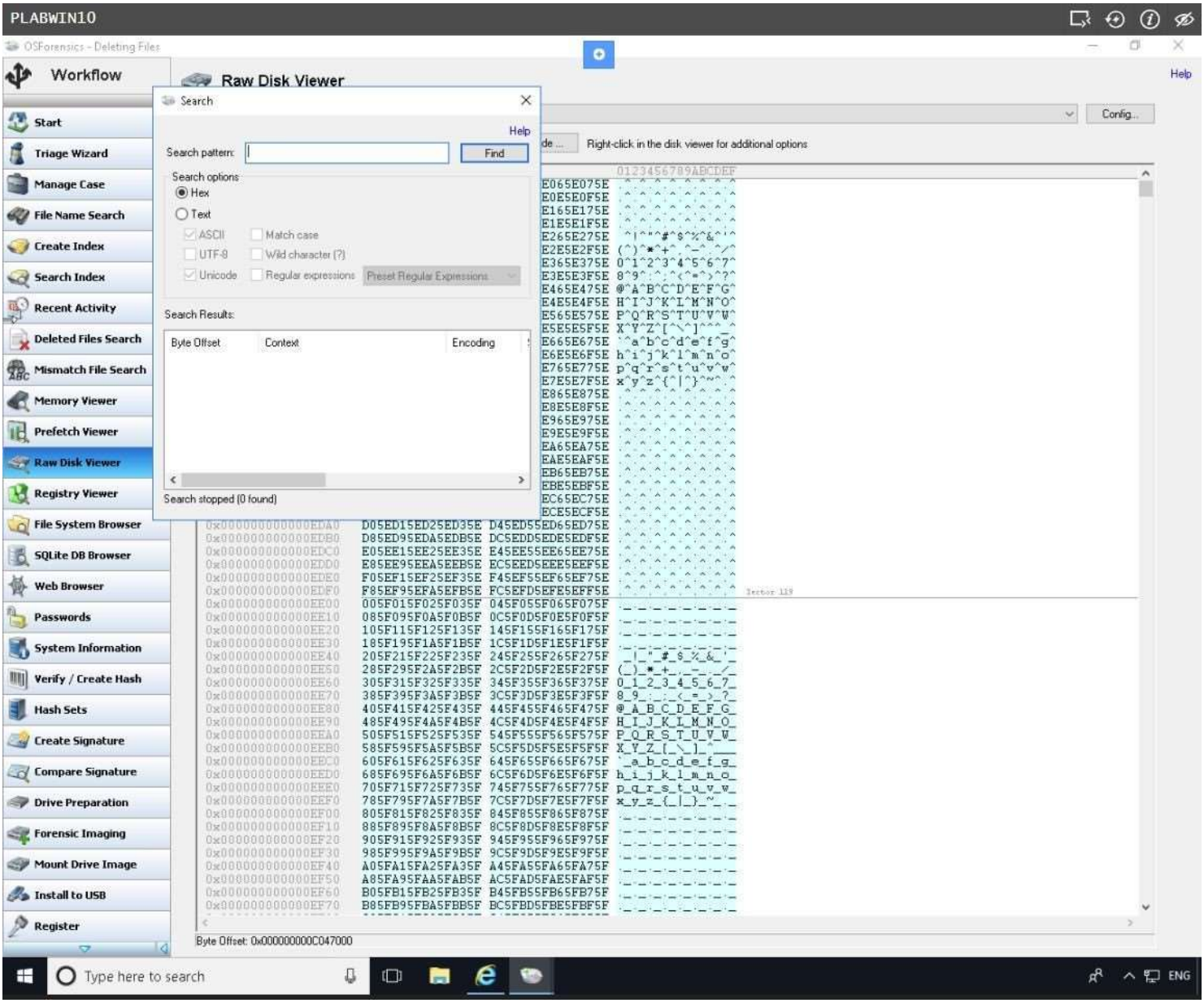
The associated clusters are designated as free—that is, marked as available for new data.



Step 26

Obviously, it's not practical to scroll through the disk map to search something that maybe of interest, as this will take considerable time.

On **Raw Disk Viewer** window, click **Search**.



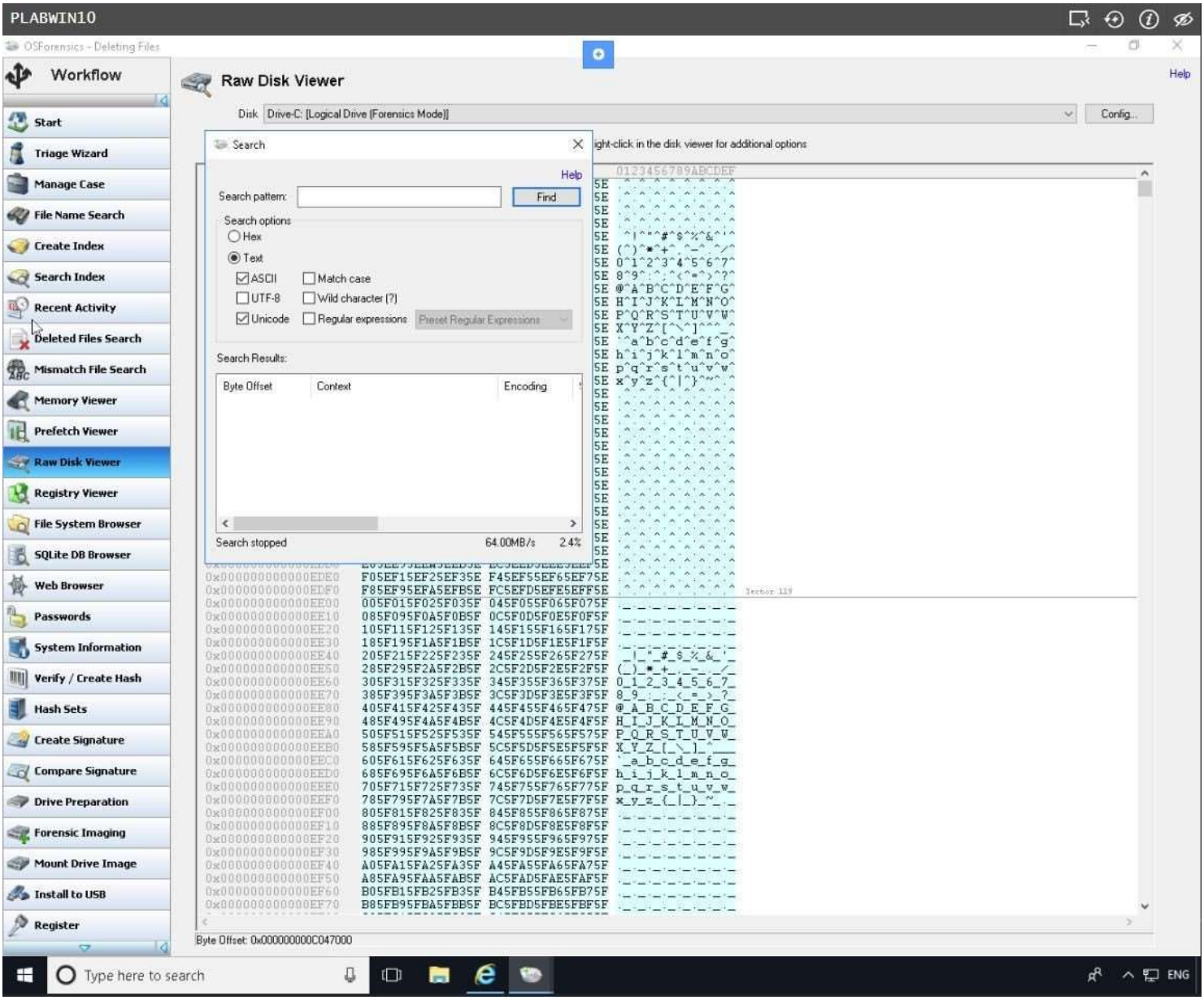
Step 27

The **Search** dialog box opens. In the **Search pattern** text box, type:

```
legatima
```

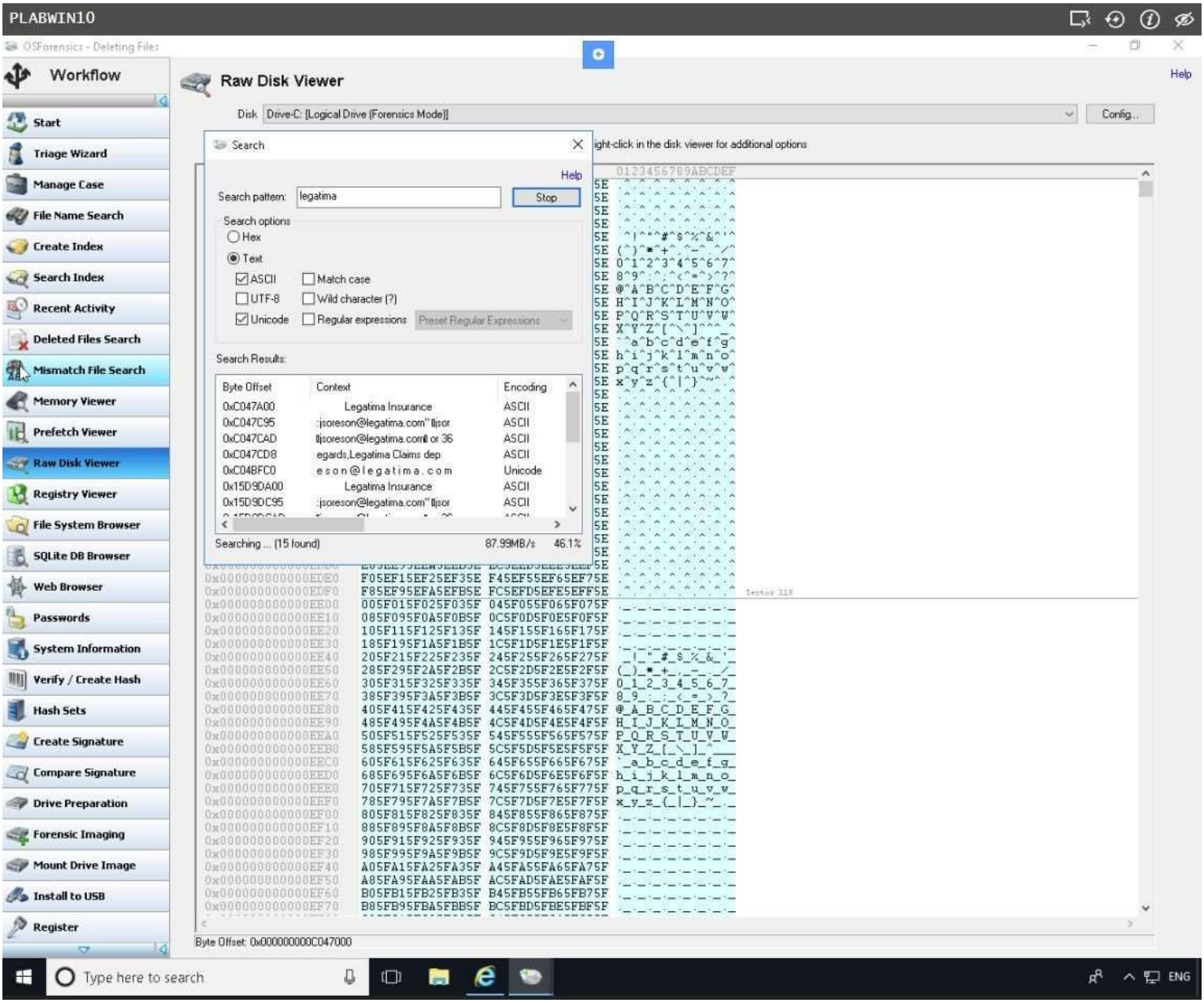
Select **Text** option and keep the other default settings.

Click **Find**.



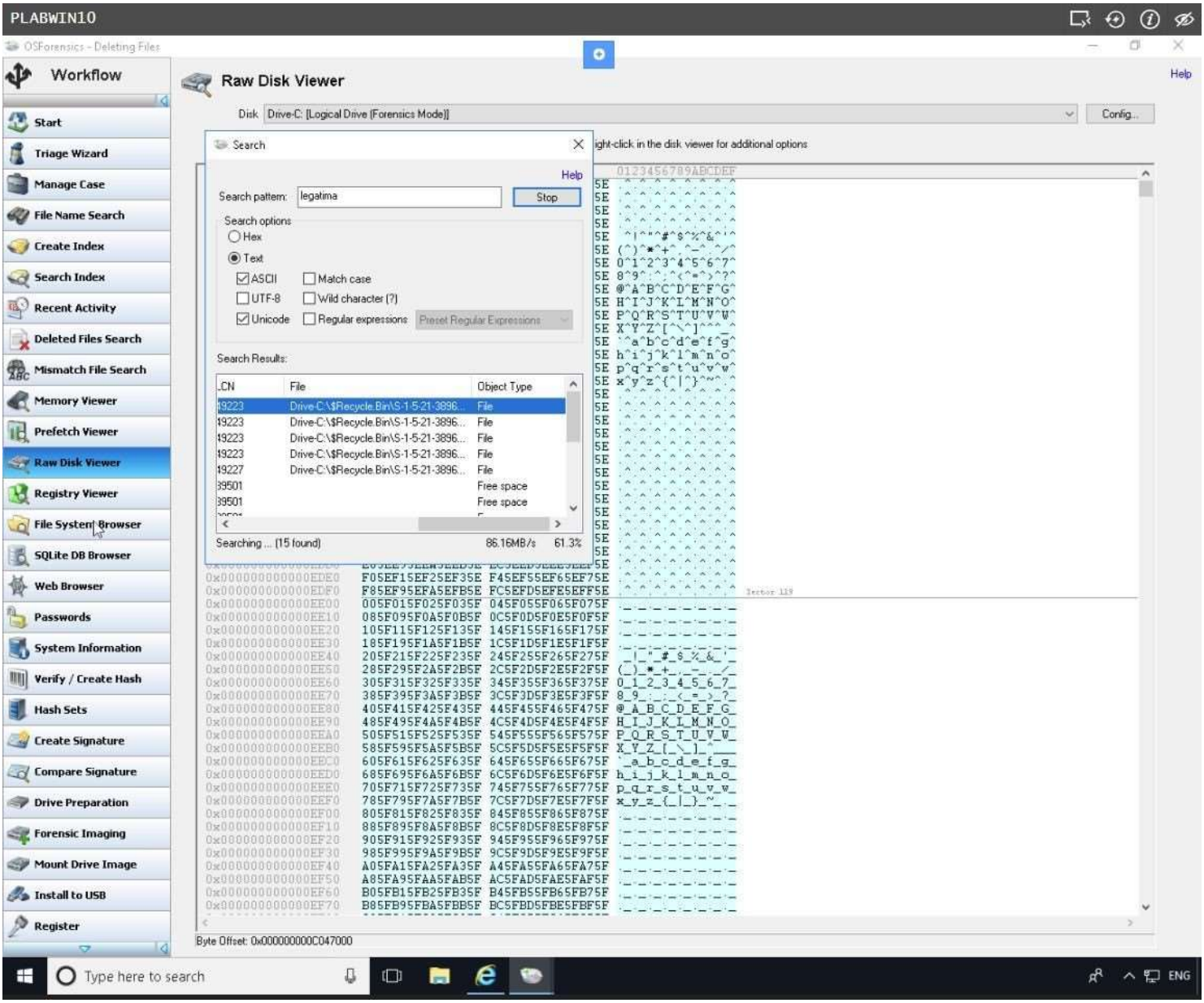
Step 28

After a few seconds, the **Search** dialog box will return results where the pattern "**legatima**" is found.



Step 29

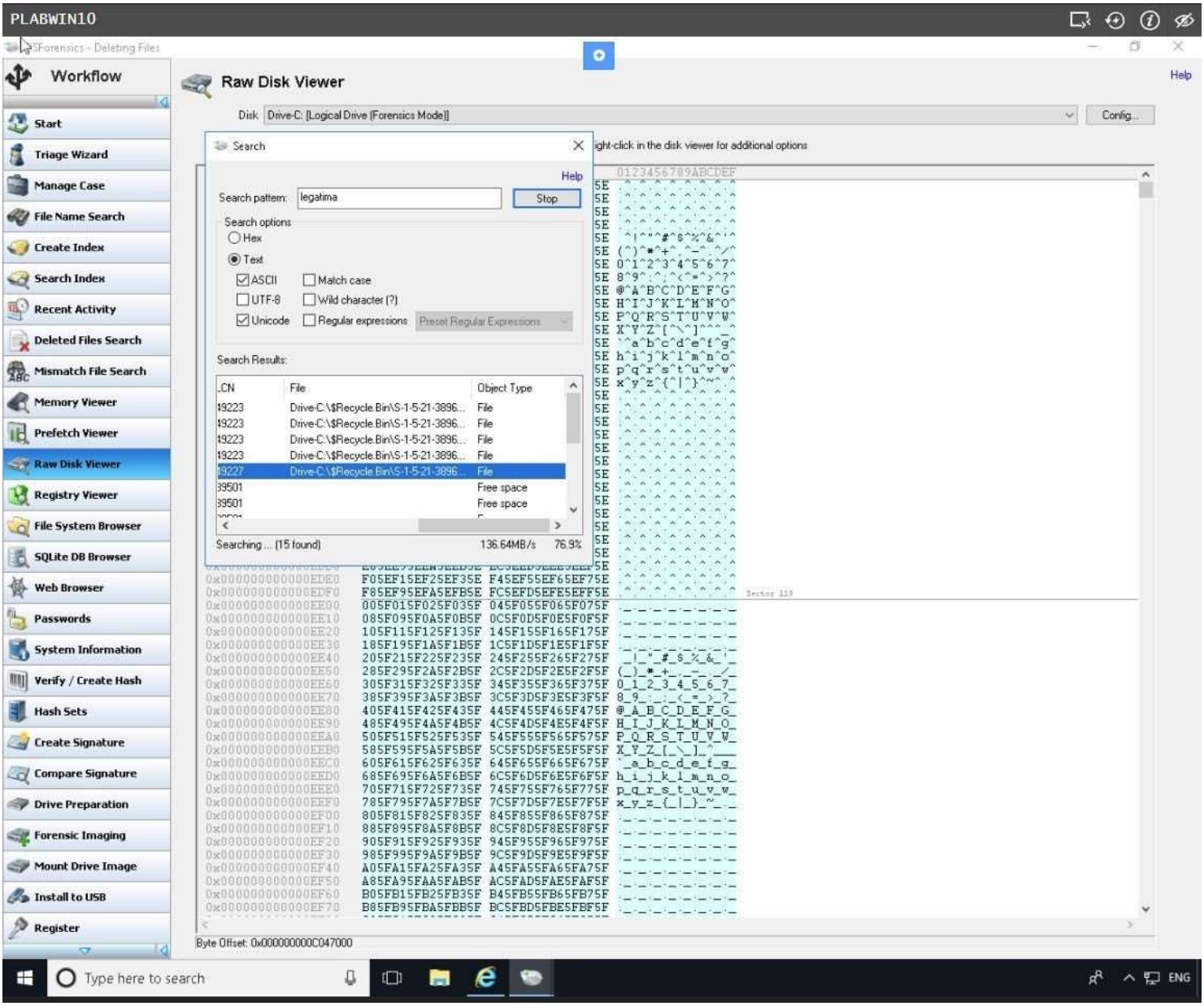
Scroll horizontally to view the additional information about the search pattern.



Step 30

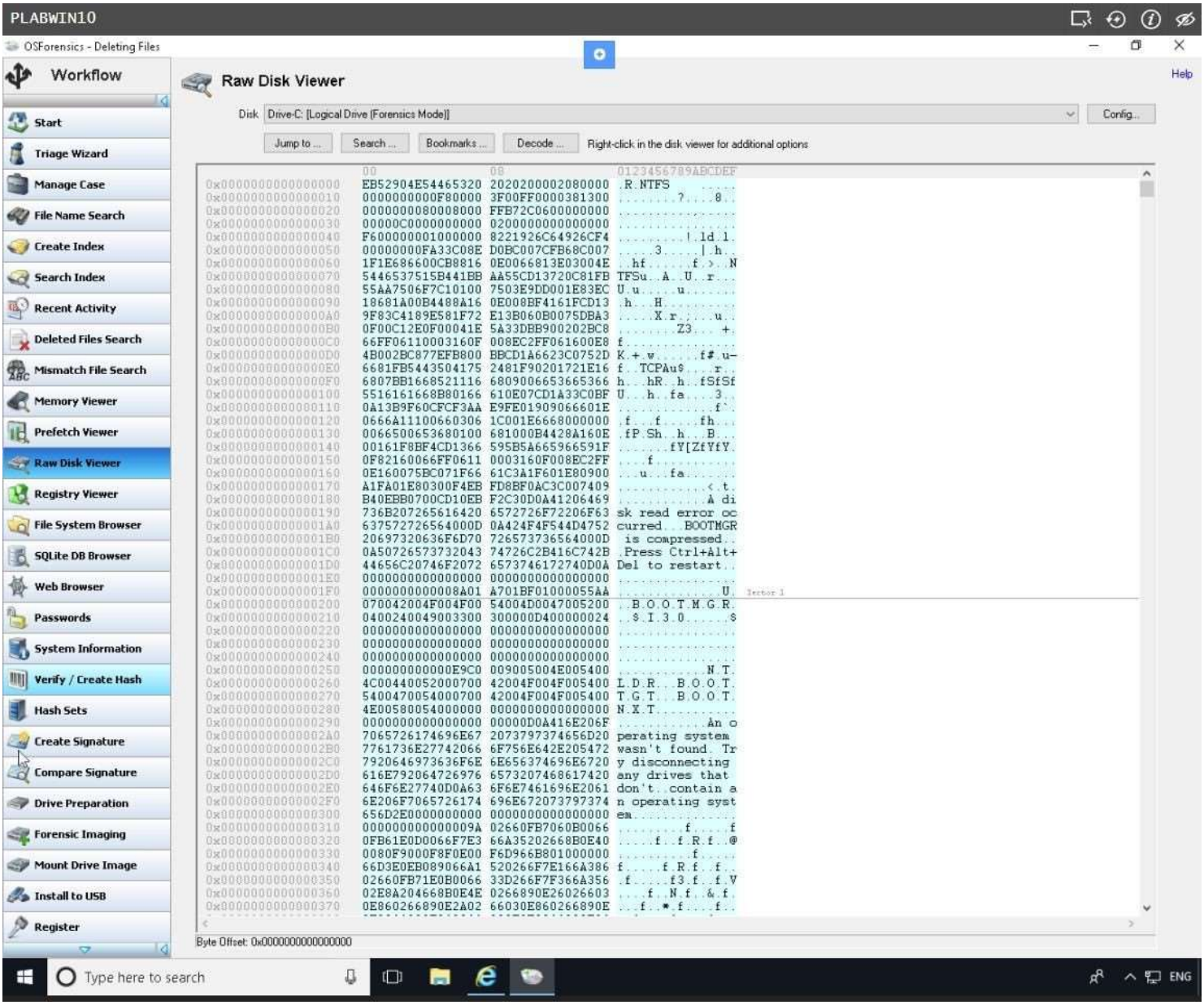
The **Search Results** indicate the Byte Offset, Content, File Encoding, Drive where deleted files are located and other information.

Close **Search** dialog box by clicking the **[X]** button when done.



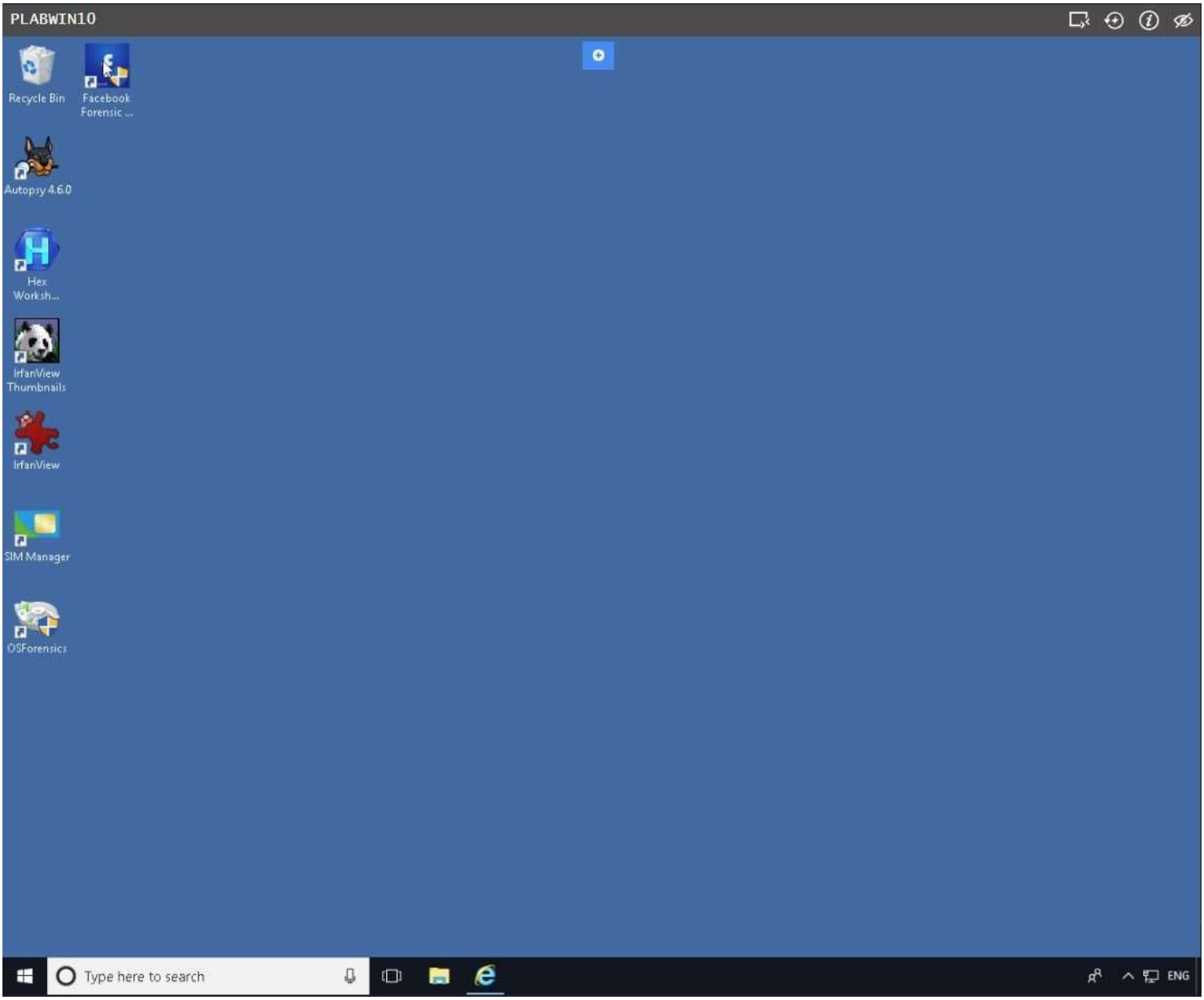
Step 31

Close **Raw Disk Viewer** window.



Step 32

You are back on **PLABWIN10** desktop.



Keep the device powered on in its current state and proceed to the next exercise.

