

Operating System Forensics

Module 06

Performing OS Forensics

Operating System (OS) forensics involves obtaining and analyzing digital information for use in evidence in civil, criminal, or administrative cases.

ICON KEY



Valuable information



Test your knowledge



Web exercise



Workbook review

Lab Scenario

A computer forensics examiner, Steve, called to investigate the laptop of a 26-year-old man who was arrested. Steve started searching the contents of the laptop. He began his investigation on Windows® event logs and processes using various Windows forensic tools and checked all the registries, event logs, and processes for evidence of any crimes. During the investigation, Steve found the paths for several images and videos of child pornography. He checked all the pictures and confirmed the existence of child pornography on the laptop. Other evidence on the laptop proved that the man in custody was its primary user.

Lab Objectives

The goal of this lab is to explain the process of finding pieces of evidence from Windows and Linux OS. Evidence in Windows OS includes Windows event logs, Windows processes, search key values, and data in Windows while in Ubuntu system includes volatile and non-volatile data. Accomplishing this task will include:

- Viewing system information and memory processes
- Viewing disk raw sectors
- Verifying the integrity of files
- Creating drive images
- Recovering deleted files and viewing cookies
- Scanning for pictures
- Analysis of volatile and non-volatile data in Linux System

Lab Environment

This lab requires:

- A computer running **Windows Server 2012, Ubuntu OS (Linux Distro), Kali Linux**
- A web browser with Internet connection.
- Administrative privileges to install and run tools.

Lab Duration

Time: 120 Minutes

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

 T A S K 1

Overview

Computer forensics is a broad concept that refers mainly to crimes committed with the use of computers. Various laws have been passed against cybercrime, but it still exists, and the guilty parties are difficult to find due to the lack of physical evidence. Computer forensics helps in solving this problem.

Lab Tasks

Recommended labs to assist you in Windows Forensics:

- Discovering and Extracting Hidden Forensic Material on Computers Using **OS Forensics**.
- Extracting Information about Loaded Processes Using **Process Explorer**.
- Viewing, Monitoring, and Analyzing Events Using the **Event Log Explorer Tool**.
- Performing a Computer Forensic Investigation Using the **Helix Tool**.
- Analyzing **Volatile Data** in Linux System.
- Analyzing **Non-volatile Data** in Linux System.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Lab

1

Discovering and Extracting Hidden Forensic Material on Computers Using OSForensics

OSForensics is a computer forensics application for locating and analyzing digital evidence found in computer systems and digital storage devices.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Searching for an evidence file in the system is like searching for a needle in a stack of hay unless you know what to look for and where. Another way around is to find a tool that would help you out. A system store logs for events along with the identity of the programs that perform any small task. A forensic investigator should be able to differentiate the data and evidence. This lab will help you use the OSForensics tools that will assist in finding evidence from loads of data.

Lab Objectives

The objective of this lab is to help students learn how to investigate a suspect's computer to locate evidence of a crime. In this lab, you will learn how to use the **OSForensics** tool.

Lab Environment

This lab requires:

- OSForensics, located at **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\OS Forensics**.
- You can also download the latest version of **OSForensics** from **www.osforensics.com/download.html**.
- If you decide to download the latest version, then screenshots shown in the lab might differ slightly.
- A computer running **Windows Server 2012**.

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

- Administrative privileges to install and run tools.
- A web browser with an Internet connection.

Lab Duration

Time: 25 Minutes

 You can also download the latest version of OSForensics from the link www.osforensics.com/download.html

Overview of OSForensics

The OSForensics suite effectively simplifies the task of analyzing vast amounts of data on live systems and storage media with an easy-to-use modular interface. OSForensics includes tools that can identify evidence material in seconds (such as searching for a particular file name), as well as more sophisticated tools for identifying harder to locate digital evidence artifacts (such as tracing incriminating data in deleted files).

Lab Tasks

TASK 1

Creating a New Case

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\OSForensics**.
2. Double-click **osf.exe** to launch the setup and follow the wizard-driven installation instructions.

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

3. In the final step of installation, check **Launch OSForensics** option and click **Finish**.
4. **OSForensics** GUI appears, along with **PassMark OSForensics** pop-up. Click **Continue Using Free Version**.

 By default, a case is created in the OSForensics folder situated in the user's My Documents folder. Upon the creation of a case, a subfolder will be created at the target location that will contain the case. There is no need to select an empty folder.

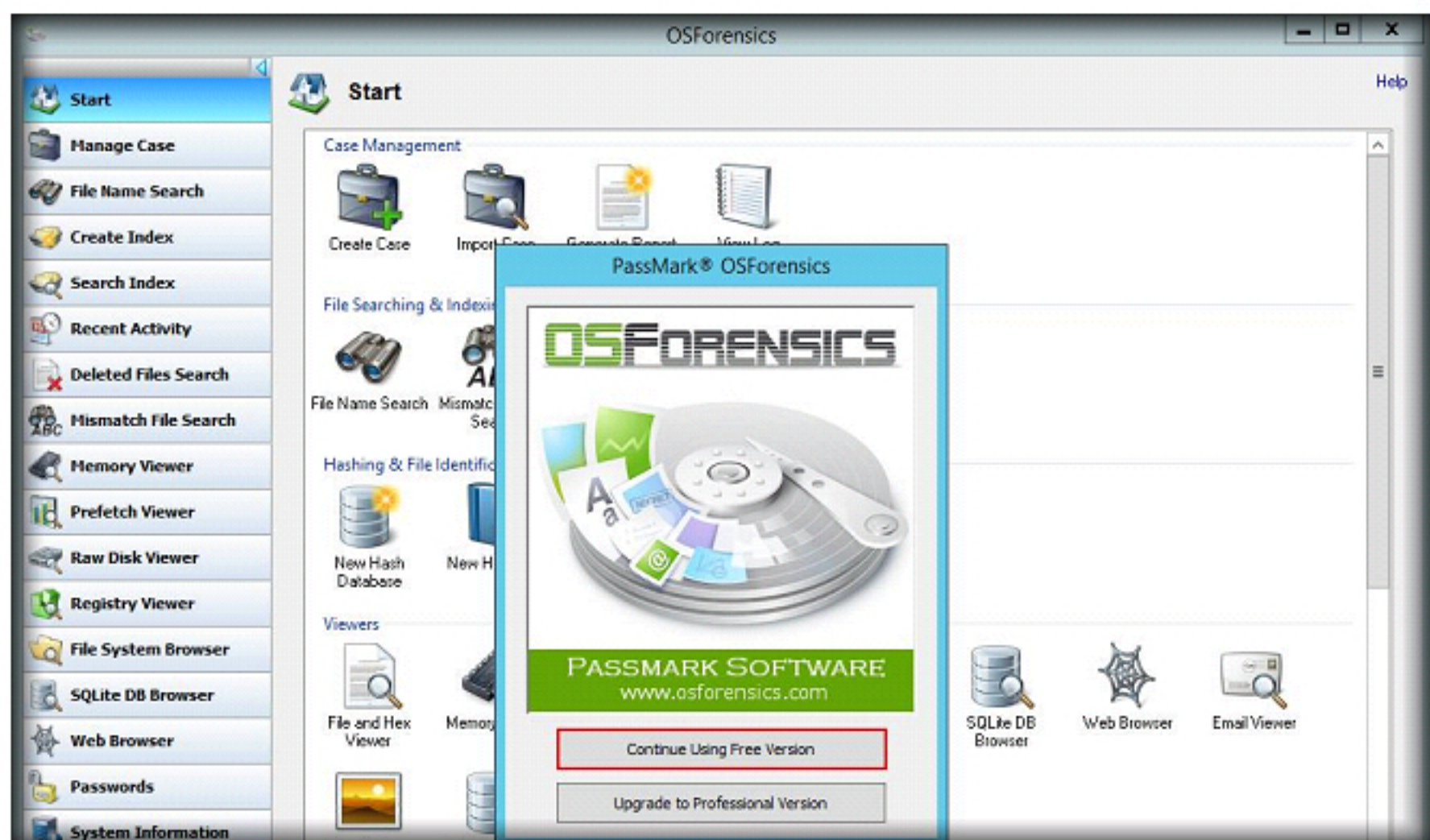


FIGURE 1.1: OSForensics main window

5. Click the **Create Case** icon in the main window to create a new case.

Once a case is created or opened; the contents of the case can also be managed from this window. Case items can be opened, deleted, or have additional properties viewed. The property viewer also allows for editing user-defined properties of the item.

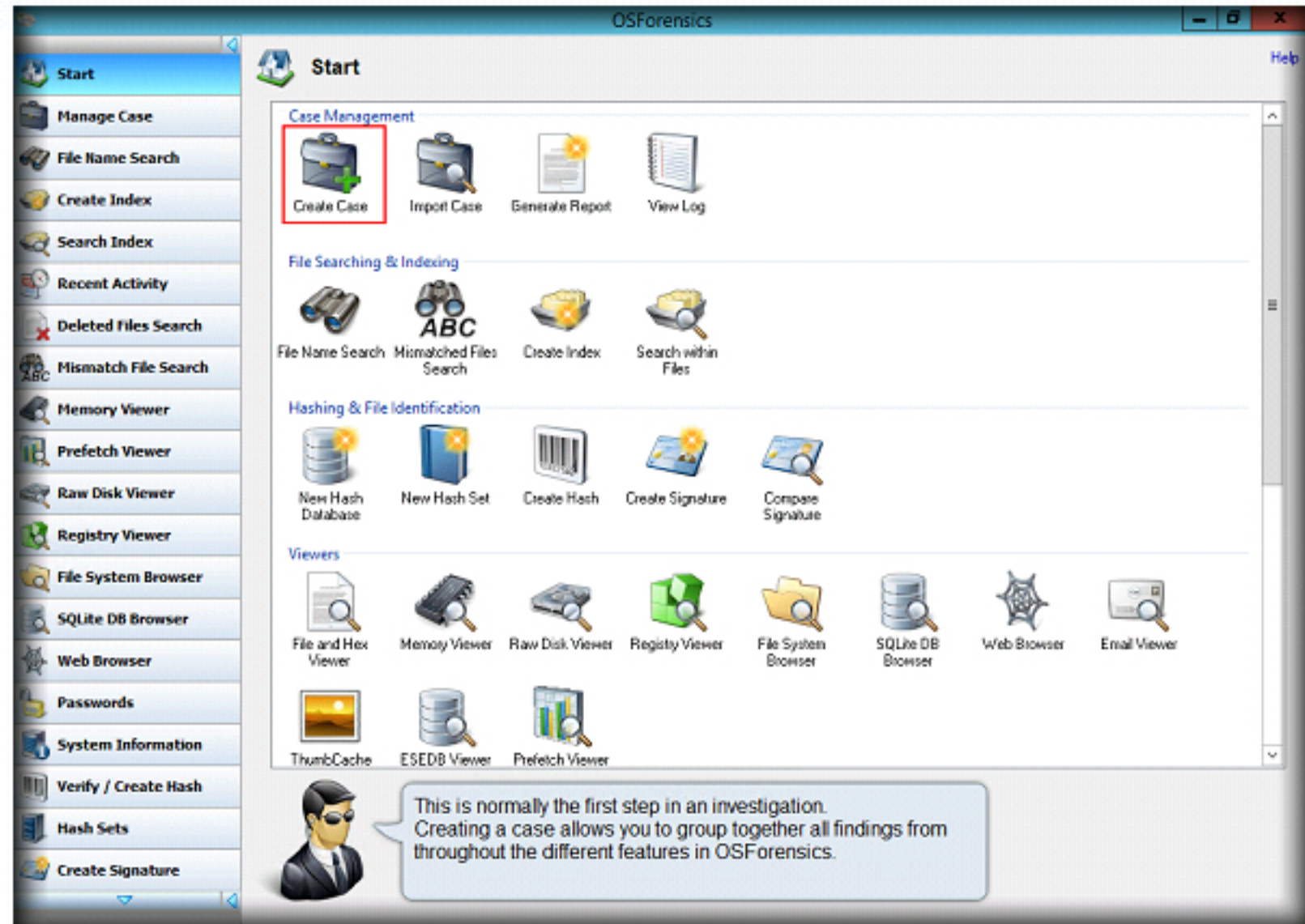


FIGURE 1.2: OSForensics Creating a New Case

6. Complete the required fields of the **New Case** wizard, and choose to save the new case folder in either the **Default** or **Custom** location and click **OK**.

Note: If you want to create a new case in a custom location, click the **Browse** button, indicate the desired path, and then click **OK**. In this lab, the Case Name is **Case 1** and the default Case Folder has been selected.

The start window contains a brief description of each feature as you mouse over it, clicking once will take you to that feature. Additionally, you can click the buttons on the left. If a button has a pulsating green light next to it, this means that the feature is currently performing a task. A blue light means that the task has been completed, but you have not yet navigated back to that window to view the result.

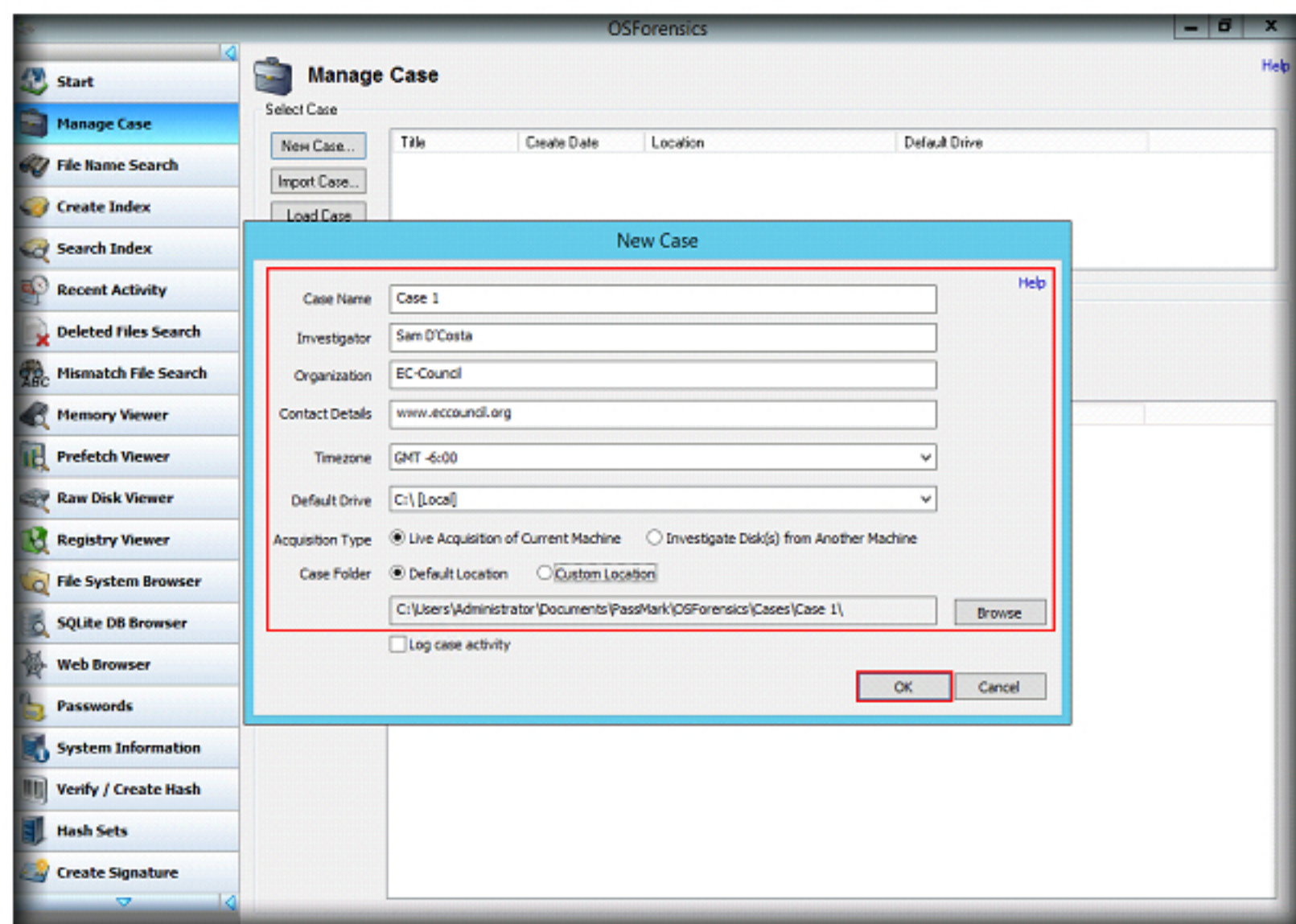


FIGURE 1.3: OSForensics New Case Wizard

7. A new case is created as shown in the below screenshot:

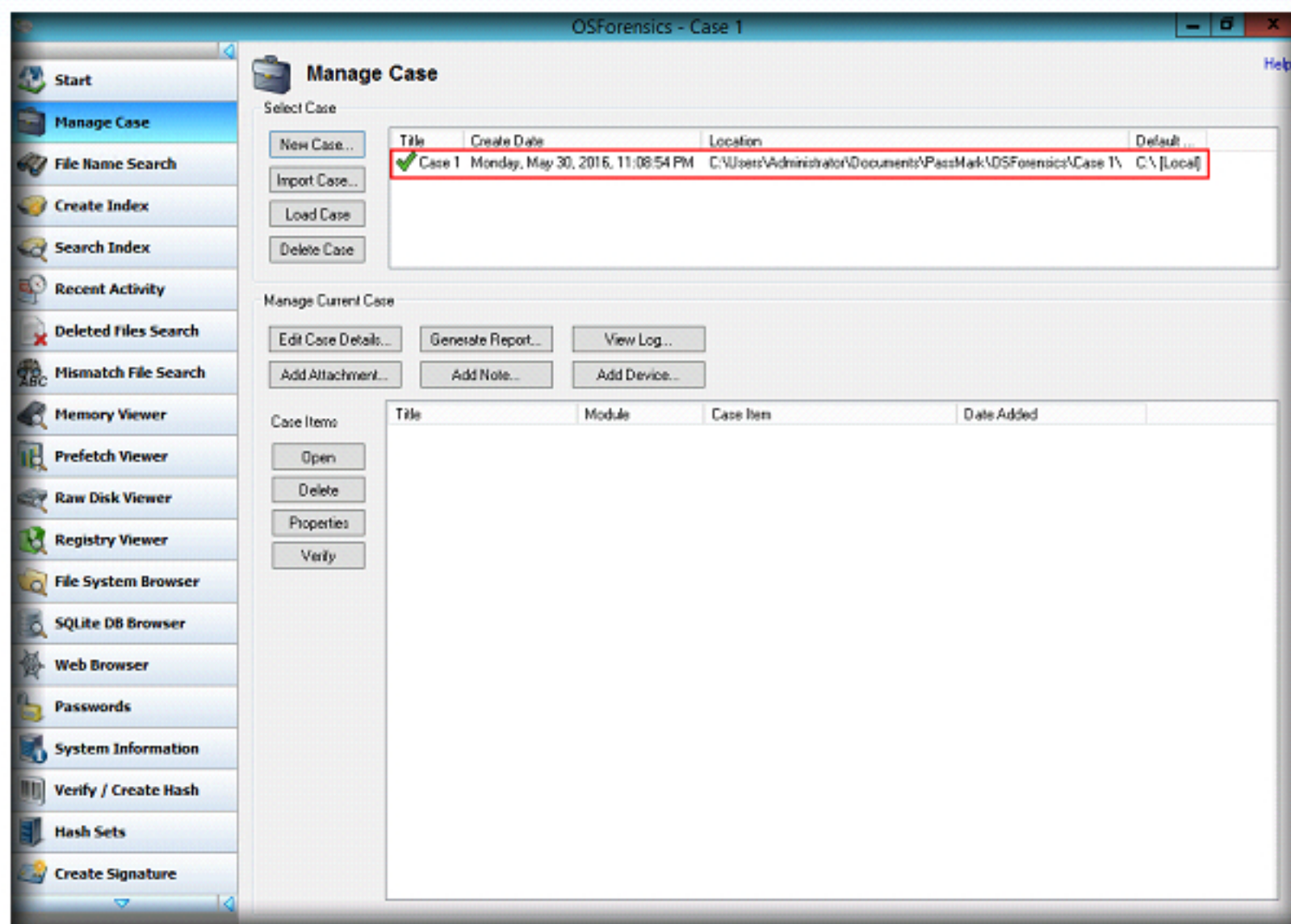


FIGURE 1.4: OSForensics New Case Created



TASK 2

File Name Search

 A basic search simply involves entering a search string and location. Any files or folders that contain the search string within their name will be displayed in the search results. For instance, searching for "File" will match "file.txt", "test.file" or "MyFile.doc". The basic search is case insensitive.

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

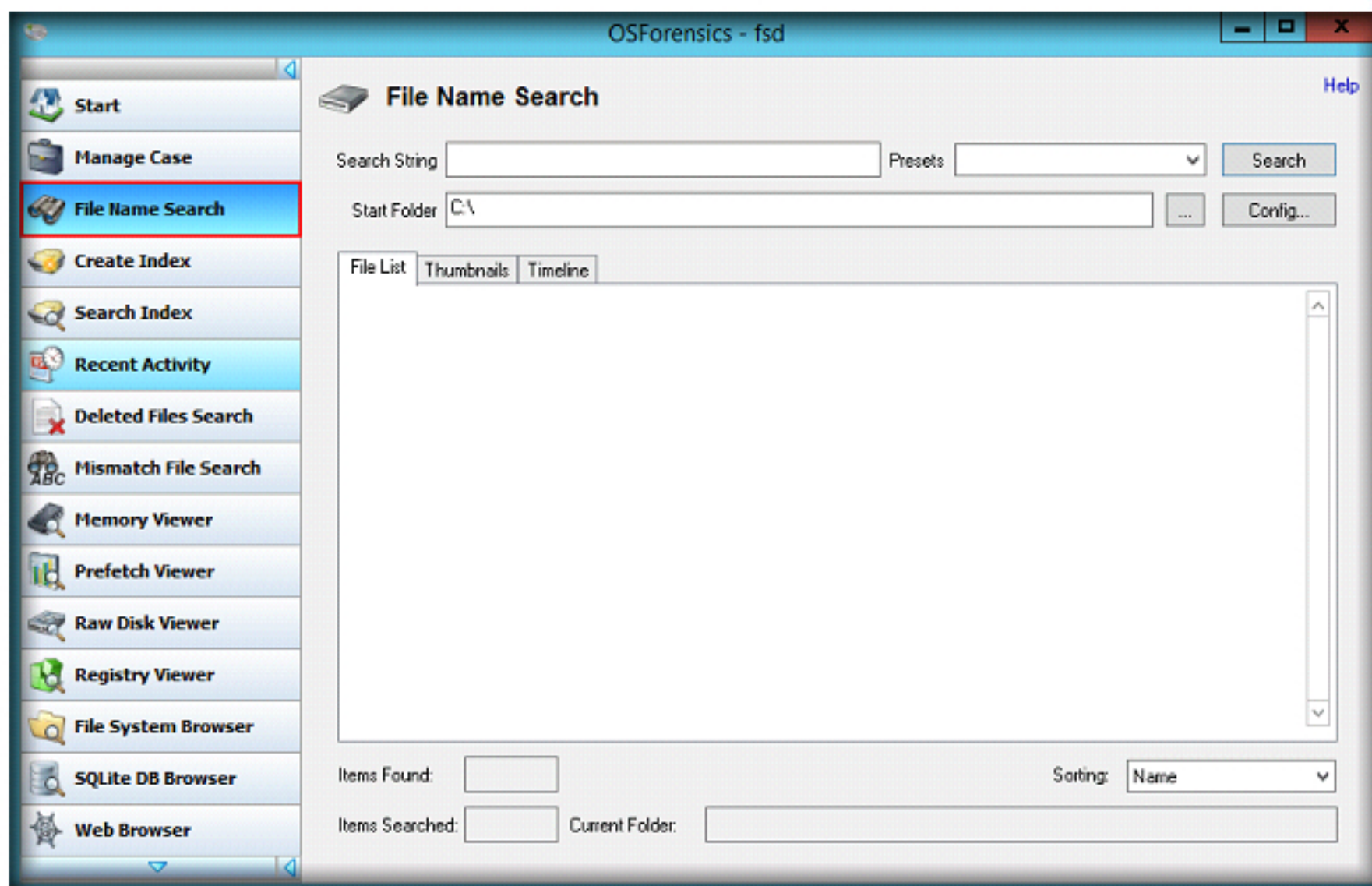


FIGURE 1.5: OSForensics File Name Search

9. To search for files, type a file name or extension in the **Search String** of the **File Name Search** window, or you can also select the file type from the **Presets** drop-down list.
10. In this lab, **Images** have been selected from the **Presets** drop-down list.

11. In the **Start Folder** field, indicate the path to search by clicking the browse button, and then click the **Search** button.
12. Here we are specifying the location **C:\CHFI-Tools\Evidence Files** to search for images in it.

If a wildcard is entered anywhere in the search field, wildcard matching is enabled on all search terms. When wildcard matching is enabled, you will need to explicitly add '*' to the start and end of the search term if you are trying to match a word that may appear in the middle of a filename.

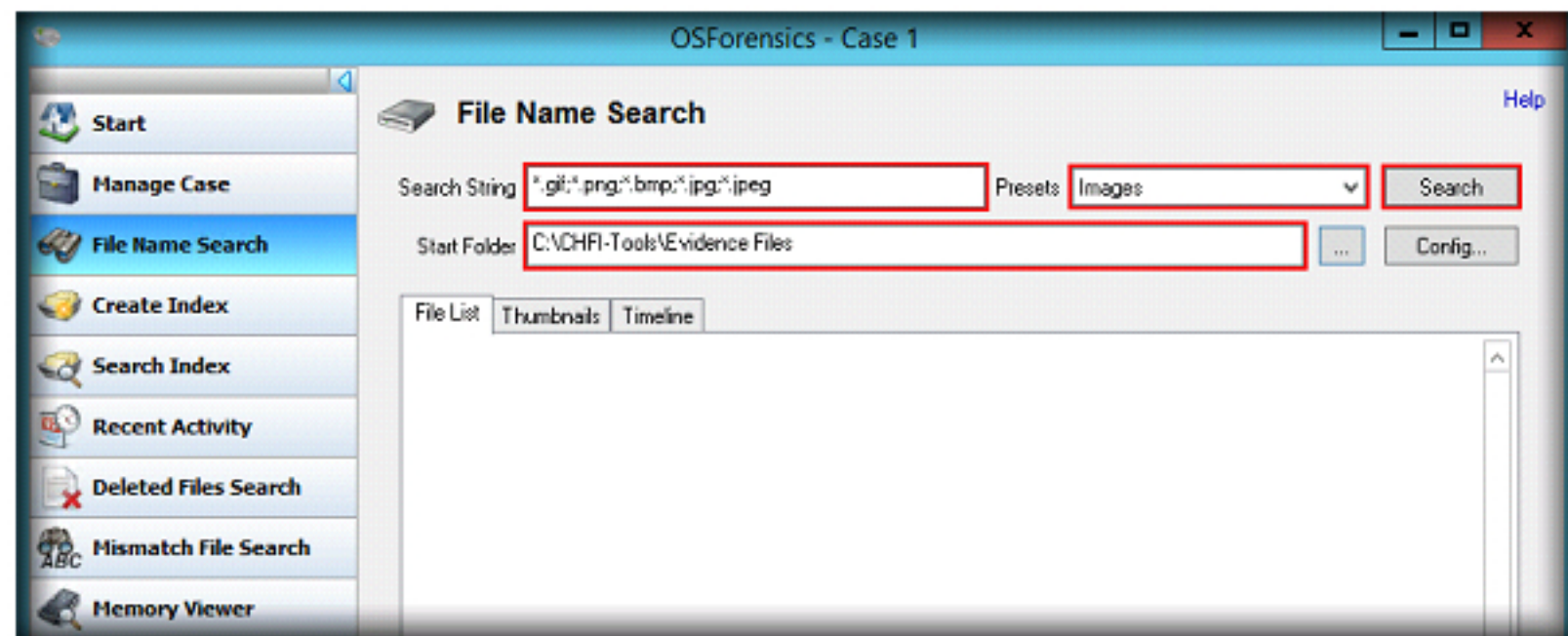


FIGURE 1.6: OSForensics File Name Search

13. This displays all the images present in the specified location. You may analyze these files, to see if any suspicious or unwanted image/images are stored in the location.

By clicking the **Config** button you will be taken to the **File Name Search Configuration** window, where more advanced options can be selected.