Exercise 5-3 - Examining the Windows Registry

Some forensics tools, such as ProDiscover, X-Ways Forensics, OSForensics, and FTK, have built-in or add-on Registry viewers. For this next activity, your company's Legal Department has asked you to search for any references in the Favorites folder in Internet Explorer of a user named Denise Robbins.

For this exercise, you use OSForensics to examine Denise Robbins' NTUser.dat file. If you find any items of interest, add them to an OSForensics case report that you can give to the paralegal. The following steps explain how to generate a case report in OSForensics.

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.

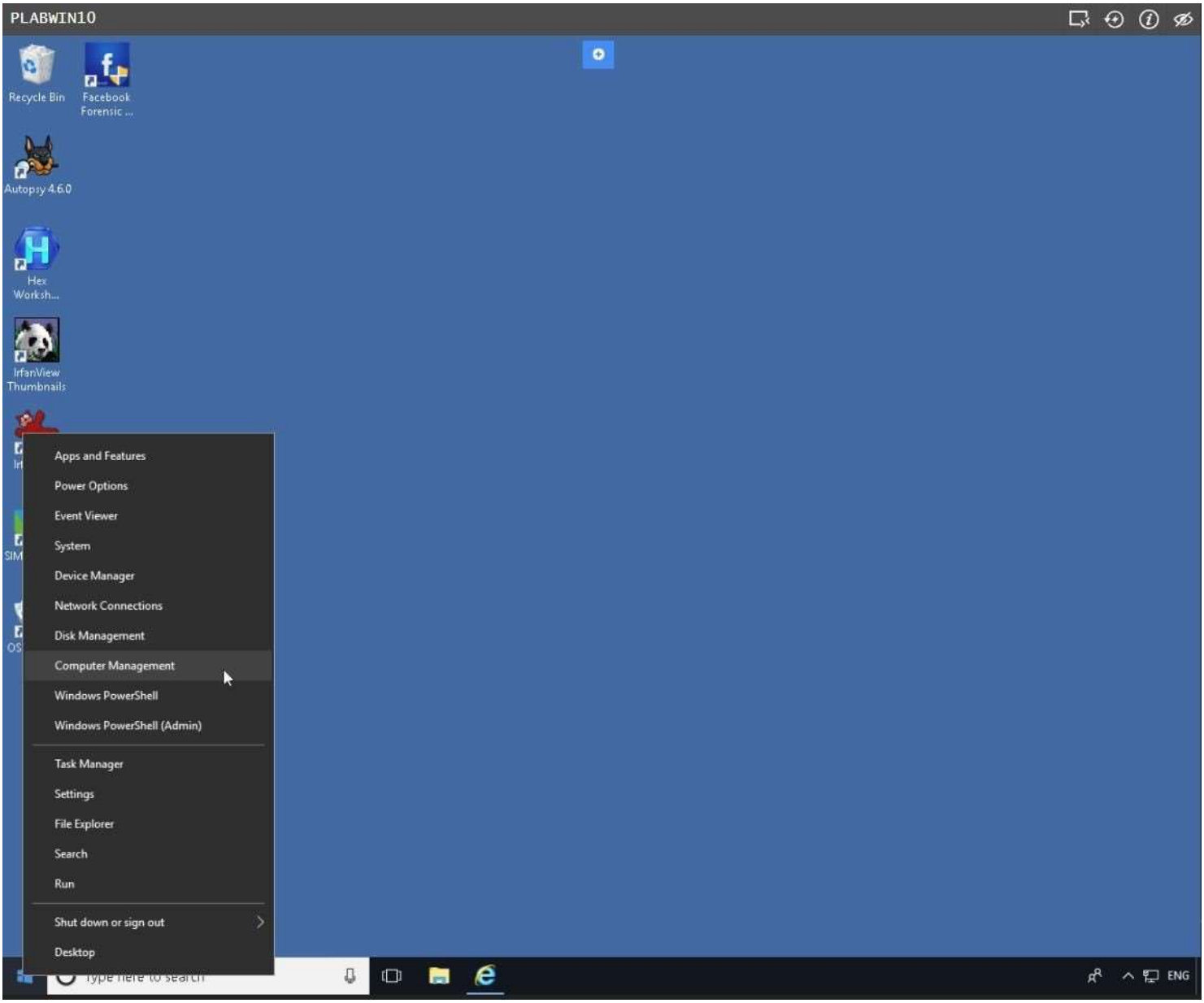
Task 1 - Create a Sample User

In this task, you will create a sample user to meet the scenario mentioned in the introduction of this exercise.

To create a sample user, perform the following steps:

Step 1

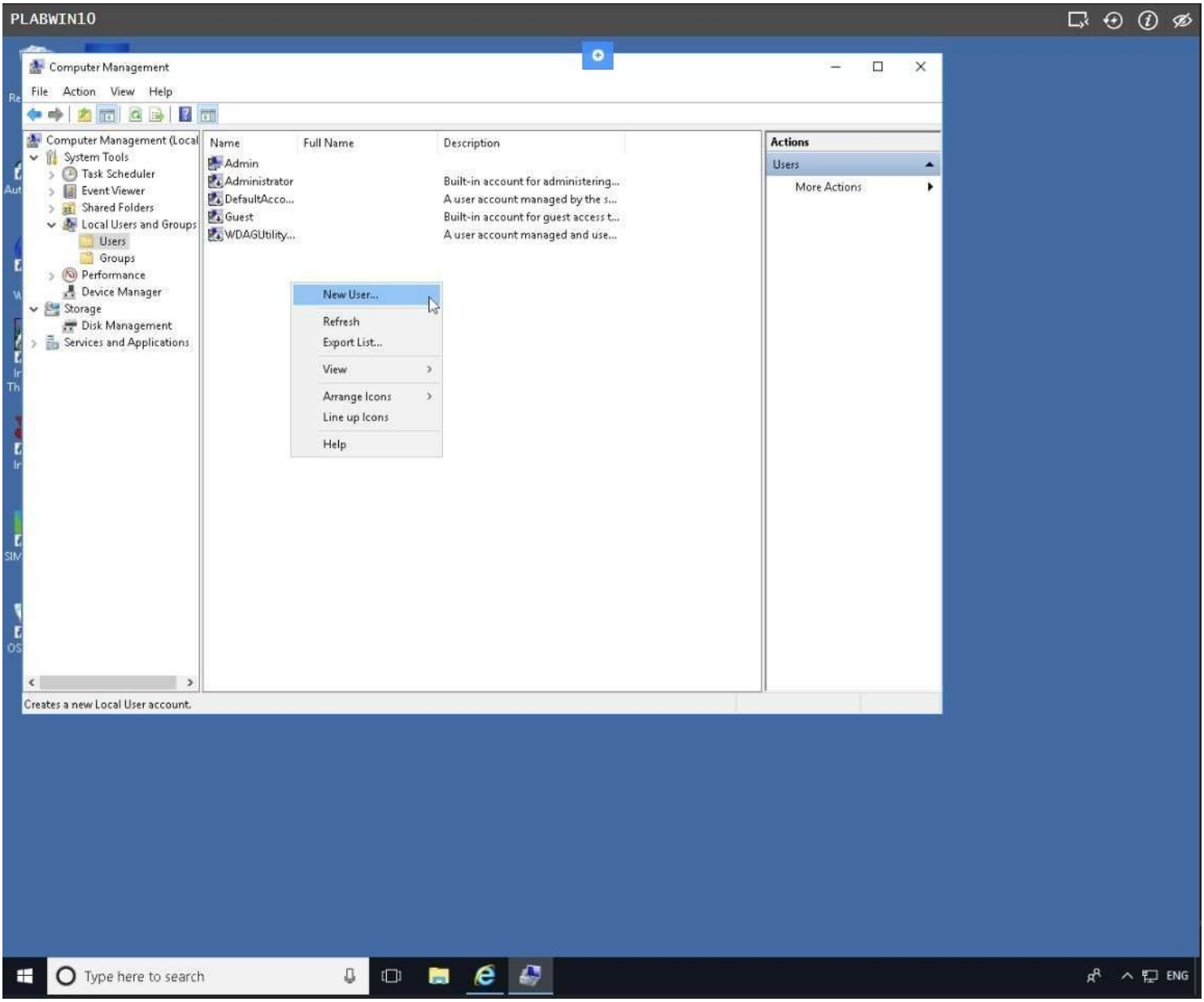
On **PLABWIN10** device, right-click **Start** and select **Computer Management**.



Step 2

On the **Computer Management** console, expand **Local Users and Groups** then click **Users** folder.

Right-click on the details pane on the right and select **New User**.



Step 3

On the **New User** dialog box, in the **User name** box, type:

```
Denise
```

In the **Full name** box, type:

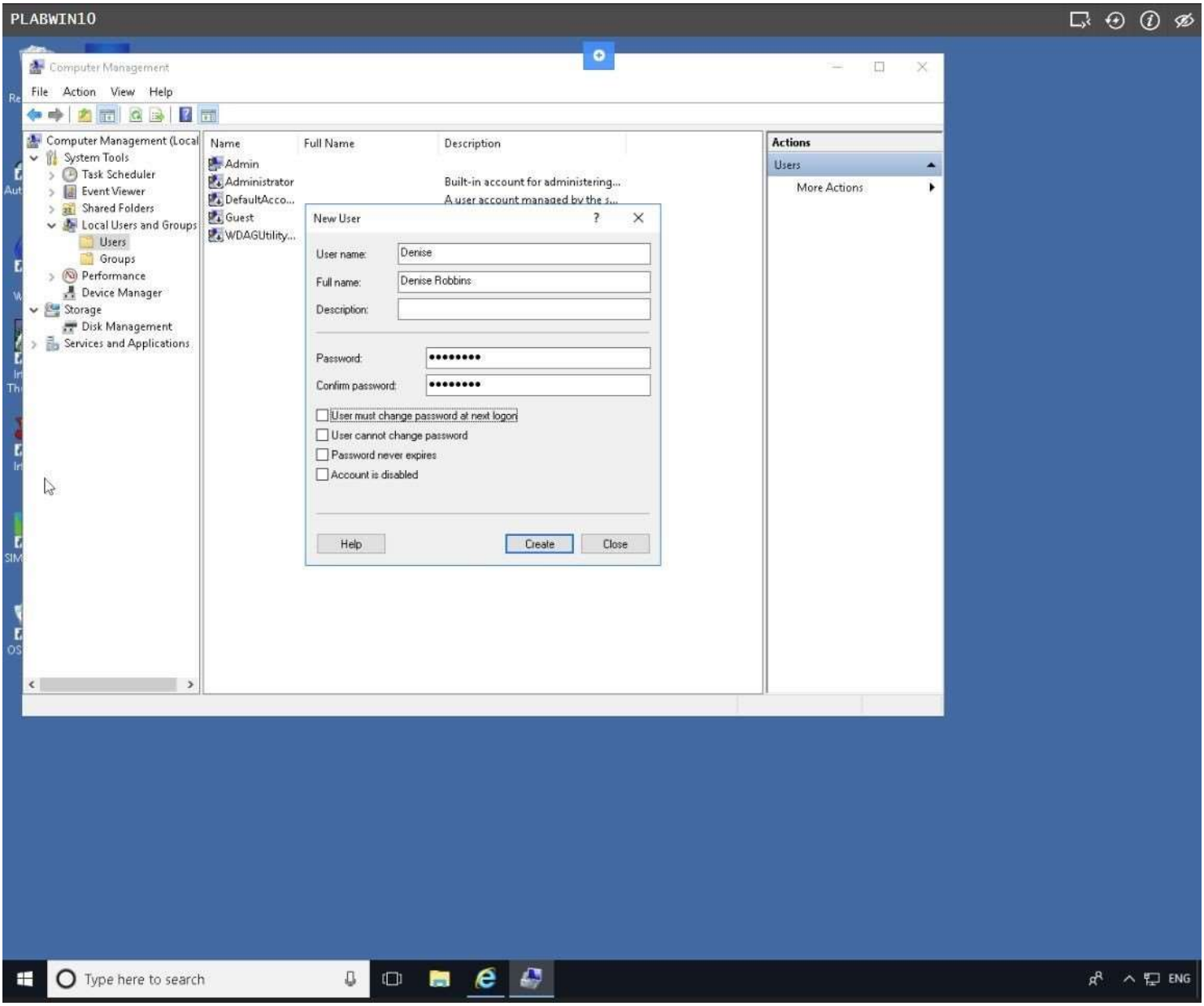
```
Denise Robbins
```

In the **Password** and **Confirm password** text boxes, type:

```
Passw0rd
```

Clear **User must change password at next logon** box.

Click **Create**.

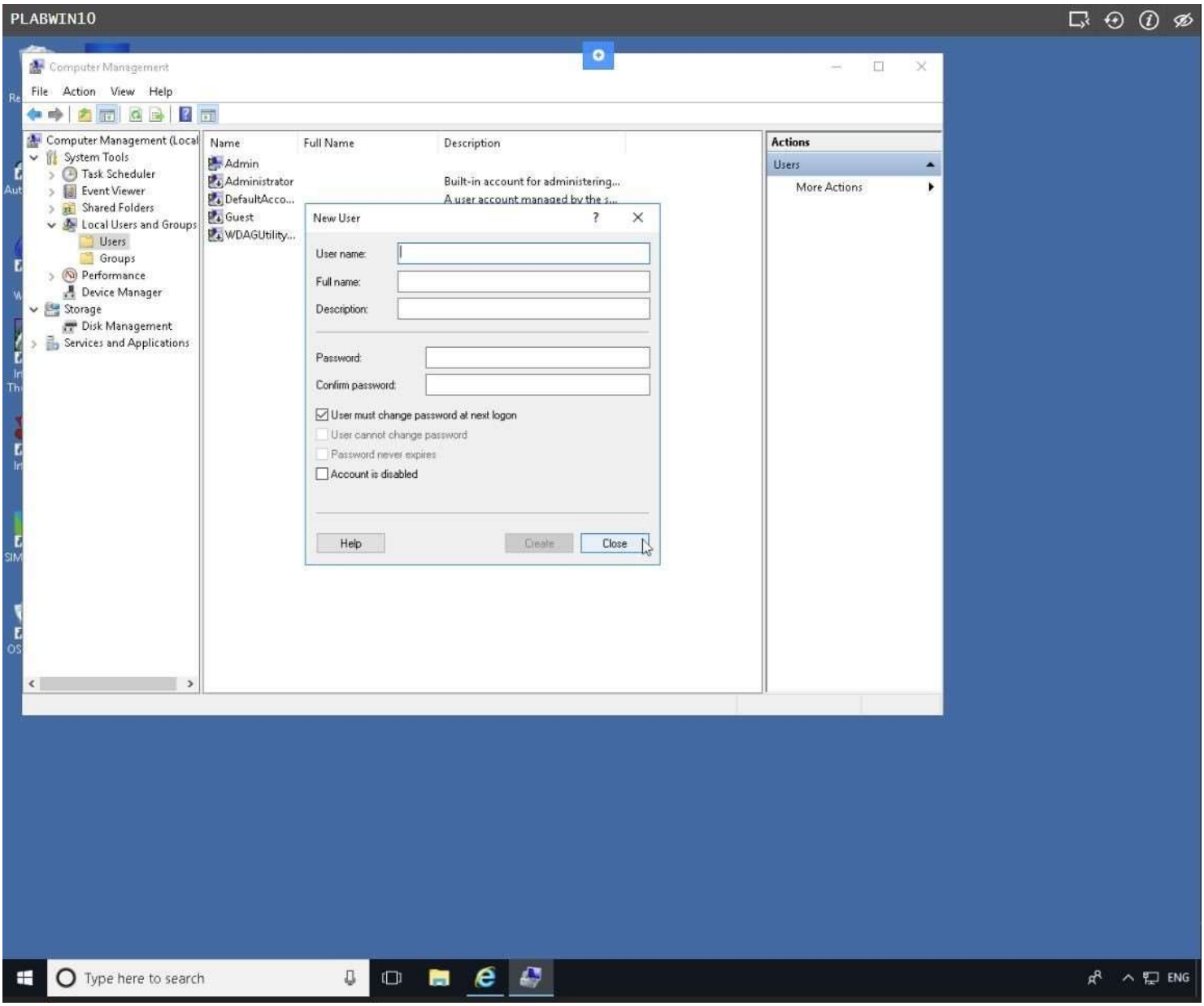


Step 4

Click **Close** to exit from **New User** dialog box.

Note: Before continuing with this task, you must add Denise to the Remote Desktop Users group. Perform the following actions:

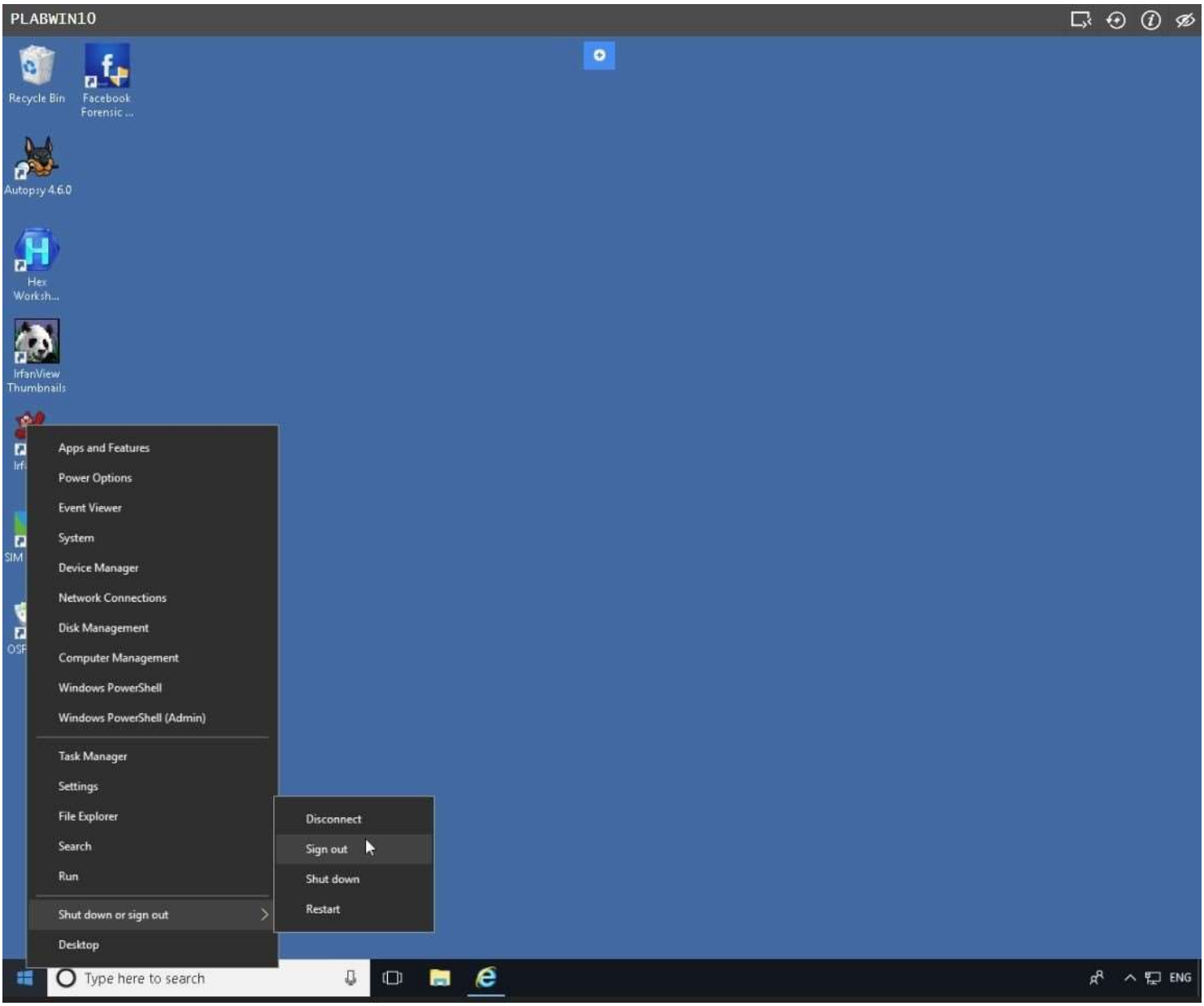
In the Users group, right-click on **Denise** and click **Properties**, then click the **Member Of** tab, click **Add**, type in **Remote Desktop Users** in the **Enter the object names** to select box, click **Check Names**, then click **OK**. Click **OK** again, then close **Computer Management**.



Step 5

The administrator account must be logged off from the workstation to give way to the other user who will use this computer.

Right-click **Start** menu and hover to Shut down or sign out then click **Sign out**.



Task 2 - Turn Off Auto Login

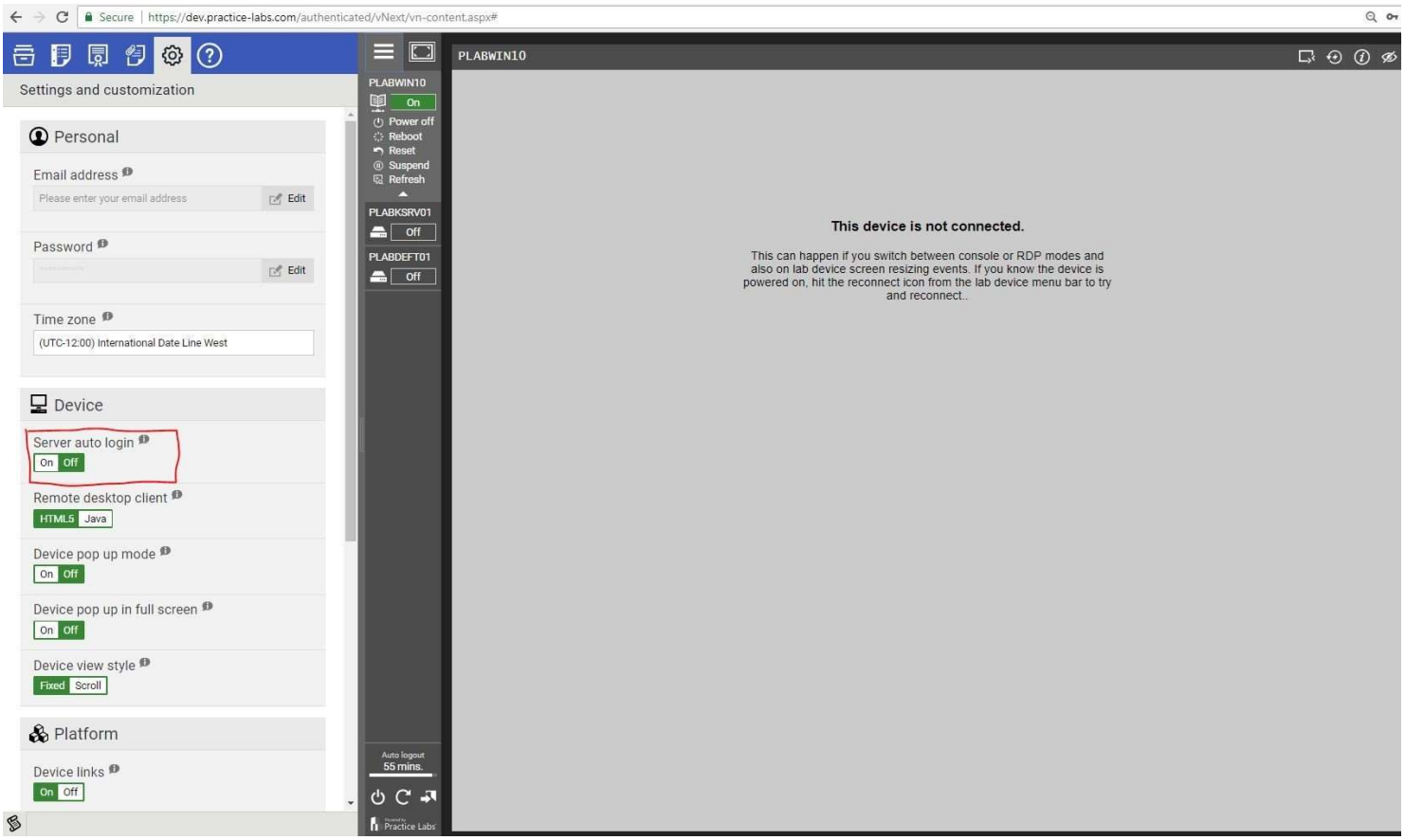
To turn off auto login on the Practice Labs devices, perform the following steps:

Step 1

Access the Practice Labs web application.

Click **Off** button next to Server auto login.

The [**X**] icon will be displayed. This means that other user accounts in the lab can logon to the devices.



Keep the device powered on in its current state and proceed to the next task.

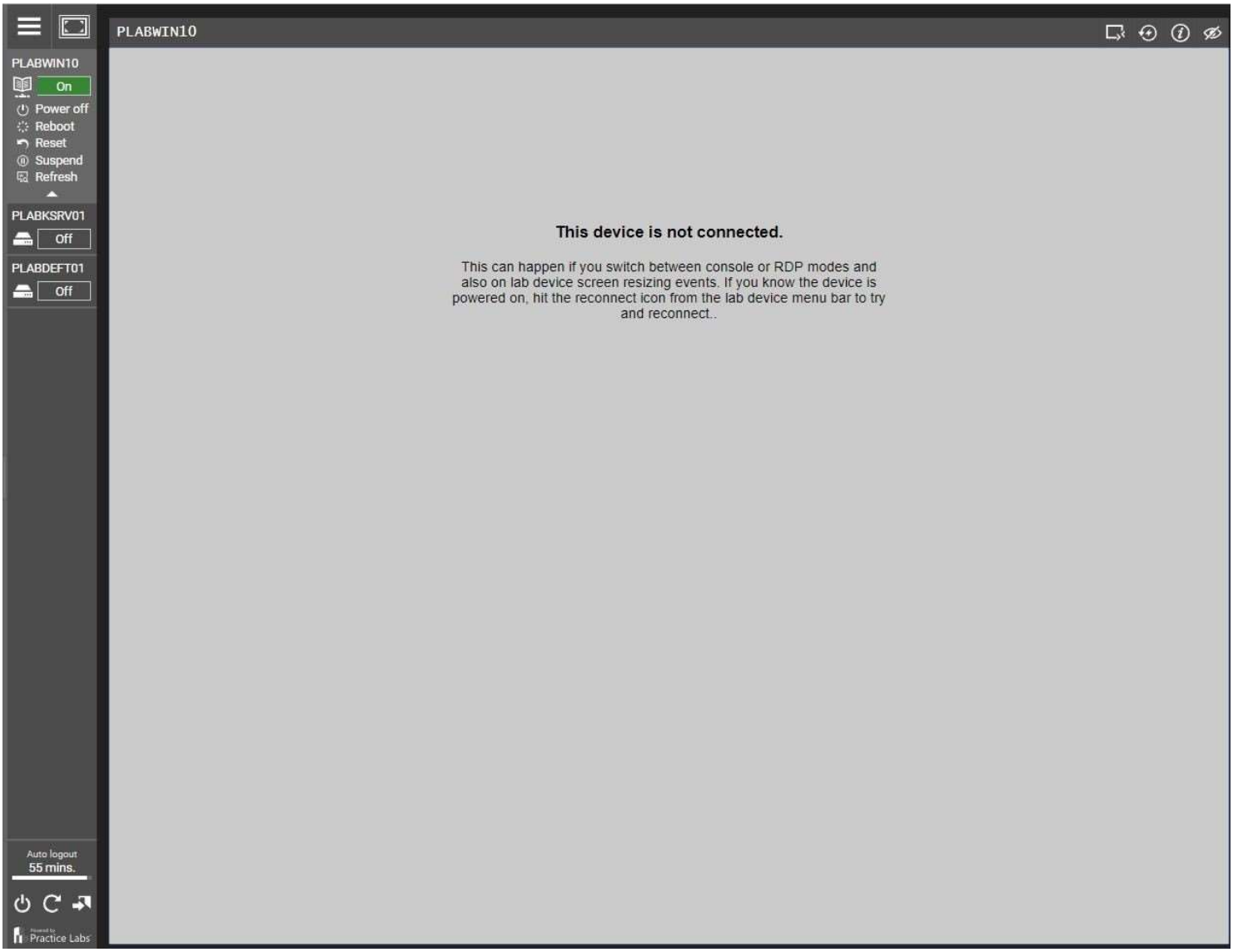
Task 3 - Customize User Environment

In this task, you will sign on as Denise Robbins and customize the user desktop environment.

To set up the user desktop settings, perform the following steps:

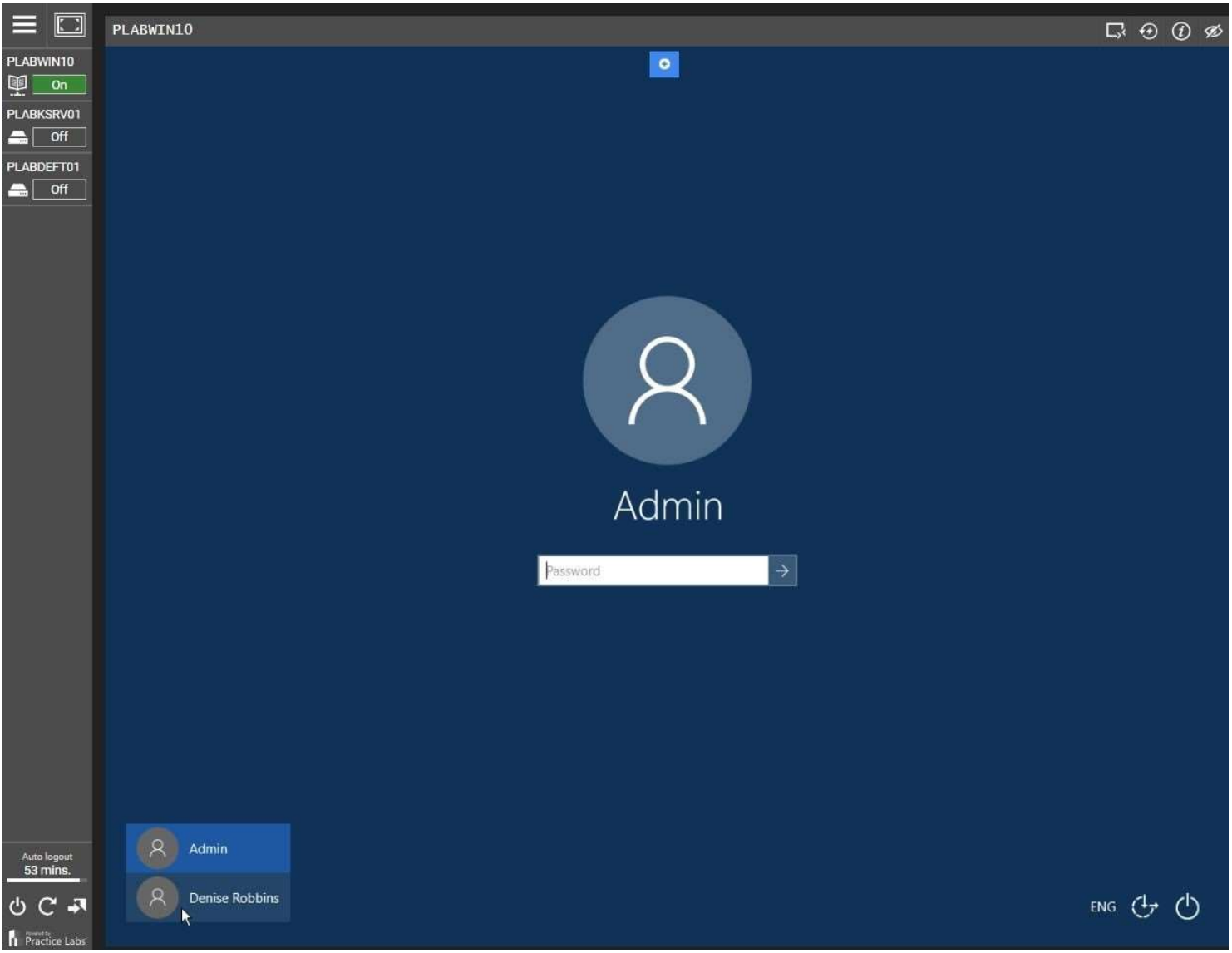
Step 1

On the Practice Labs web application, connect to **PLABWIN10** device.



Step 2

On the sign on screen, click **Denise Robbins**.

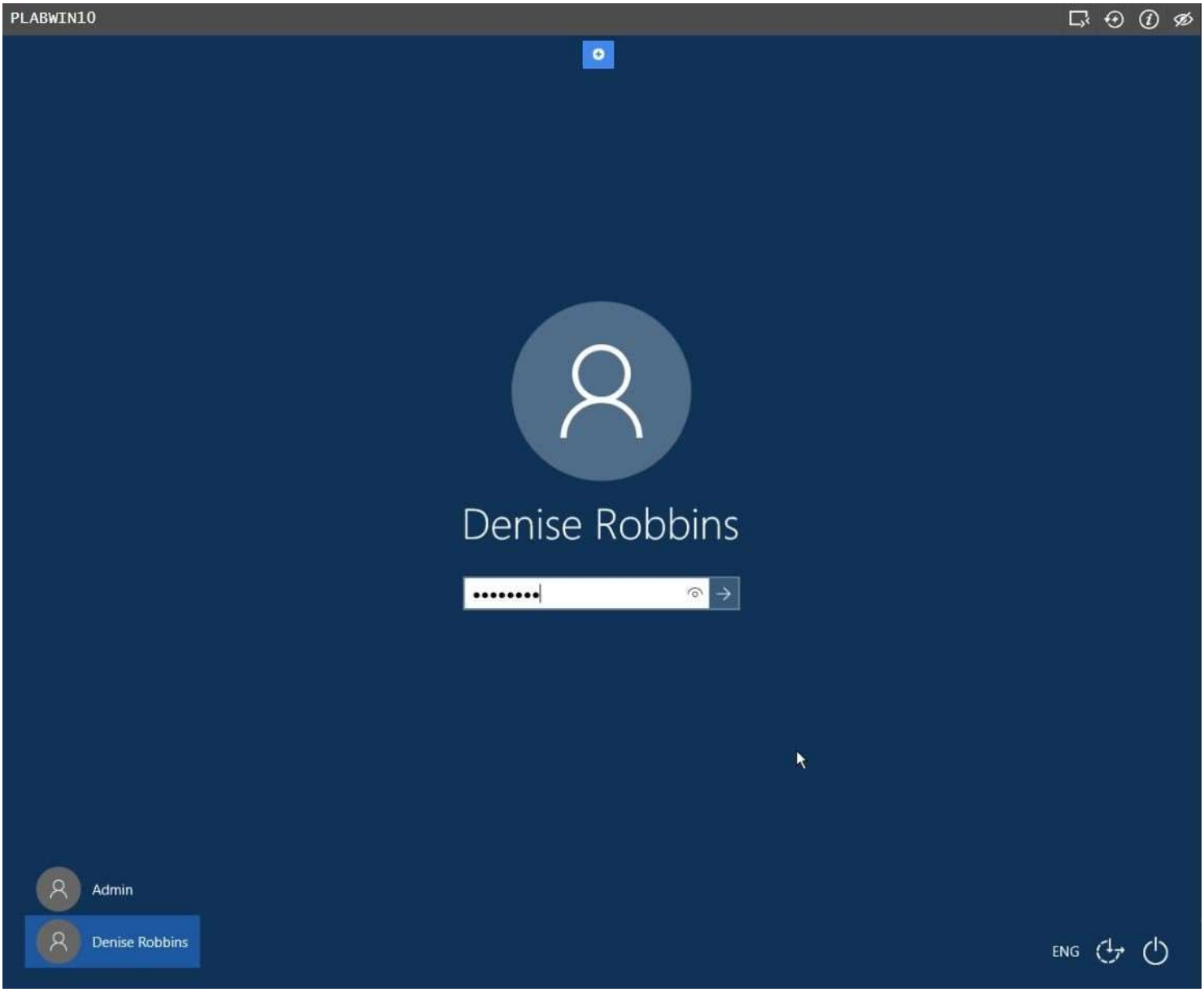


Step 3

On the password text box, type:

`Passw0rd`

Press **Enter**.

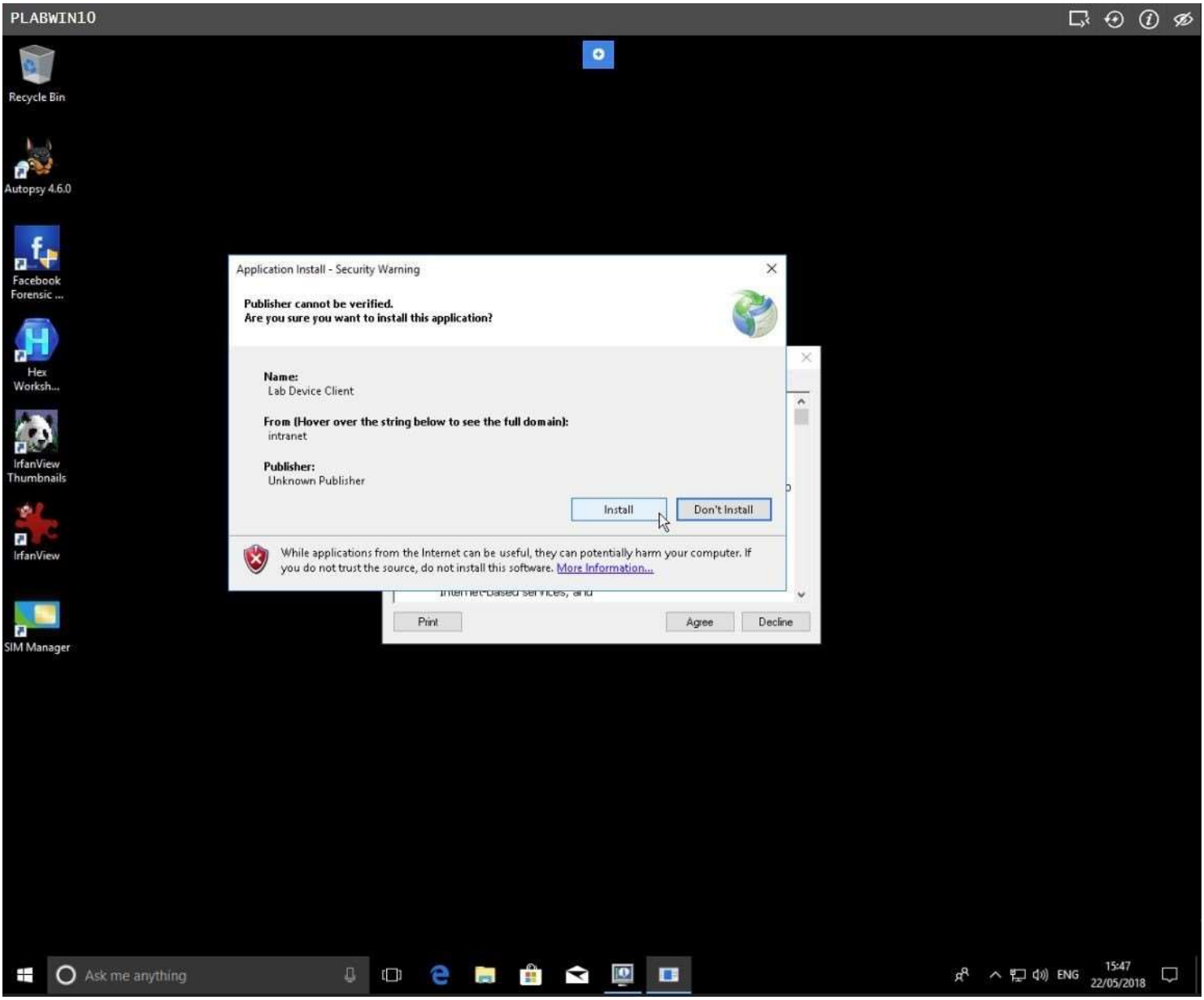


Step 4

You will get a number of system prompts upon sign-on.

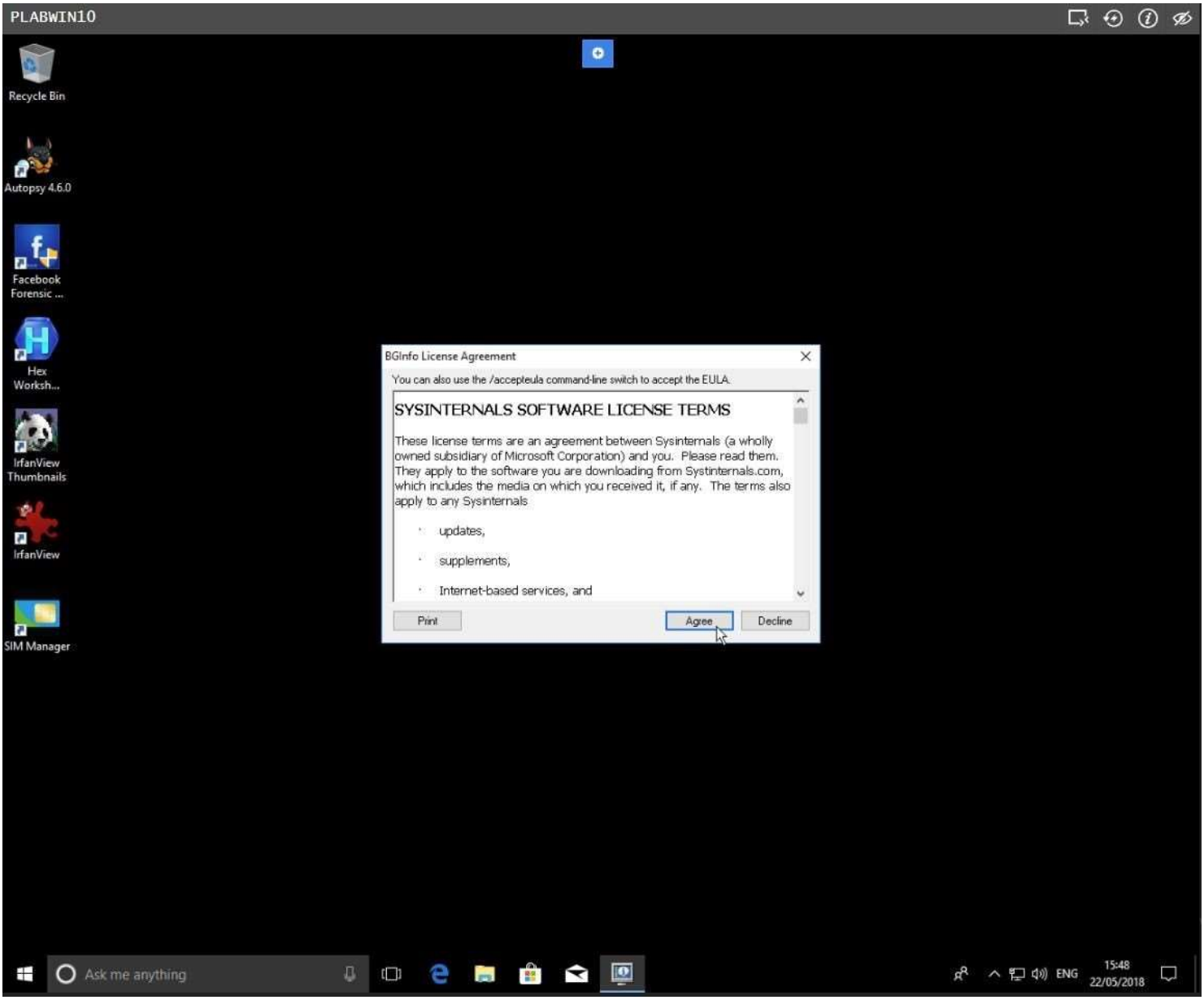
On the **Application Install-Security Warning** dialog box, click **Install**.

> *Note: This is an agent software in the Practice Labs device.*



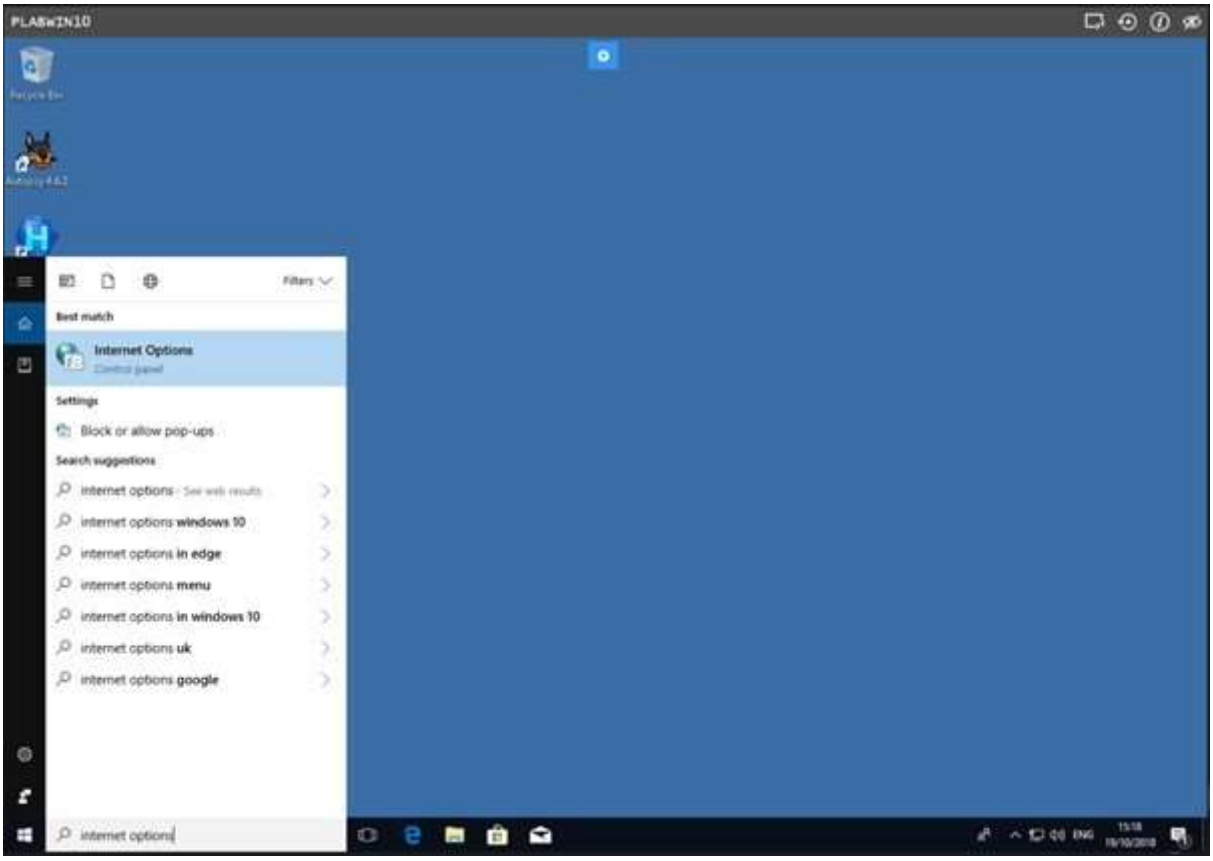
Step 5

On the **BGInfo License Agreement** dialog box, click **Agree**.



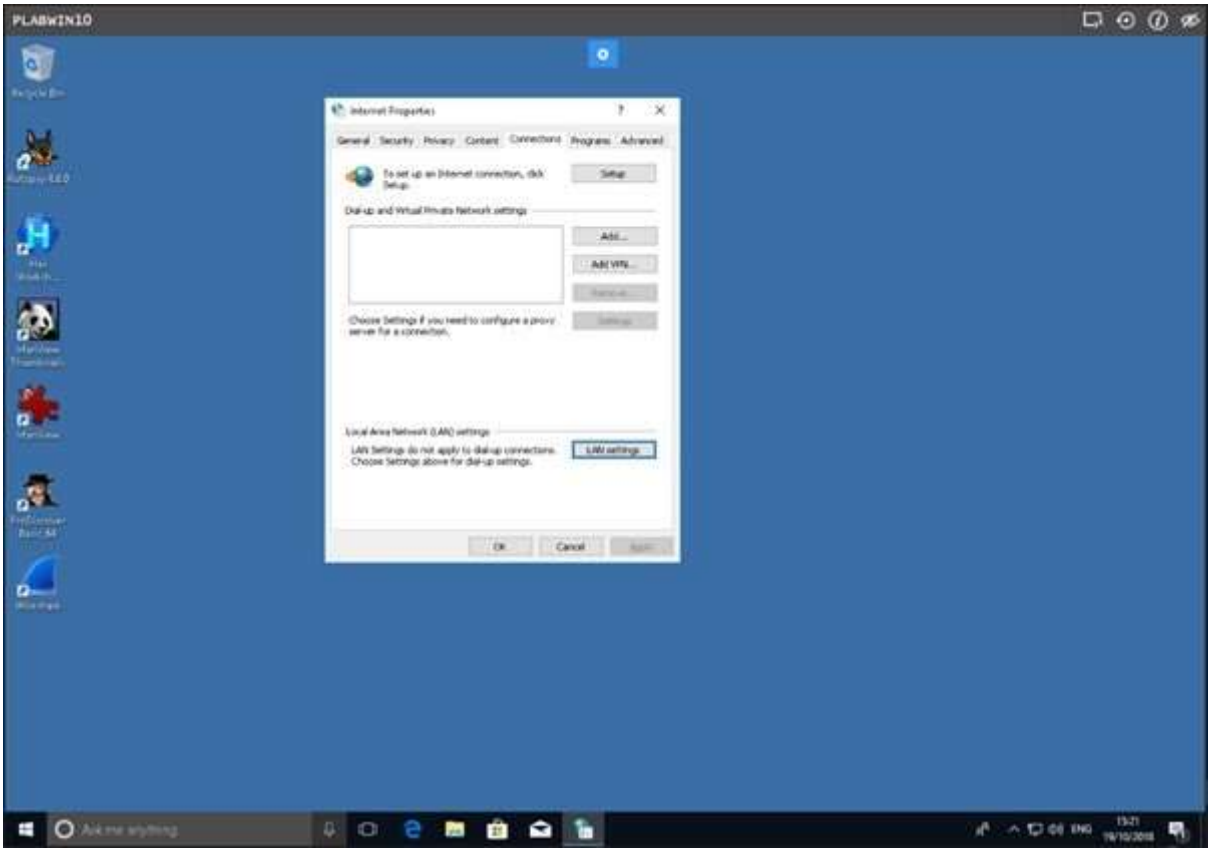
Step 6

In order to access the Internet, you will need to edit the proxy settings in Internet Options. Click the Start charm and type **Internet Options** and press **enter.**



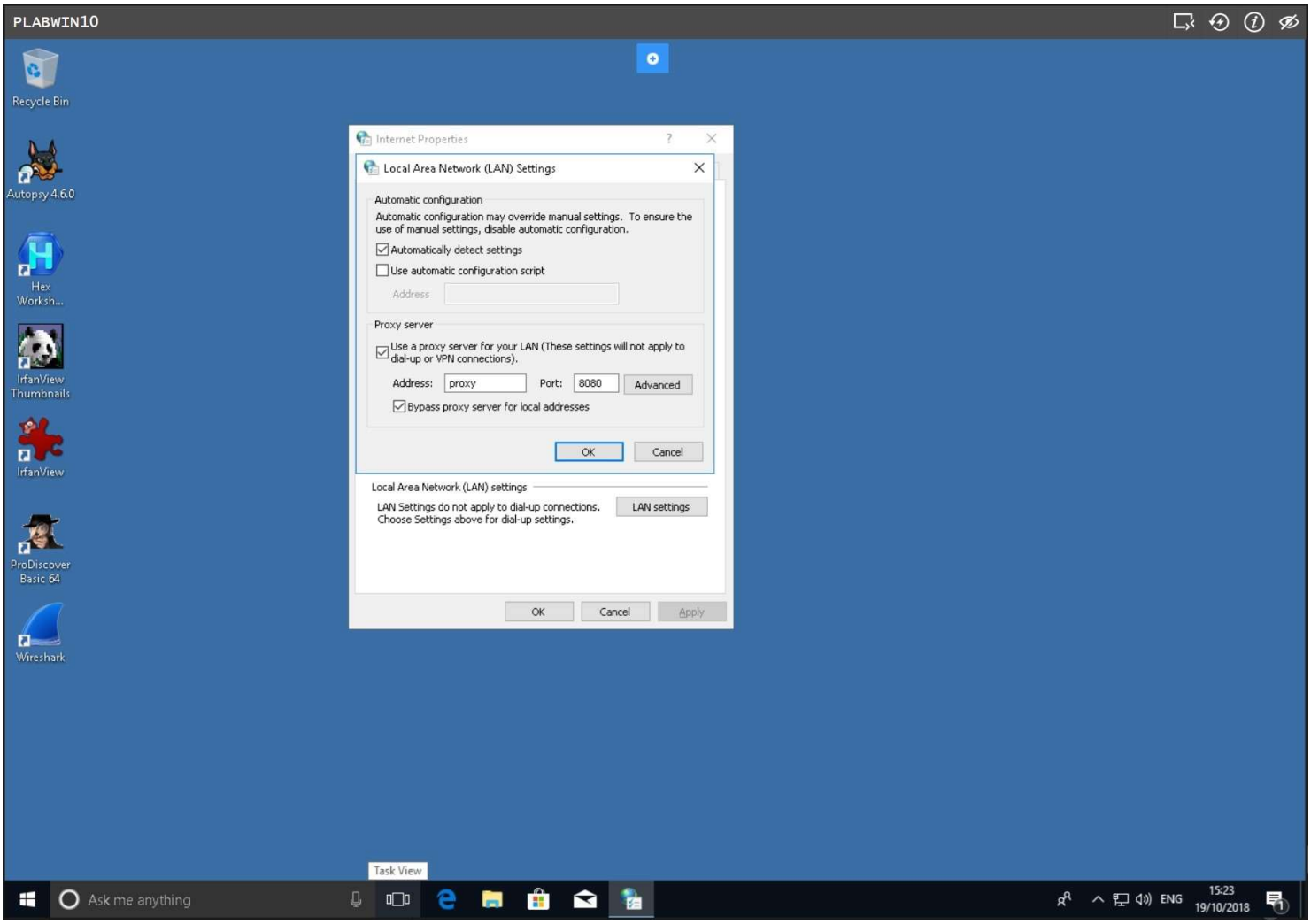
Step 7

Click the **Connections** tab and then click **LAN settings**.