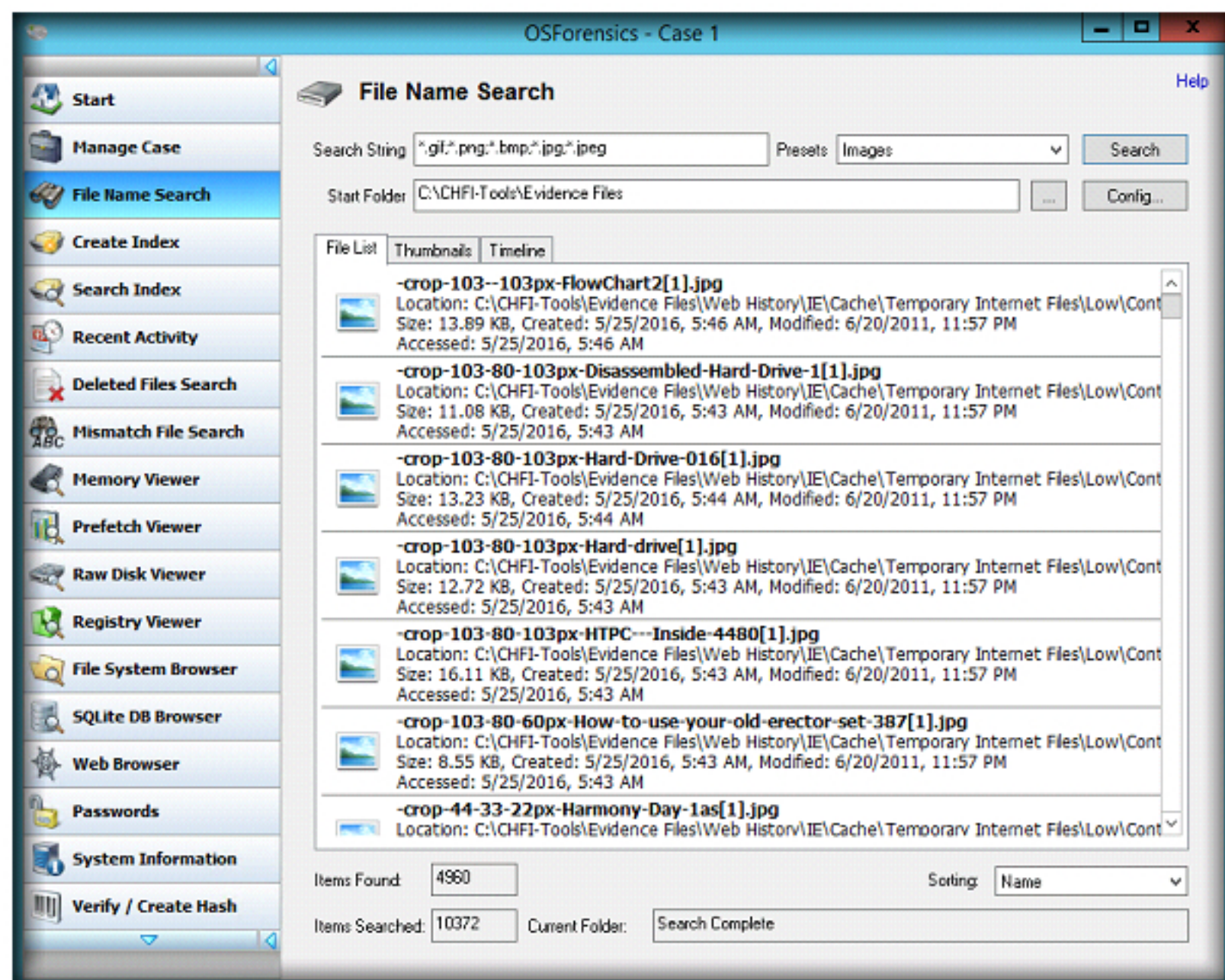


FIGURE 1.7: OSForensics File Name Search

TASK 3

Creating Index

The Indexer Advanced Configuration Window allows users to configure various indexing parameters. This window can be accessed by clicking the **Config** button in the **Create Index** window.

The list of file types whose contents will be scanned are configured here. Typical file extensions are added to the list by default. To add a new file extension, click **Add** button.

14. You may view the images either in **File List** view or in **Thumbnail** view. The **Timeline** tab allows you to see/sort the files according to their modified, accessed or created times.
15. Now click **Create Index** in the left pane of the window. It will create an index of the content.
16. It is a five-step process to create an index:
 - **Step 1:** Select the **Use Pre-defined File Types** option for creating the Index and check the required options listed below (here, **Images** option has been selected) for selecting the file types, then click **Next**.

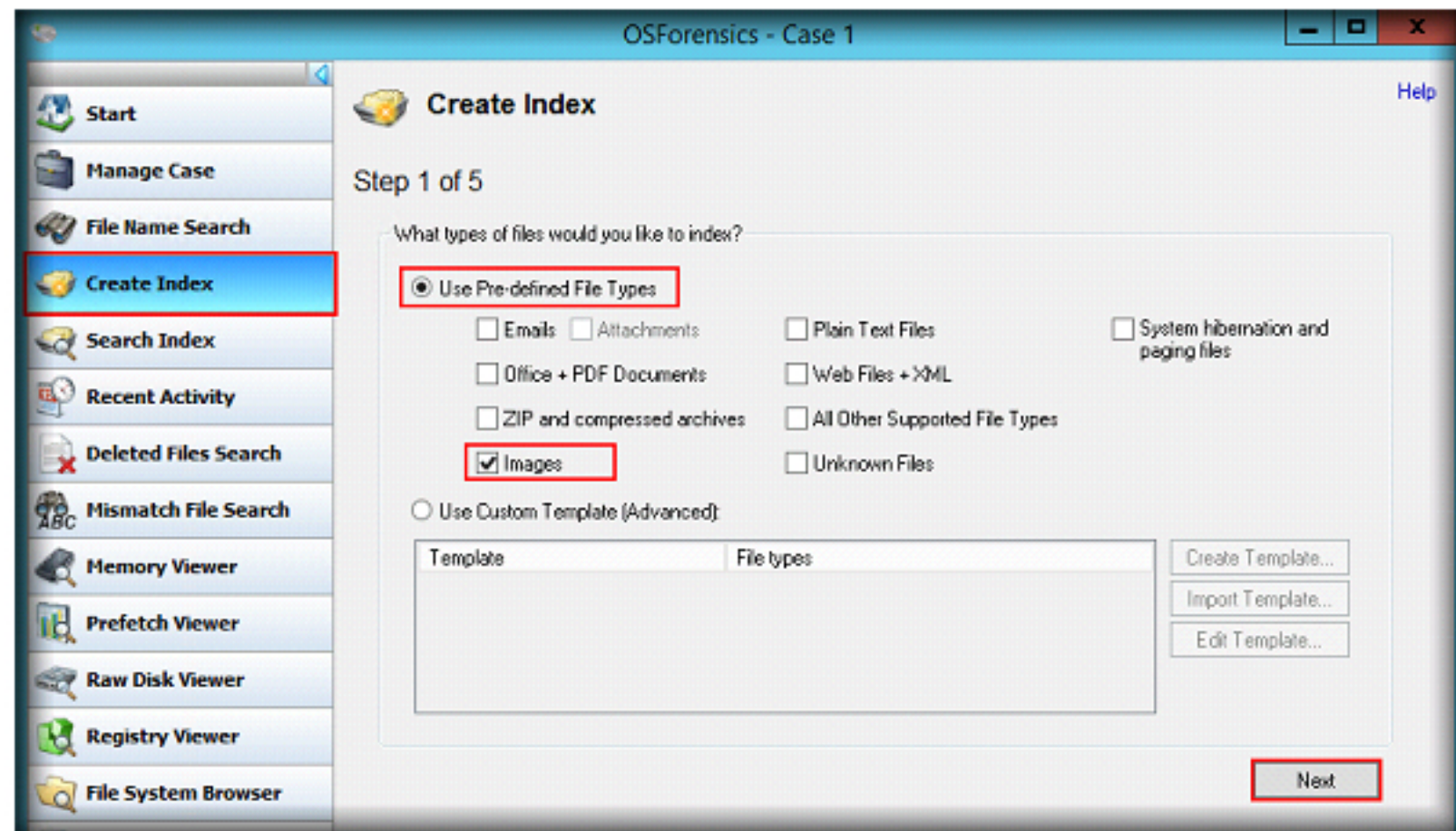


FIGURE 1.8: OSForensics Create Index Step 1

- **Step 2:** Now click the **Add** button to select the drive you want to index.

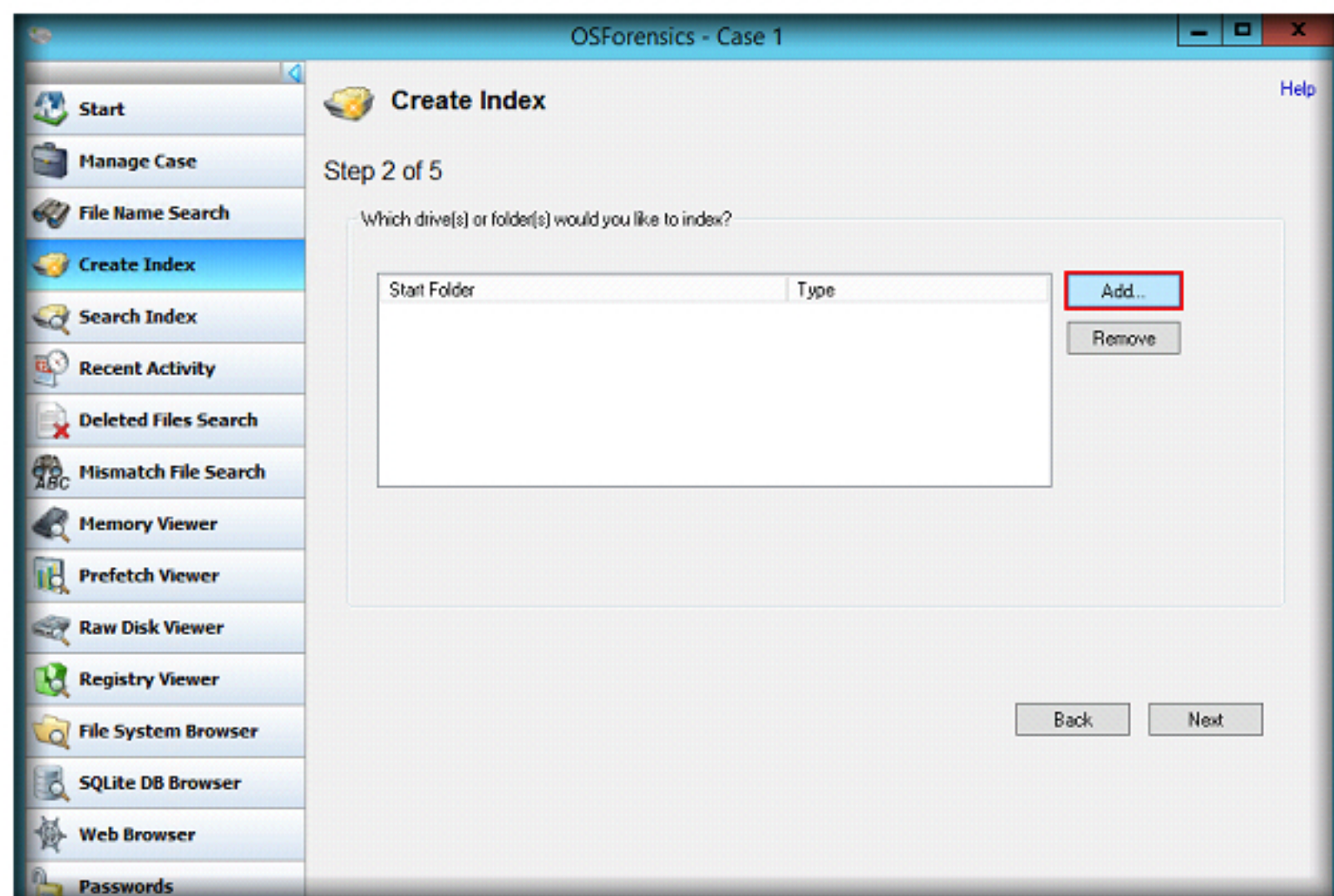


FIGURE 1.9: OSForensics Creating Index Step 2

- Select the **Specific Folder** radio button, and click the **ellipsis** button to add folders. For this lab, select the **C:\CHFI-Tools\Evidence Files\Image Files** folder and click the **OK** button.

 Pages and folders containing particular words can be excluded from the scan by adding the words to the list. Note that the folder the created index files are written to are also automatically added so that the indexing process does not index the files it is creating. This folder is a subfolder of the currently active case folder.

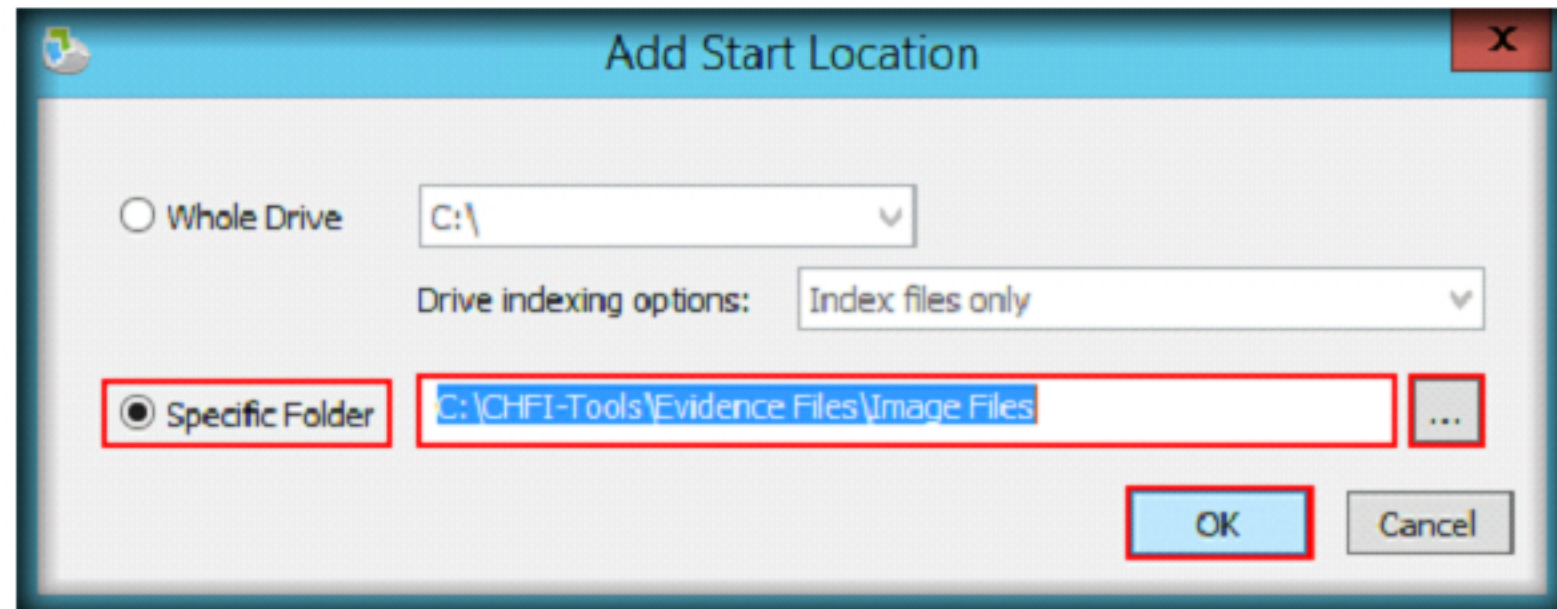


FIGURE 1.10: OSForensics Creating Index Step 2

- Click the **Next** button in the **Create Index** section.

 Stemming refers to similar words derived from the search terms. For example, searches for "fish" would return results for "fishing," "fishes," and "fished." To enable stemming, check the **Enable stemming for:** checkbox and select a language.

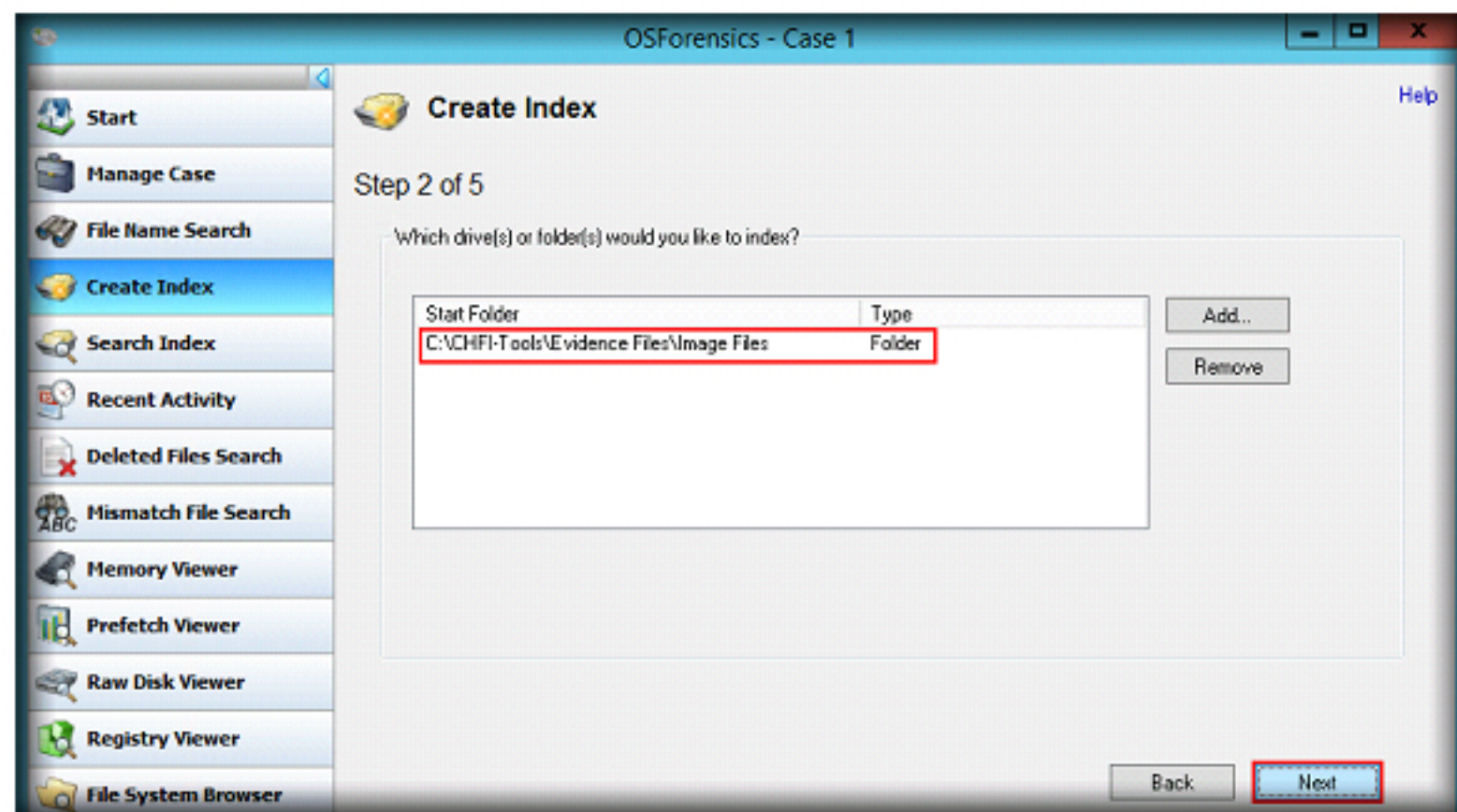


FIGURE 1.11: OSForensics Creating Index Step 2

- **Step 3:** Specify an **Index Title (Case 1)** and **Index Notes** (optional), then click **Start Indexing**.

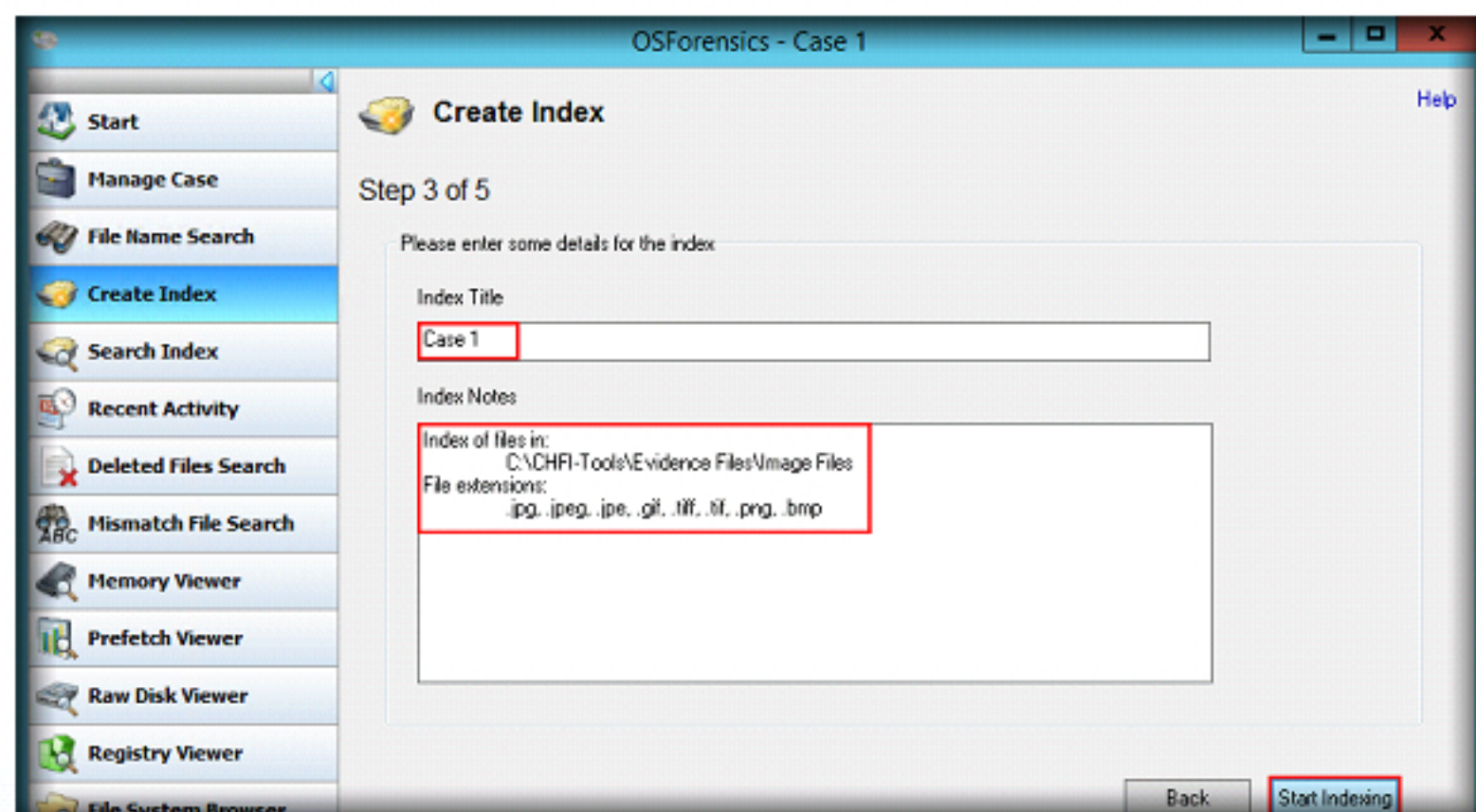


FIGURE 1.12: OSForensics to start Indexing Step 3

- **Step 4:** In Step 4, the application begins to perform a Pre-Scan on the specified folder.

Note: If a **Maximum page limit in Free Version** dialog box appears while scanning, click **OK** to close it.

 **Binary String Extraction Level:**
When trying to get words out of binary data, the indexing process has to make a decision as to what is a word and what is just random data. Changing this option will determine how lenient or strict the indexer is when making this decision. Leaving this on default, the most stringent option, is recommended, as this will aggressively remove irrelevant data and keep the index to a more manageable size. The **Code Words** setting is useful if you are trying to find things like passwords missed by the default option.

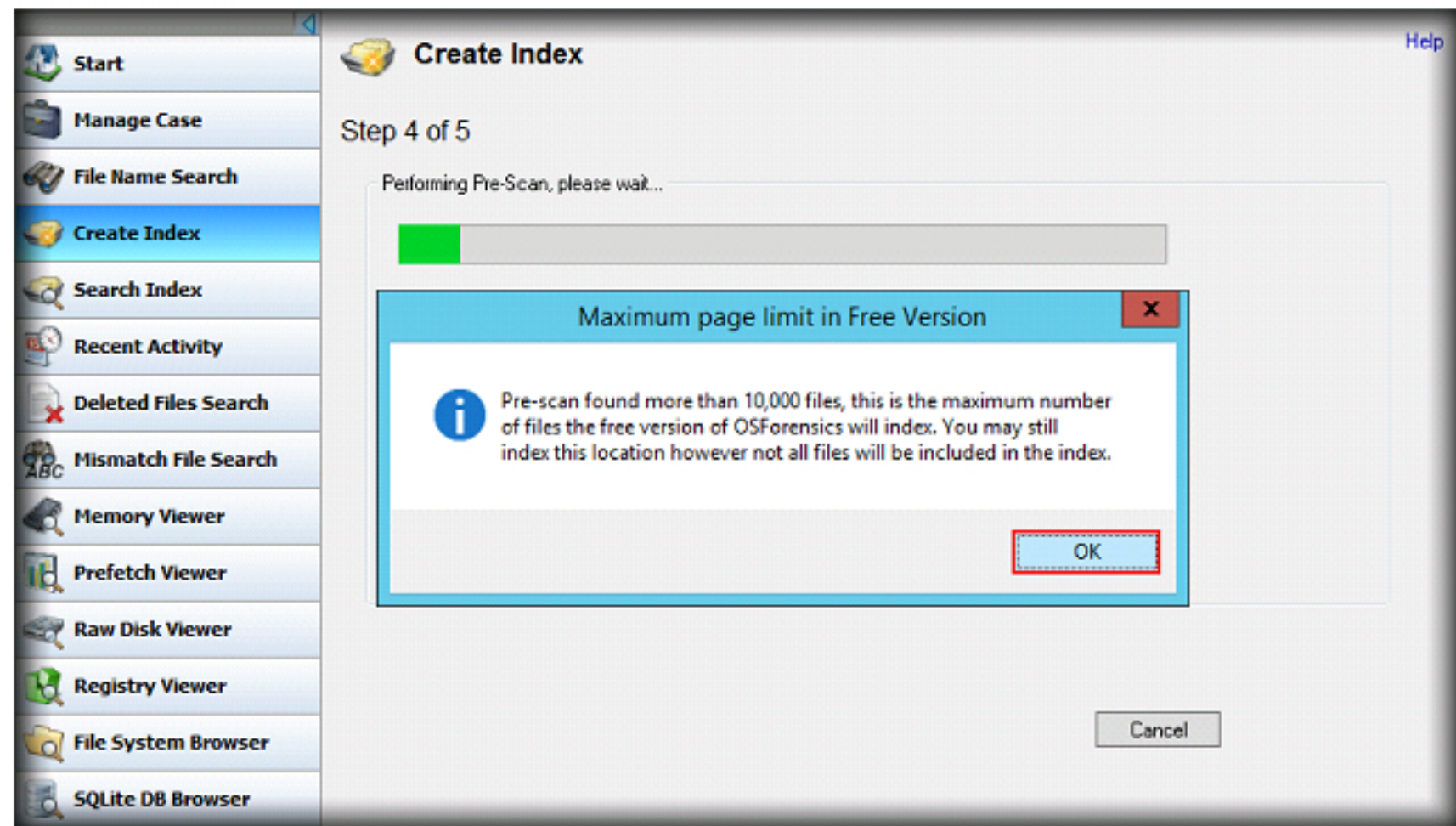


FIGURE 1.13: OSForensics to start Indexing Step 4

- **Step 5** displays the status of the Indexing. Once the Indexing is completed, an **OSForensics - Created Index** pop-up appears, click **OK**.

 The log file shows many errors about files being locked. If you are indexing an active system drive (the drive that Windows is running from), this is quite common as many programs, and Windows itself will be using the files on the drive, making them inaccessible. Usually, these files are system files without much interesting text in them, and this should not be a problem.