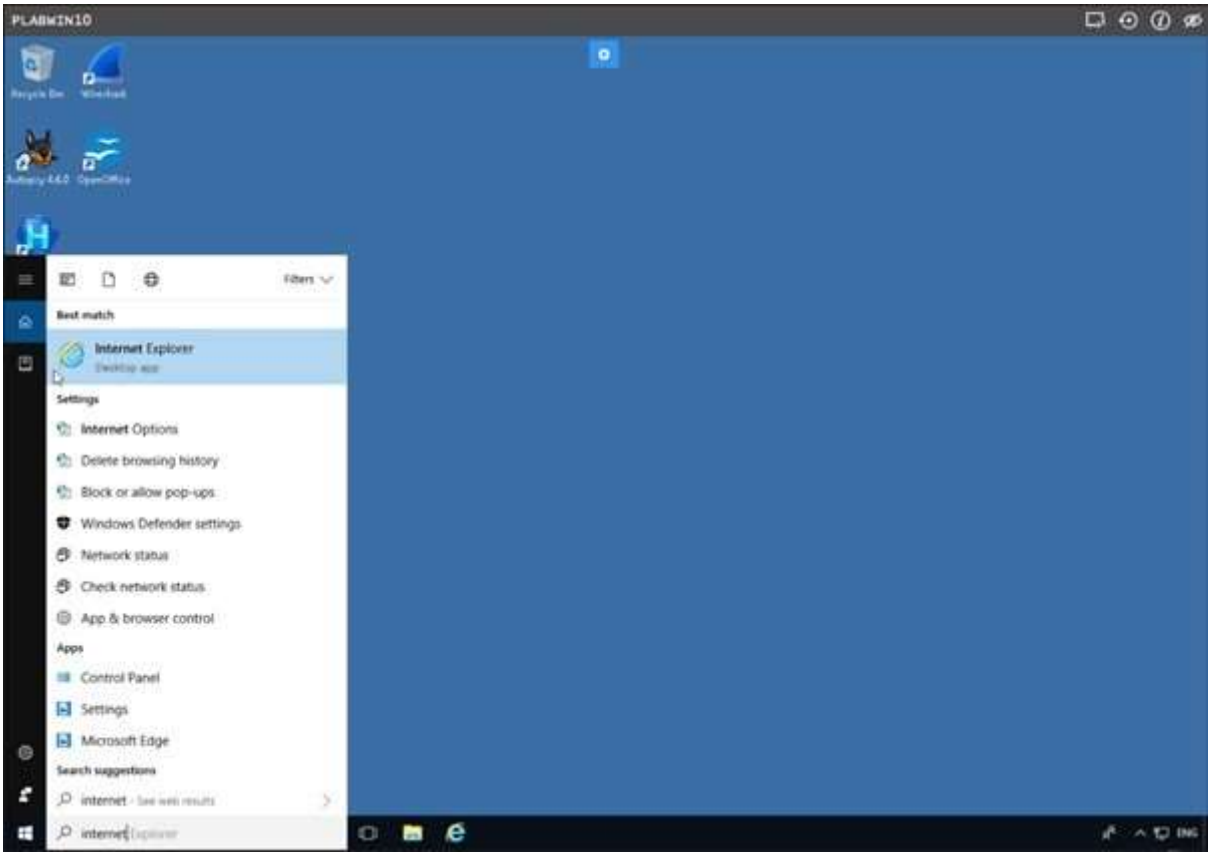
Step 8

On the **Local Area Network Settings** page, choose **Use a proxy server for your LAN** and type in **proxy** in the address box and **8080** in the port box. Check the **Bypass proxy server for local addresses** box. Then click **Ok** twice.



Step 9

Open **Internet Explorer** from the Start menu.

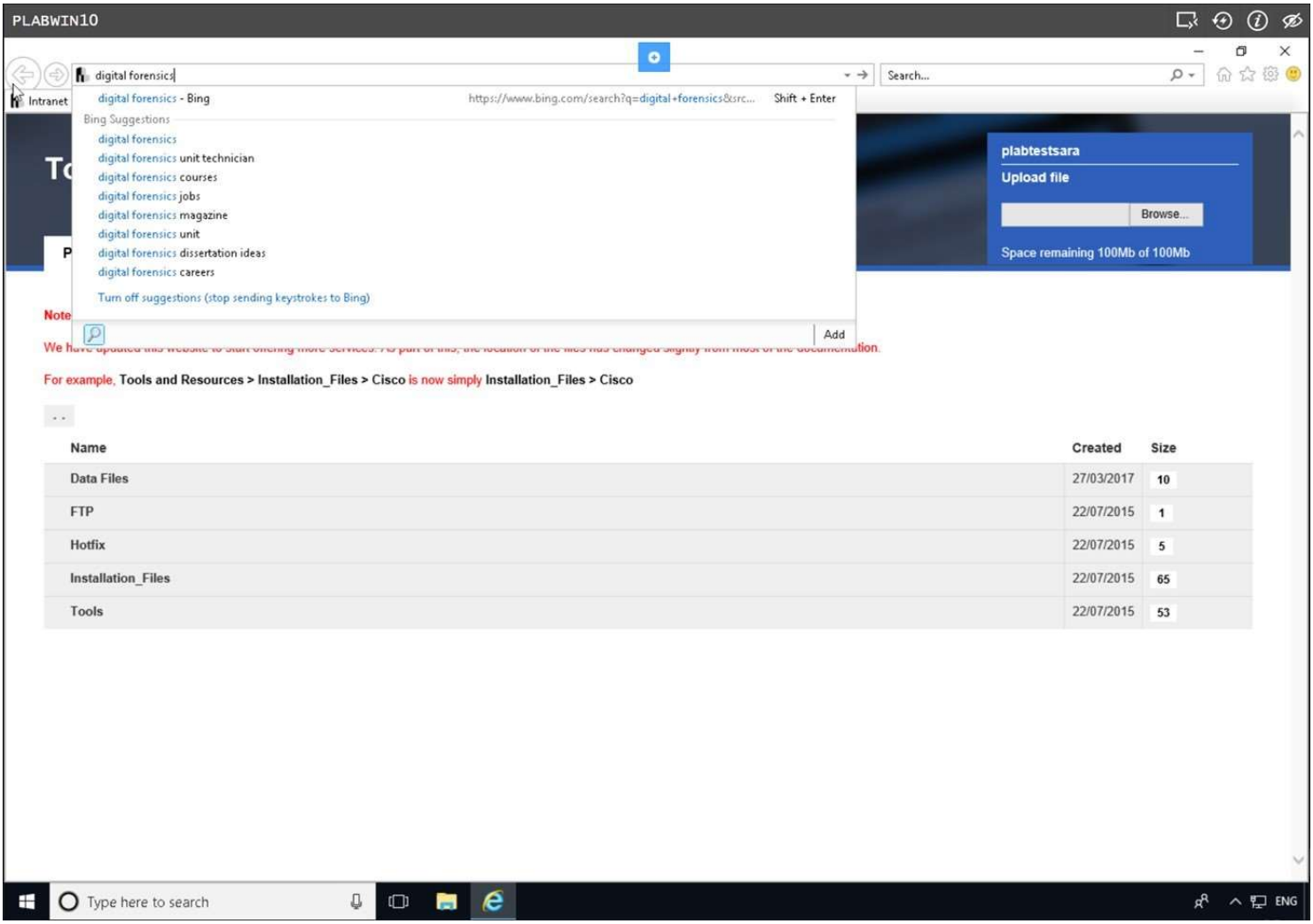


Step 10

Click in the address bar and type:

```
Digital forensics
```

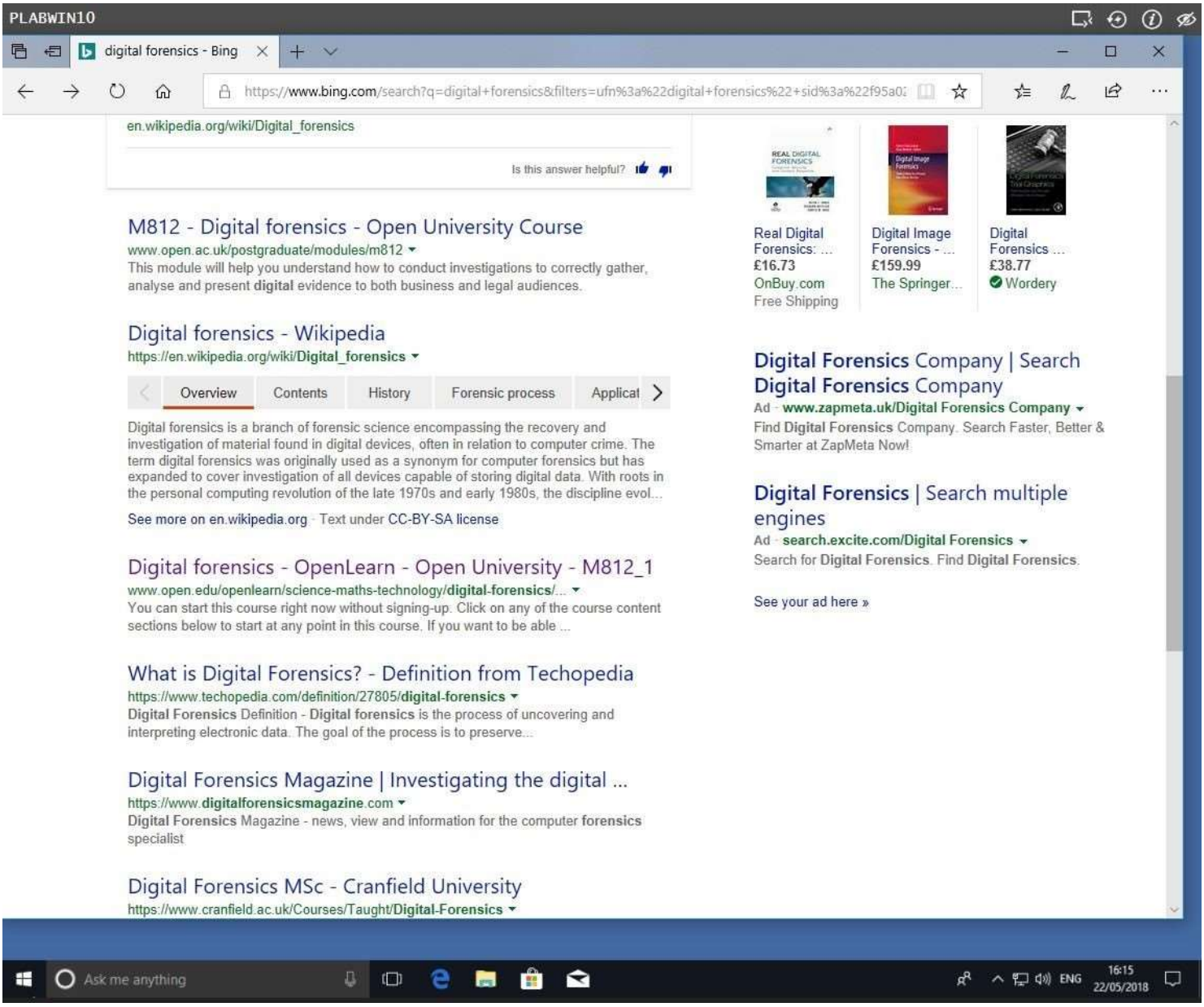
Press **Enter**.



Step 11

On the collected results by the search engine, click **Digital forensics - OpenLearn....**

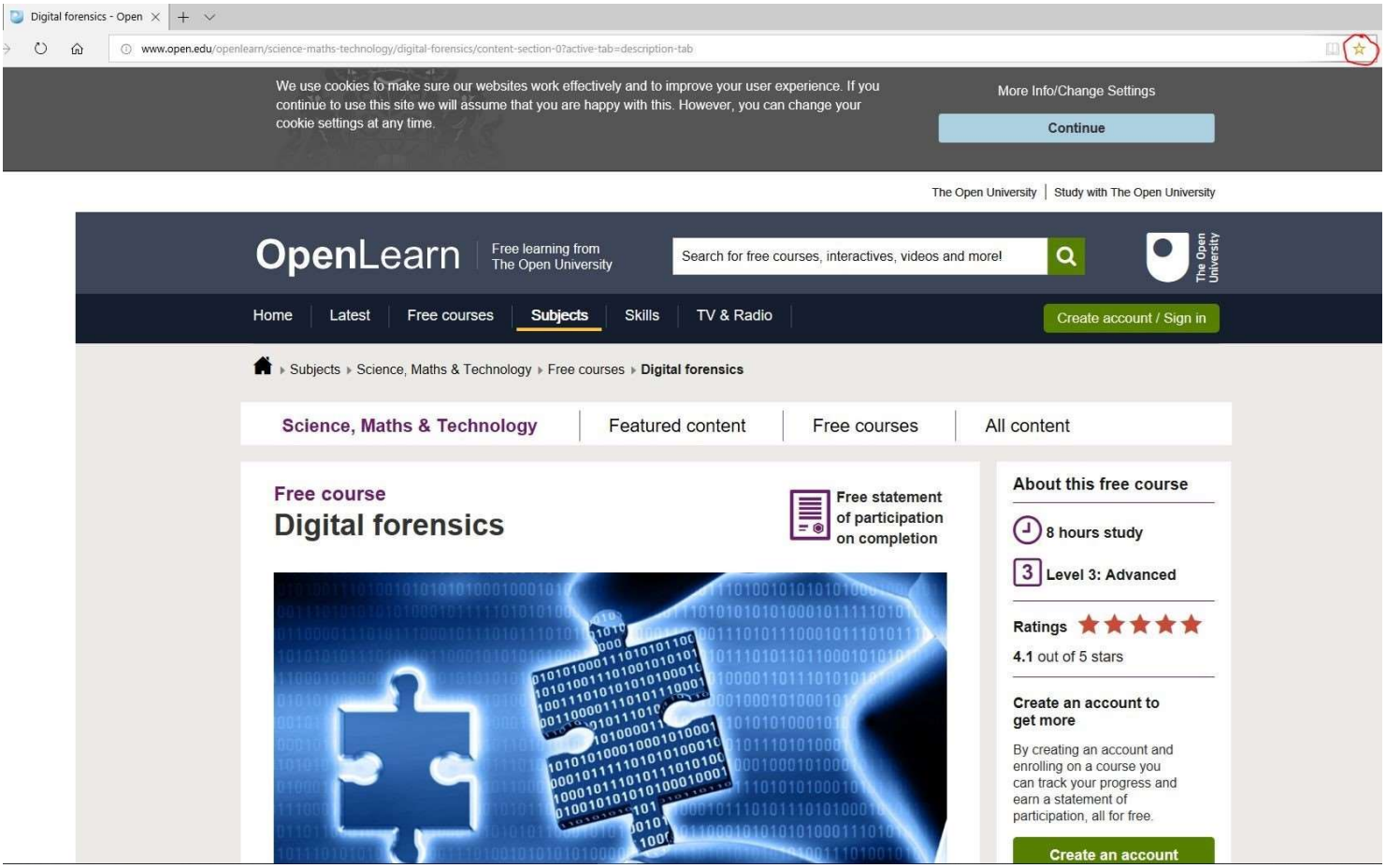
Alternatively, you may click on the other results but make sure they aren't blocked by the firewall policy in the Practice Labs devices.



Step 12

The **OpenLearn** web site is displayed.

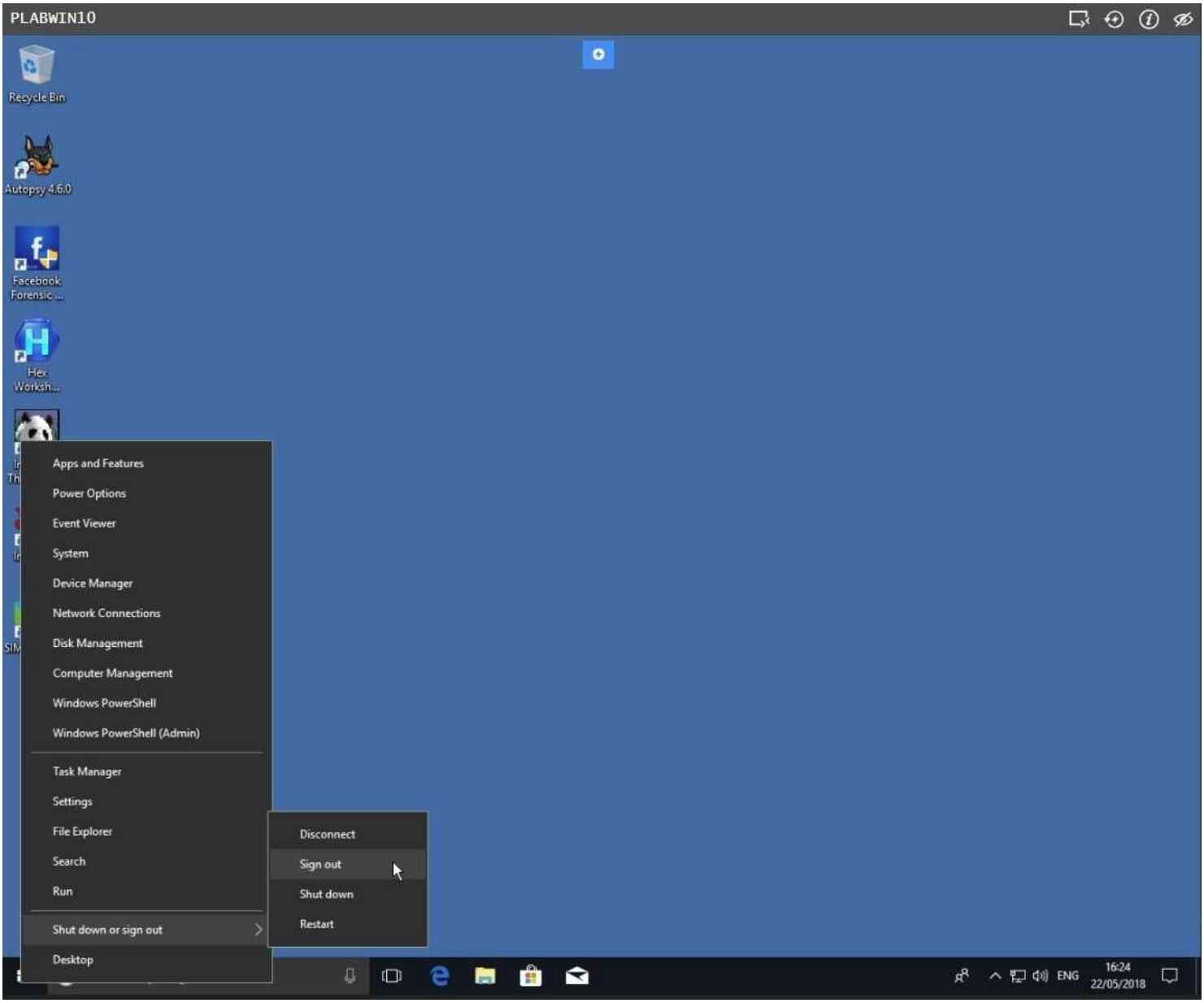
Click **Favorites** star to the right of the address bar.



Step 13

To prepare for the next task where you will examine the user profile of Denise Robbins, you will log off this user.

Right-click **Start** menu, hover **Shut down or sign out** and click **Sign out**.

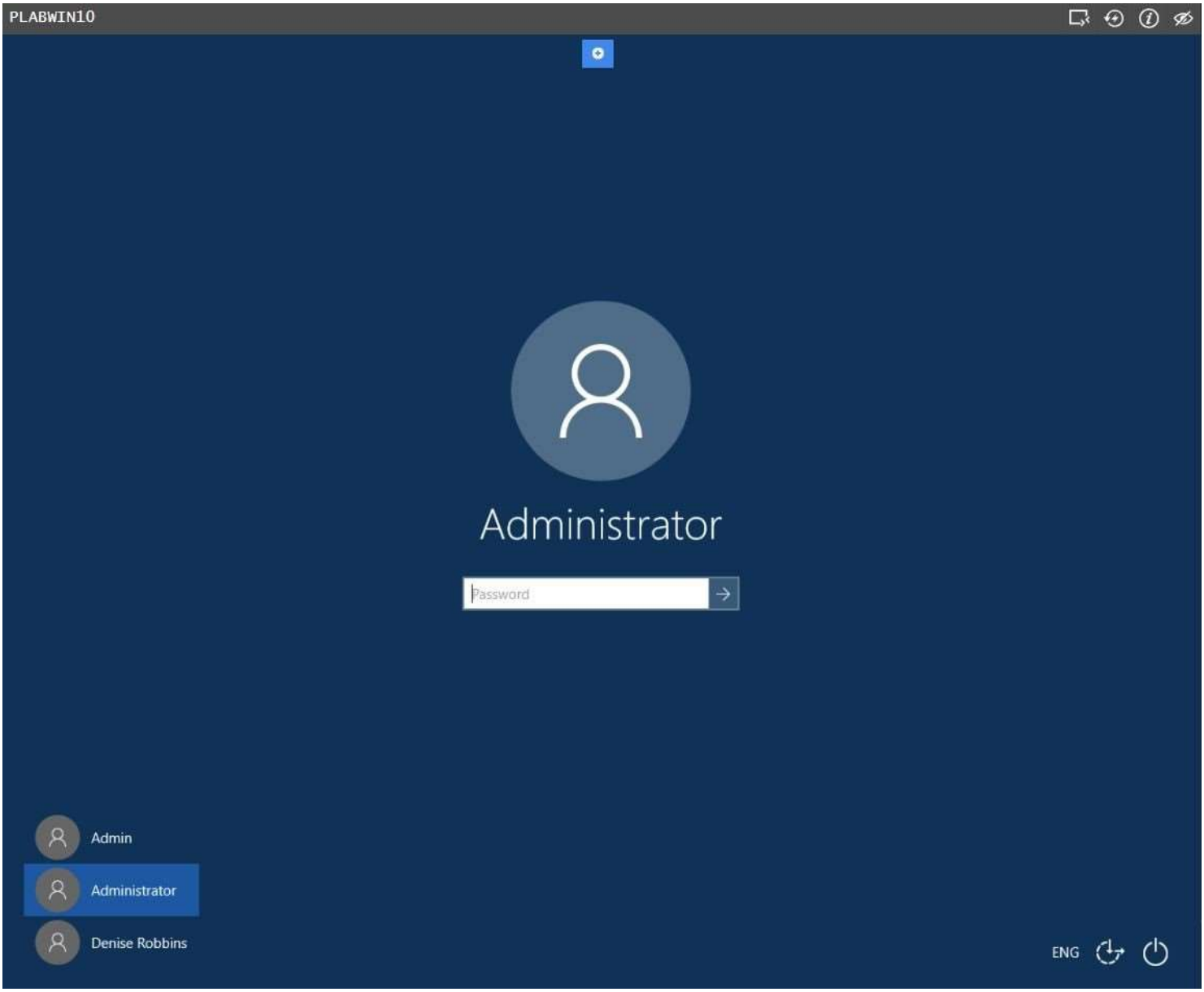


Task 4 - Examine Windows Registry

Step 1

Reconnect to **PLABWIN10** as you did before.

On the sign-on screen, click **Administrator**.

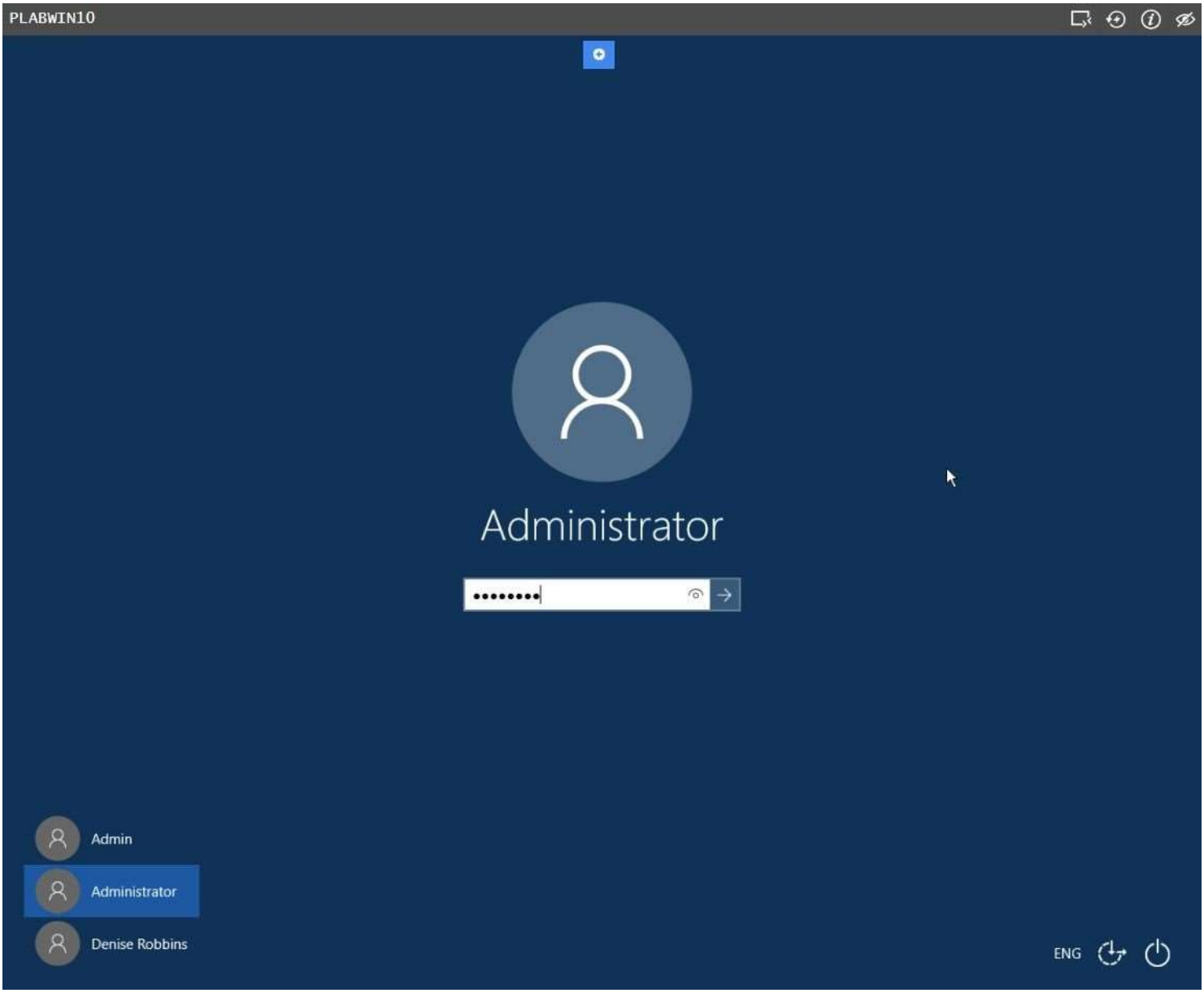


Step 2

On the password text box, type:

`Passw0rd`

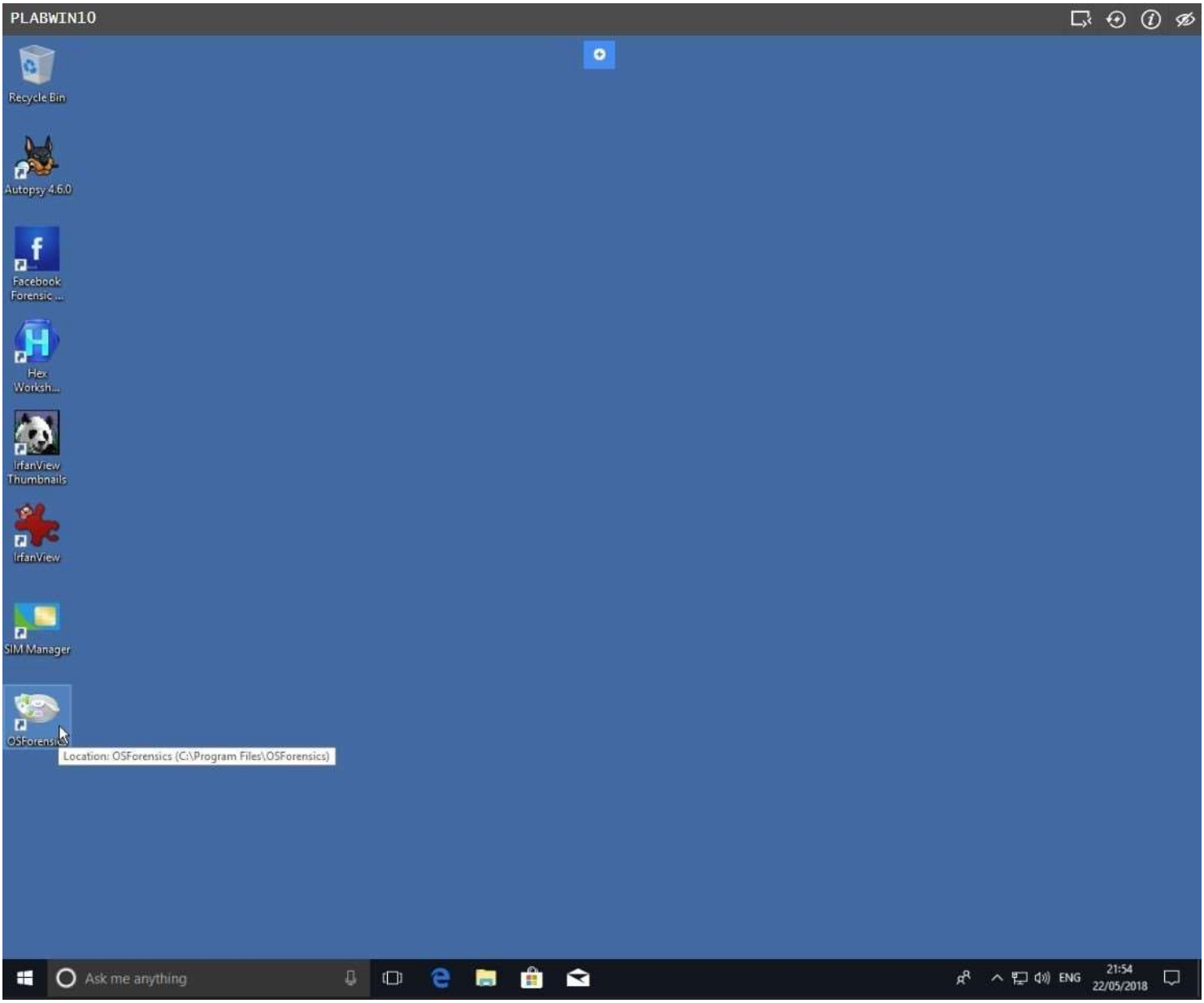
Press **Enter**.



Step 3

Double-click the **OSForensics** icon on the desktop.

Note: If OSForensics is not installed, you will need to download and install it from the Tools and Resources page on the Intranet.

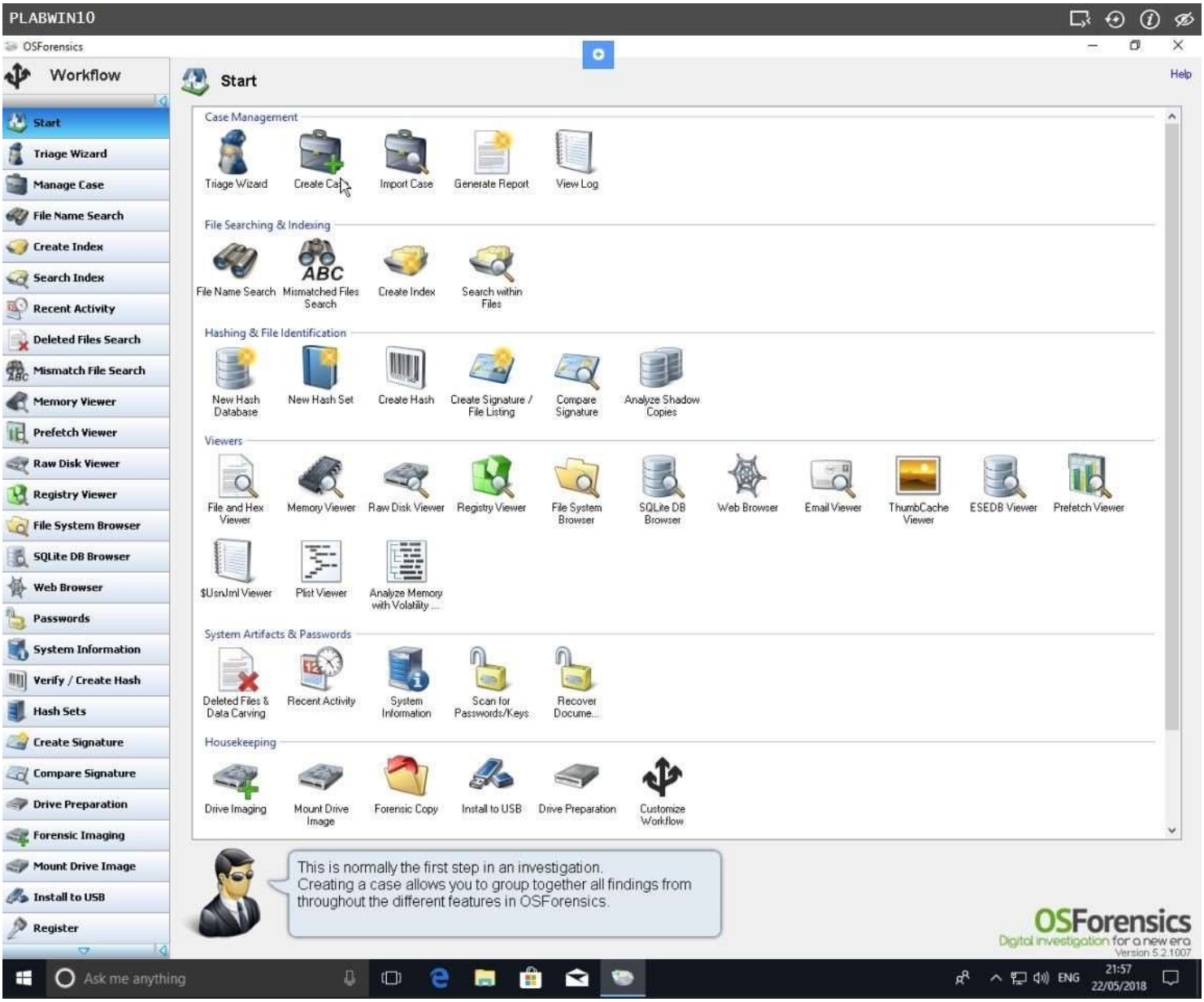


Step 4

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

Step 5

In the center pane, click the **Create Case** button.



Step 6

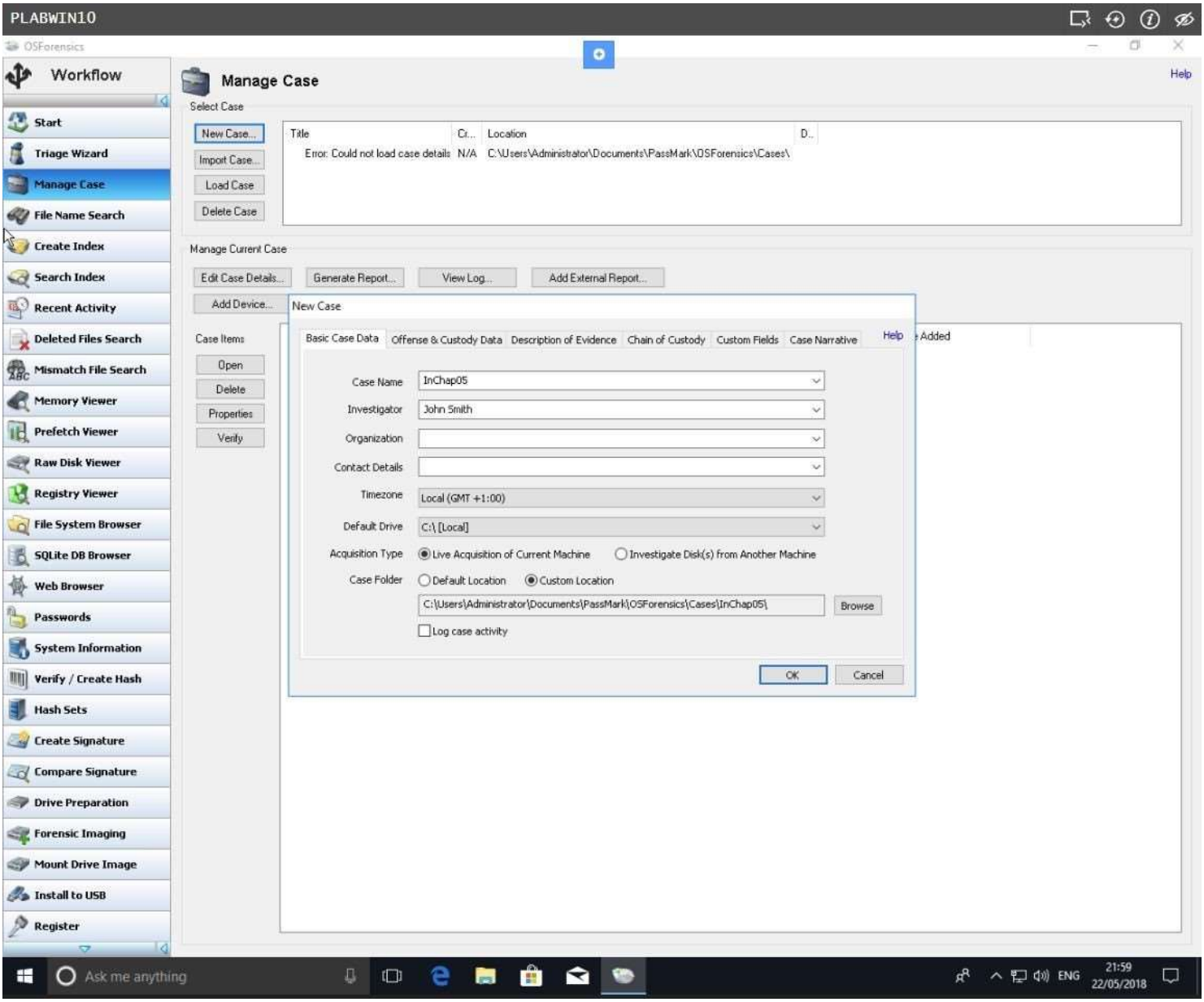
In the **New Case** dialog box, click in the **Case Name** text box type:

```
InChap05
```

Enter your name in the **Investigator** text box.

For the **Acquisition Type** setting, ensure that the **Live Acquisition of Current Machine** option button is selected.

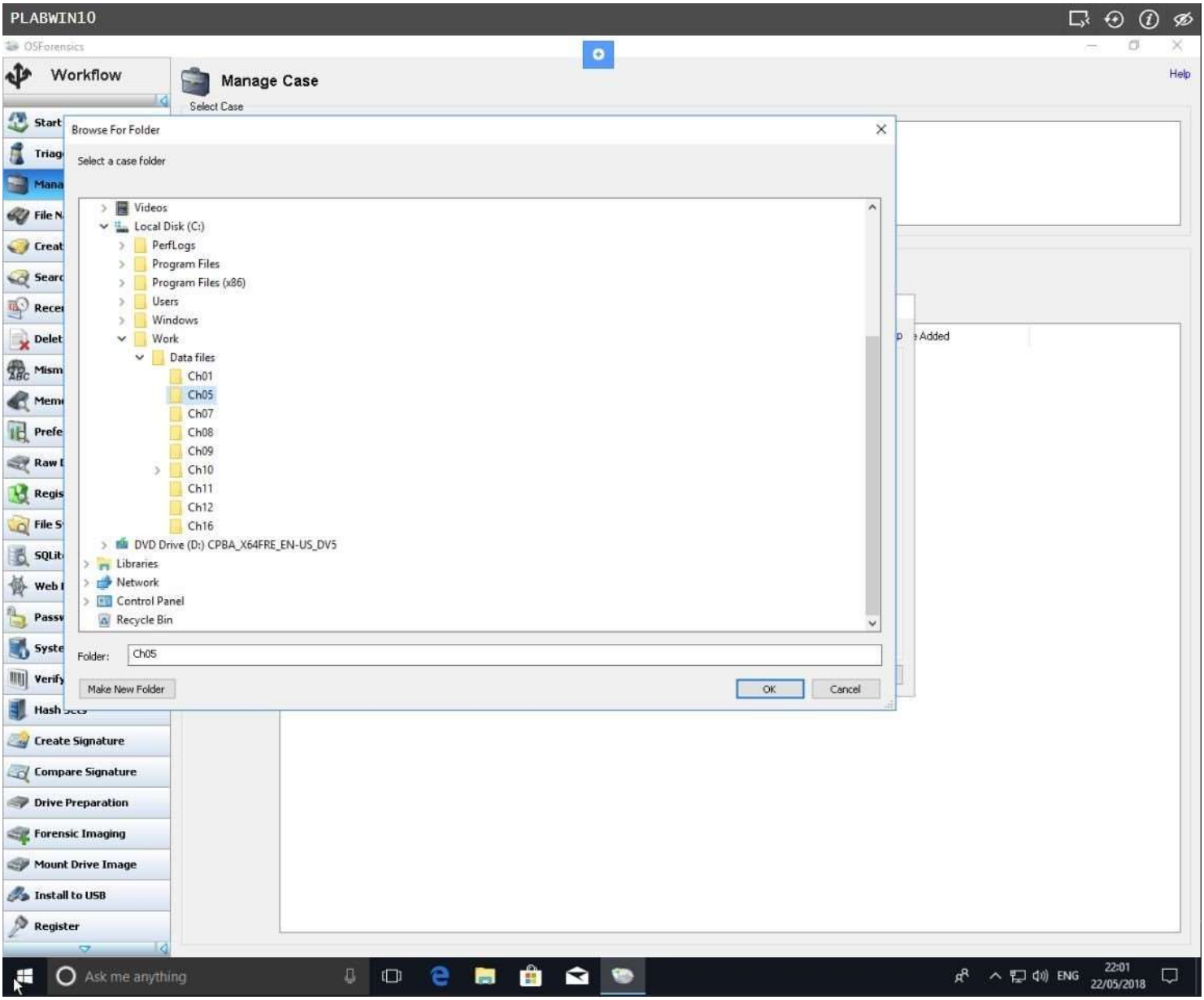
Click **Custom Location for the Case Folder option**. Select the **Browse** button on the lower right.



Step 7

On the **Browse For Folder** dialog box, expand **This PC > Local Disk (C:) > Work > Data files** and select **Ch05** folder.

Click **Make New Folder**.

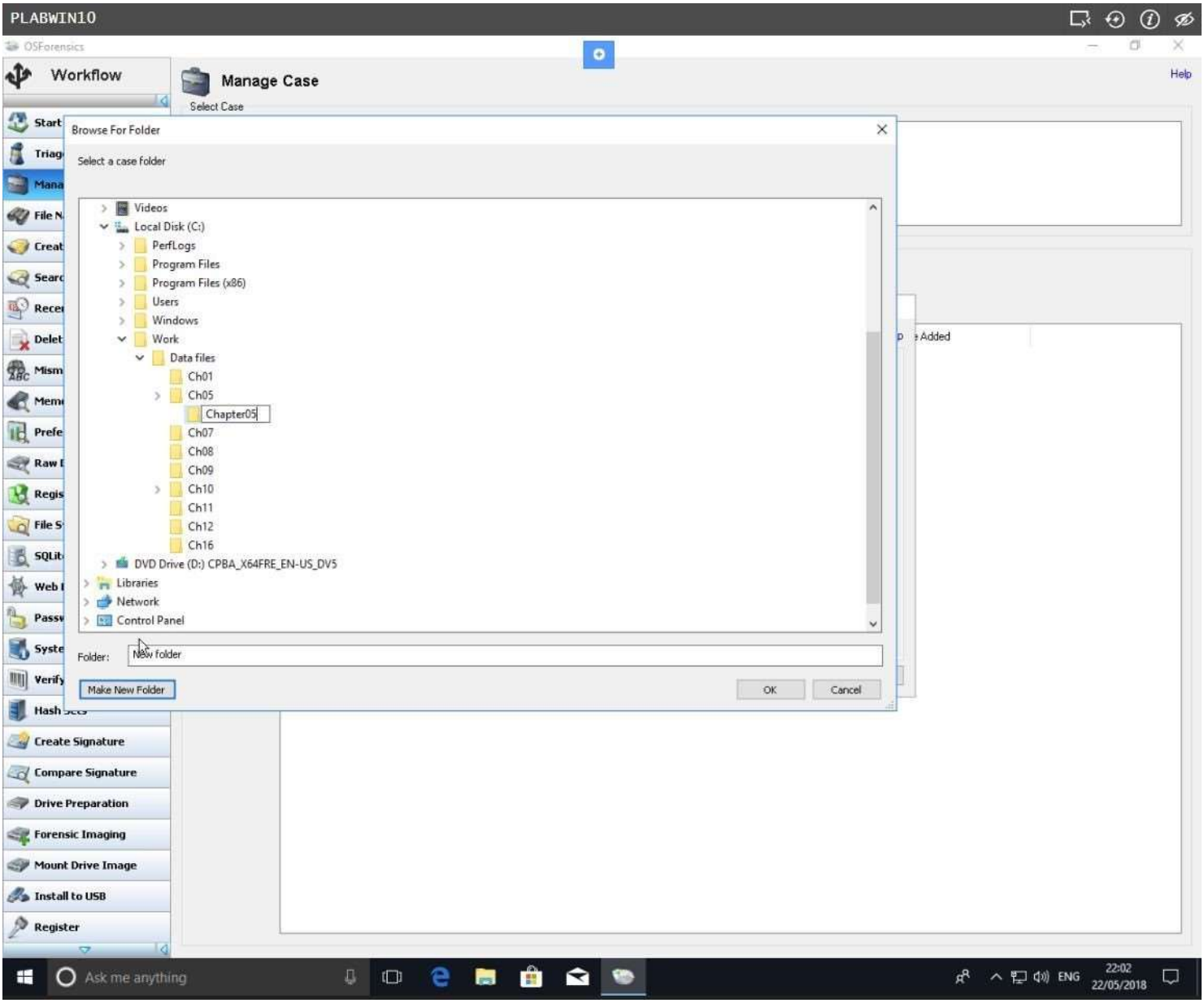


Step 8

Name the folder as:

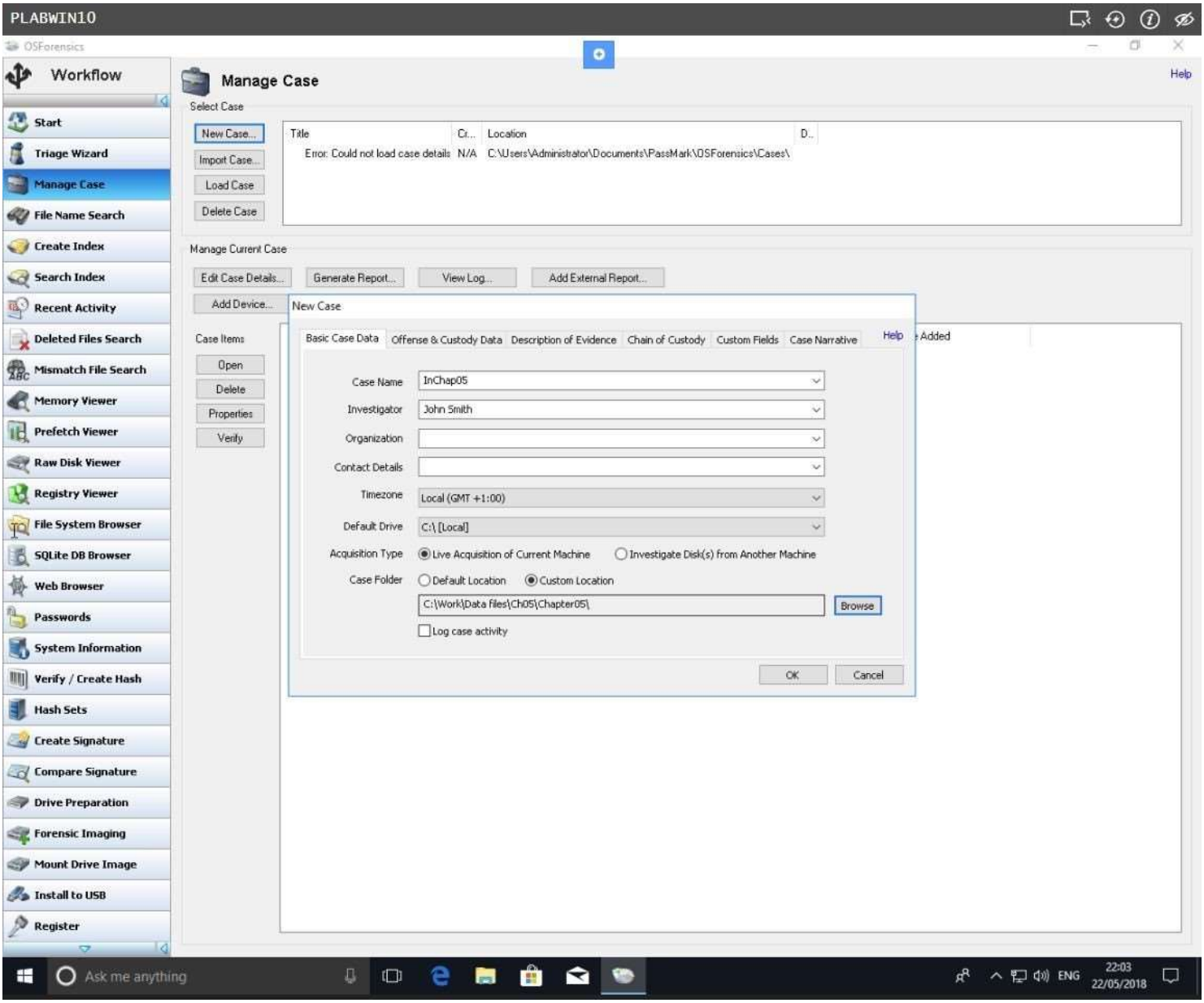
```
Chapter05
```

Click **OK**.



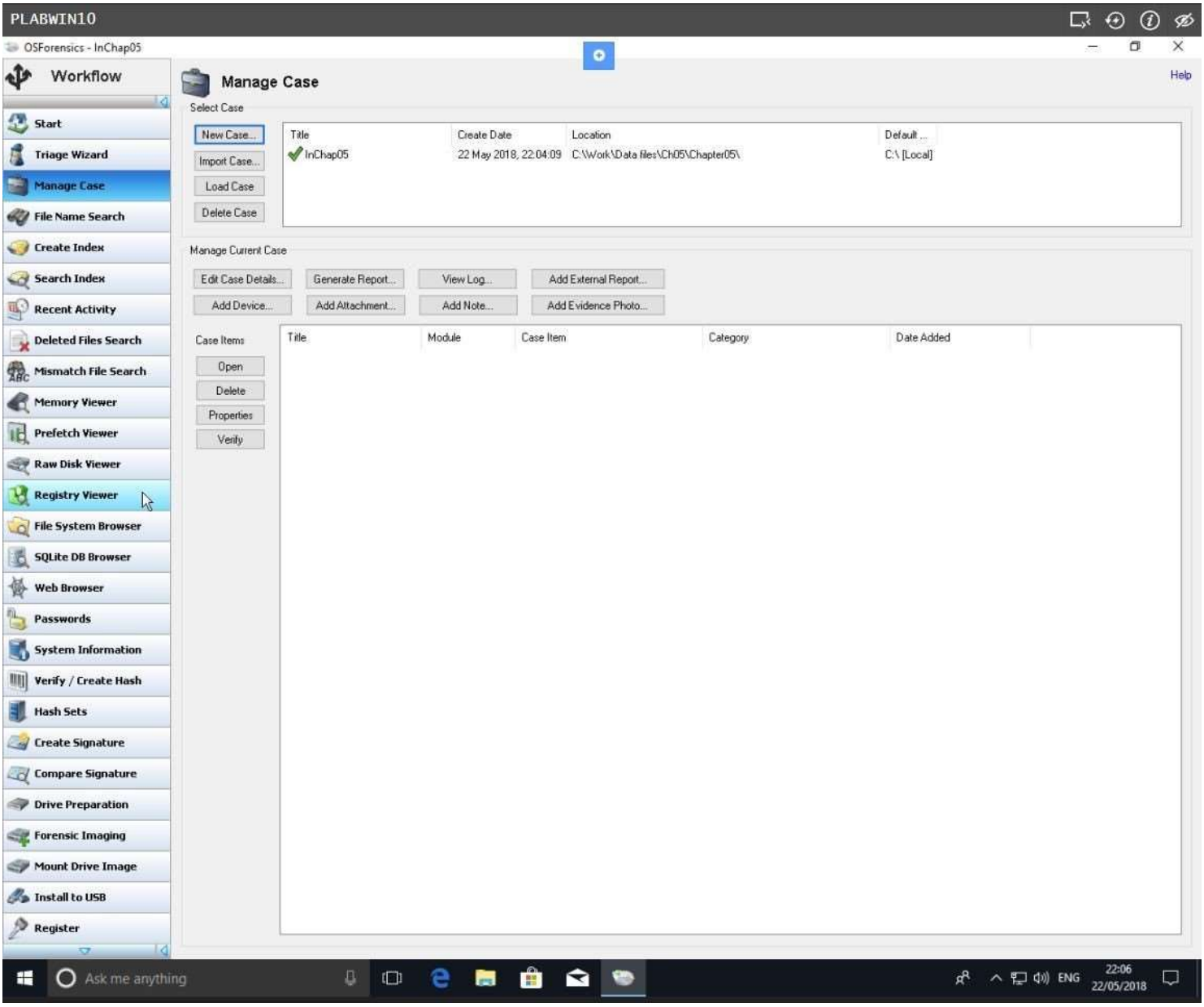
Step 9

Back on the **New Case** dialog box, click **OK**.



Step 10

On **OSForensics - InChap05** window, click **Registry Viewer** on the left panel.