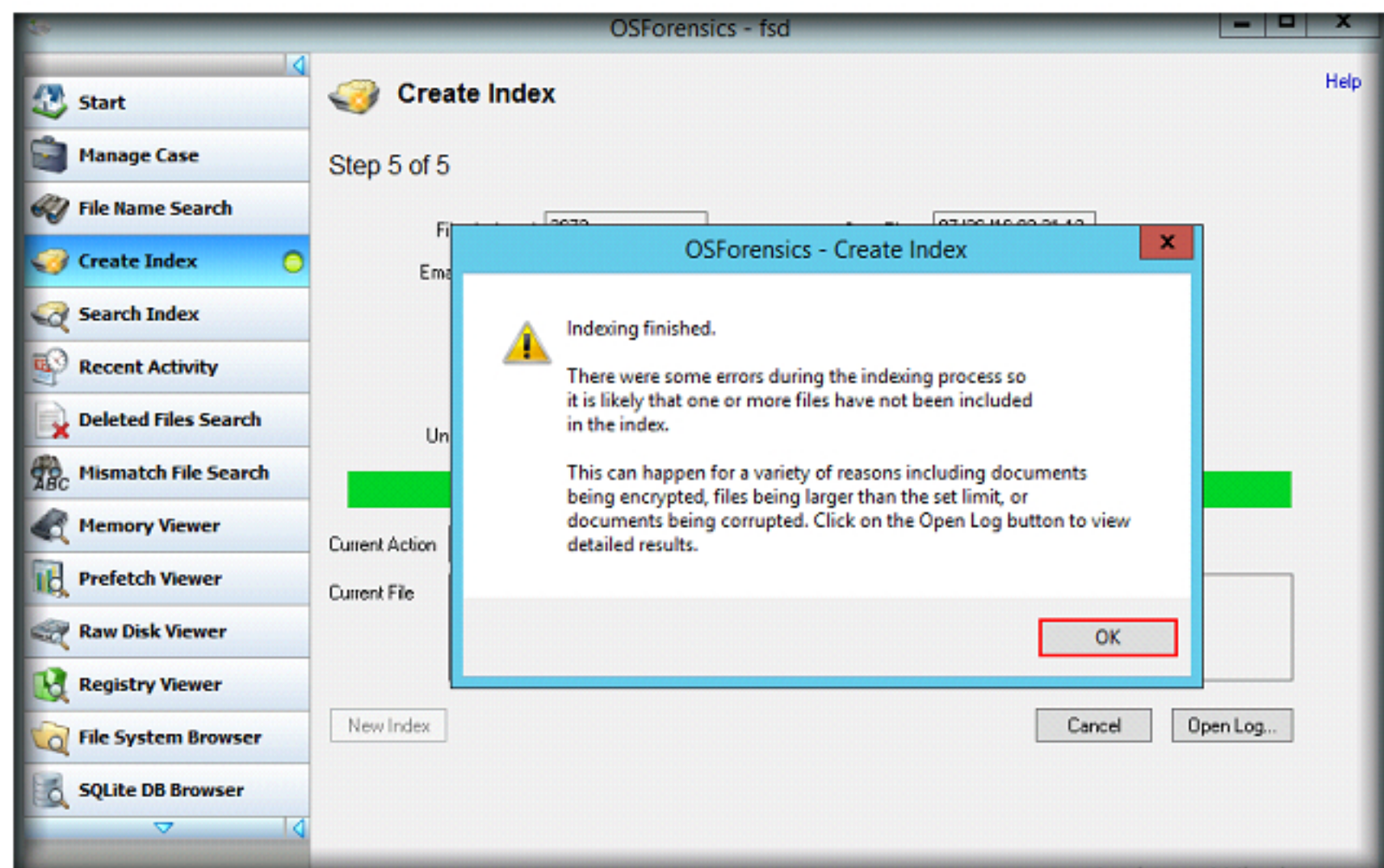


FIGURE 1.14: OSForensics Step 5

17. Select **Search Index** section from the left pane, enter the keyword to search in the **Enter Search Words** field (optional), select the **Index to Search** (here, **Case 1**) from the drop-down menu. Click the **Search** button.

Note: The free version of OSForensics returns a maximum of **250** results. So, if the Search results exceed this number, an **OSForensics - Notice** pop-up appears where you need to click **OK**.

During the pre-scan step, OSForensics tries to detect the number of files that will be included in the index and sets this as the maximum which the indexing process will scan. Because the pre-scan is a basic and fast scan, it may sometimes get this wrong. If this is the case, you should try indexing again by setting the maximum pages manually in the advanced options.

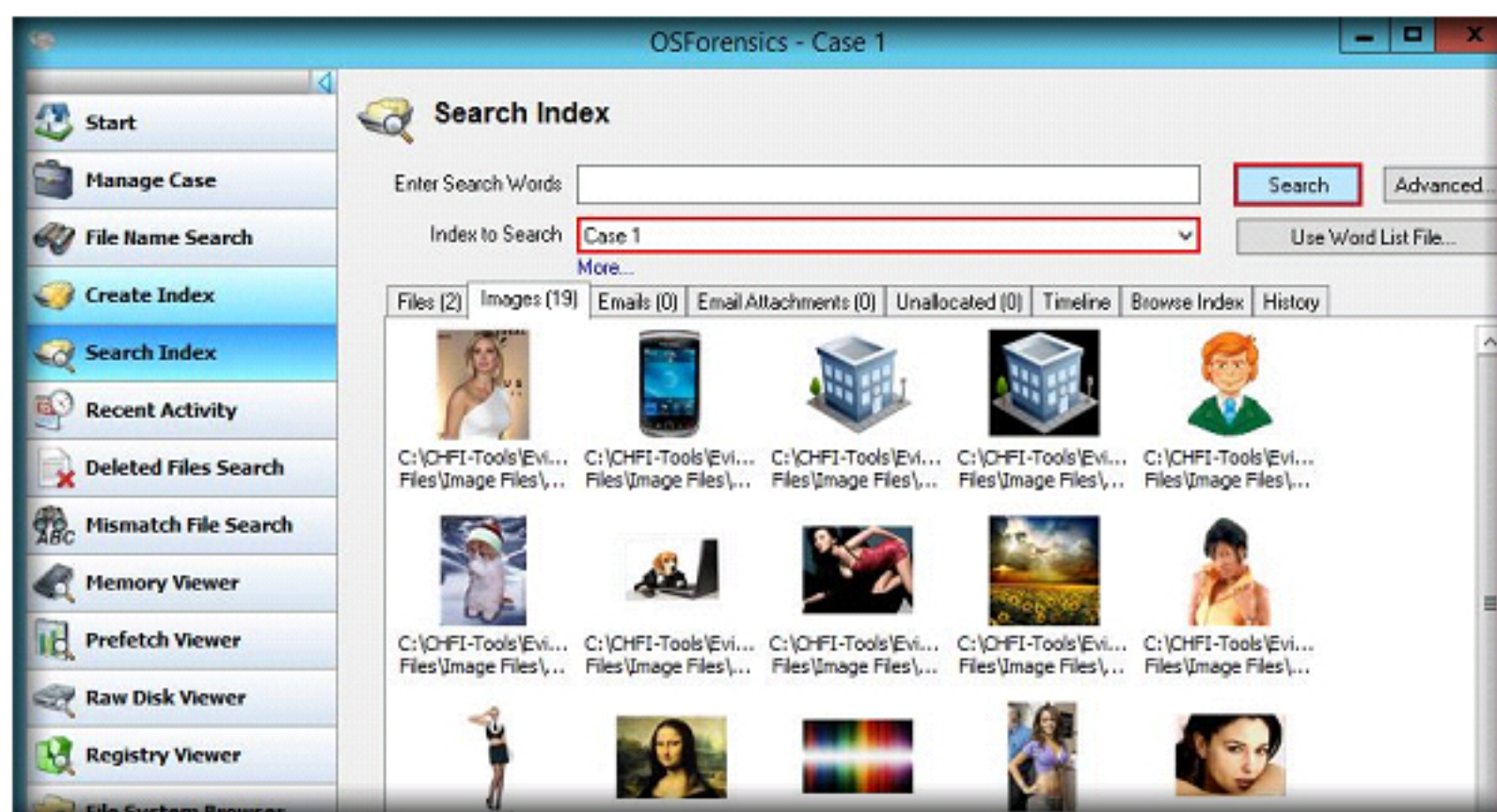


FIGURE 1.15: OSForensics Searching Index (Image Files)



TASK 4

Searching Recent Activities

18. Click **Recent Activity** to scan for evidence such as browsed websites, USB drives, recent downloads, and Wireless networks.
19. Select **Scan Drive** radio button, select **C:** Drive and click **Scan** to scan for evidence such as browsed websites, USB drives, recent downloads, and Wireless networks in the drive.

Note: If a **Warning** pop-up appears, click **Yes**. If an **OSForensics Error** appears during the scan, click **OK**.

20. On completion of scan, a **Recent Activity - Summary** window appears, click **OK**.

OSForensics scans known locations for web browser profiles and their related history and cache files to detect cookies, visited URL history, downloads, and saved logins and passwords.

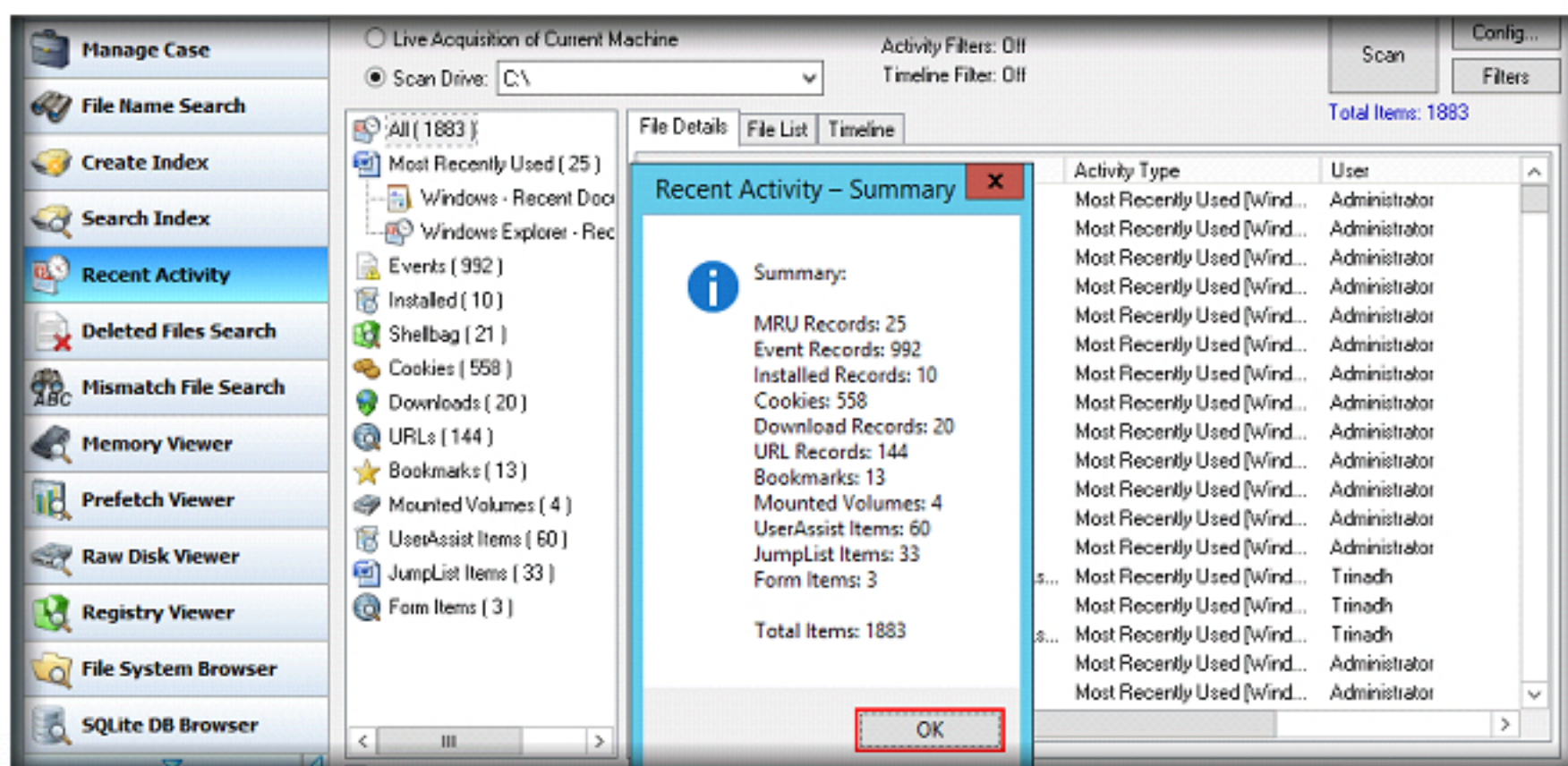


FIGURE 1.16: OSForensics Recent Activity

**T A S K 5****Searching Deleted Files**

21. To recover the deleted files from the filesystem, click **Deleted Files Search** in the left pane, select a disk on which you want to perform the deleted file search (here, **Partition 1, C:**), and click the **Search** button.

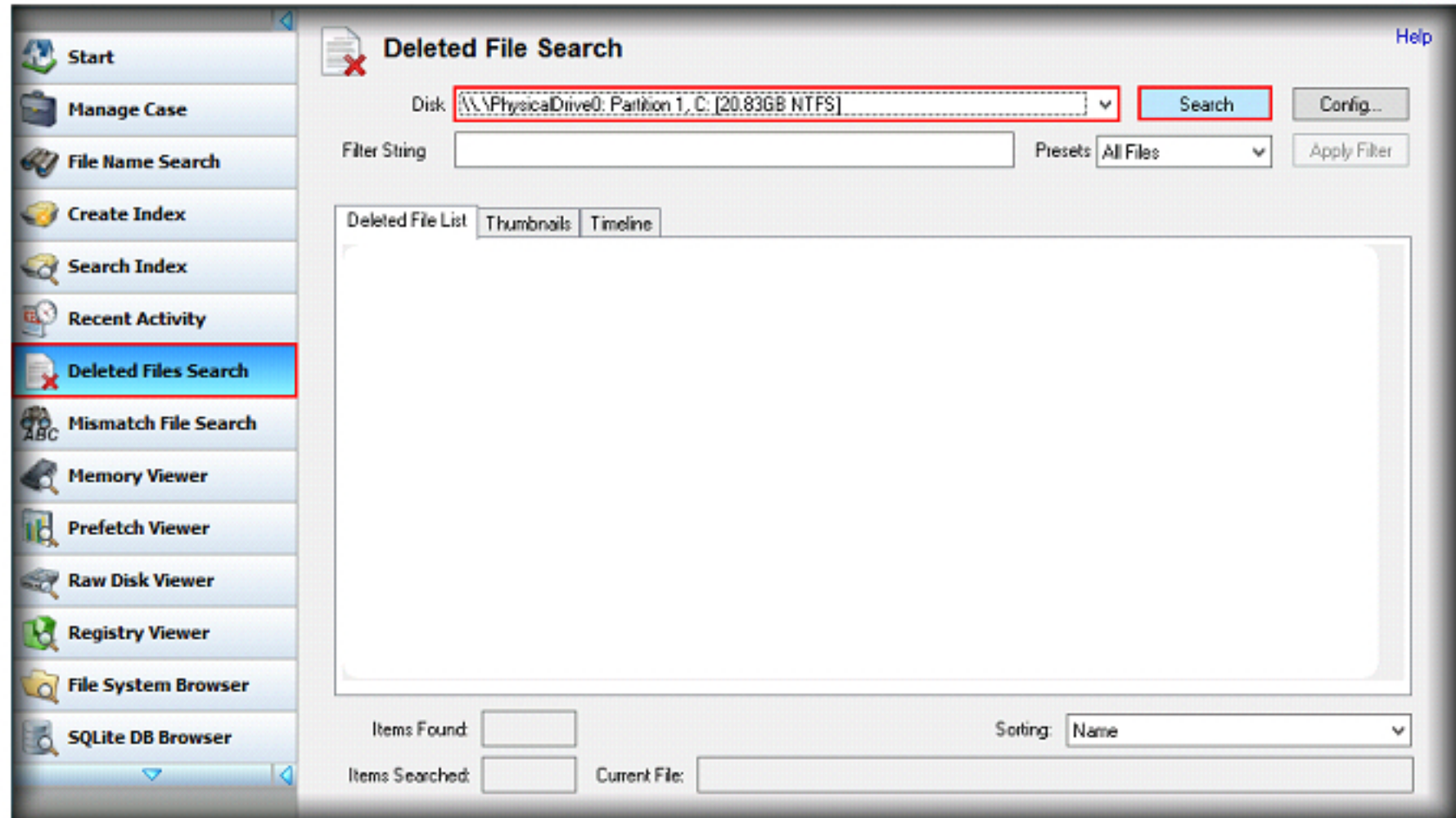


FIGURE 1.17: OSForensics Deleted Files Search to recover files

22. The application searches for the deleted files in **C:** Drive and displays them as shown in the following screenshot:

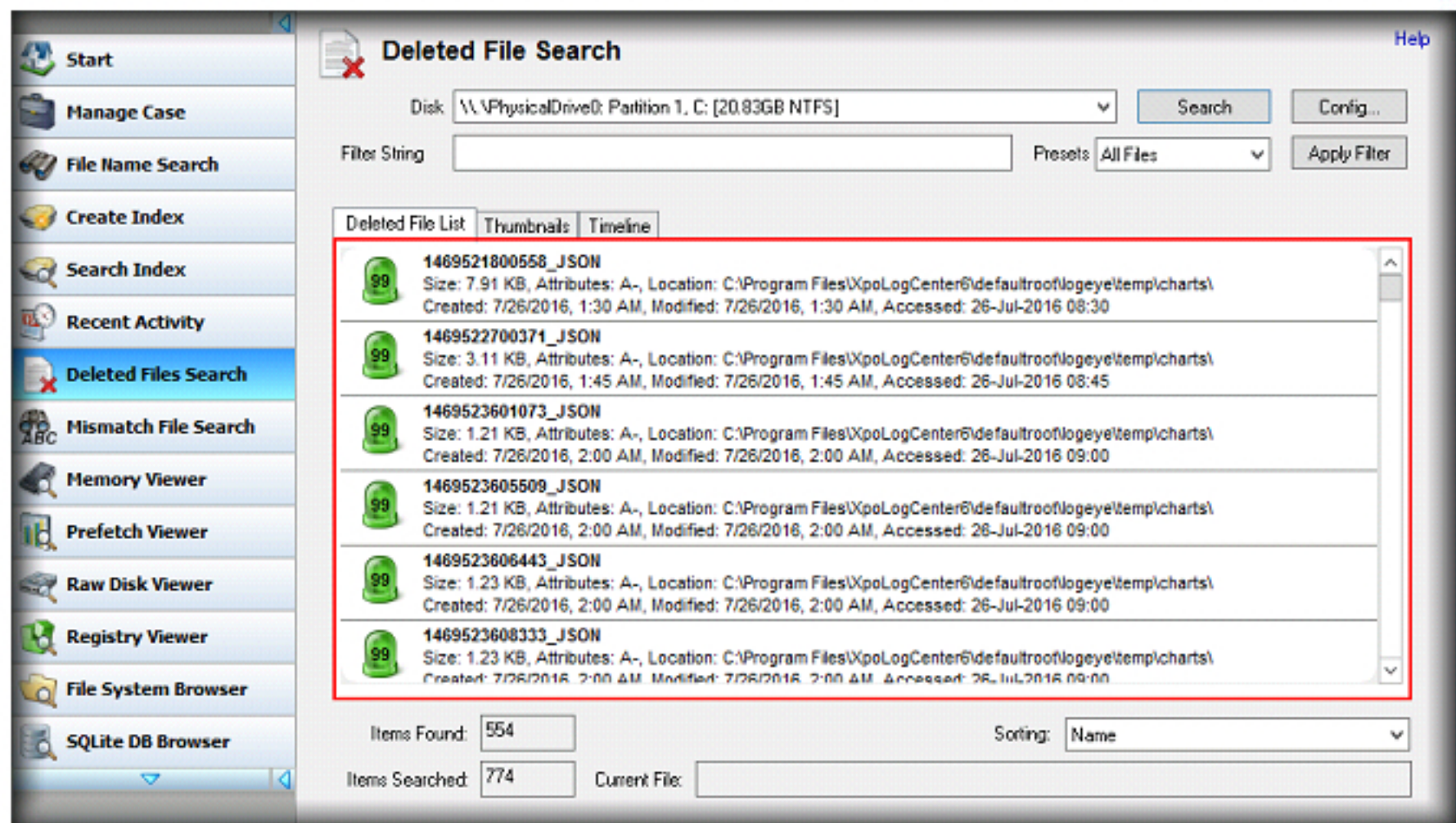


FIGURE 1.18: OSForensics Deleted Files display

TASK 6

Searching
Mismatch File

Connected USB devices:

USB devices that have been connected to the computer, and include USB memory sticks, portable hard drives and other external USB devices like CD-Rom drives. A manufacturer name, product ID, serial number and the last connection date should be displayed for each device.

23. To locate files whose contents do not match with the file extensions, click **Mismatch File Search** in the left pane of the window.
24. Click the **Browse** button to give the location path to search. In this lab, navigate to **C:\CHFI-Tools\Evidence Files\Image Files** and click the **Search** button.
25. This option will uncover attempts to hide files under a false name and extension, and it also verifies the actual file format.

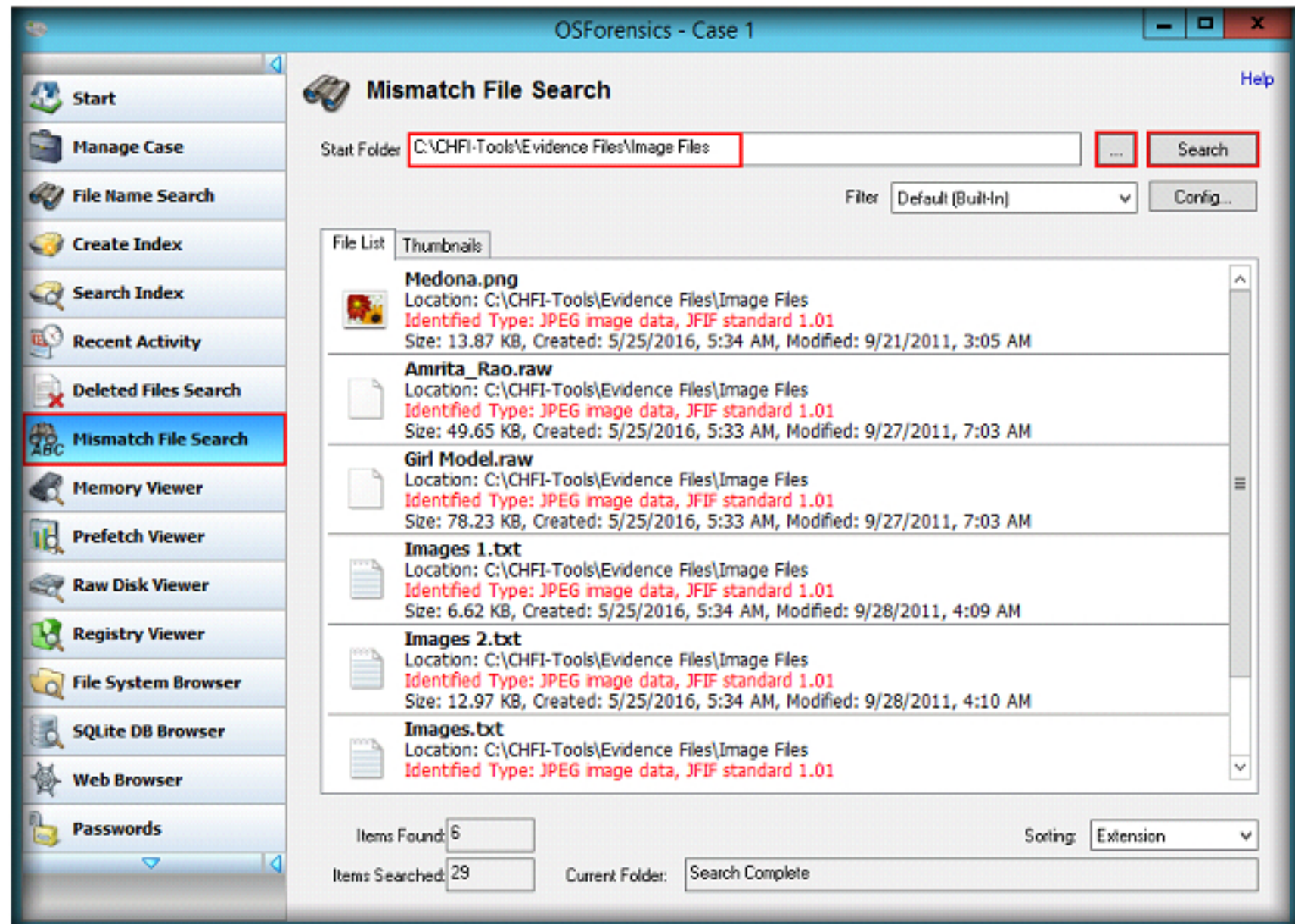


FIGURE 1.19: OSForensics Mismatch File Search

TASK 7

Viewing Memory
Processes

OSForensics checks several known registry locations that store MRU data; this includes locations for Microsoft Office, Microsoft WordPad, Microsoft Paint, Microsoft Media Player, Windows Search, recent documents, connected network drives, and the Windows Run command.

26. To view the processes that are running on the system, click **Memory Viewer** in the left pane of the window.
27. An **OSForensics - Warning** pop-up appears, click **OK**.

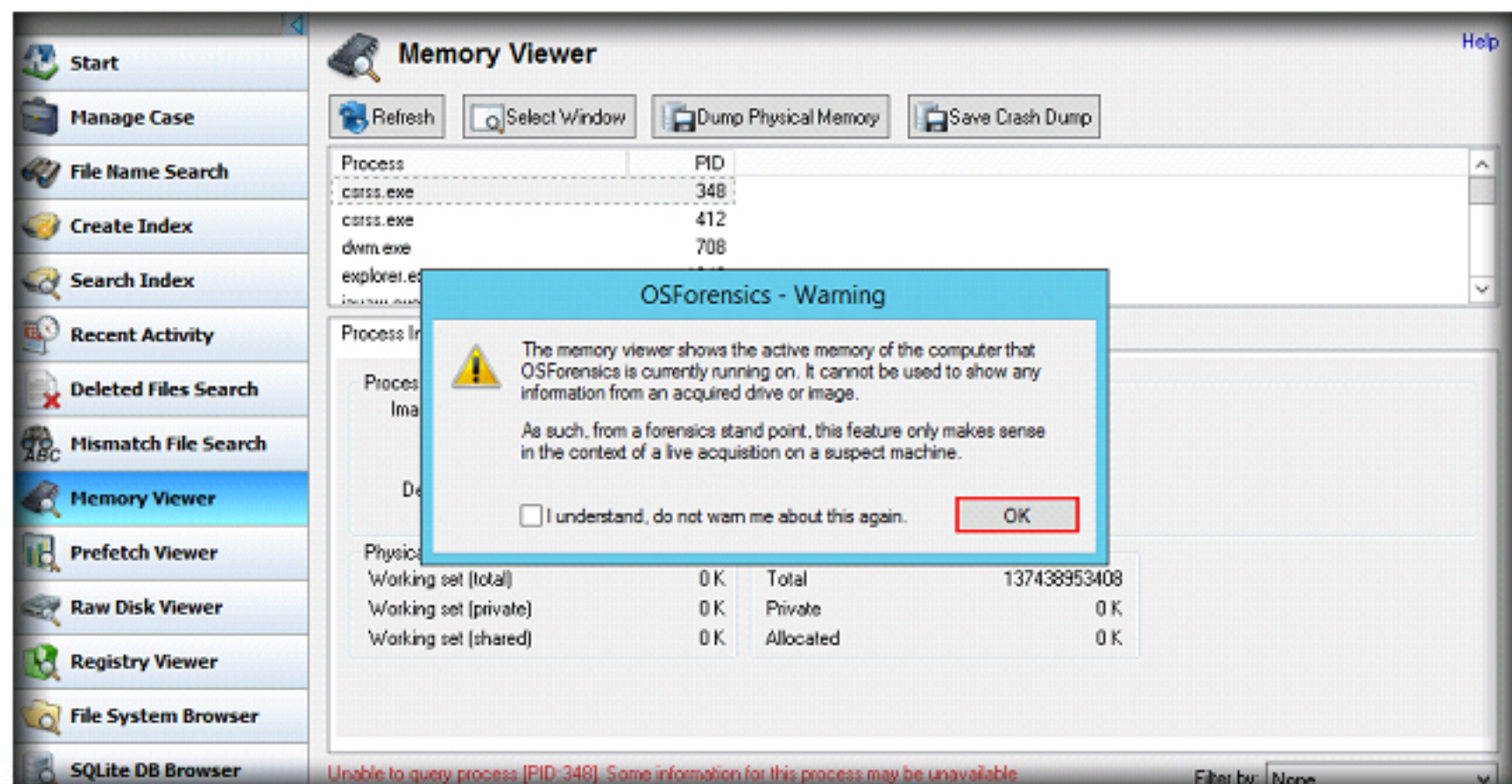


FIGURE 1.20: OSForensics - Warning pop-up

28. Select a **Process** from the list of running processes, and select the **Memory Space** tab to view complete memory details of that process.