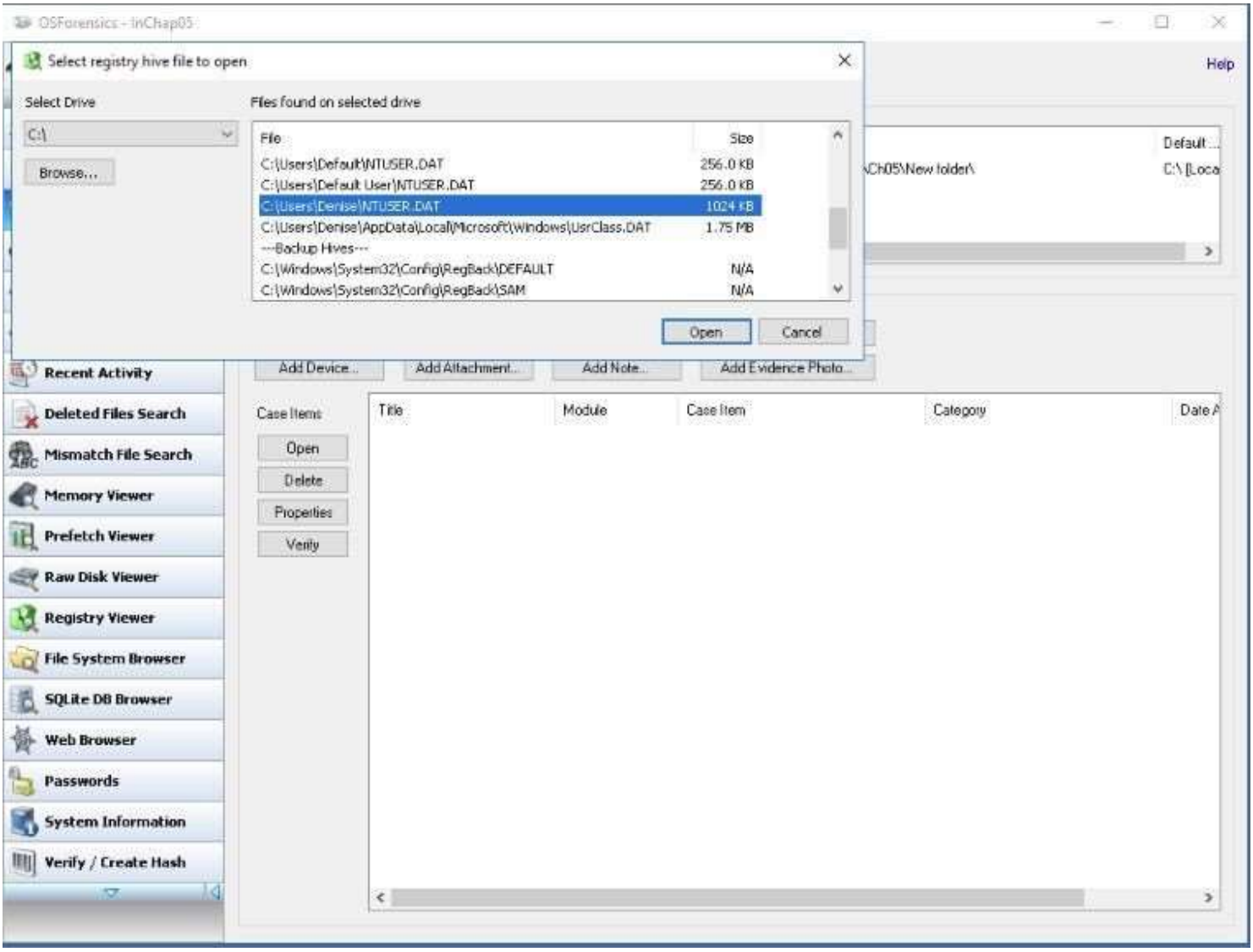


Step 11

On the Select registry hive file to open dialog box, notice the Registry files found on the local computer. Select the following:

```
c:\users\Denise\NTUSER.DAT
```

Click **Open**.

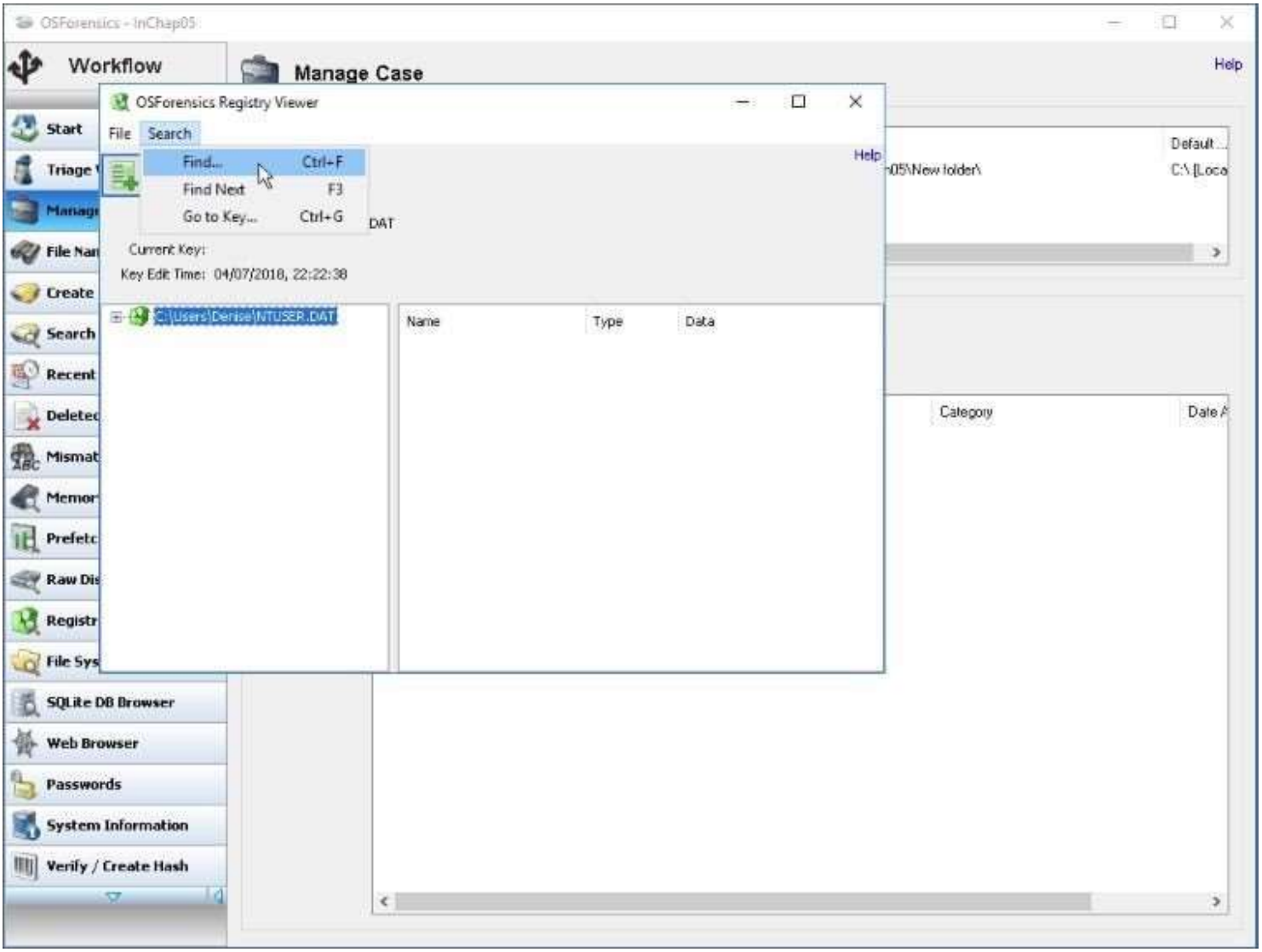


Step 12

The **OSForensics Registry Viewer** window opens.

Ensure that **C:\users\Denise\NTUSER.DAT** is selected.

Click **Search** and select **Find**...



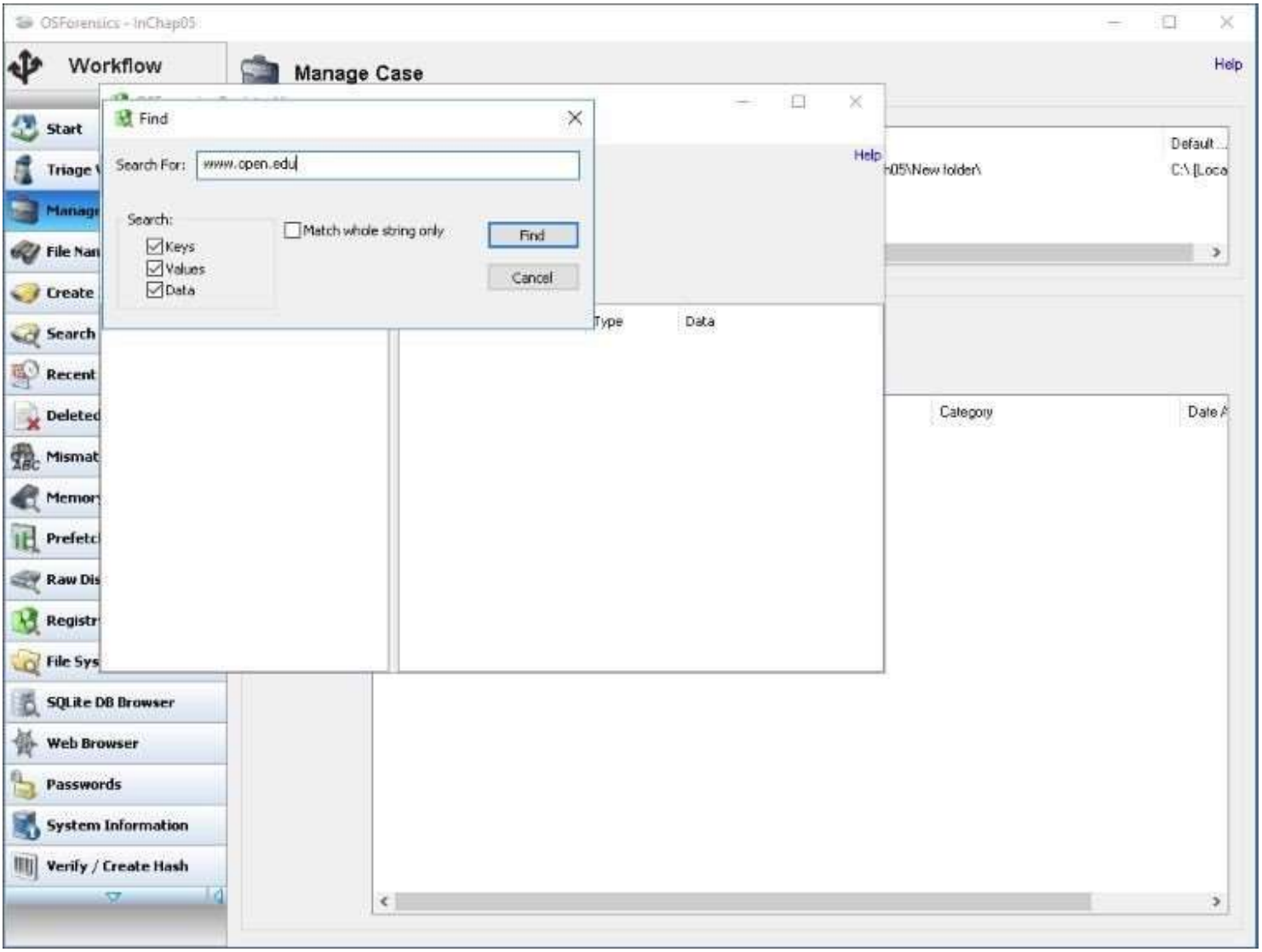
Step 13

On the **Find** dialog box, in the **Search For** text box, type:

```
www.open.edu
```

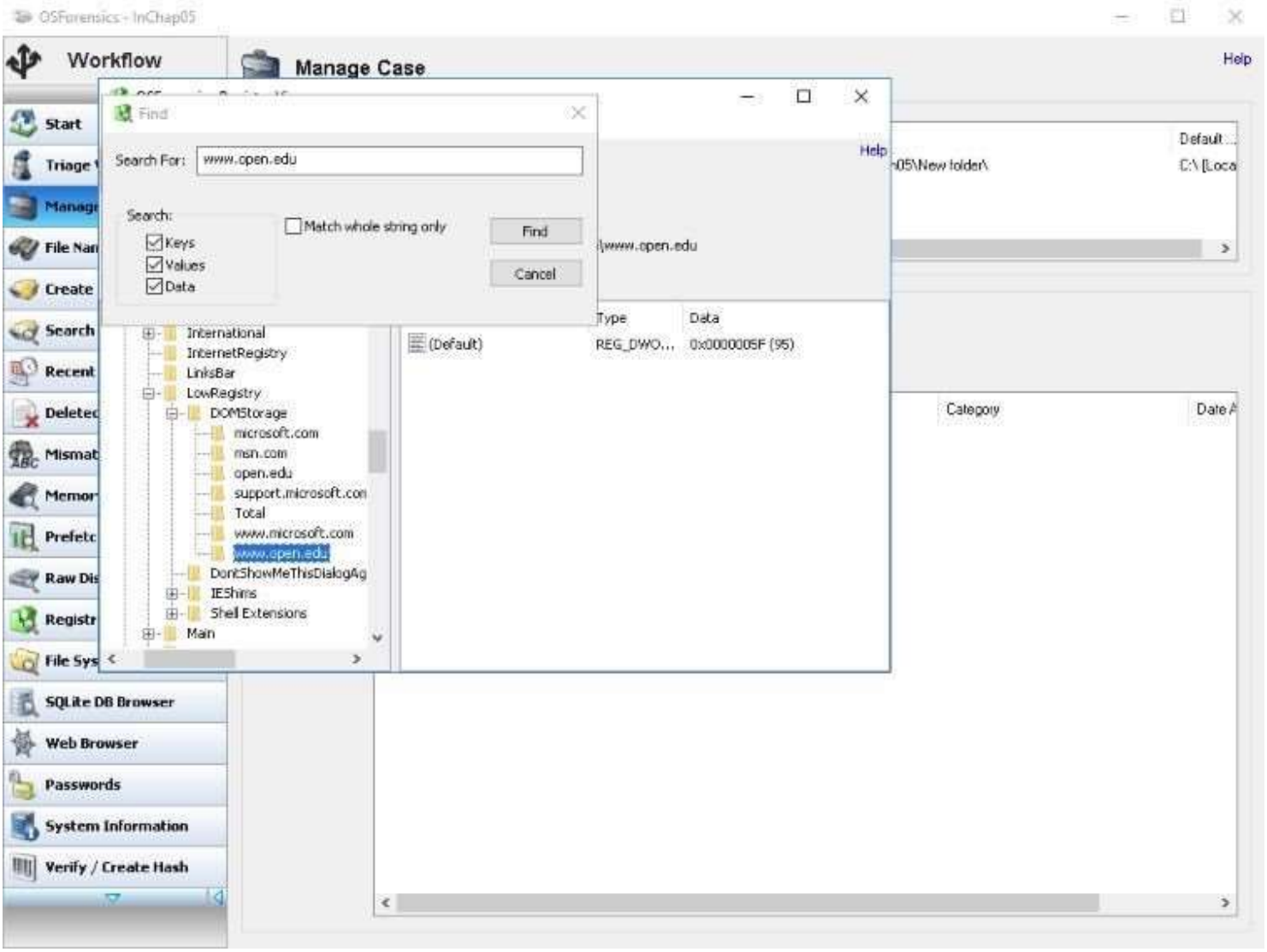
If necessary, select **Keys**, **Values** and **Data** check boxes.

Click **Find**.



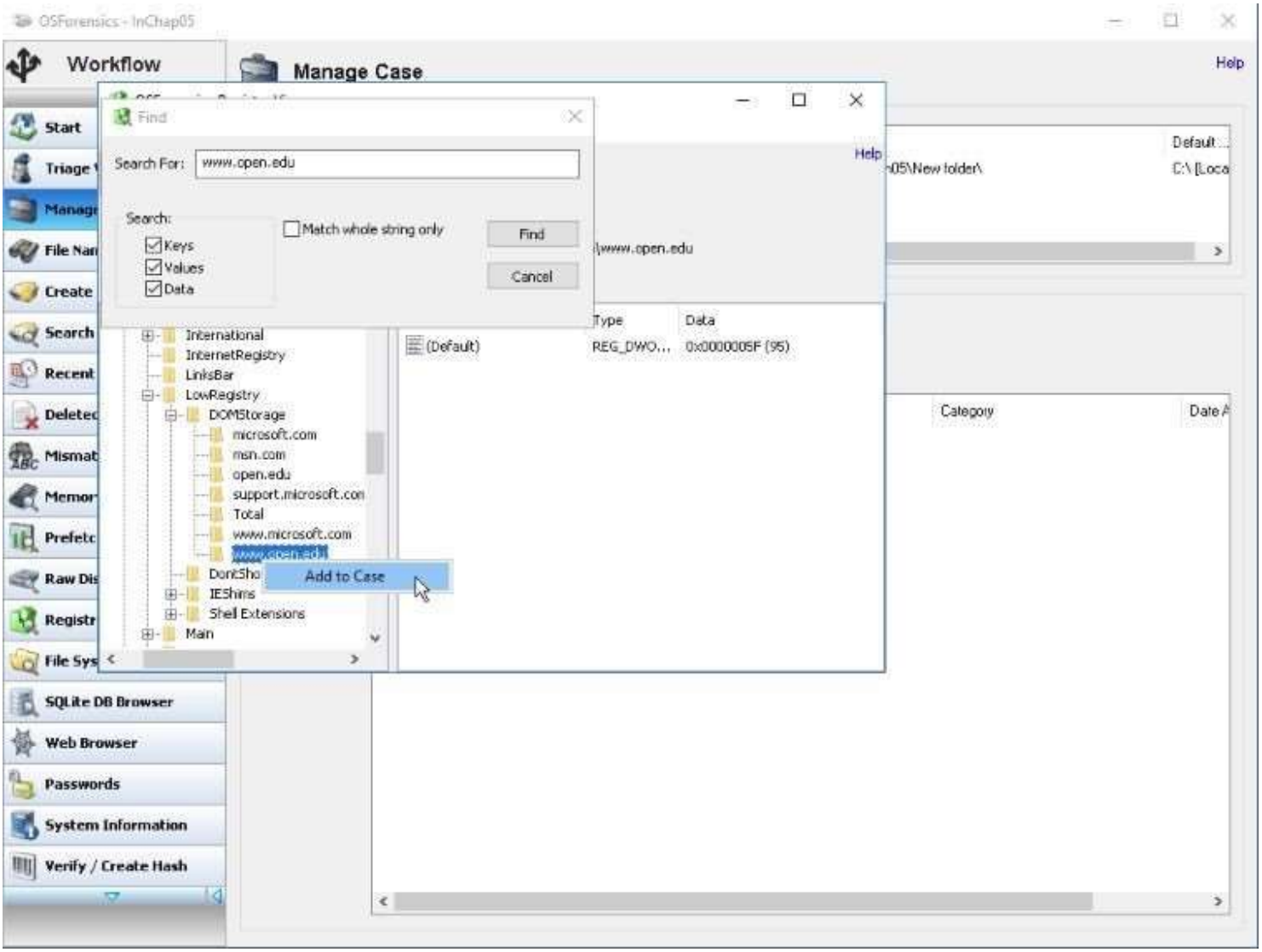
Step 14

Notice that web page **www.open.edu** bookmarked by **Denise** is selected in the background.



Step 15

Right-click on **www.open.edu** and select **Add to Case**.

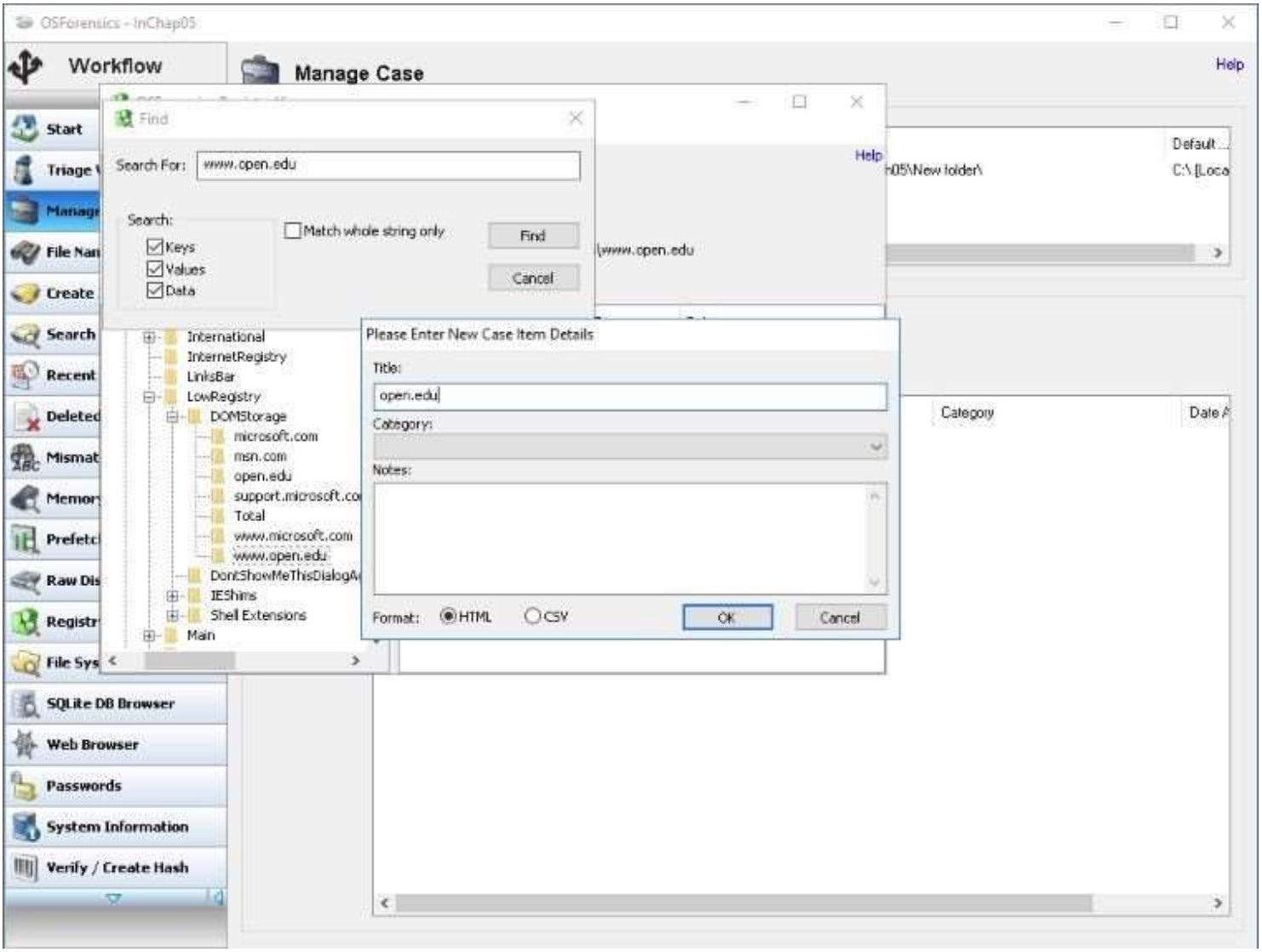


Step 16

On the **Please Enter New Case Item Details** dialog box, type:

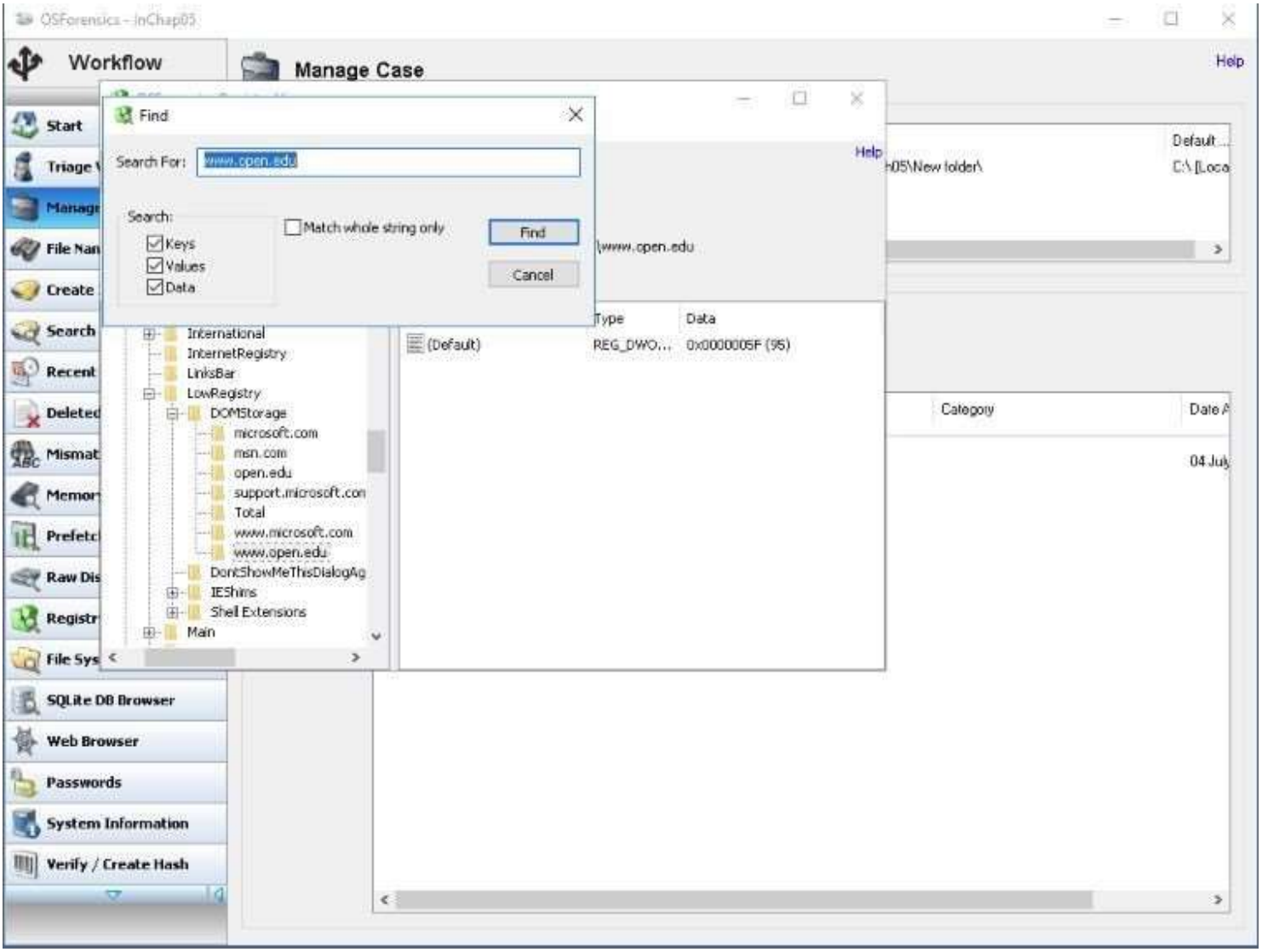
```
open.edu
```

Click **OK**.



Step 17

Back on **Find** dialog box, click again **Find**.