Performing a process memory dump saves the contents of a process' virtual memory space (both in physical memory or paged out to hard disk) into a file. This is useful especially if there is a particular process that the user has identified to contain information of interest potentially.

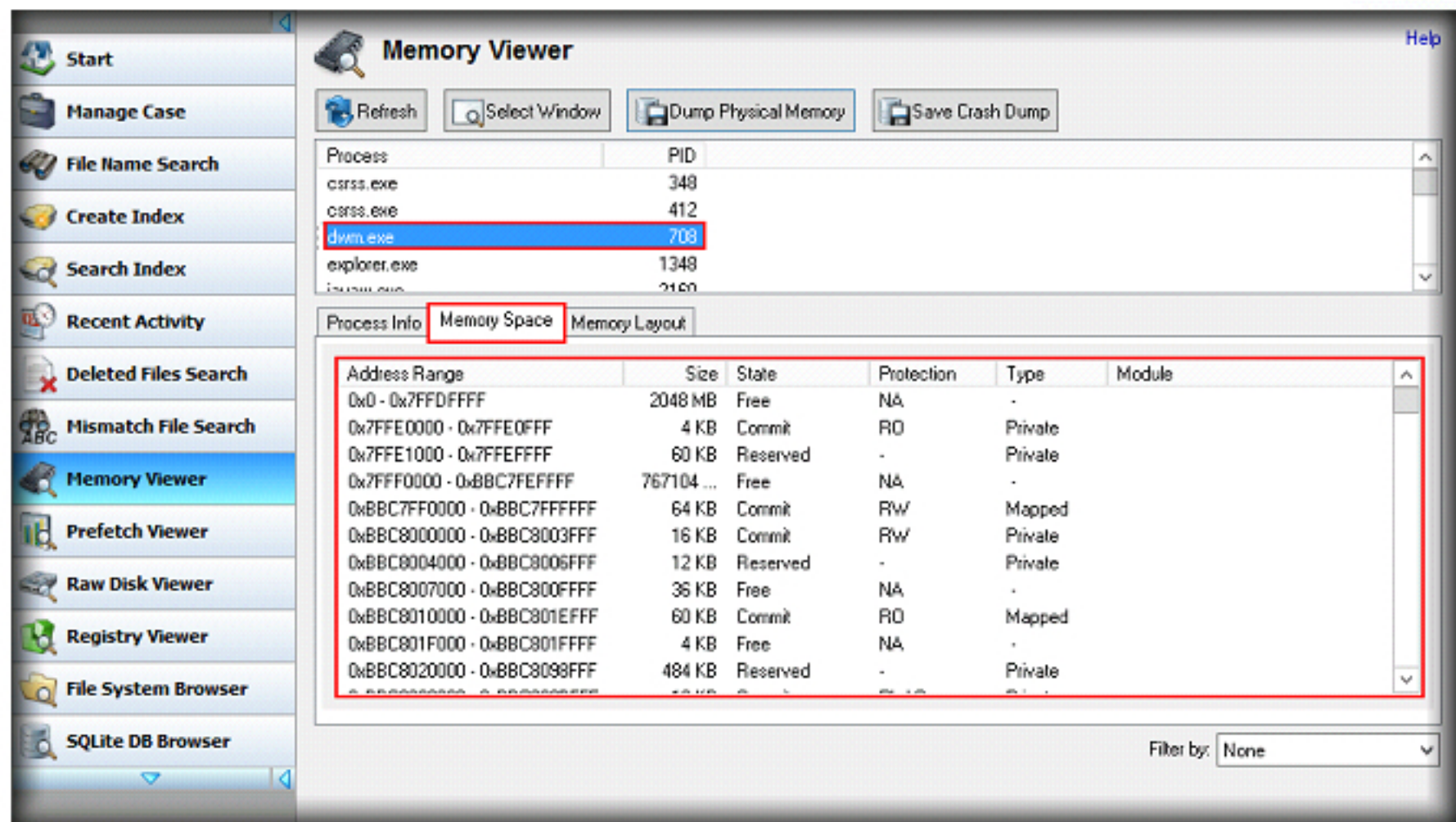


FIGURE 1.21: OSForensics Memory Viewer

TASK 8

Viewing Disk Raw Sectors

Generating a physical memory dump in the Microsoft Crash Dump format allows the user to perform a deeper analysis of the system state at the time the snapshot was taken.

29. To analyze the raw sectors of all physical disks and partitions, click **Raw Disk Viewer**, and select a disk (here, **C: Drive**) to view its raw contents.

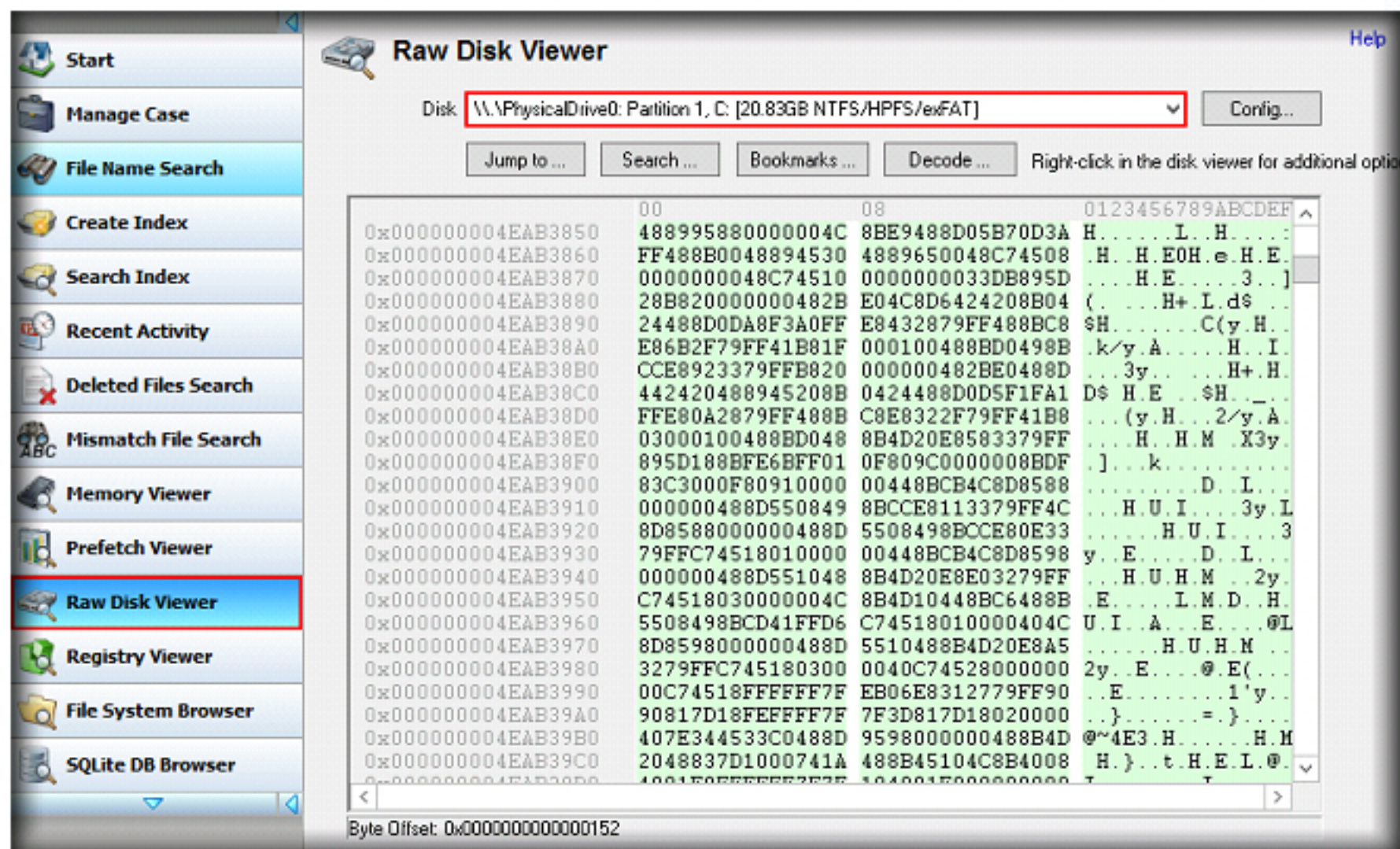


FIGURE 1.22 OSForensics Raw Disk Viewer

TASK 9

Viewing System Information

New third-party tools can be easily added to the test suite. Many applications can be helpful in retrieving system information. These tools must be installed first if these commands are to run correctly.

30. To retrieve detailed information about the core components of the system, click **System Information**.
31. You may use any of the following options from the **List** drop-down menu:
 - Basic DOS commands used
 - Basic system information
 - System Information From Registry
 - All commands used

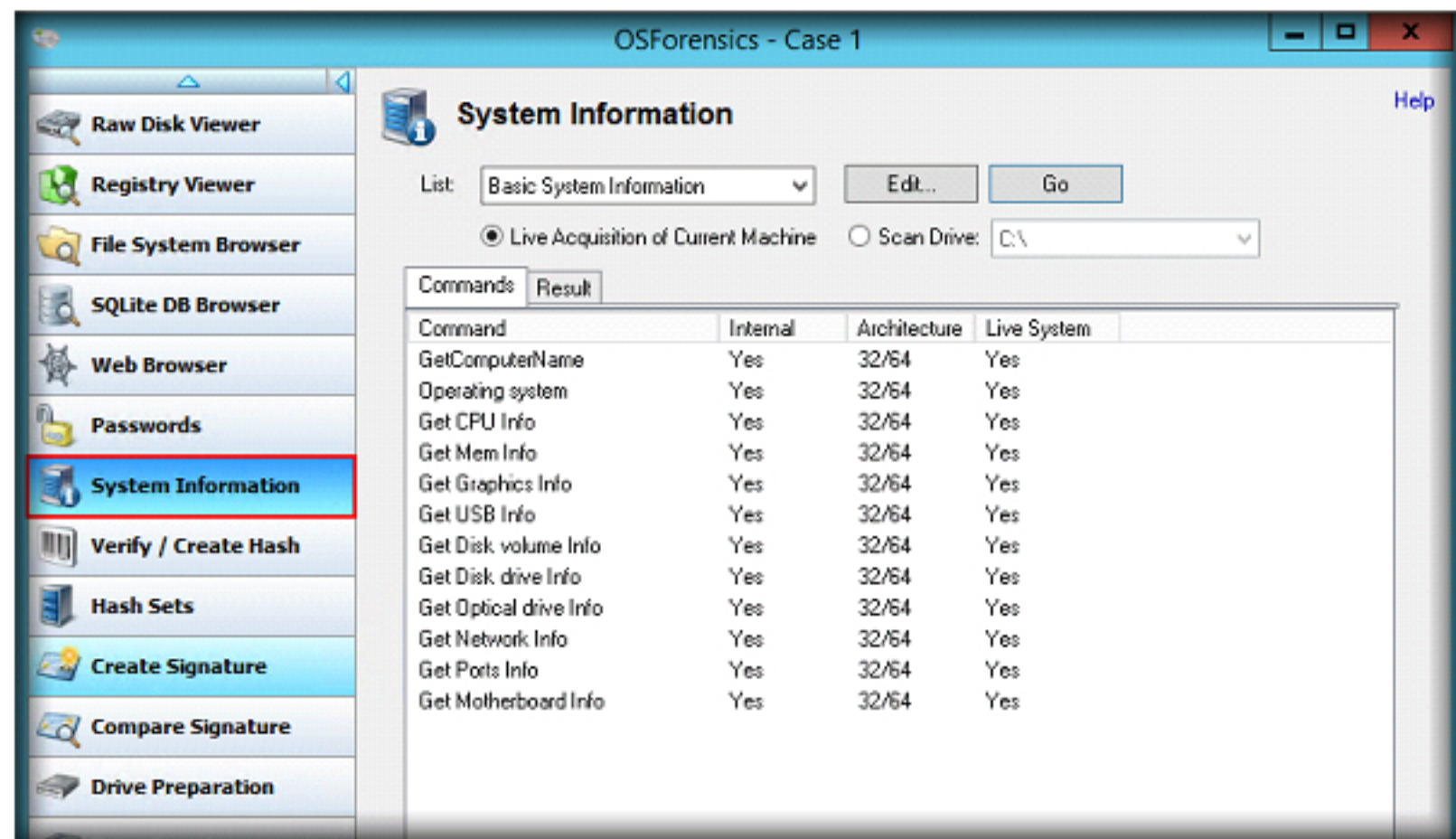


FIGURE 1.23 OSForensics System Information

32. From the **List** drop-down menu, select the type of information that you want to retrieve, and click **GO**.
33. Here, **All Commands** has been selected from the drop-down menu. By selecting this, the application executes all the commands displayed under the **Commands** tab on the machine.

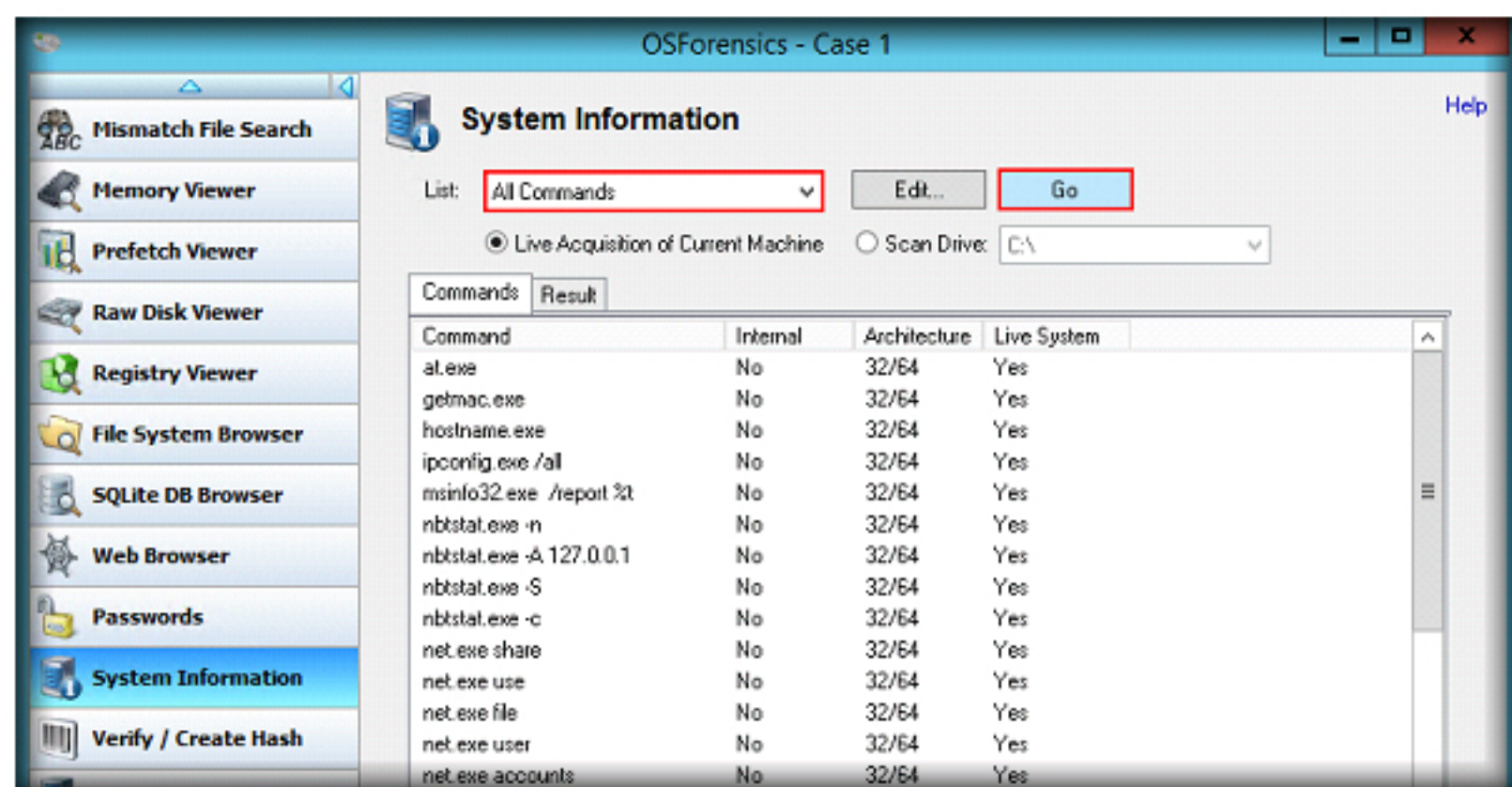


FIGURE 1.24 OSForensics System Information All Commands

Architecture specifies whether this command should be restricted to 32 or 64 bit systems. Live system specifies whether this command is safe to run during a live acquisition.

34. It displays the commands executed, with complete details in the **Result** tab as shown in the following screenshot:



srvcheck.exe:

SrvCheck is a simple ping-like program, which can check the availability of a given server. It is part of the Windows Server 2003 Resource Kit Tools package. It supports Windows Server 2003 and Windows XP but is not supported on a 64-bit platform.

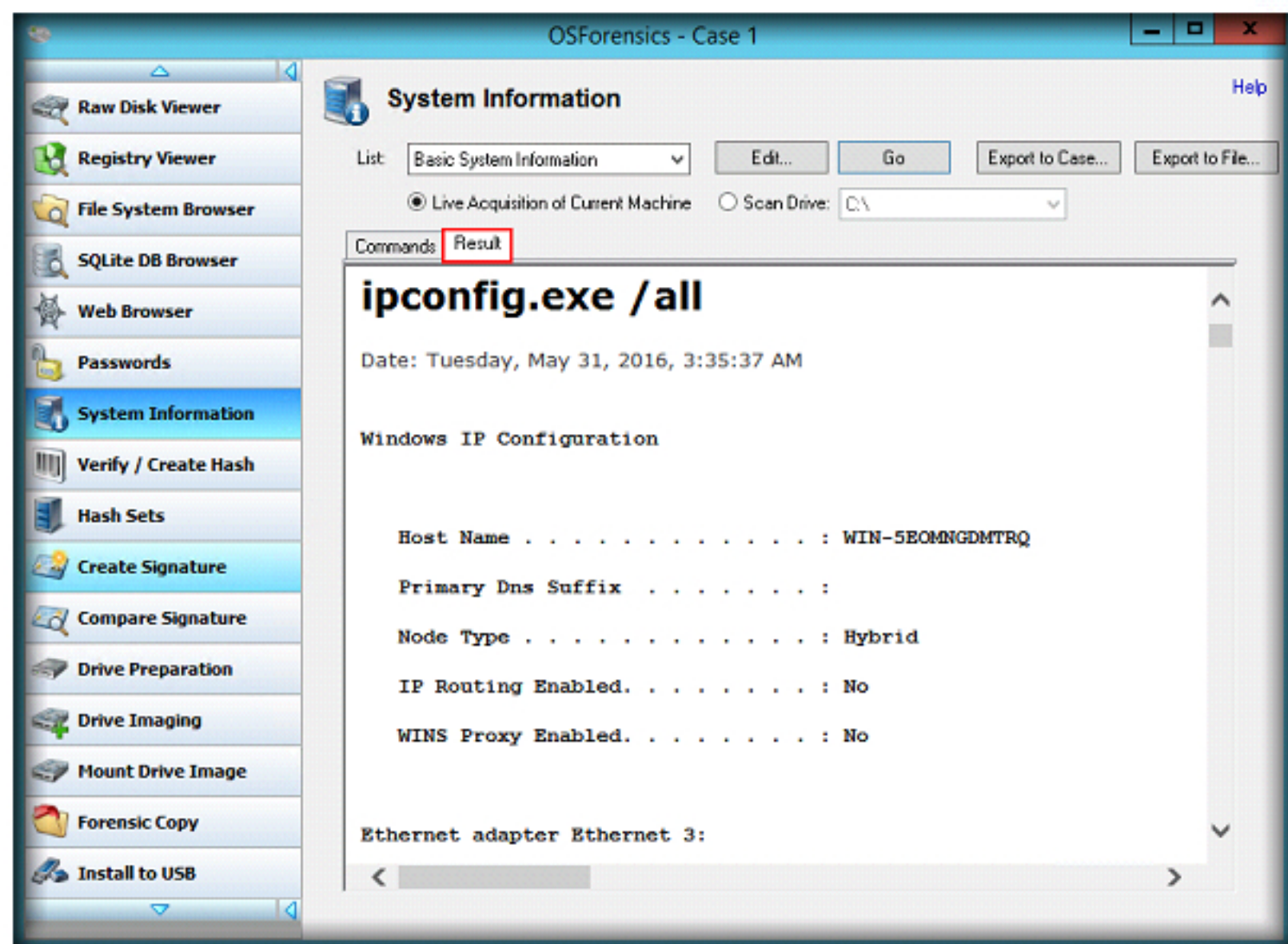


FIGURE 1.25 OSForensics Basic System Information



TASK 10

Verifying the Integrity of Files



To calculate a hash for a file, just input the file path, choose one of the available hash functions and click **Calculate**. To verify the calculated hash with a known hash value, copy the known hash value into the **Comparison Hash** field.

35. To verify the integrity of files by calculating their hash values, click **Verify / Create Hash** from the left pane
36. You can also create a hash of a complete partition, a physical disk drive, or a simple text string by selecting the respective options.

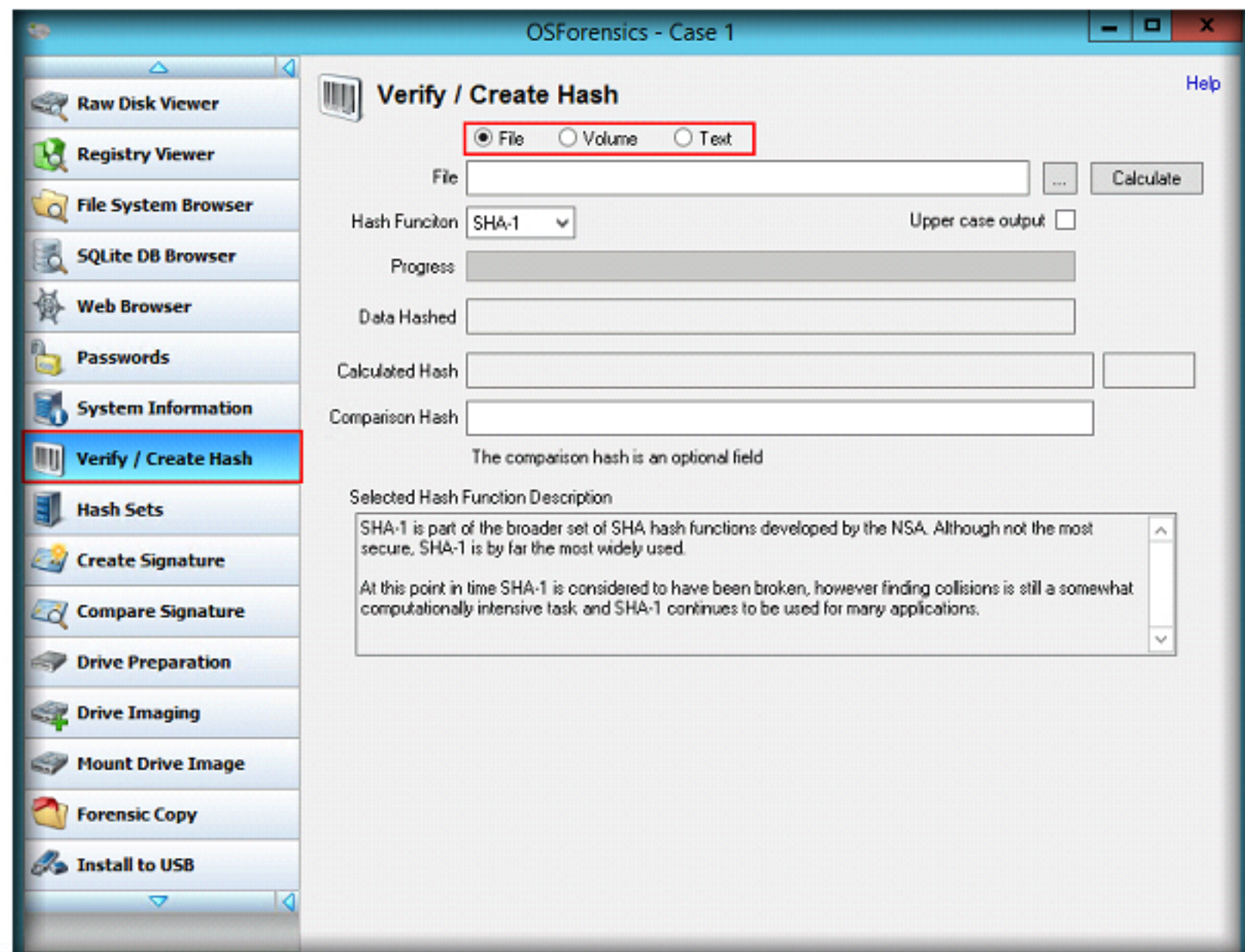


FIGURE 1.26 OSForensics Verify / Create Hash

37. Click the **Ellipsis** button to specify a **File** or **Volume** or **Text** to calculate the hash value. (In this lab, navigate to the file **C:\CHFI-Tools\Evidence Files\Image Files\Images.txt** to calculate the hash value of **Images.txt**).
38. Select **Hash Function** (here, **MD5**) from the drop-down menu and then click **Calculate**.
39. The calculated hash value appears in the **Calculated Hash** field as shown in the following screenshot:

To create a hash of a line of text, select the text option and type or paste the text you want to hash into the text field.

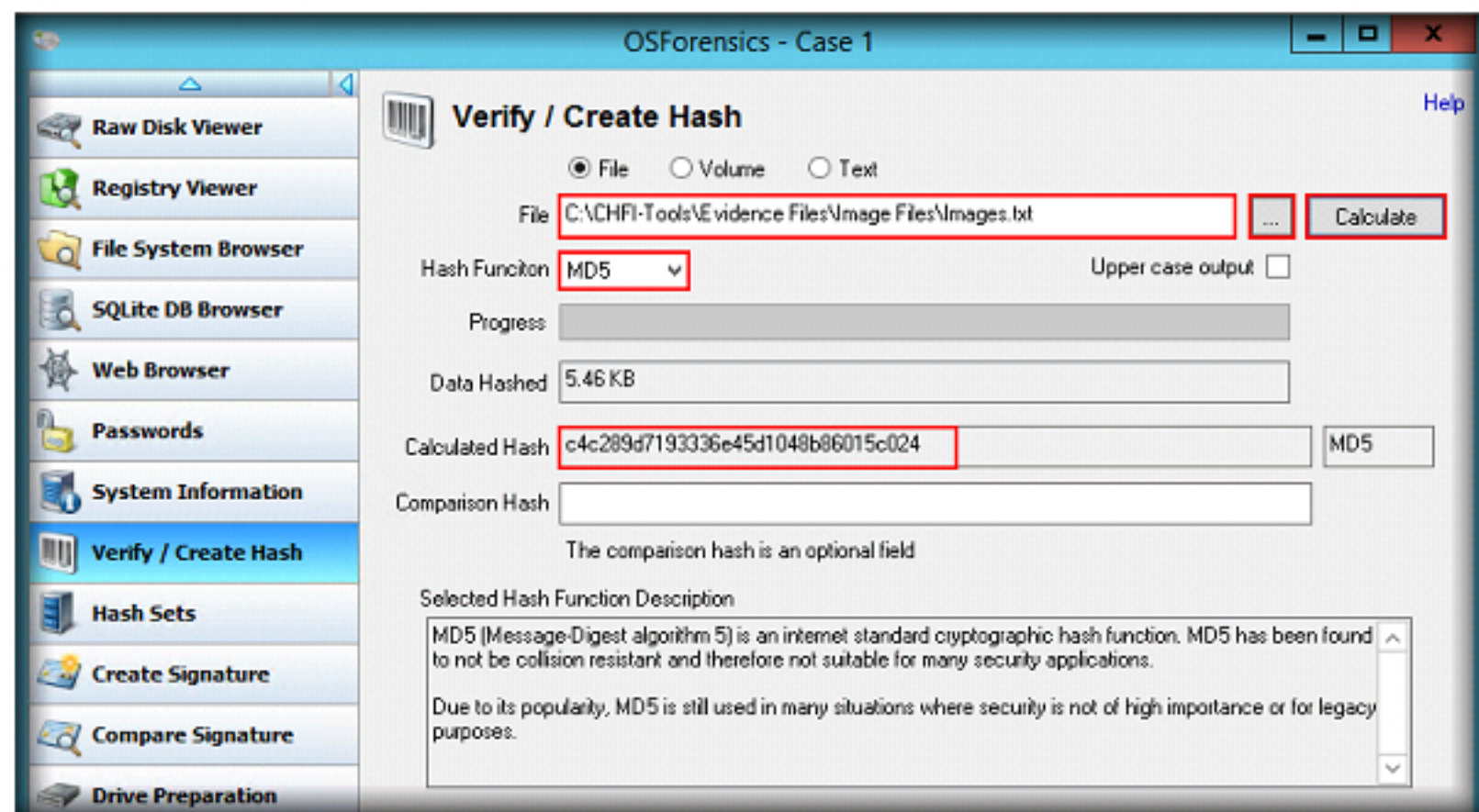


FIGURE 1.27: OSForensics Verify / Create Hash result



TASK 11

Hash Sets



Origin:
The origin of the files belonging to the hash set. Depending on the scope of the database this could be as accurate as "Bob's PC" or as broad as an entire organization.