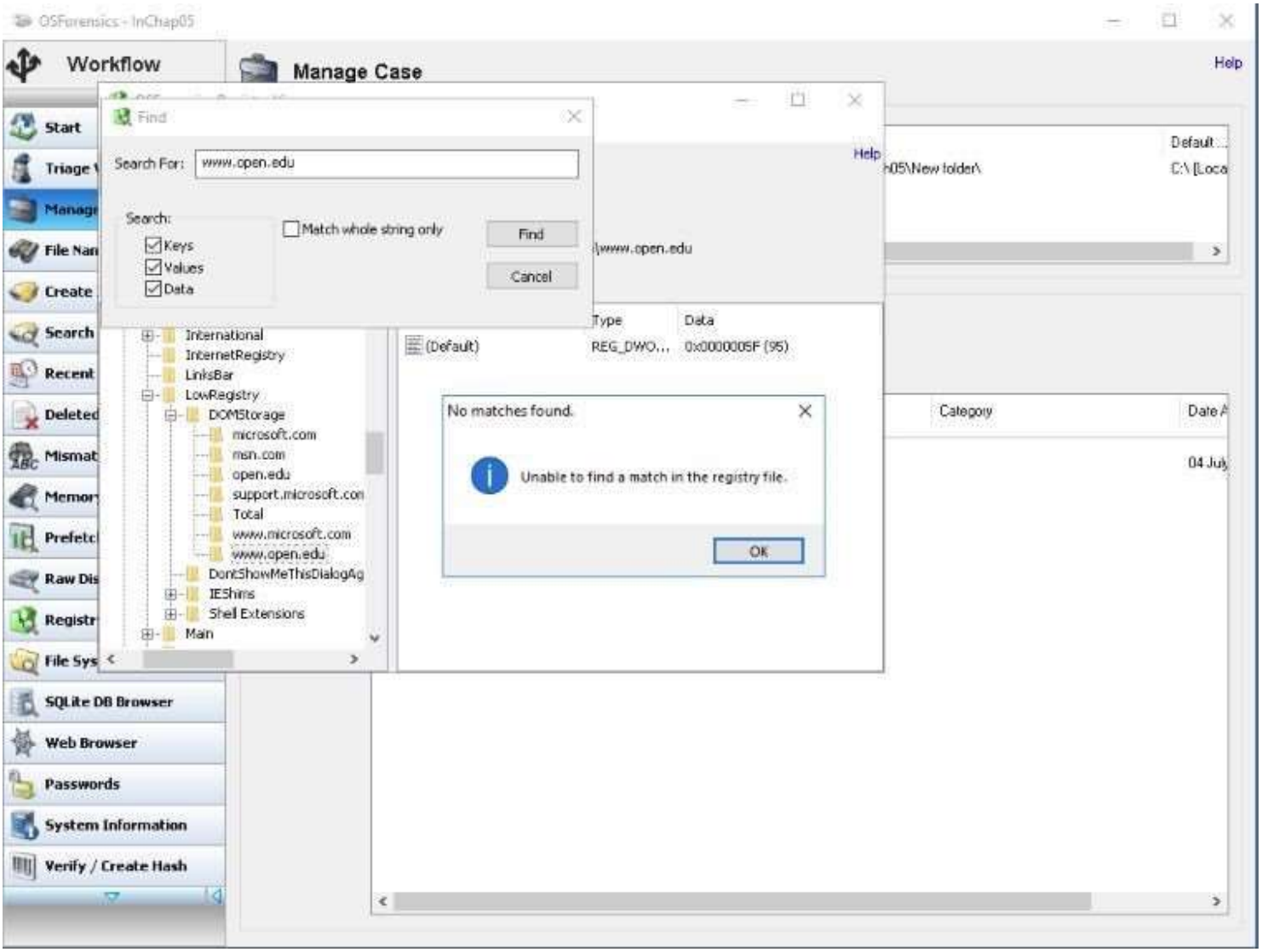


Step 18

The No matches found dialog box indicates that it's unable to find a match.

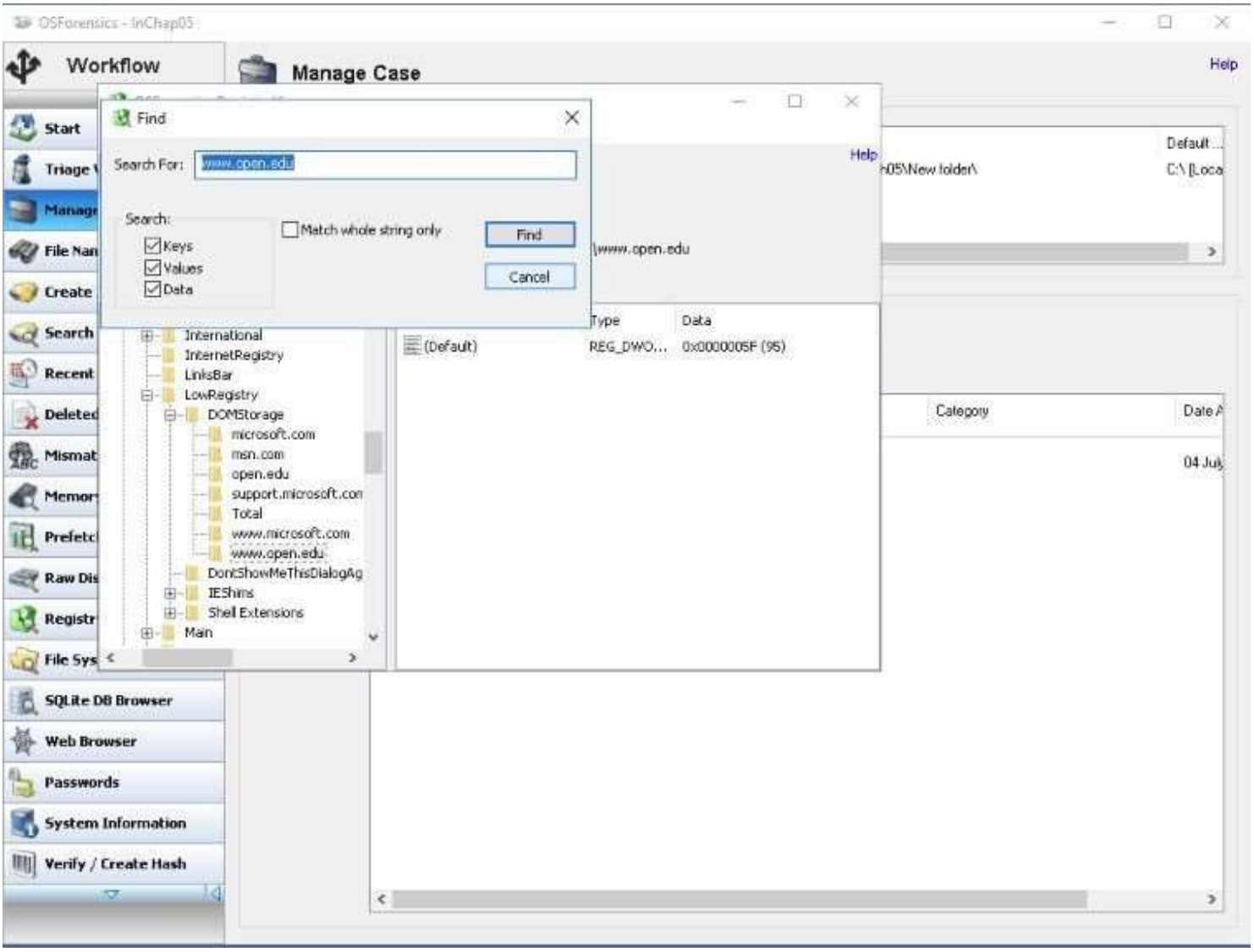
This means that only one match was found in the registry.

Click **OK**.



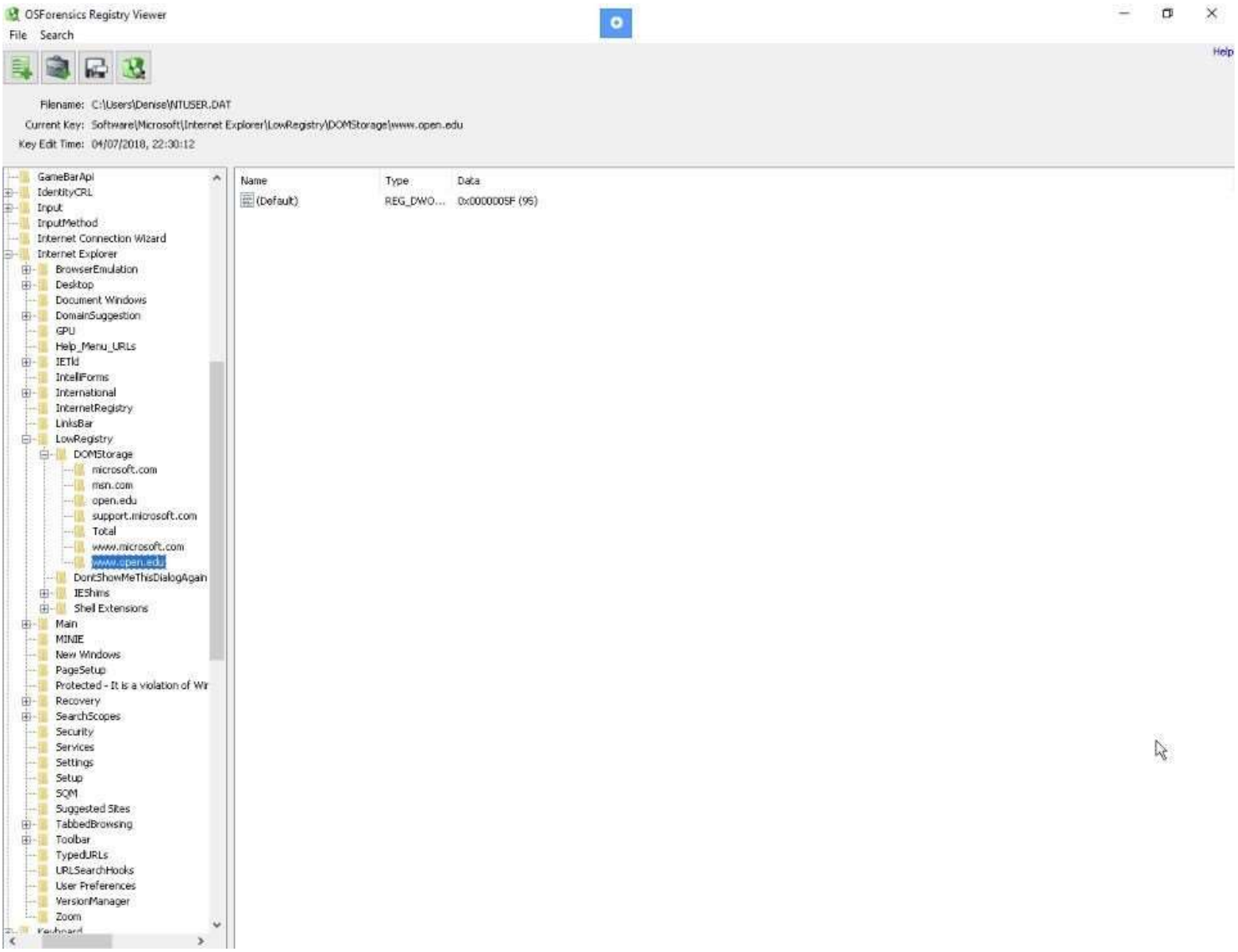
Step 19

Click **Cancel** to close **Find** dialog box.



Step 20

Exit Registry Viewer.



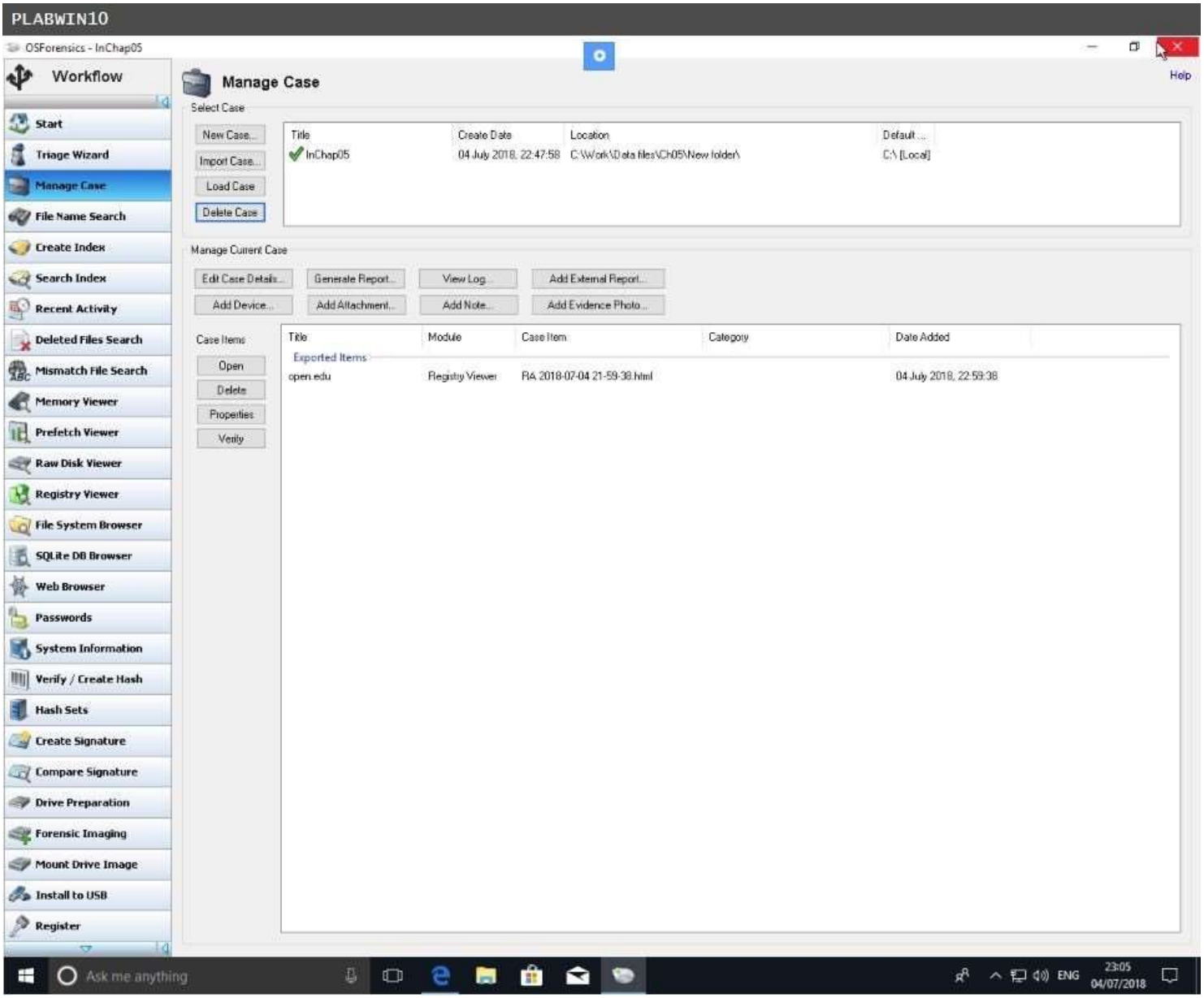
Task 5 - Creating a Report

To create a report on the case being managed, perform the following steps:

Step 1

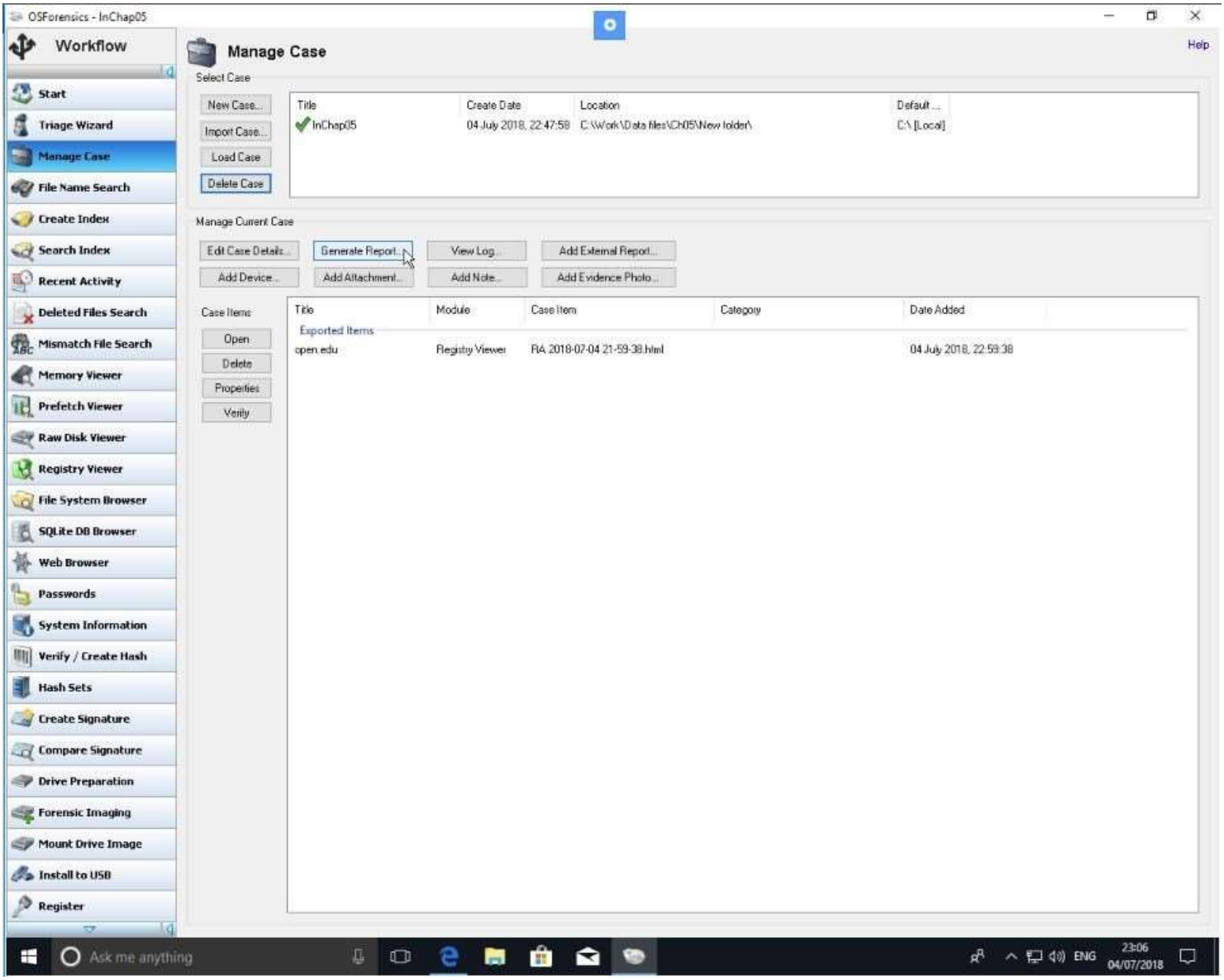
On **PLABWIN10** device, the **OSForensics - InChap05** window is open.

In the main **OSForensics** window, click **Manage Case** in the navigation bar on the left.



Step 2

In the **Manage Current Case** pane on the middle, click the **Generate Report** button.

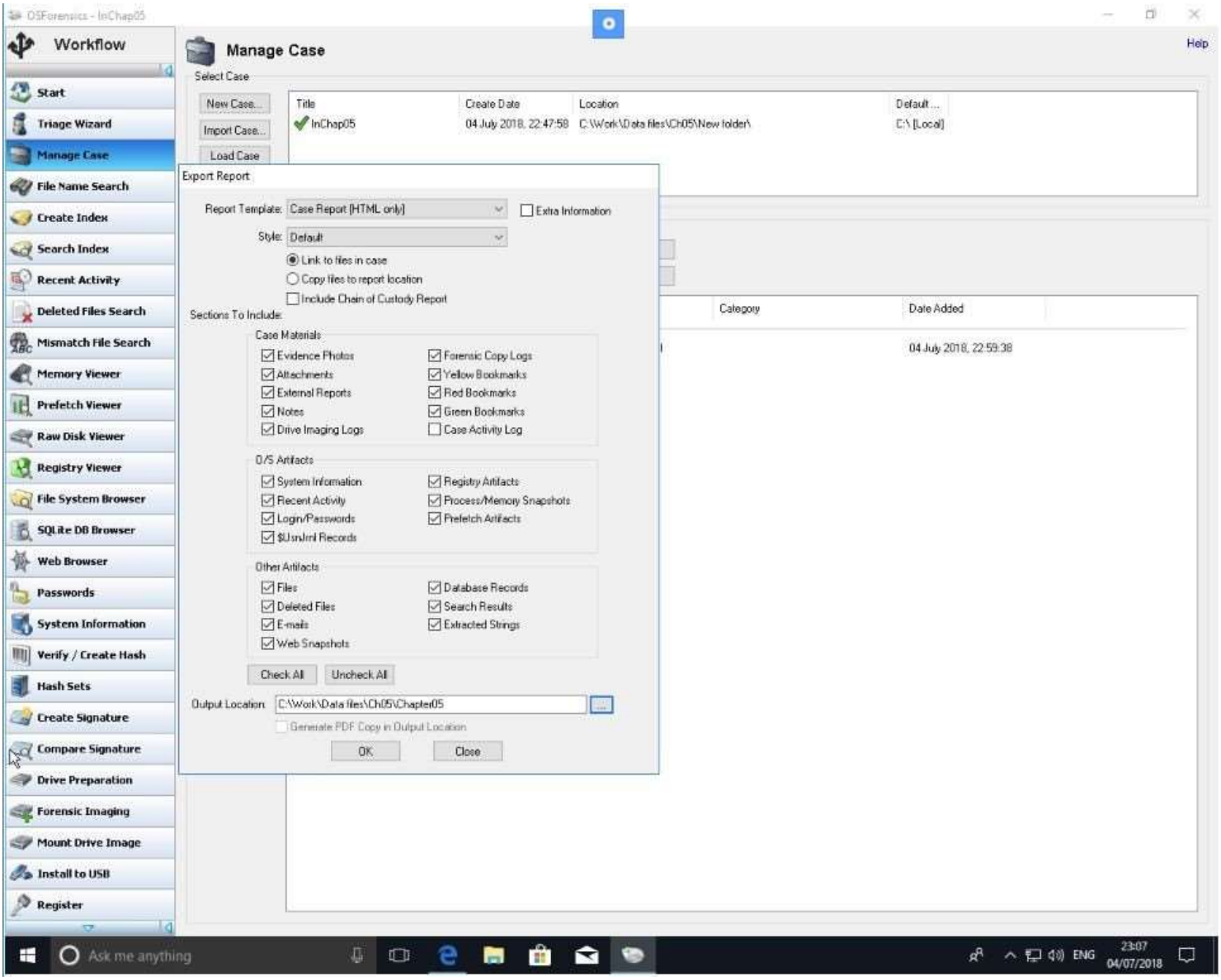


Step 3

In the **Export Report** window, the **Output Location** text box must point to the following location:

```
C:\Work\Data files\Ch05\Chapter05\
```

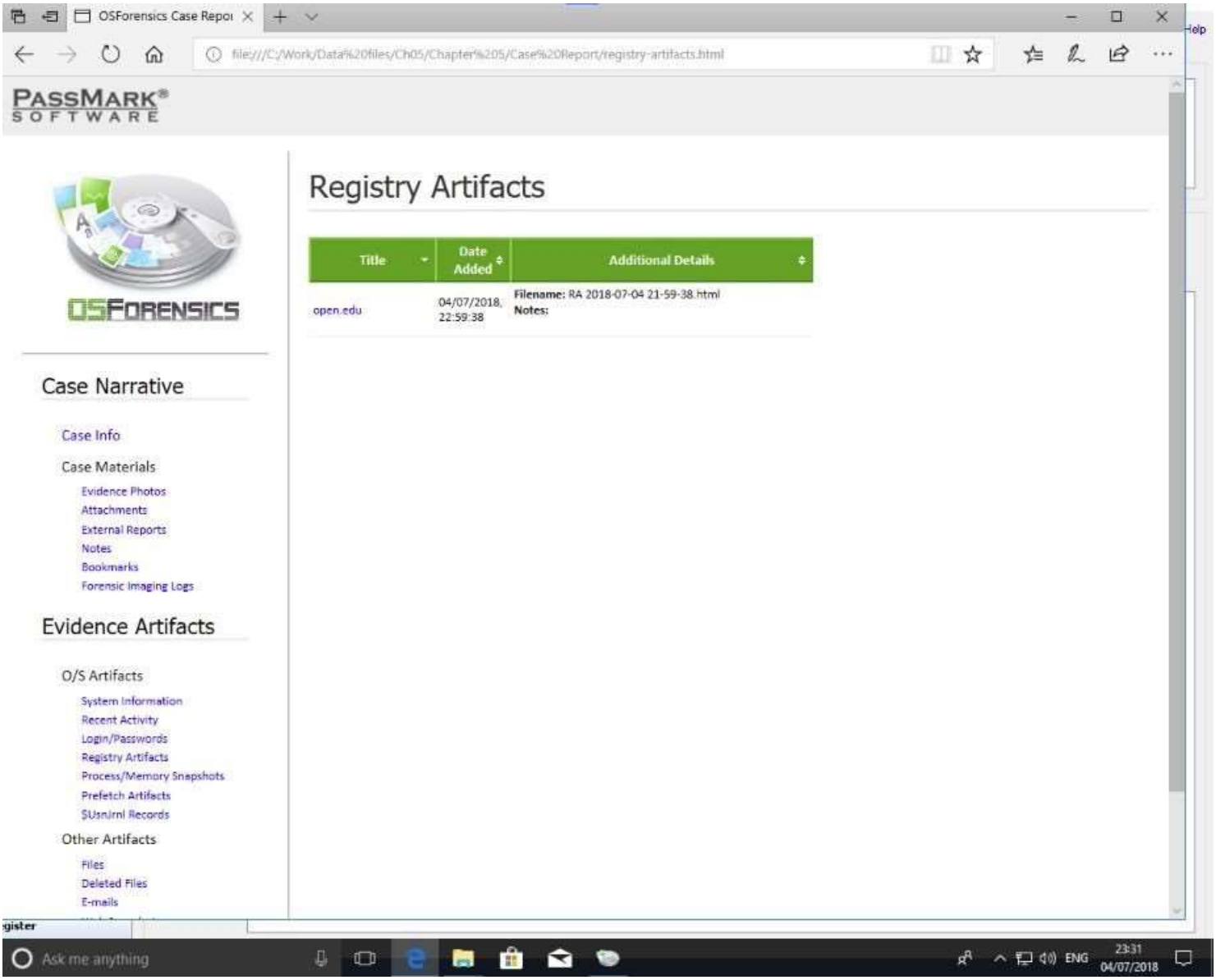
Keep the other settings and click **OK**.



Step 4

The report opens in the Browser. Click **Registry Artifacts** to see the bookmark found earlier. Close **OSForensics** application window.

Important: An extensive amount of information is stored in the Registry. With Registry data, you can ascertain when users went online, when they accessed a printer, and many other events. A lot of the information in the Registry is beyond the scope of this book, so you're encouraged to expand your knowledge by attending training sessions or classes.



Keep the device powered on in their current state and proceed to the next exercise.

Hands-On Project 5-1

There are no data files to extract for this chapter's projects, navigate to **C:\Work\Data files\Ch05** folder on your system before starting the projects.

In this project, you compare two files created in OpenOffice to determine whether the files are different at the hexadecimal level. Keep a log of what you find. Follow these steps:

Step 1

Connect to **PLABWIN10** computer as default administrator account.

Start **OpenOffice** then select **Text Document**.

In the new document, type:

```
This is a test.
```

Step 2

Save the file as **Mywordnew** in your work folder, using **Word 97/2000/XP (.doc) Document (*.doc)** as the file type.

When prompted by the application, select **Keep Current Format**.