40. To identify known safe files or known suspected files, click **Hash Sets** to reduce the need for further time-consuming analysis.

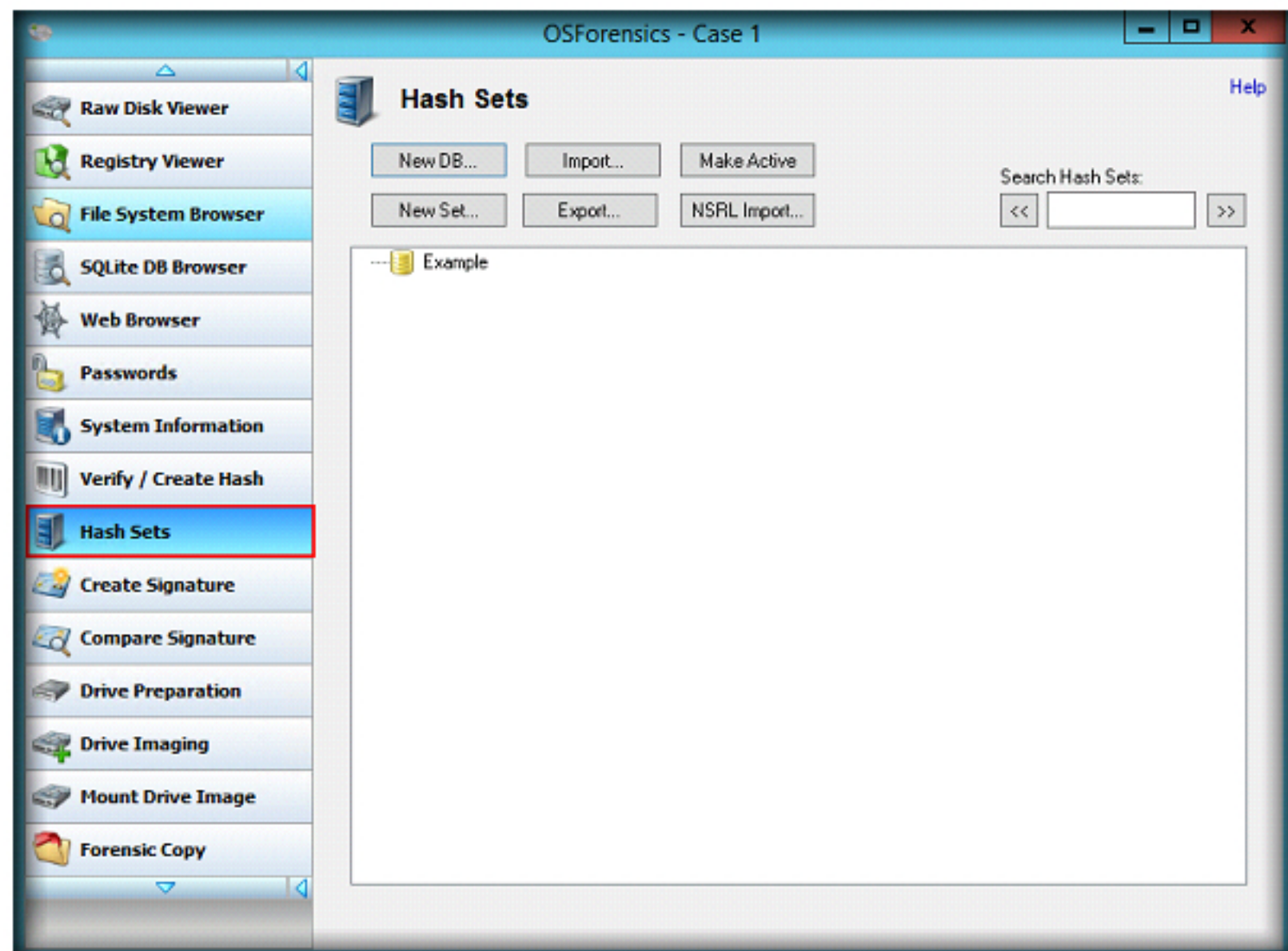


FIGURE 1.28: OSForensics Hash Sets

41. To create a new database click **New DB**, enter the new database name in the **Database Name** field, and click **OK**.

 **Product Type:**
The product type files are associated with, for example, word processor, image editor, operating system.

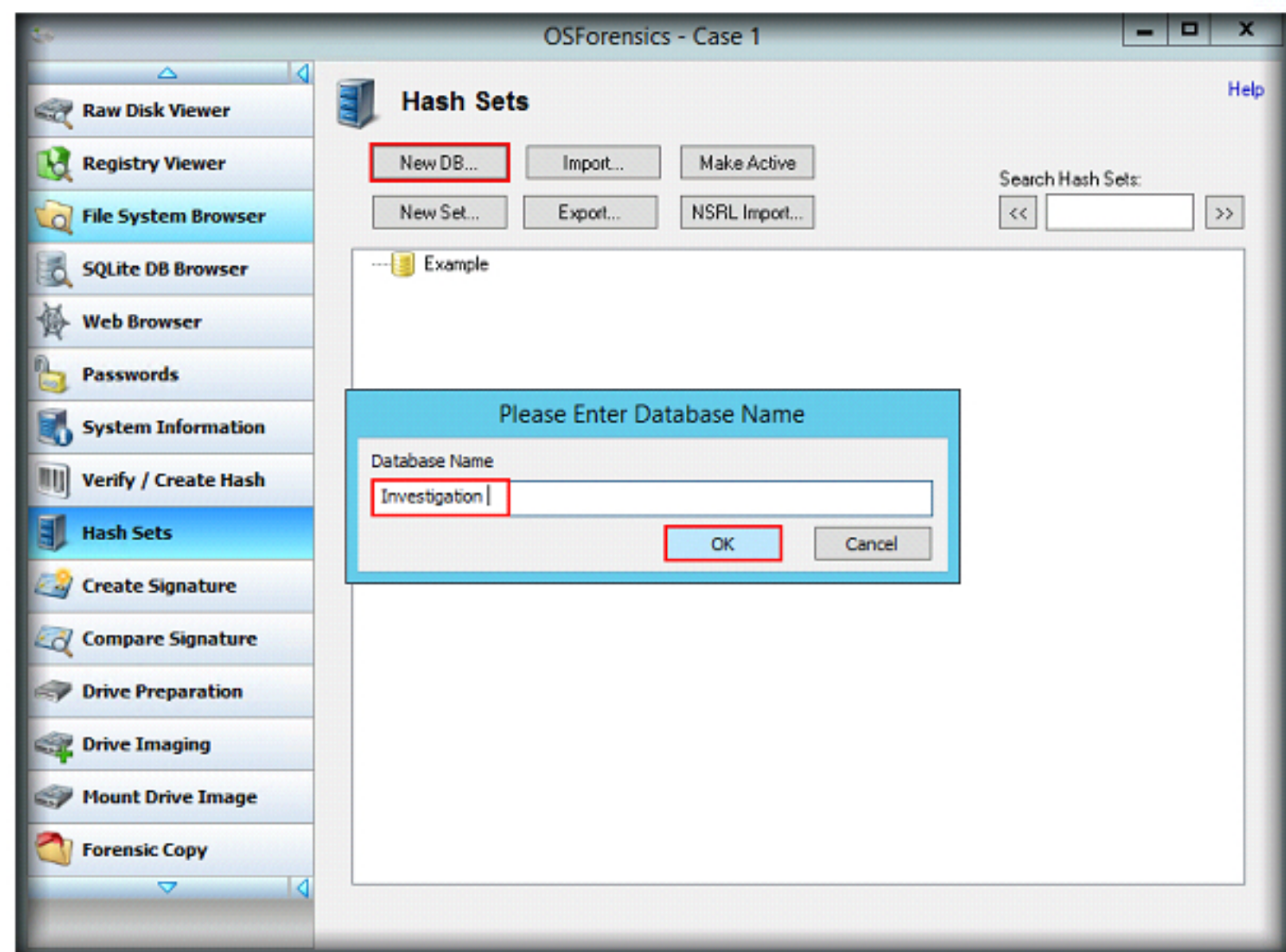


FIGURE 1.29: OSForensics Hash Sets new data base create

42. Right click on the **Investigation** database and select **Make Active** option from the context menu.

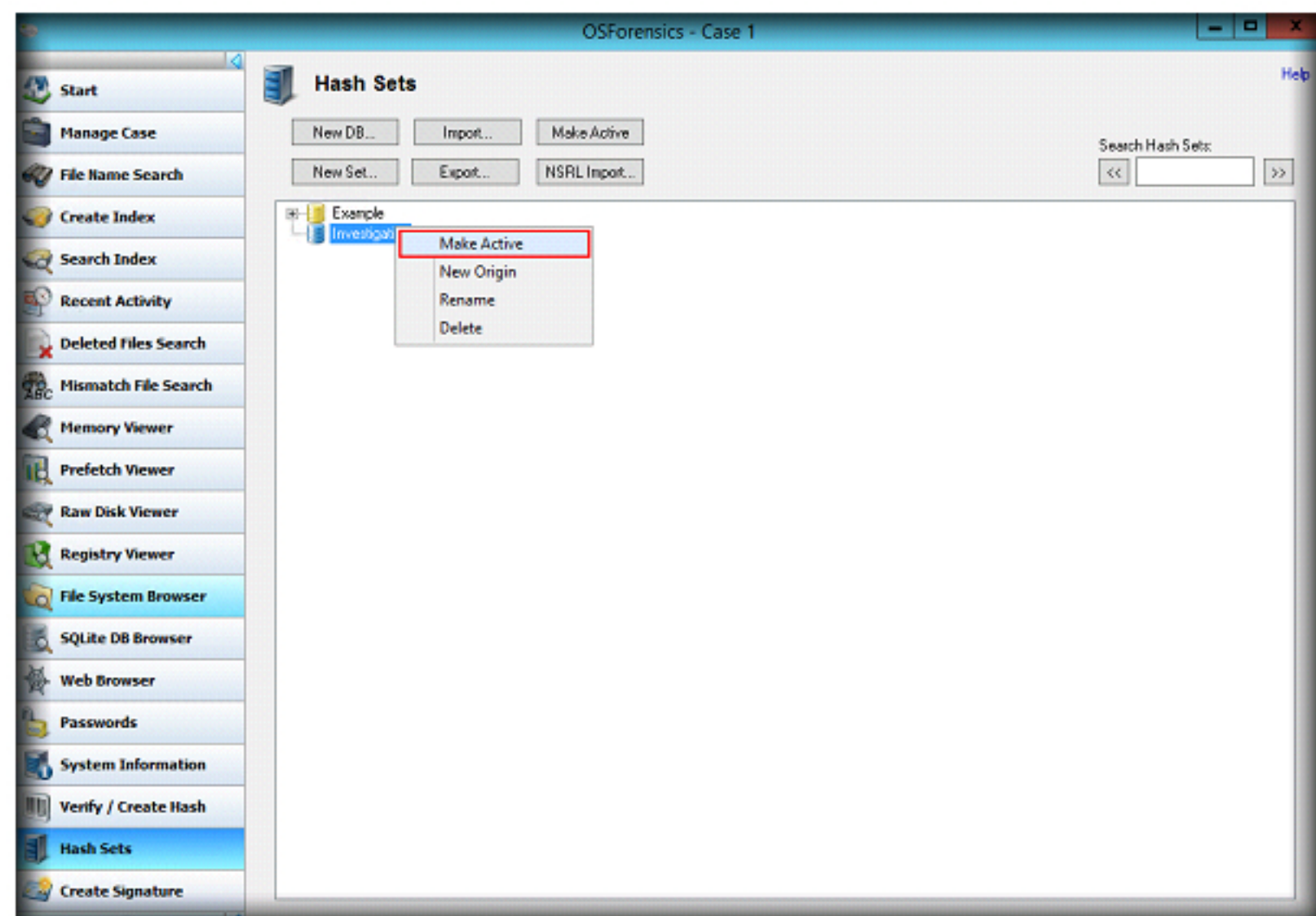


FIGURE 1.30: OSForensics Hash Sets New Hash Set

43. To generate a new hash set, click **New Set...** in the **Hash Sets** wizard, complete the required fields in the **New Hash Set** wizard, and then click **Create**.

44. To add a folder, navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image**.

 The Hash Set Viewer window allows the user to view the details about an existing hash set. This window can be accessed by double clicking on a hash set or via the right click context menu in the main Hash Sets window.

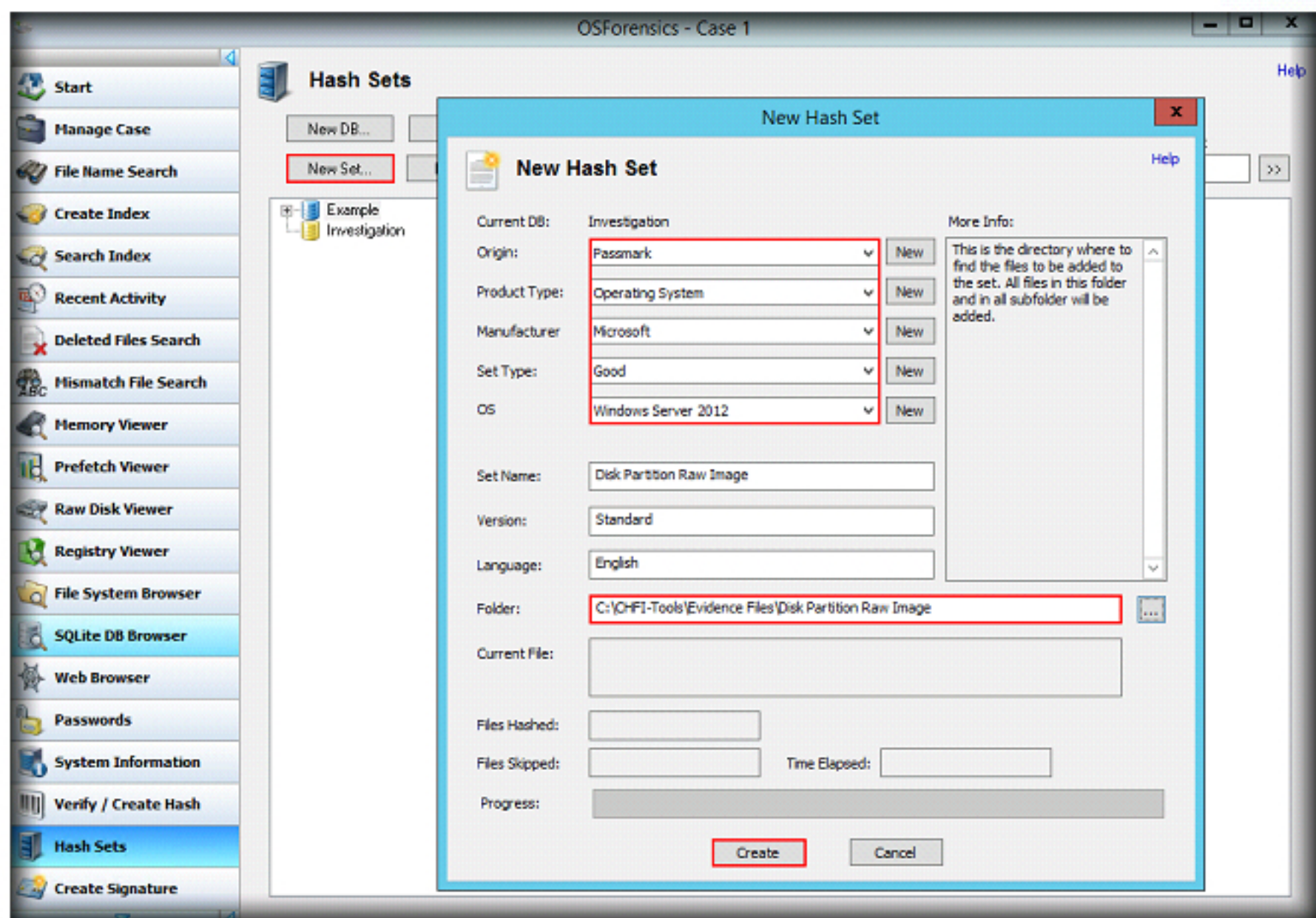


FIGURE 1.31: OSForensics Hash Sets New Hash Set

45. It takes some time to create the new hash set.
46. Double click the newly created set of hashes to view the hash value of the selected folder.

 Multi File Hash Lookup:
When hash compares multiple files, the individual matches are not shown, rather summary of how many files found a match are shown.

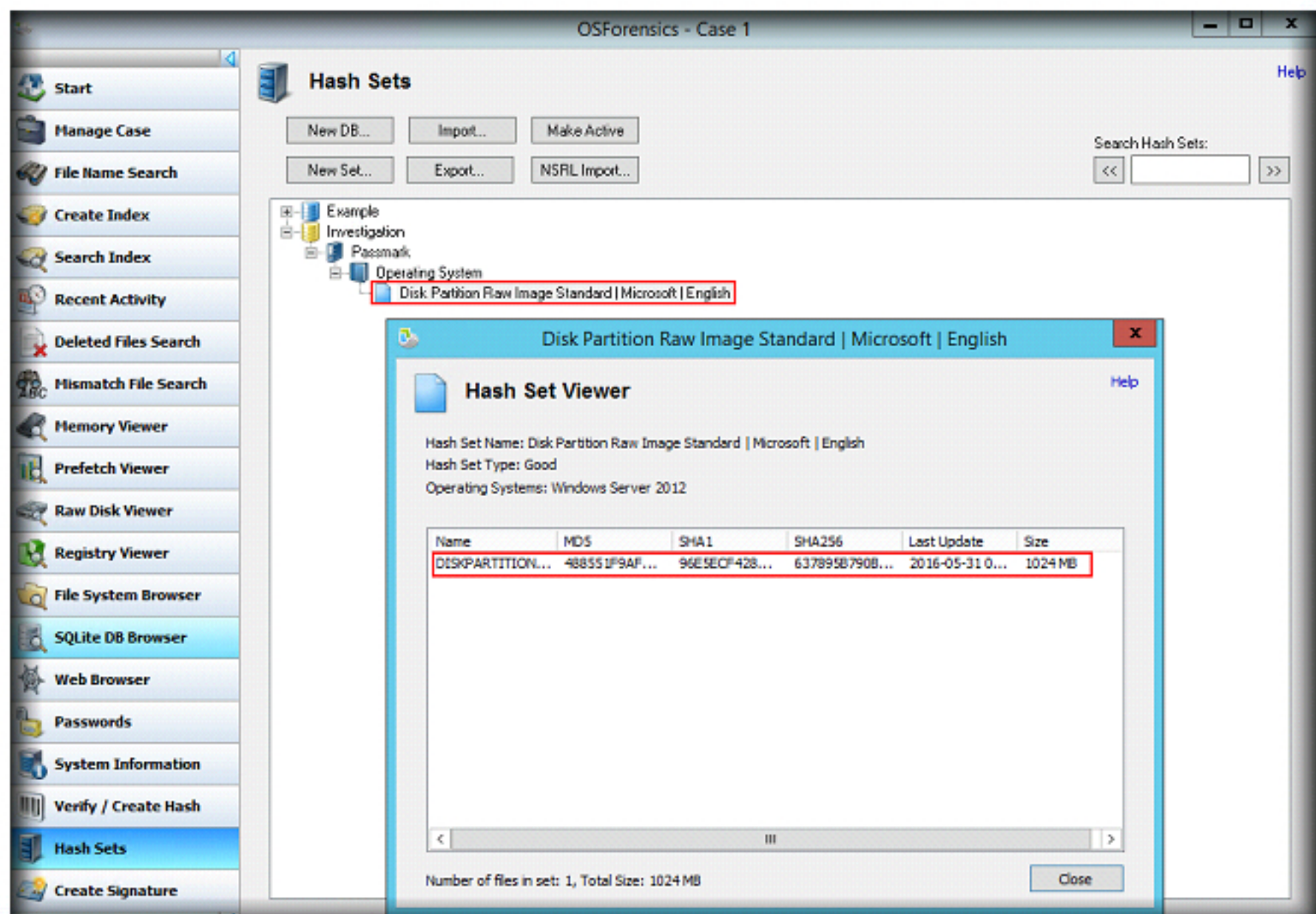


FIGURE 1.32: OSForensics Hash Set Viewer

**T A S K 1 2****Creating Drive Image**

47. To generate exact copies of partitions or whole drives on an active system, click **Drive Imaging** from the left pane.
48. Select the source volume (**E:** drive) from the drop-down list of **Source Disk**.
49. Mention the path to store the **Target Image File** by clicking the **Browse** button. Complete the respective fields, check the **Verify Image file After Completion** option, and click the **Create Image** button.

Note: It will take time to create a drive image.

It is suggested to abort the imaging process as it requires huge amount of free space.

 Drive imaging, where possible, uses the Volume Shadow Copy service built in to Windows. This allows OSF to make copies of drives that are in use without resulting in data corruption from reading files that are currently being written to.

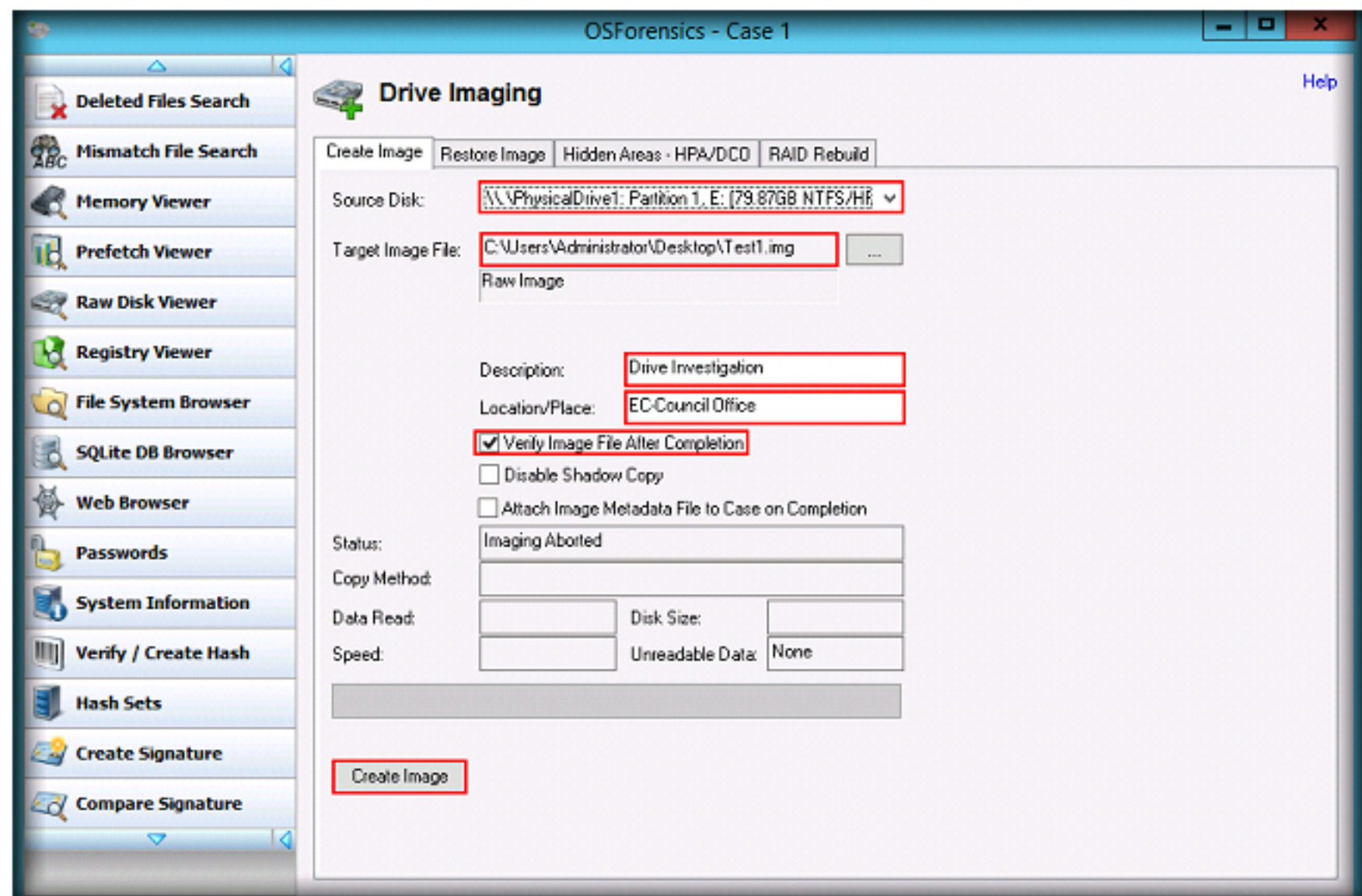


FIGURE 1.33: OSForensics Creating Drive Image

**TASK 13****Mounting Drive Image**

 This is especially important for imaging main system drives that Windows is continuously modifying. Once a shadow copy has started, a snapshot state of the drive is frozen then, so even if necessary evidence is being removed by another process in the background, it will still appear in the image OSForensics creates.

50. To mount a drive image and to view the content of that drive image, click **Mount Drive Image**.
51. **PassMark OSFMount** window appears, click **Mount New...** button and navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd** in **Image File** path. Leave the other settings to default click **OK**.

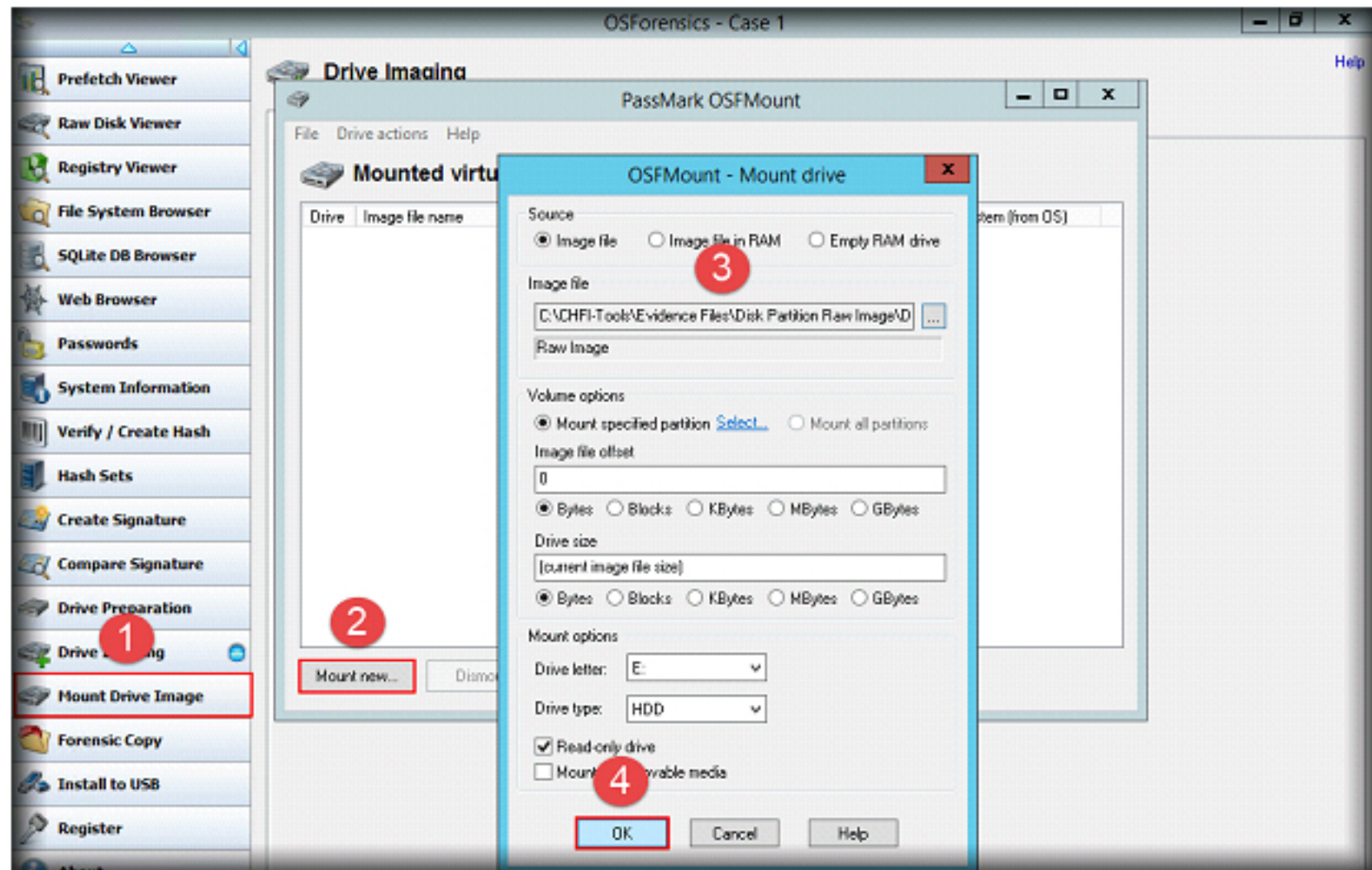


FIGURE 1.34: OSForensics Mounting Drive Image

**TASK 14****Creating a Forensic Copy**

 The log, in addition to general status messages, will also output error messages about any files that failed to copy. The most common reason for failure is that another process locks them or the current user does not have permission to access them.

52. To view the mounted drive, click **E:**.
53. To copy the contents of one directory to another while maintaining the same timestamps as the original, click **Forensic Copy**.
54. Mention the **Source Directory** and **Destination Directory** by clicking the **Ellipsis** button and then, click **Start**.
55. For **Source Directory** navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image** and for **Destination Directory**, create a folder named **Test Files** on Desktop and navigate to it.

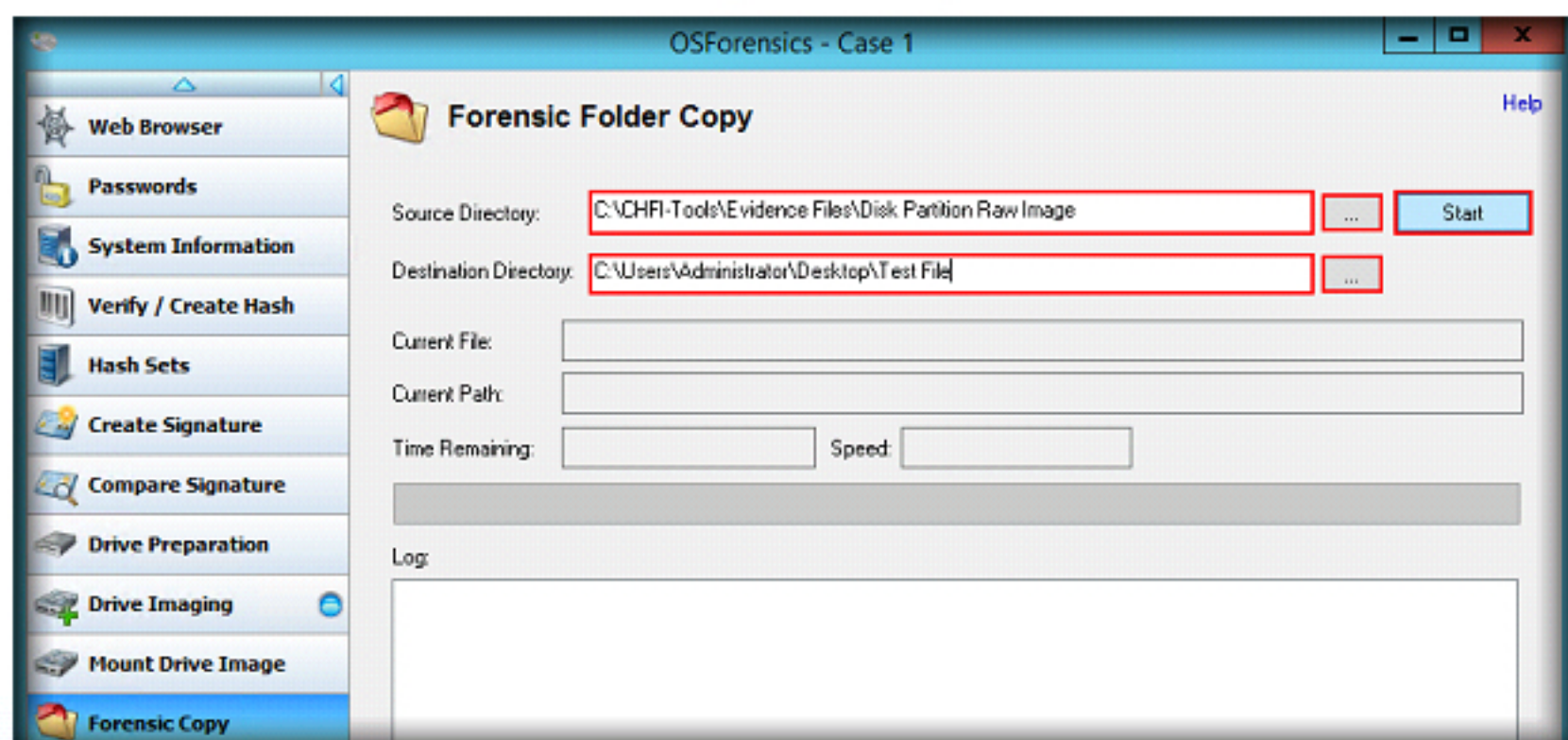


FIGURE 1.35: OSForensics Creating Forensic Copy

56. A forensic copy has been created in the following path, with the results in the bottom pane of the window.

OSFClone is a free, self-booting solution that enables you to create or clone exact raw disk images quickly and independently of the installed OS. After creating or cloning a disk image, you can mount the image with PassMark OSFMount before conducting analysis with PassMark OSForensics.

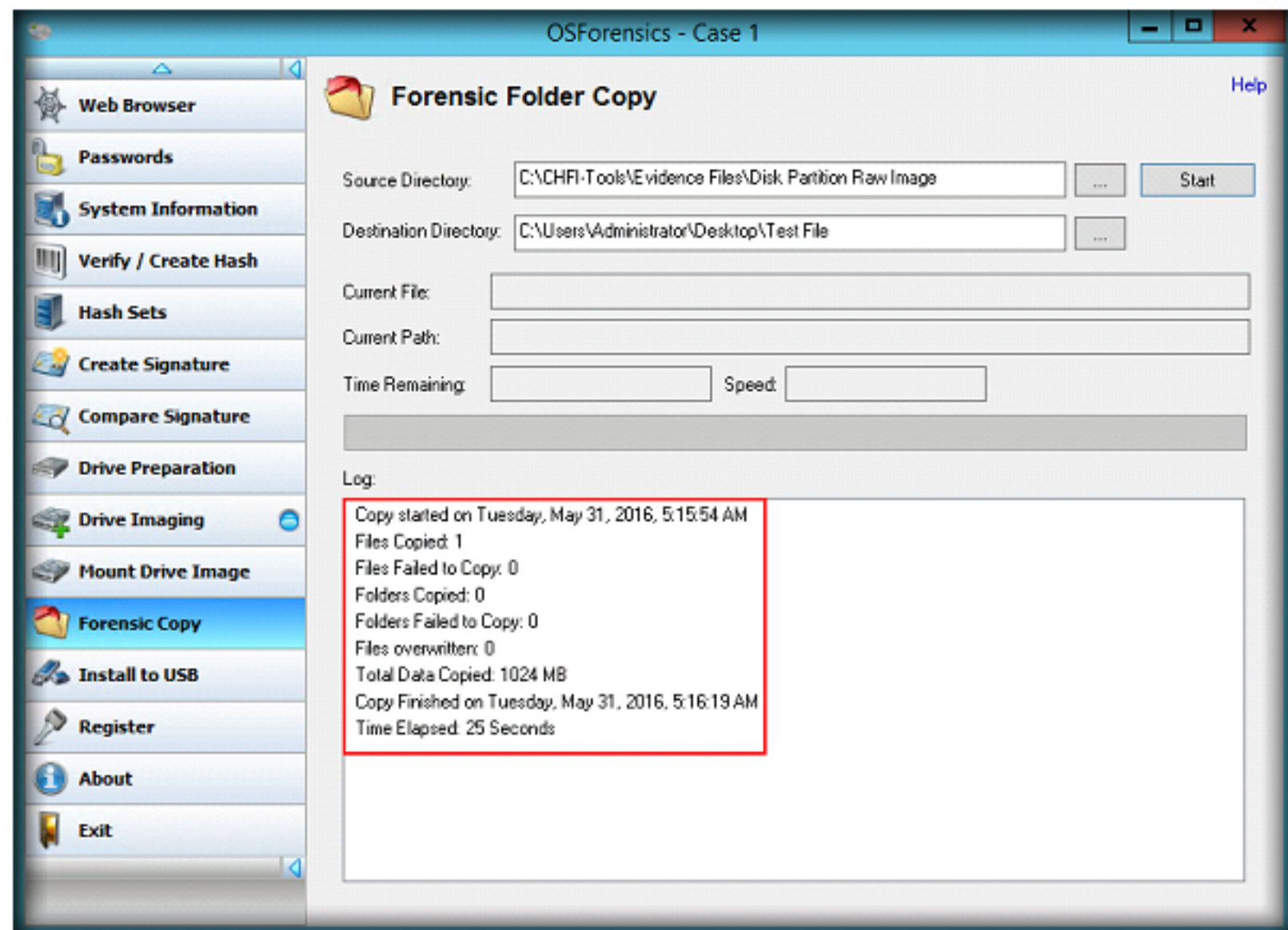


FIGURE 1.36 OSForensics Creating Forensic Copy Result

Lab Analysis

Document the complete results of this lab.

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

Internet Connection Required

☐ Yes

☒ No

Platform Supported

☒ Classroom

☒ iLabs

Extracting Information about Loaded Processes Using Process Explorer

Process Explorer shows you information about which handles and DLL processes have opened or loaded.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

Processes are the instances of computer programs running on a system and contain the code required activity. Any program or malware will have various methods that will combine to give the result. An investigator should know the default processes to separate the suspicious ones. To be an expert computer forensics investigator, you must understand how to extract information about loaded processes on the victim computer.

Lab Objectives

The purpose of this lab is to help students learn how to investigate loaded processes. In this lab, you will learn how to use Process Explorer.

Lab Environment

This lab requires:

- Process Explorer, which is located at **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Process Explorer**.
- You can also download the latest version of **Process Explorer** from **<https://technet.microsoft.com/en-us/sysinternals/processexplorer.aspx>**.
- If you decide to download the latest version, then the screenshots shown in this lab might differ slightly.
- A computer running **Windows Server 2012**.

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

- Administrative privileges to install and run tools.

Lab Duration

Time: 15 Minutes

Overview of Extracting Information about Loaded Processes Using Process Explorer

 You can also download the latest version of Process Explorer from the link <http://technet.microsoft.com/en-us/sysinternals/bb896653>

The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owner accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in. If it is in handle mode, you'll see the handles opened by the process selected in the top window. If Process Explorer is in DLL mode, you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

Lab Tasks



TASK 1

Viewing System Information

- Navigate to **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Process Explorer**.
- Double-click the **procexp.exe** file, and accept the license agreement, if you are running this tool on your system for the first time.

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

- Process Explorer GUI appears, displaying the details of all the processes running on the machine, as shown in the screenshot:

 Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

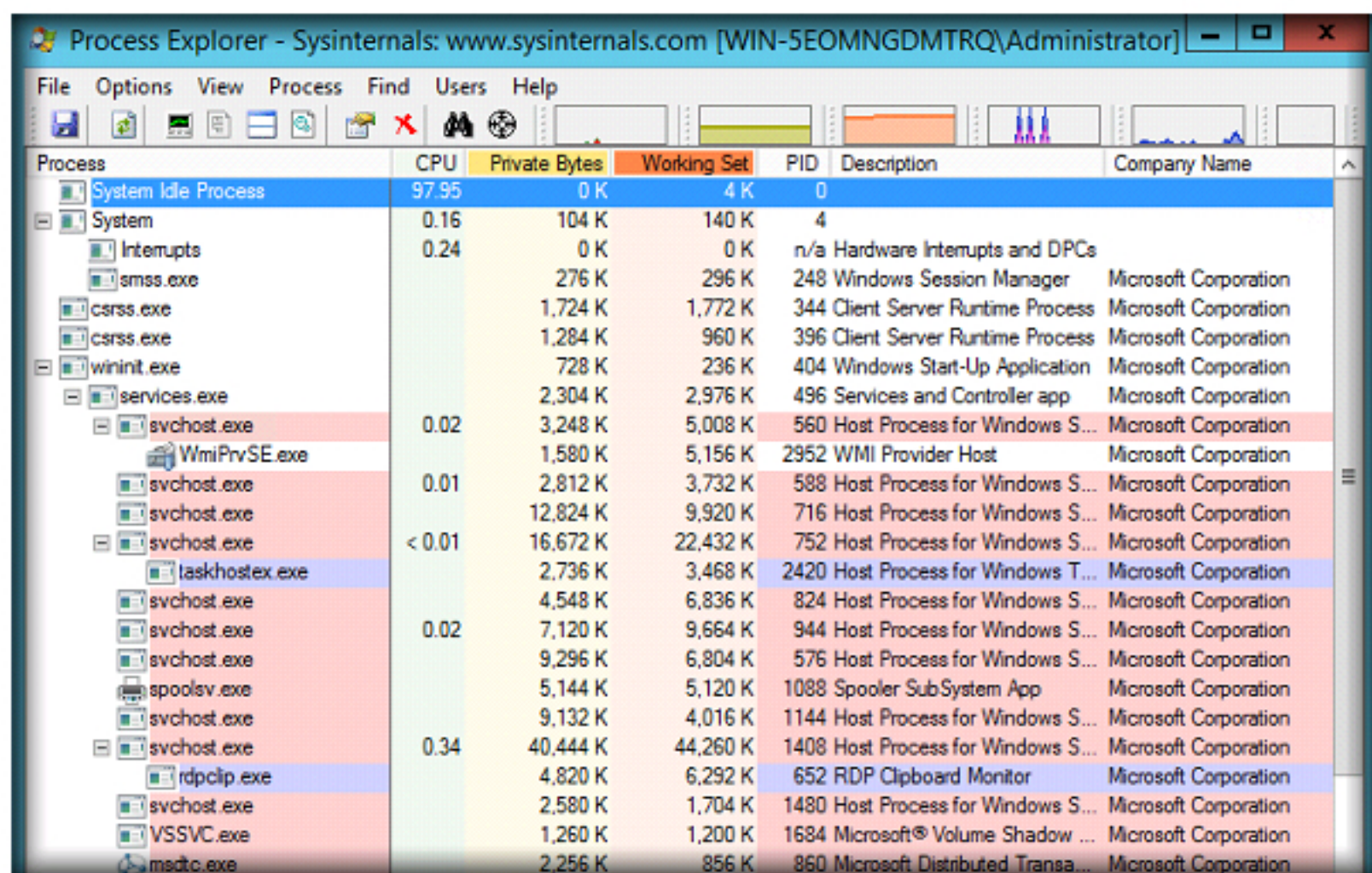


FIGURE 2.1: Process Explorer Main Screen

4. Process Explorer lists all the running processes in the left pane, and details of each process (such as CPU usage, PID, etc.) in the right pane.

The unique capabilities of Process Explorer make it useful for tracking down DLL-version problems or handle leaks, and it provides insight into the way Windows and applications work.

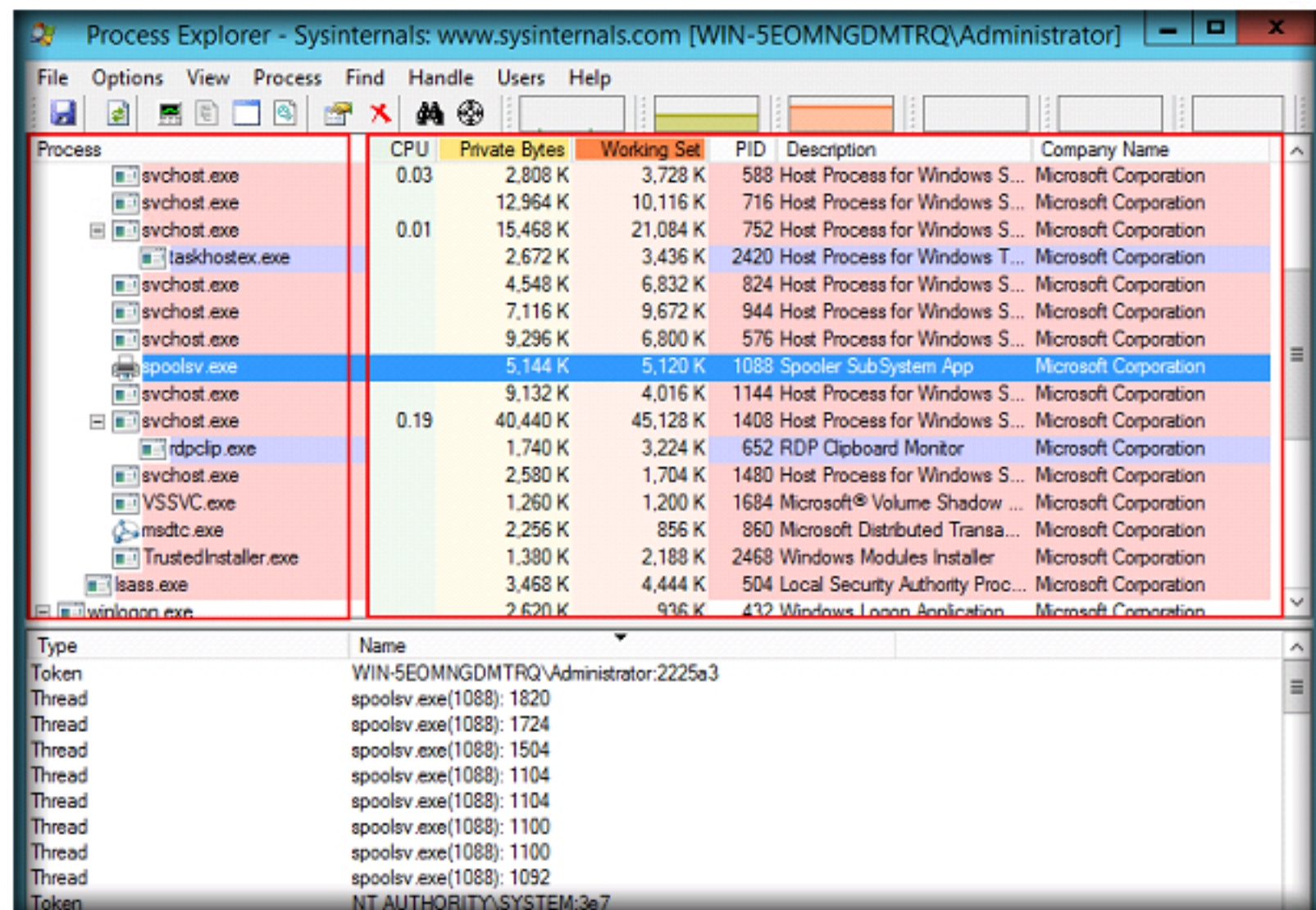


FIGURE 2.2: Process Explorer Processes Details

5. To view system information, go to **View** from **Menu** bar and click **System Information...** or click the **System Information** icon  on the toolbar.

The Process Explorer window illustrates two panes by default: the upper pane is always a process list and the bottom either shows the list of DLLs loaded into the process selected in the top pane, or the list of operating system resource handles (files, Registry keys, synchronization objects) the process has open. The view mode determines which information is shown in the bottom pane.

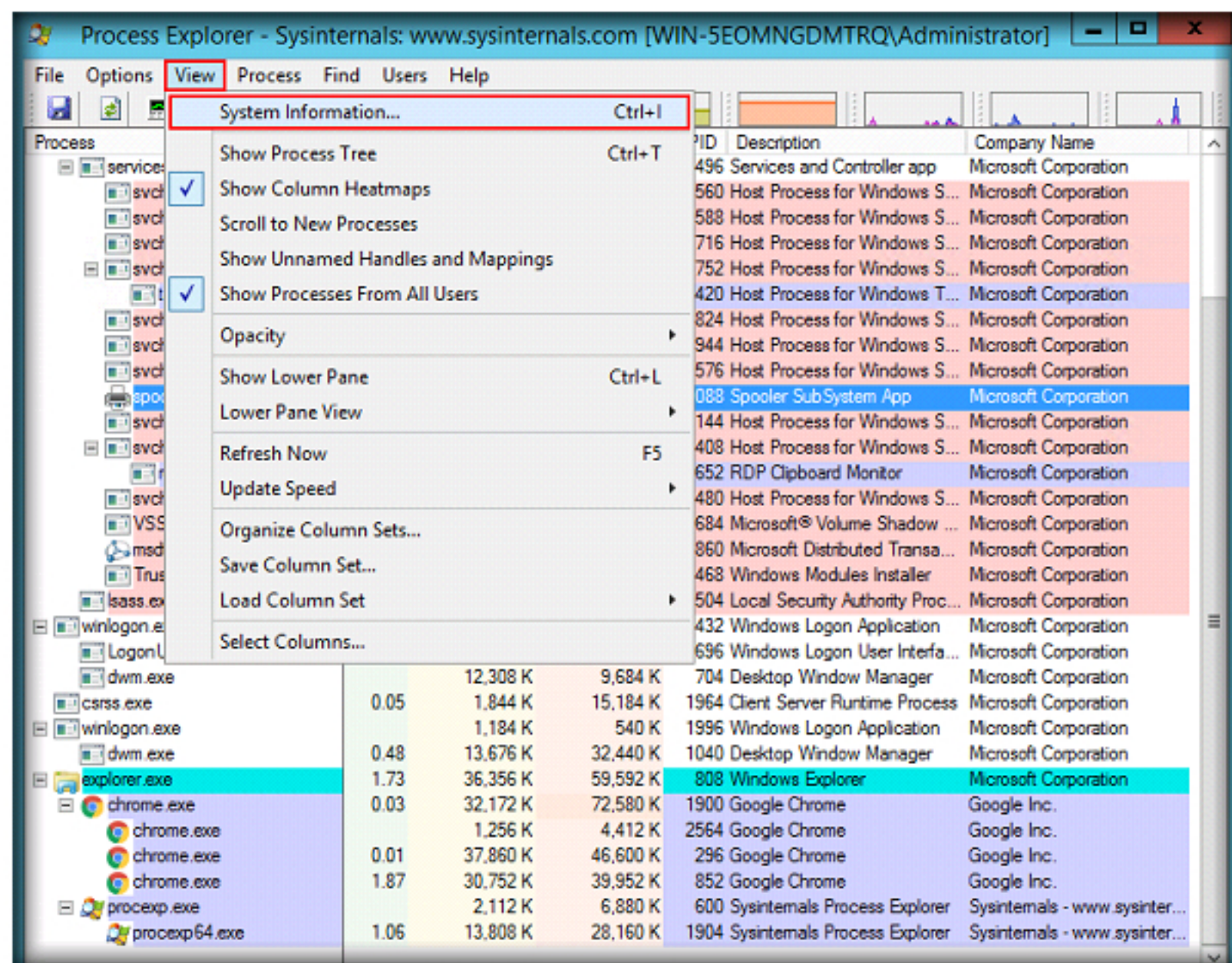


FIGURE 2.3: Process Explorer View menu system information

6. The **System Information** wizard displays global system performance metrics as shown in the **Task Manager** in a **Graphical** view.

Malware, including viruses, spyware, and adware, is often stored in a packed encrypted form on disk to attempt to hide the code it contains from antispysware and antivirus programs. Process Explorer uses a heuristic to determine if an image is packed. If it is, Process Explorer changes the text above the full path display field to include the message "(Image is probably packed)."

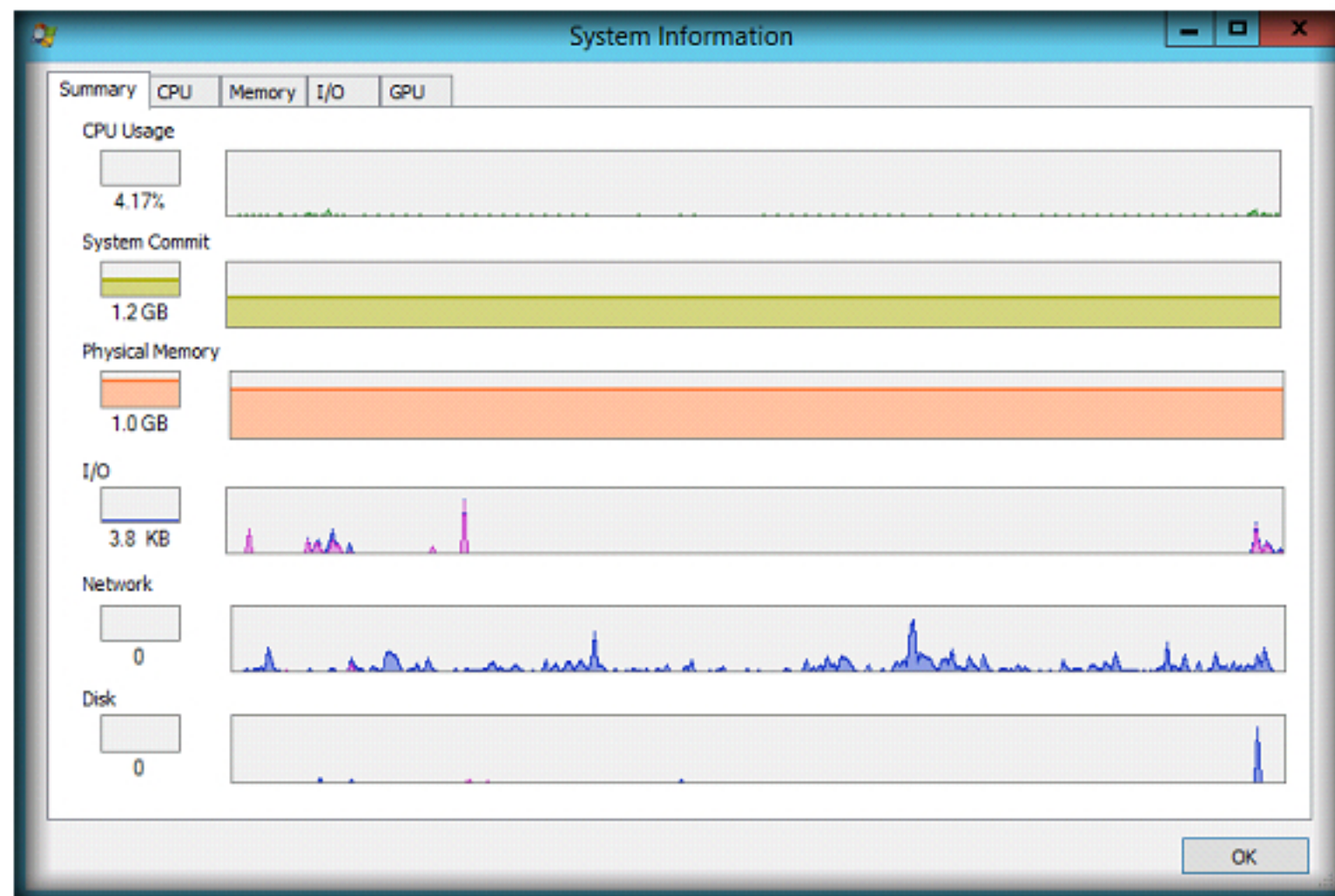


FIGURE 2.4: Process Explorer System Information-Global system performance metrics

7. Click **OK** to close the **System Information** wizard.
8. To view the DLLs, select a required process and click the **View DLLs** icon  from the toolbar, or navigate to **View → Lower Pane View → DLLs** on the **Menu** bar.