Exit **OpenOffice Writer**.

Step 3

From the **OpenOffice** window, select **Spreadsheet**.

In the new workbook, enter a few random numbers. Save the file in your work folder as **Myworkbook**, using Microsoft **Excel 97/2000/XP (*.xls)** as the file type.

When prompted by the application, select **Keep Current Format**.

Step 4

Exit **OpenOffice Calc** and start **Hex Workshop** from desktop. If necessary, click **Continue**, then click **OK**.

Step 5

Click **File**, **Open** from the menu. In the Open dialog box, navigate to your work folder and double-click **Mywordnew.doc**.

Step 6

Notice the file hexadecimal header **D0 CF 11 E0 A1 B11A E1** starting at offset 0. Select the file header, then click **Copy** from the Edit menu.

Step 7

Start Notepad, and in a new document, press **Ctrl+V** to paste the copied data. Leave this window open.

Step 8

Click **File**, **Open** from the Hex Workshop menu. In the Open dialog box, navigate to your work folder and double-click **Myworkbook.xls**.

Step 9

Repeat Step 6.

Step 10

Paste the data you just copied under the Word document header information you pasted previously.

Step 11

In the Notepad window, add your observations about the two files' header data. Save this file as **C5Prj01.txt** and turn it in to your instructor.

Step 12

Exit **Hex Workshop** application.

Hands-On Project 5-2

In this project, you explore the MFT and learn how to locate date and time values in the metadata of a file you create. These steps help you identify previously deleted fragments of MFT records that you might find in unallocated disk space or in residual data in Pagefile.sys. You need the following for this project:

- A system running Windows 7 or later, with the C drive formatted as NTFS
- Notepad to create a small text file
- Hex Workshop to analyze the metadata in the MFT (available on the book's DVD)

Task 1

Step 1

On **PLABWIN10** device, start Notepad.

Create a text file with one or more of the following lines:

A countryman between two lawyers is like a fish between two cats.

A slip of the foot you may soon recover, but a slip of the tongue you may never get over.

An investment in knowledge always pays the best interest.

Drive thy business or it will drive thee

Step 2

Save the file in your work folder **C:\Work\Data files\Ch05** as **C5Prj02** and exit Notepad.

Step 3

Launch **Hex Workshop**. Open **C5Prj02.txt**.

Next, review the material in “Data Inspector pane,” paying particular attention to attributes **DATE** and **FILETIME**.

Close Hex Workshop when finished.

> *Note: The offsets listed in the following charts are from the first byte of the MFT record, not the starting position of the specific attributes 0x10 and 0x30.*

0x10 $Standard Information (data starts at offset 0x18)

Description of field	Offset position	Byte size
C Time (file creation)	0x50	8
A Time (file altered)	0x58	8
L Time (Last accessed)	0x60	8

0x30 $File Name (data starts at offset 0x18)

Description of field	Offset position	Byte size
C Time (file creation)	0xB8	8
A Time (file altered)	0xC0	8
R Time (file read)	0xC8	8
M Time (MFT change)	0xD0	8

Task 2

Next, you examine the metadata of the **C5Prj02.txt** file stored in the $MFT file. Follow these steps:

Step 1

Click **Start**, scroll down to **OSForesnics**, then click **OSForensics**.

On the **OSForensics** welcome 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

On the **New Case** dialog box, type **InChap05** as the **Case Name**.

Keep the other default selection.

Step 4

Under **Manage Current Case**, click **Add Device**...

Step 5

On the **Select device to add**, ensure that Drive Letter is set to C:\.

Click **OK**.

Step 6

Click **Raw Disk Viewer**.

Step 7

On **Raw Disk Viewer** window, using Search look for **C5Prj02.txt**.

Use **Text** option.

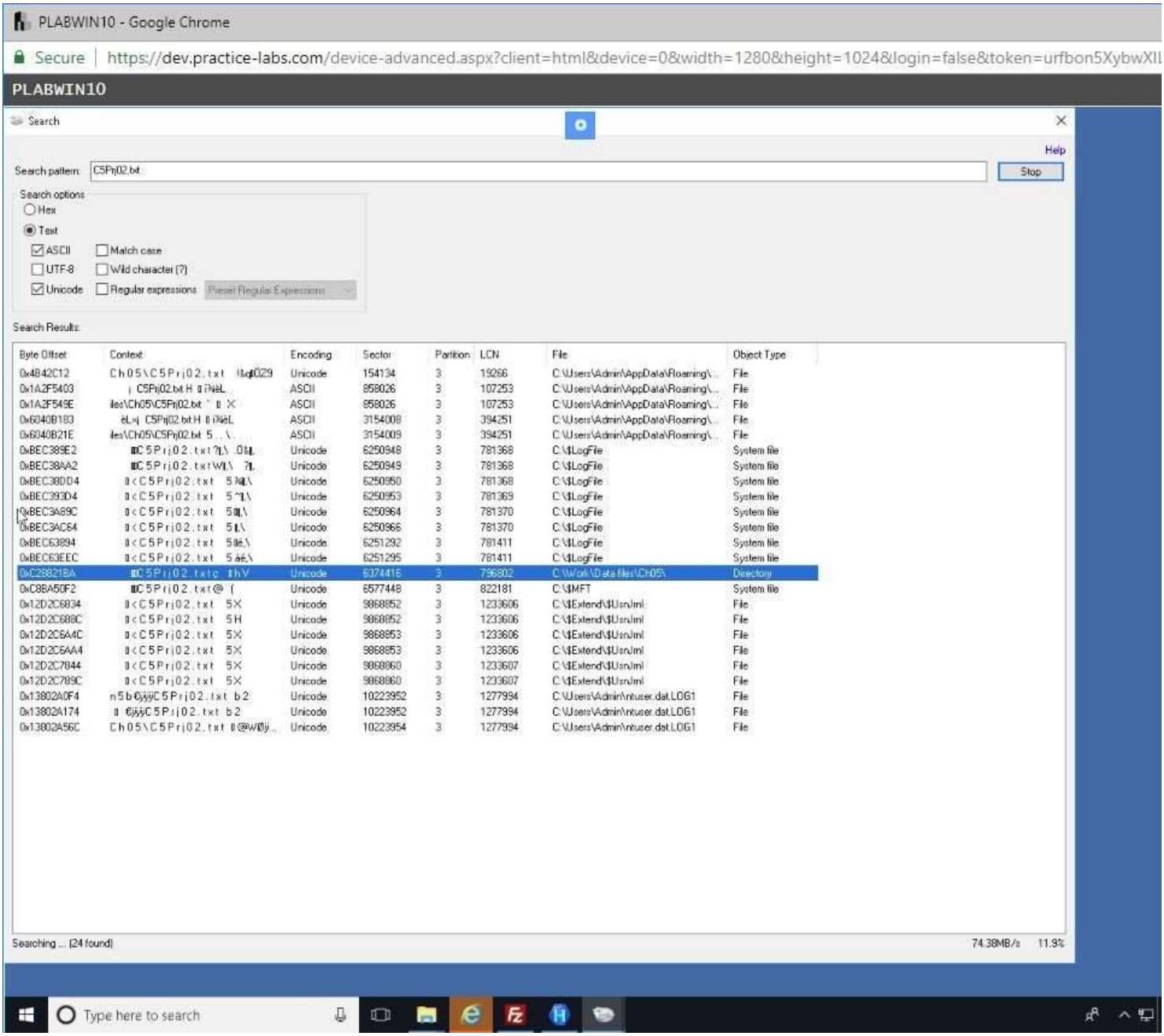
Then click **Find**.

Step 8

Verify that you can find **C5Prj02.txt** similar to the screenshot provided.

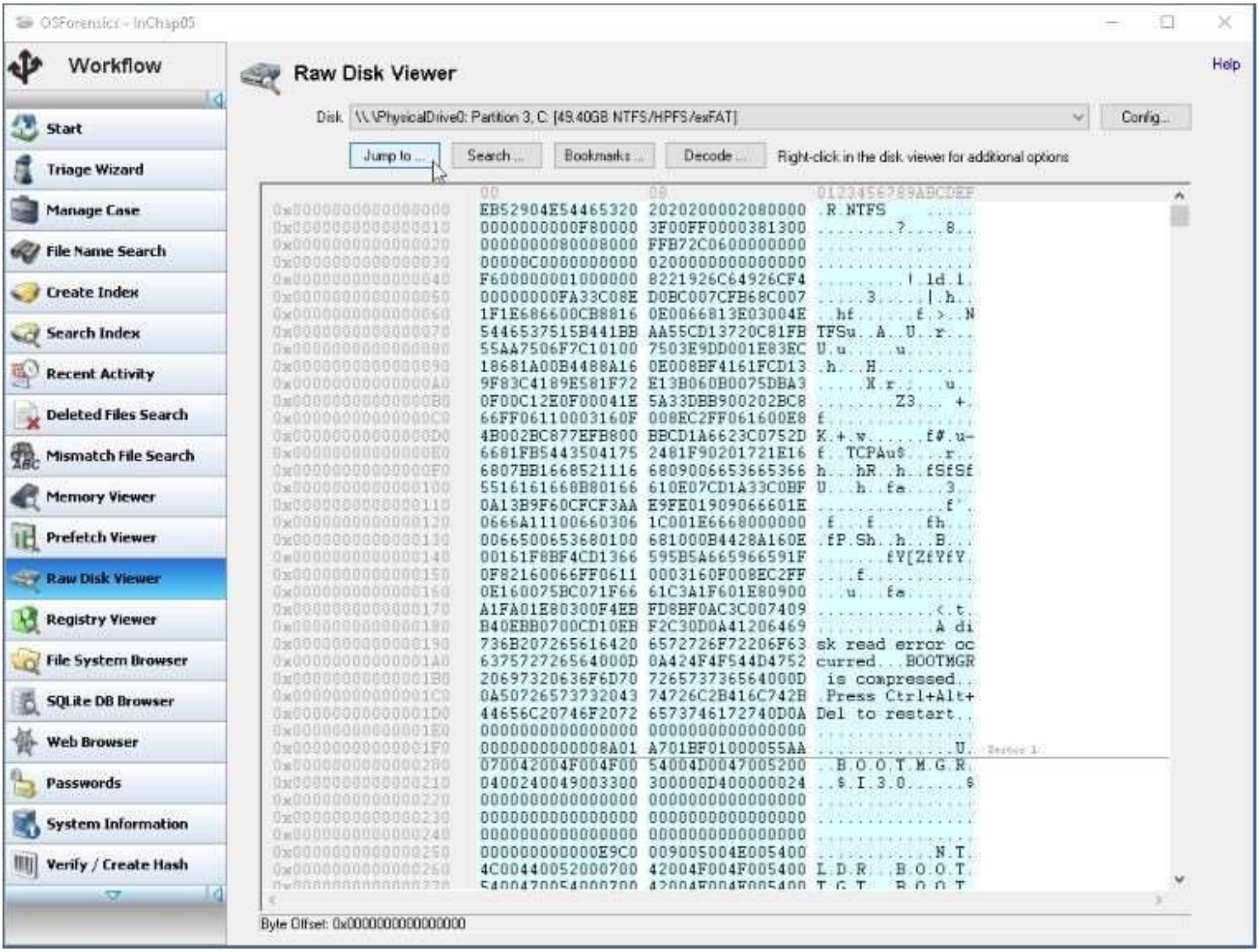
Record the **Byte Offset** as seen in your search. Do not use the value indicated in the screen grab as you may get a different value in your project.

Close **Search** window.



Step 9

On the **Raw Disk Viewer**, click **Jump to**...

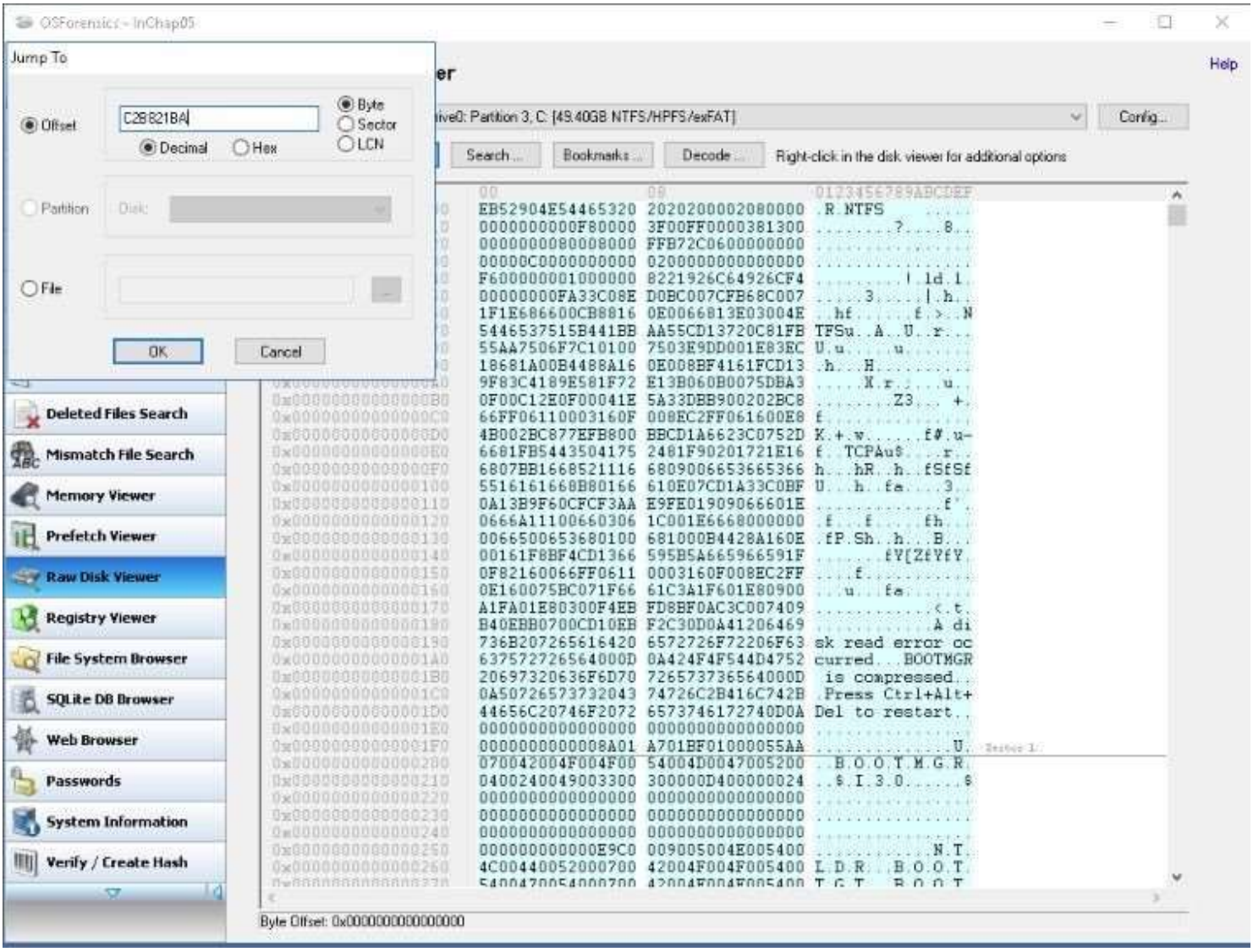


Step 10

On the **Jump to** dialog box, Hex option is selected.

Enter the Offset without the “ox” prefix.

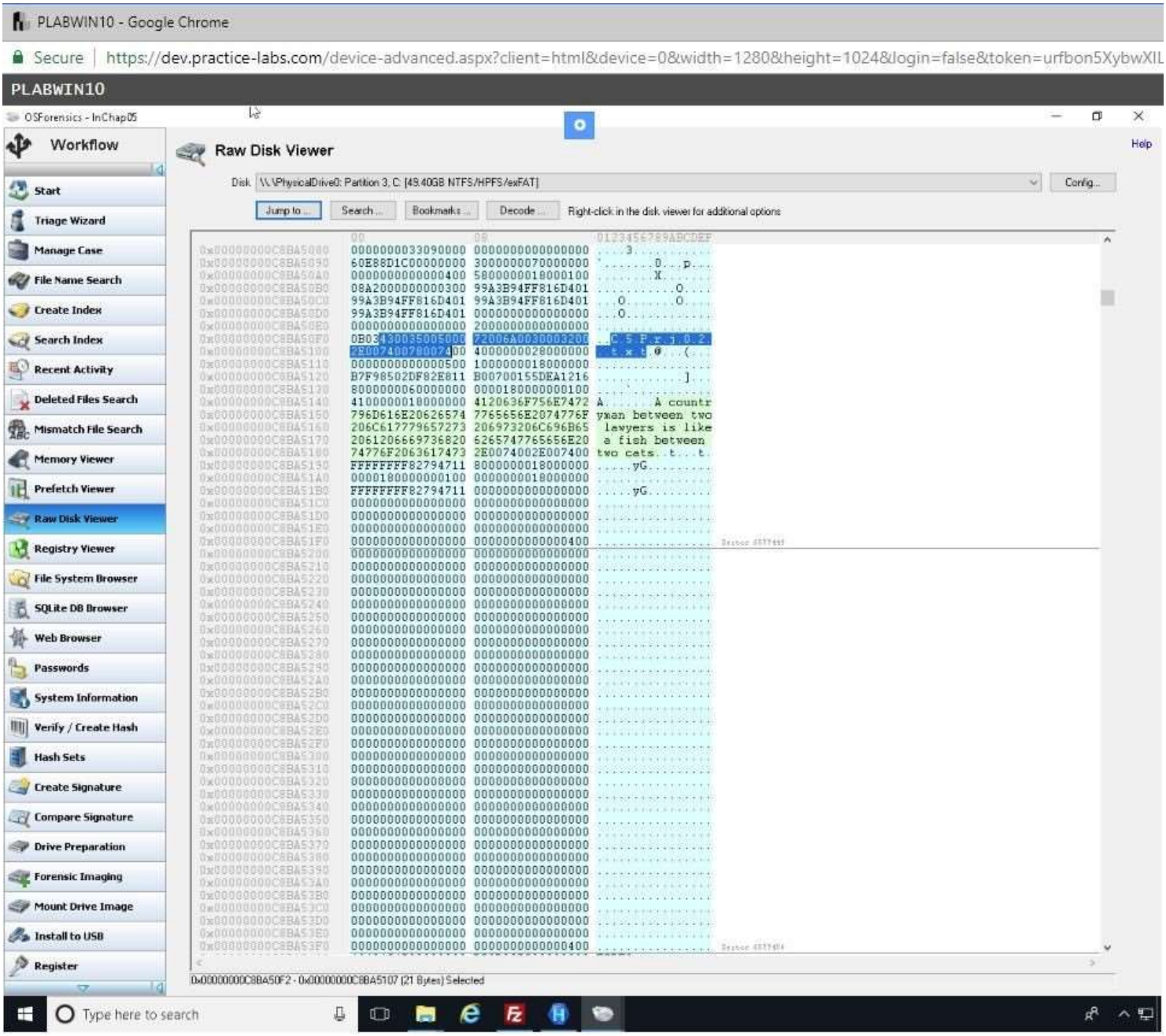
Click **OK**.



Step 11

Notice that the **C5Prj02.txt** file is found in the disk based on the offset you specified.

Close **OSForensics** application.



Keep the device powered on in their current state and proceed to the next exercise.

Hands-On Project 5-3

In this project, you use Hex Workshop to become familiar with different file types.

Follow these steps:

Step 1

Locate or create **OpenOffice Calc (.xls), OpenOffice Write (.doc)** files that you created earlier.

The files are in **C:\Work\Data files\Ch05 folder**.

Step 2

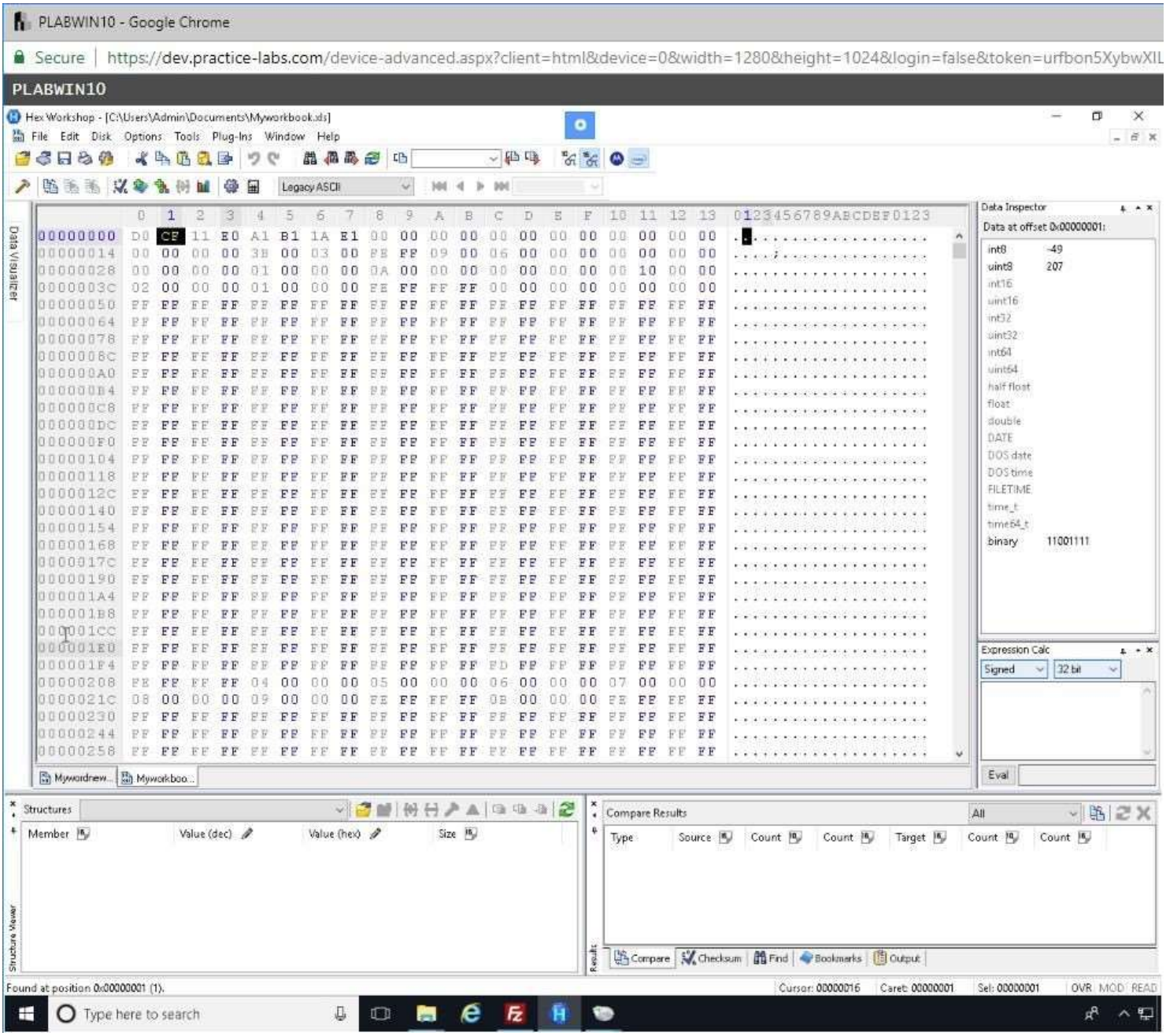
Start Hex Workshop.

Step 3

Open each file type in Hex Workshop.

Search for Hex value **CF** using the **Find** command.

Record the hexadecimal codes for each file in a text editor, such as Notepad or WordPad. For example, for the Word document, record Word Header: **D0 CF 11 E0**.



Step 4

Save the file, and then print it to give to your instructor.

Close Hex Workshop application.

Keep the device powered on in its current state and proceed to the next exercise.

Hands-On Project 5-4

This project is a continuation of the in-chapter activity done with OSForensics.

The paralegal has asked you to see whether any passwords are listed in the image of Denise Robinson's computer. Follow these steps:

Step 1

On **PLABWIN10** device, click **Start**, scroll down to **OSForesnics**, then click **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

Mount the **C:** as described in the in-chapter activity.

Step 3

In the main window, click **Manage Case** in the navigation bar on the left, if necessary.

> **Important**: Up to 3 cases can be added in the trial version of OSForensics. If you have 3 cases loaded, you need to delete some of them.

In the **Select Case** pane on the right, double-click **InChap05** if a green checkmark isn't displayed next to it.

Step 4

In the navigation bar on the left, click **Passwords**.

In the pane on the right, click the **Find Passwords & Keys** tab, if necessary.

Click the **Scan Drive** button, and then note that drive letter C:\ is automatically selected.

Step 5

In the navigation bar on the left, click **Acquire Passwords**.

Step 6

Please note that no passwords will be detected as this is a live system.

Step 7

Exit OSForensics, and print the report displayed in your Web browser. Turn the report in to your instructor.

Summary

- The Master Boot Record (MBR) stores information about partitions on a disk.
- Microsoft used FAT12 and FAT16 on older operating systems, such as MS-DOS, Windows 3.x, and Windows 9x. The maximum partition size is 2 GB. Newer systems use FAT32. FAT12 is now used mainly on floppy disks and small USB drives. VFAT, created for Windows 95, allows filenames longer than eight characters.
- To find a hard disk's capacity, use the cylinders, heads, and sectors (CHS) calculation.
- To find a disk's byte capacity, multiply the number of heads, cylinders, and sectors.
- Sectors are grouped into clusters and clusters are chained because the OS can track only a given number of allocation units (65,536 in FAT16 and 4,294,967,296 in FAT32).

- Solid-state disk drives use wear-leveling to ensure even use of memory cells. It transfers data to unused memory cells so that all cells have an equal amount of reads and writes.
- The previously assigned memory cells are listed as unallocated space. After a predetermined time, the unallocated memory cells are overwritten with binary 1s.
- When files are deleted in a FAT file system, the hexadecimal value 0x05 is inserted in the first character of the filename in the directory.
- NTFS is more versatile because it uses the Master File Table (MFT) to track file information.
- Approximately the first 512 bytes of data for small files (called resident files) are stored in the MFT. Data for larger files (called nonresident files) is stored outside the MFT and linked by using cluster addresses.
- Records in the MFT contain attribute IDs that store metadata about files.
- In NTFS, alternate data streams can obscure information that might be of evidentiary value to an investigation.
- File slack, RAM slack (in older Windows OSs), and drive slack are areas in which valuable information, such as downloaded files, swap files, passwords, and logon IDs, can reside on a drive.
- NTFS can encrypt data with Encrypting File System (EFS) and BitLocker. Decrypting data with these methods requires using recovery certificates. BitLocker is Microsoft's whole disk encryption (WDE) utility that can be decrypted by using a one-time passphrase.
- The Resilient File System (ReFS), available only in Windows 8 and Windows Server 2012, provides access to large disk storage systems.
- With a hexadecimal editor, you can determine information such as file type and OS configurations.
- NTFS can compress files, folders, or an entire volume. FAT16 can compress only entire volumes.

- The Registry in Windows keeps a record of attached hardware, user preferences, network connections, and installed software. It also contains information such as passwords in two binary files: System.dat and User.dat.

- Every user with an account on a Windows computer has his or her own Ntuser.dat file. Windows 9x user information is stored in User.dat.

- Virtualization software enables you to run other OSs on a host computer. Virtual machines are beneficial if, for example, you need to run a previous OS to test old software that won't run on newer OSs.