TASK 2

Viewing DLLs

Mini Graphs:
Process Explorer includes a toolbar and mini graphs for CPU, memory, and if on Windows 2000 or higher, I/O history, at the top of the main window. They can be resized with respect to one another or dragged such that each is on a separate row. The mini-graphs show a history of system activity, and moving the cursor over a point on a graph displays a tooltip containing the associated time and process information for a point in time. For example, the tooltip for the mini-CPU graph shows the process that was the largest consumer of CPU. Clicking on any of the mini-graphs opens the **System Information** dialog box.

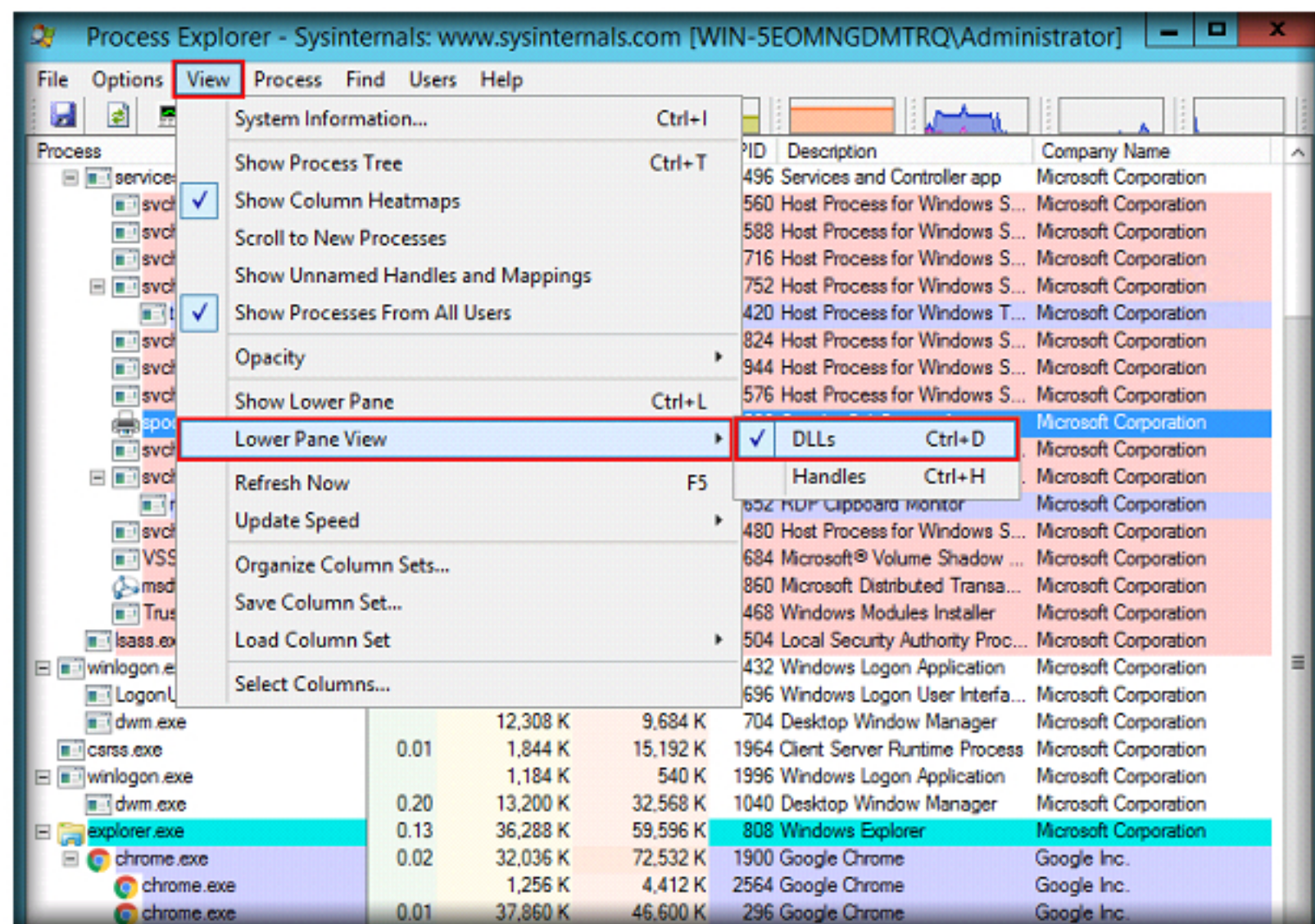


FIGURE 2.5: Process Explorer DLLs view

9. Select a process. You can view the list of DLLs for the selected process in the bottom pane of the window.

 **Highlight Relocated DLLs:**
When you select the Relocated DLLs entry in the **Options | Configure Highlighting** dialog box, any DLLs that are not loaded at their programmed base address are show in yellow. DLLs that cannot load at their base address because other files are already mapped there are relocated by the loader, which consumes CPU and makes parts of the DLL, that are modified as part of the relocation, un-sharable.

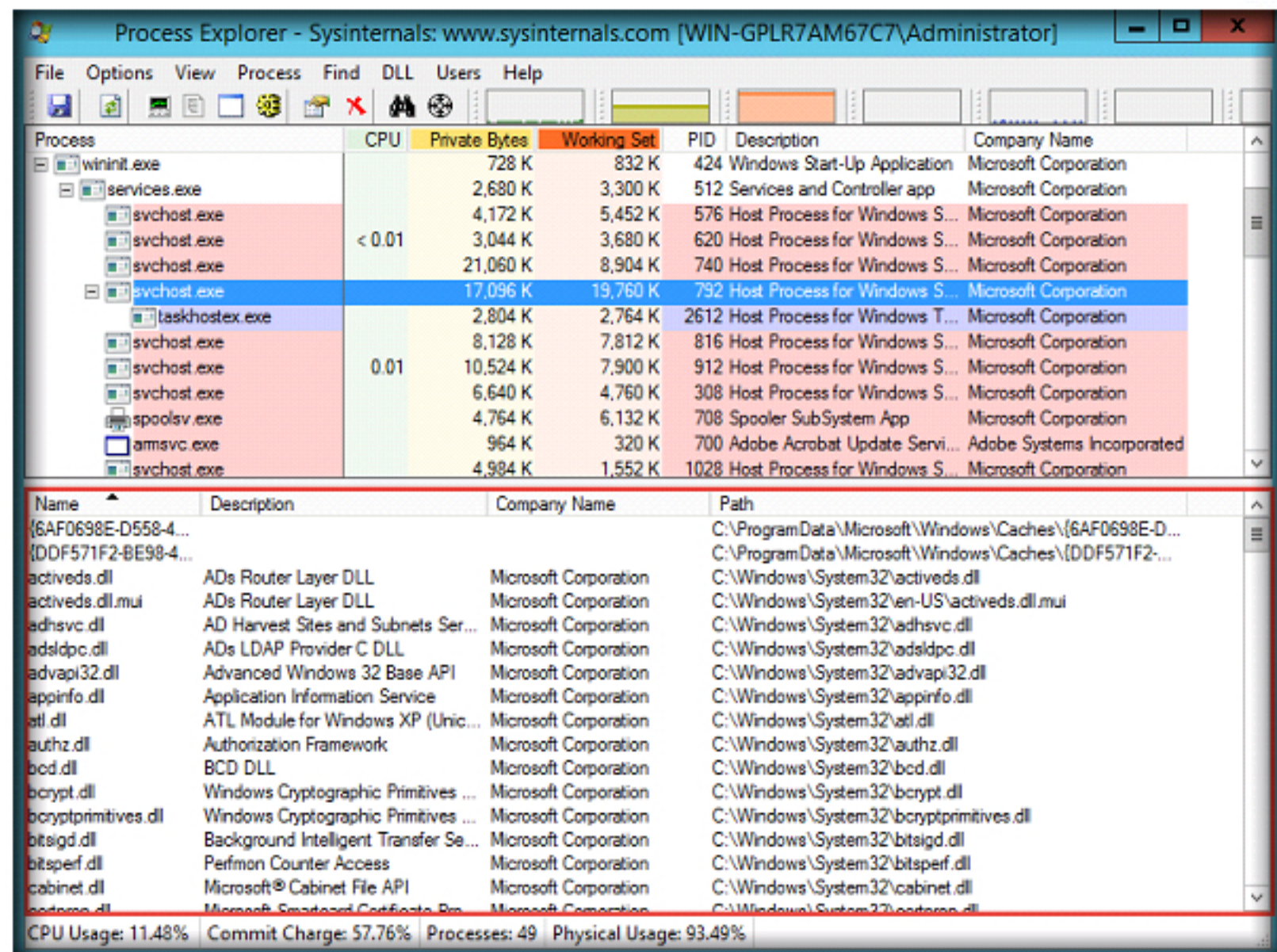


FIGURE 2.6: Process Explorer DLLs view

10. To view DLL properties, select a dll, choose **DLL → Properties** from the **Menu** bar, or right-click on the required DLL from the DLL list displayed for a particular process, and select **Properties....**

 On systems that include Terminal Services, Process Explorer displays a **User's** menu that lists the currently connected sessions. Process Explorer creates a menu entry for each session with a name that includes the session ID and the user logged into the session.

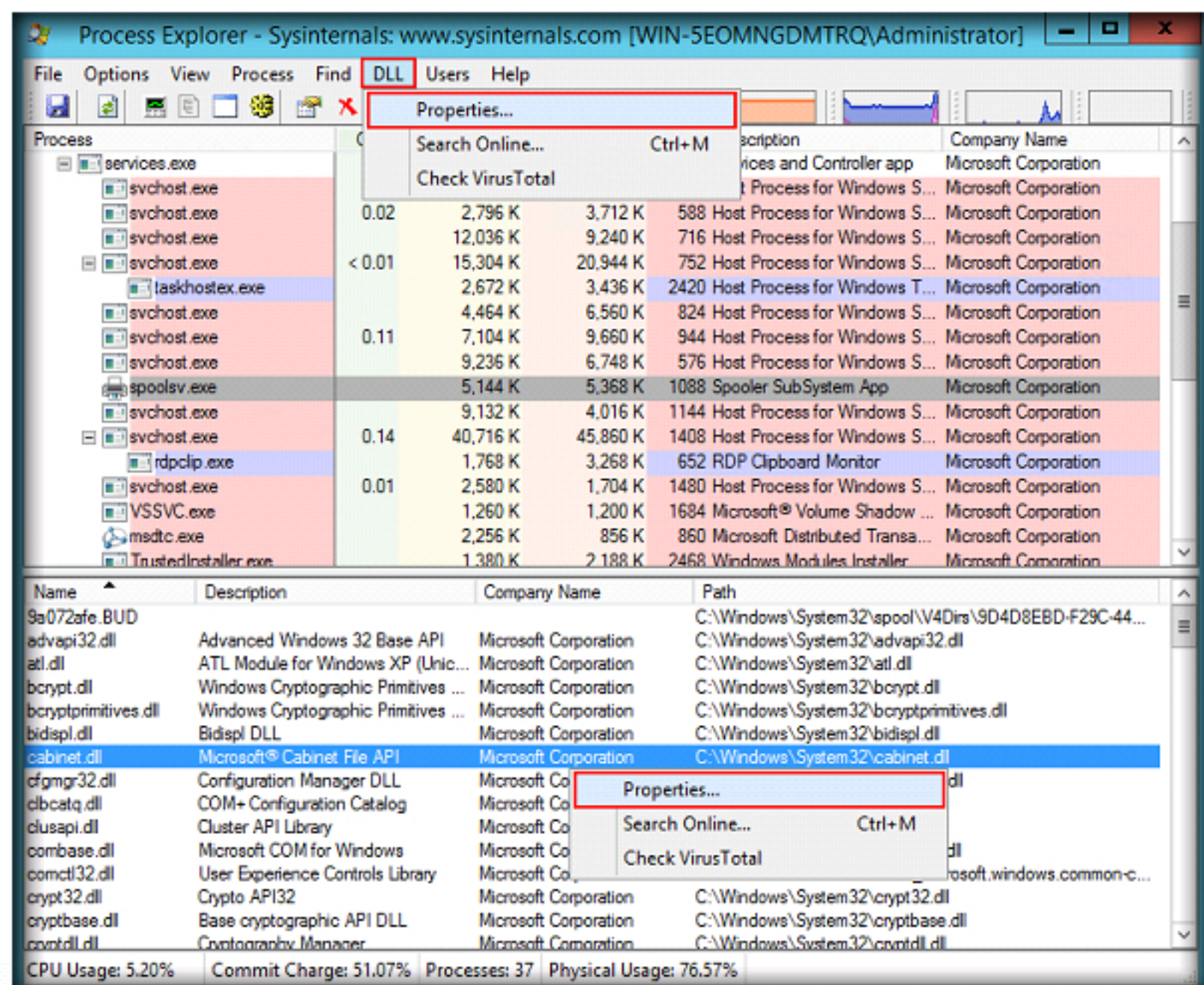


FIGURE 2.7: Process Explorer DLLs Properties view

11. This displays the DLL properties in the **Image** and **Strings** tabs.



Show Unnamed

Handles:

By default, Process Explorer shows only handles to objects that have names. Select the **Show Unnamed Handles** item under the **View** menu to have Process Explorer list all the handles opened by a selected process, even those to objects that are nameless. Note that Process Explorer consumes significantly more CPU resources when this option is selected.

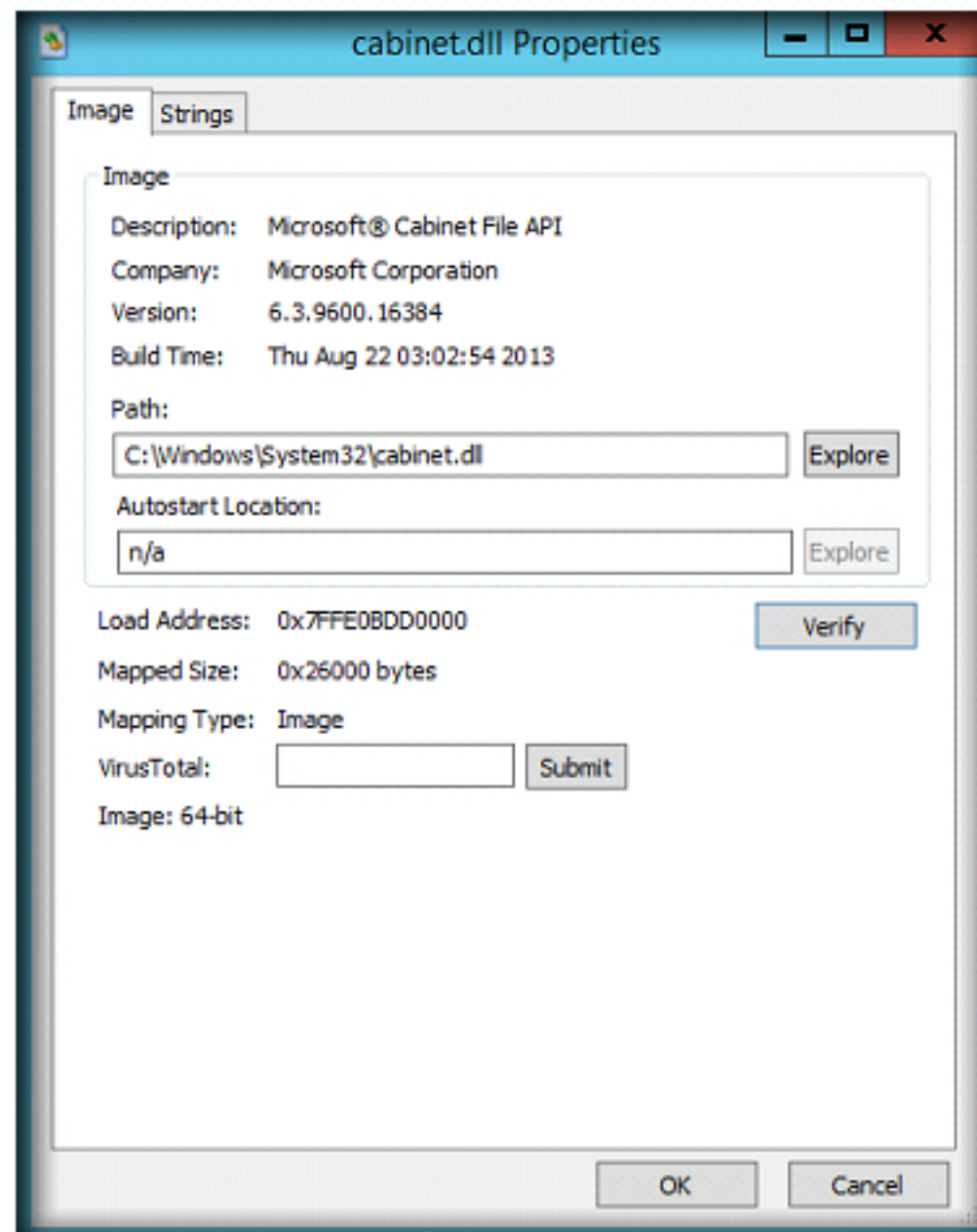


FIGURE 2.8: Process Explorer DLLs Properties wizard

12. The **Image** tab contains details of the DLL such as Company name, Version, path of the DLL, etc.
13. Click **Verify** button to check for signature of a process.

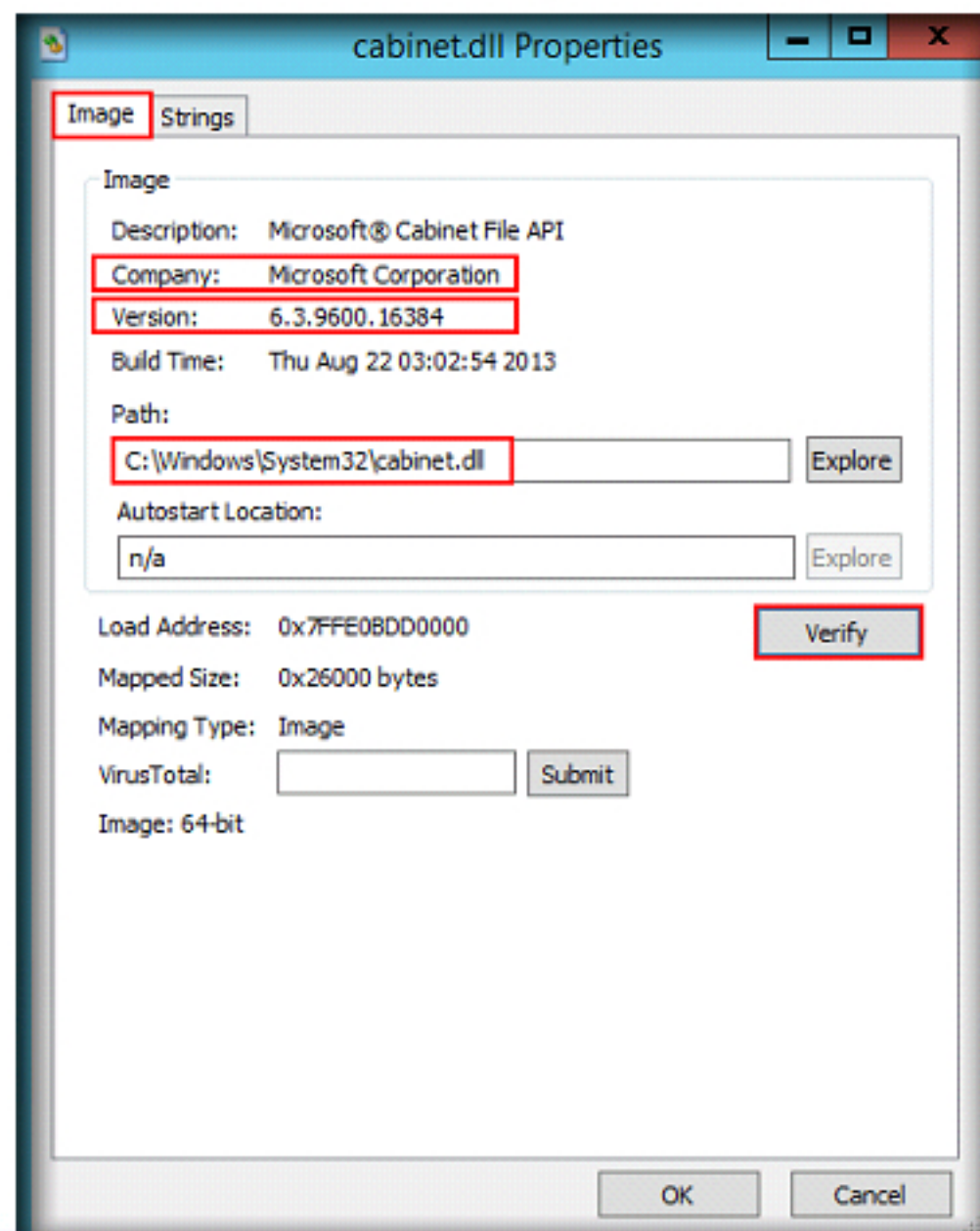


FIGURE 2.9: Process Explorer DLLs Image tab

14. Once you click the **Verify**, if the company's name appears to be **Microsoft Windows**, then the process is said to be legitimate, as shown in the screenshot:

 You can also download the latest version of Process Explorer from the link

<http://technet.microsoft.com/en-us/sysinternals/bb896653>

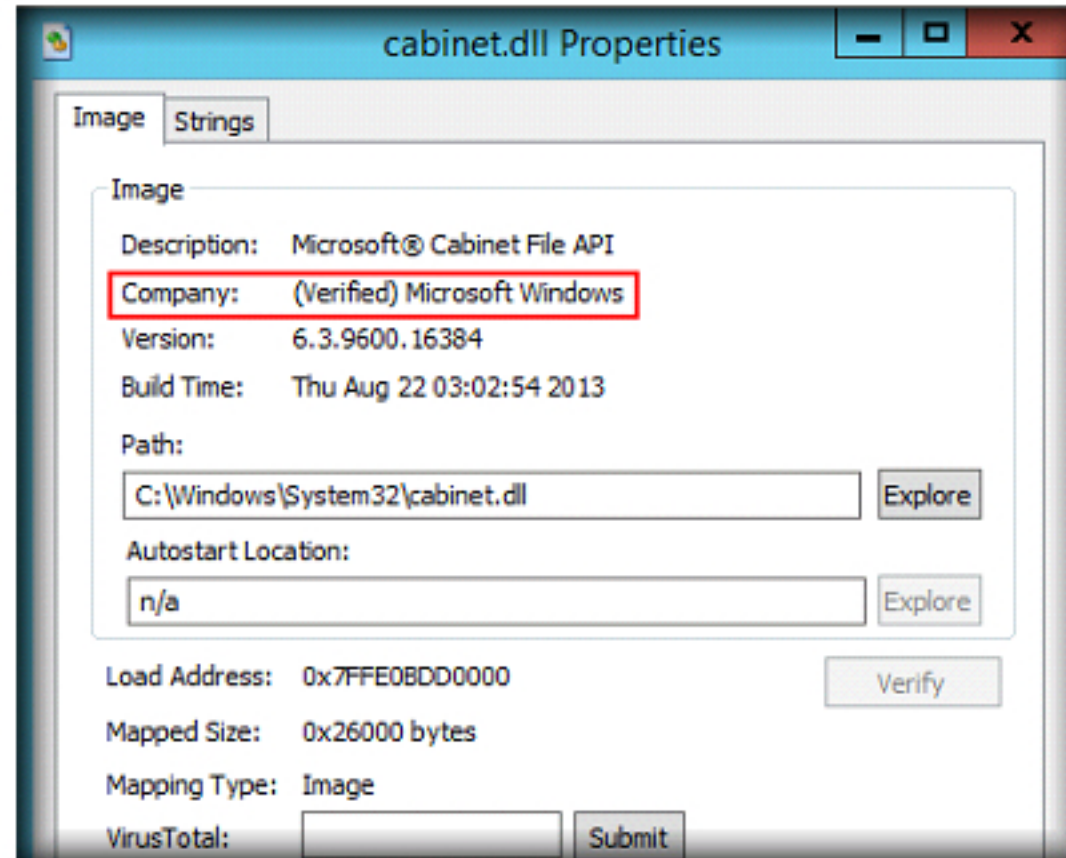


FIGURE 2.10: Process Explorer DLLs Image Signature Verified

15. Click the **Strings** tab. The Strings tab lists any Unicode strings found in the selected process. Examining this tab helps you to find if the process is associated with any malware.
16. When the **Strings** tab is clicked, we have two options for viewing the image and memory strings. Click either the **Image** or **Memory** radio button at the bottom of the window to view either image or memory strings respectively.

 By default, Process Explorer sorts processes into the system process tree. The process tree reflects the parent-child relationship between processes where child processes are shown directly beneath their parent and right-indented. Processes that are left-justified are orphans; their parents have exited. To change the sort order, simply click on the column by which you wish to sort. To return the sort to the process tree, choose **View→Show Process Tree**, click the **Process Tree** toolbar button or press **Ctrl+T**.

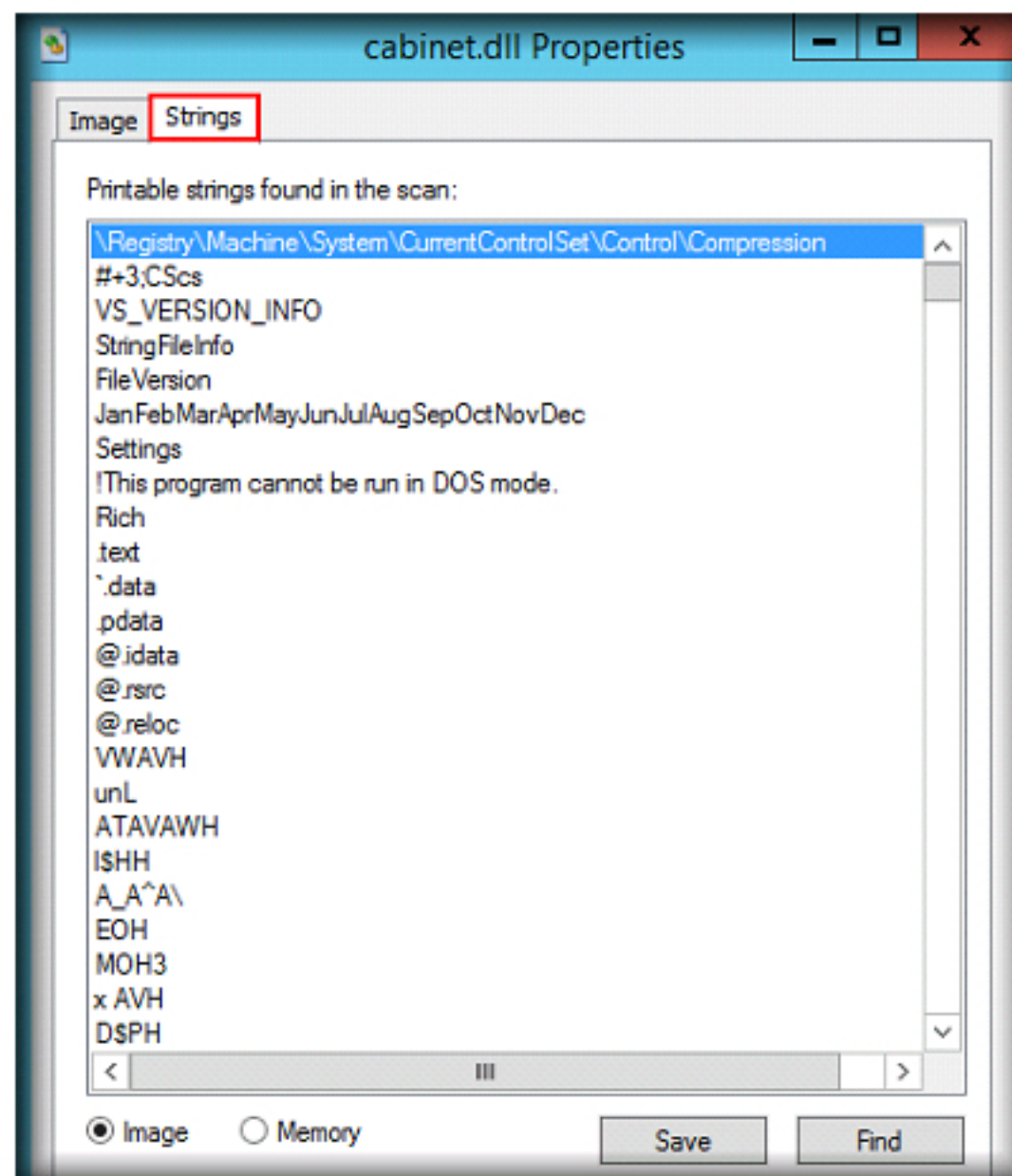


FIGURE 2.11: Process Explorer DLLs Strings

17. You can also save the Image or/and Memory strings in text file format. In this lab, we are saving the Image strings. To save, select Image radio button, and click **Save**.
18. **Save Process Explorer Strings** window appears, specify a location (here, **Desktop**) to save the file, enter a file name (**cabinet.dll.txt**) and click **Save**.

On Windows NT-based systems, Process Explorer shows two artificial processes: Interrupts and DPCs. These processes reflect the amount of time the system spends servicing hardware interrupts and Deferred Procedure Calls (DPCs), respectively. High CPU consumption by these activities can indicate a hardware problem or device driver bug. To see the total number of interrupts and DPCs executed since the system booted, add the **Context Switch** column. Another sometimes useful metric is the number of interrupts and DPCs generated per refresh interval, which you see when you add the **CSwitches Delta** column.

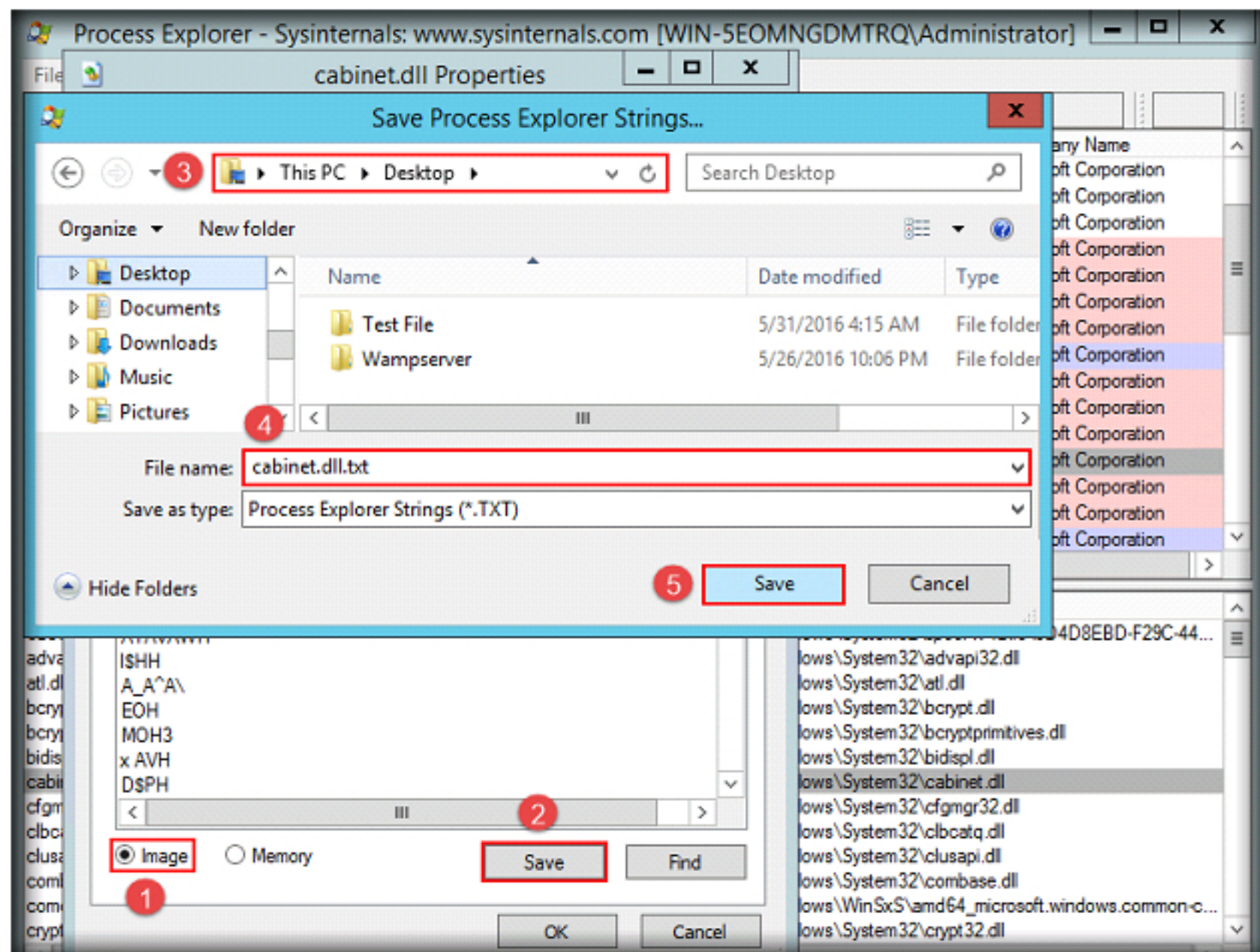


FIGURE 2.12: Process Explorer DLLs saving strings

19. On saving the file, click **OK** in the DLL's **Properties** window to close it.
20. The **Search Online** option searches the selected DLL on the Internet by launching an **Internet Browser**.
21. To search online, choose a DLL, and select **DLL → Search Online** from the **Menu** bar.

Find Windows Process:
You can highlight the process that owns a window visible on the desktop by dragging the target-like toolbar button over the window in question. Process Explorer will select the owning process entry in the process view.

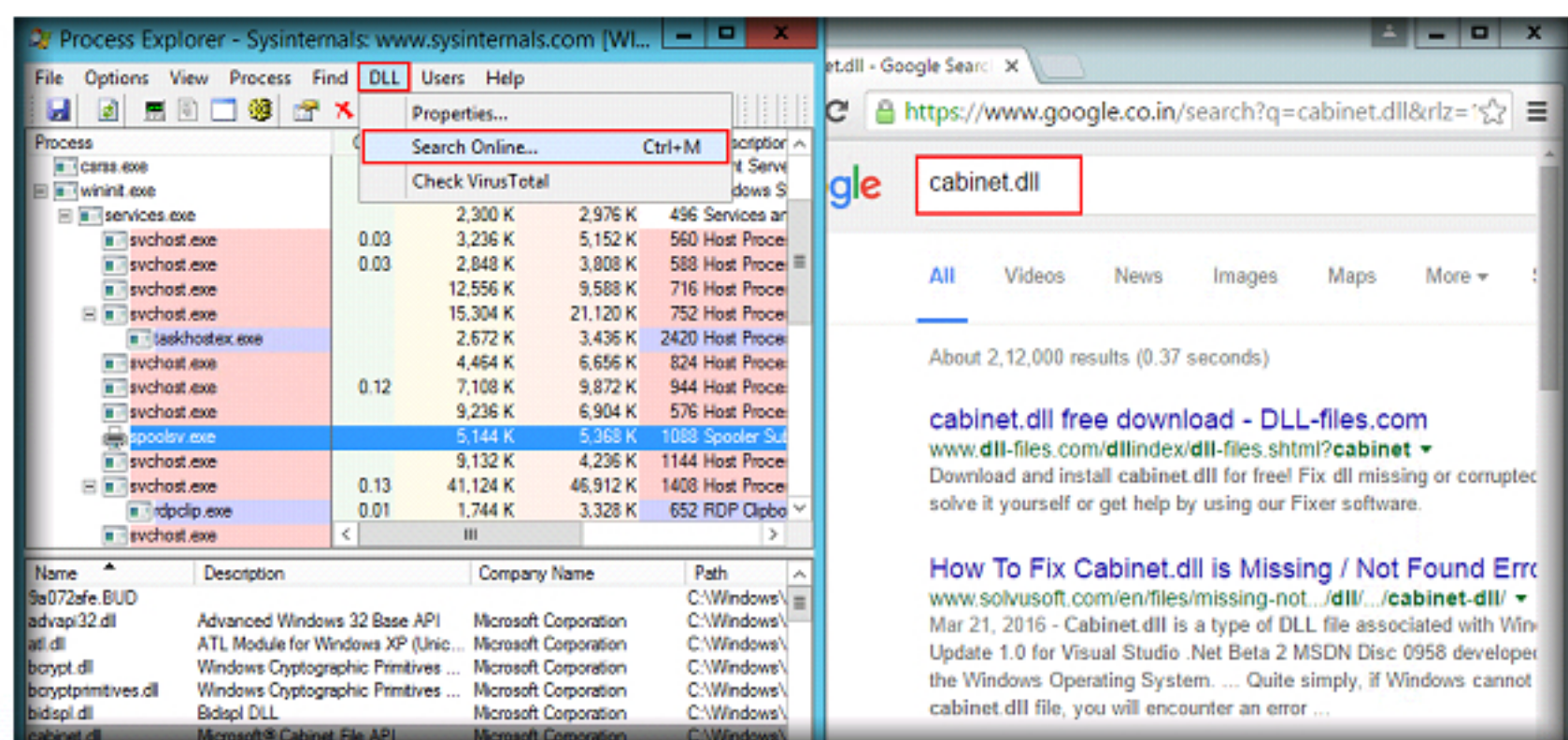


FIGURE 2.13: Process Explorer DLLs searching online

22. To view the handles of a particular process, select the process and choose **View → Lower Pane View → Handles** from the **Menu** bar.

 **Highlight Services:** on Windows NT and higher, this option has Process Explorer show processes that are running Win32 services in the service process highlight color. The **Services** tab of the **Process Properties** dialog box shows the list of services running within a process.

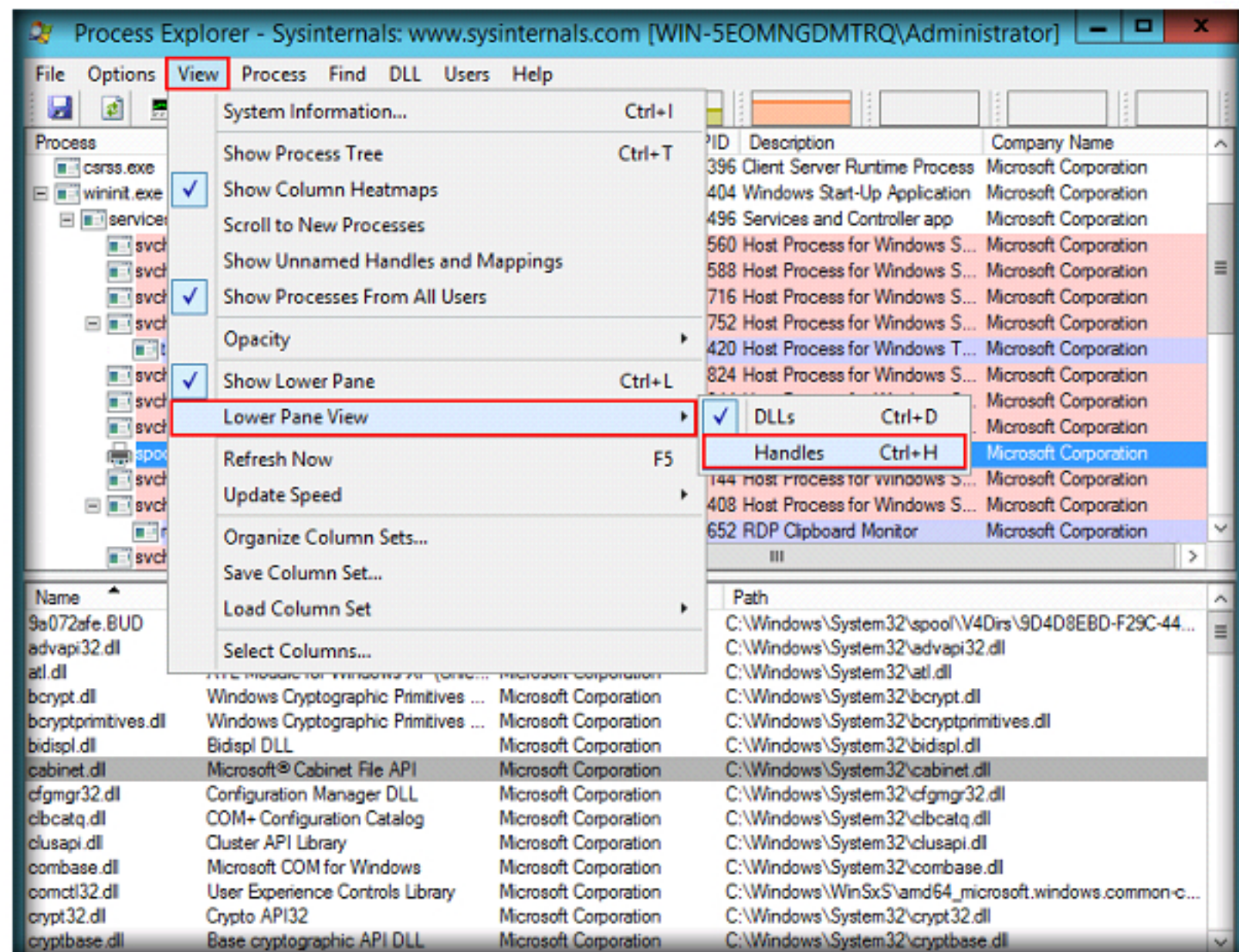


FIGURE 2.14: Process Explorer to view handles

23. To close handles running in the process, right-click the handle to be closed and click **Close Handle**, or select a handle and then, choose **Handle → Close Handle** from the **Menu** bar.

 **Highlight Jobs:** On Windows 2000 and higher choose this option to have Process Explorer show processes that are part of a Win32 Job in the **Job** object highlight color. Jobs group processes together so that they can be managed as a single item and are used by the **Runas** command, for example. Use the **Job** tab of the **Process Properties** dialog box to see the list of processes running in the same job as the selected process and to see job limits that have been applied to the job.

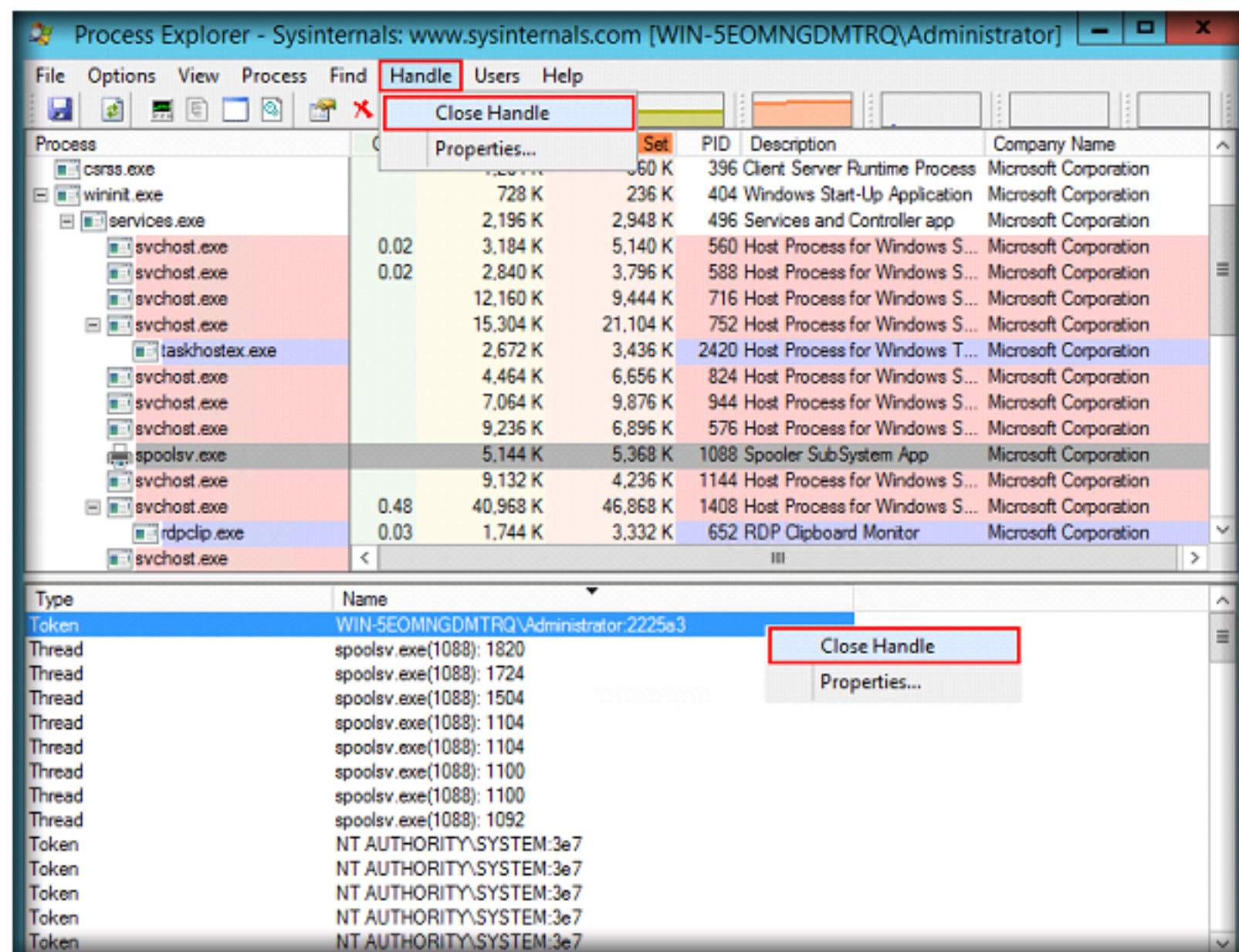


FIGURE 2.15: Process Explorer to close handles

24. A **Process Explorer Warning** dialog-box appears; if you are sure you want to close the handle, click **Yes**. It then closes the selected handle.

 Highlight Packed Images: Malware, including viruses, spyware, and adware is often stored in a packed encrypted form on disk in order to attempt to hide the code it contains from antispysware and antivirus.

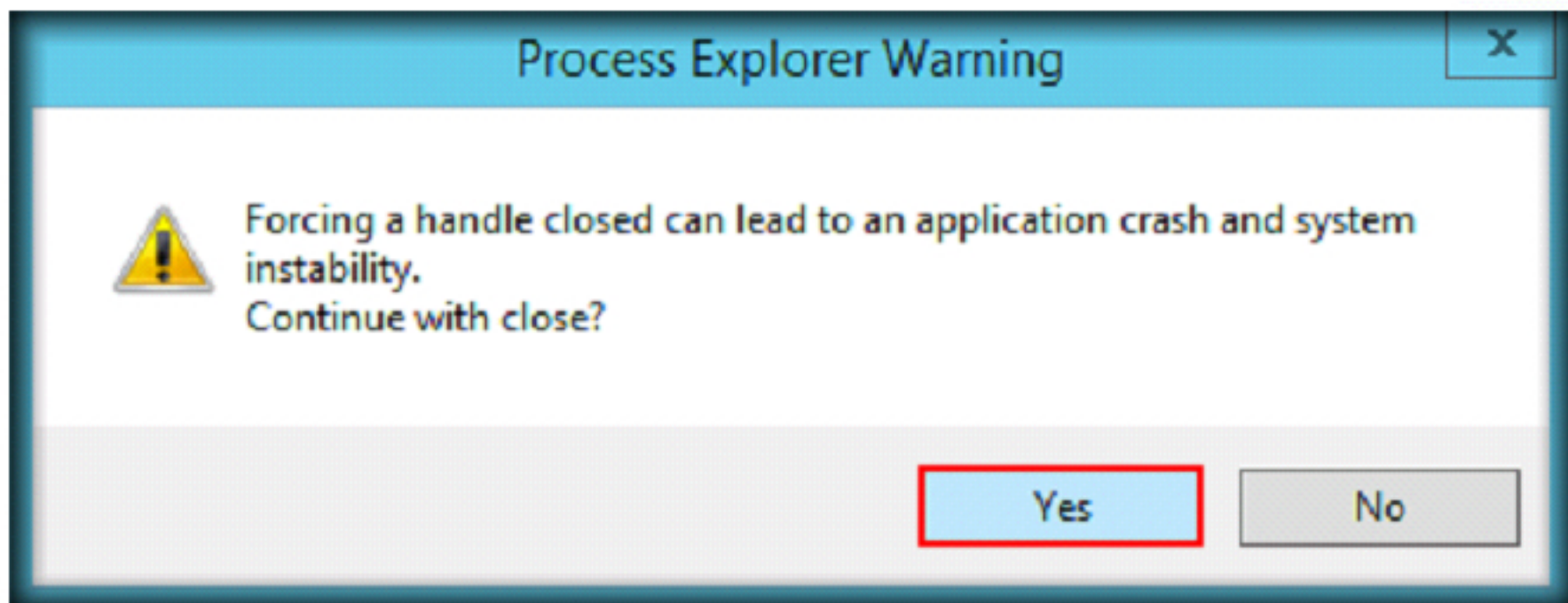


FIGURE 2.16: Process Explorer Close Handle: Warning

25. To view handle properties, right-click on the required handle and select **Properties**; or choose **Handle → Properties** from the **Menu** bar.

 Highlight .NET Processes: This option appears on Windows NT-based systems that have the .NET Framework installed. When the option is checked, managed applications (those that use the .NET Framework) are highlighted in the .NET process highlight color.

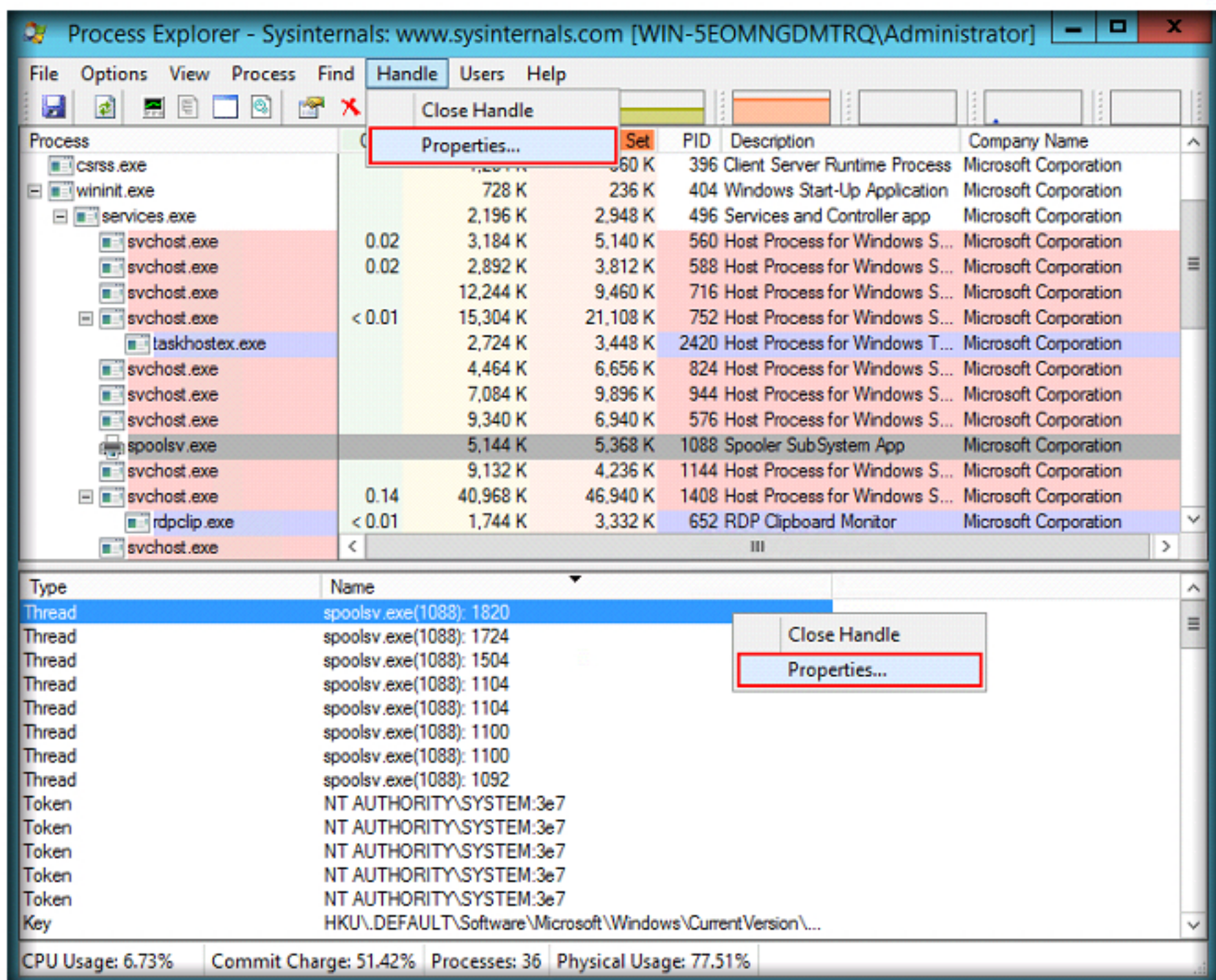


FIGURE 2.17: Process Explorer Handle Properties

26. Properties window appears for the selected handle. The **Details** tab displays basic information about the selected handle.

 **Kill:** This item terminates a process with the **Terminate Process** API. Note that a process terminated in this way is not warned of its termination, and therefore does not write any unsaved data.

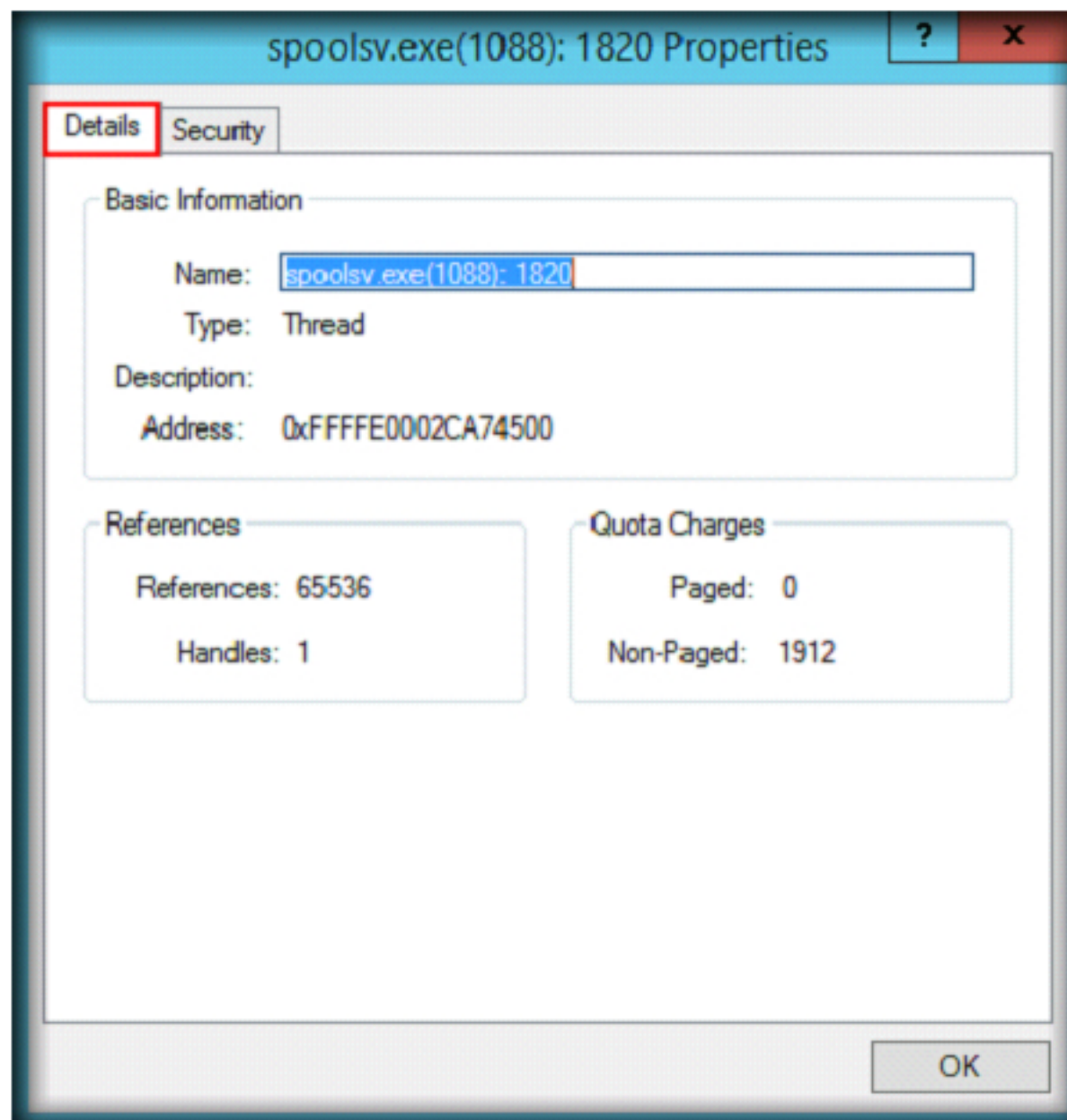


FIGURE 2.18: Process Explorer Handle Details tab

27. The **Security** tab displays the level of security assigned to each group or user for the selected handle.

 **Highlight Own Processes:** In Windows NT and higher, checking this option results in Process Explorer showing the processes that are running in the same user account as Process Explorer in the own-process highlight color.

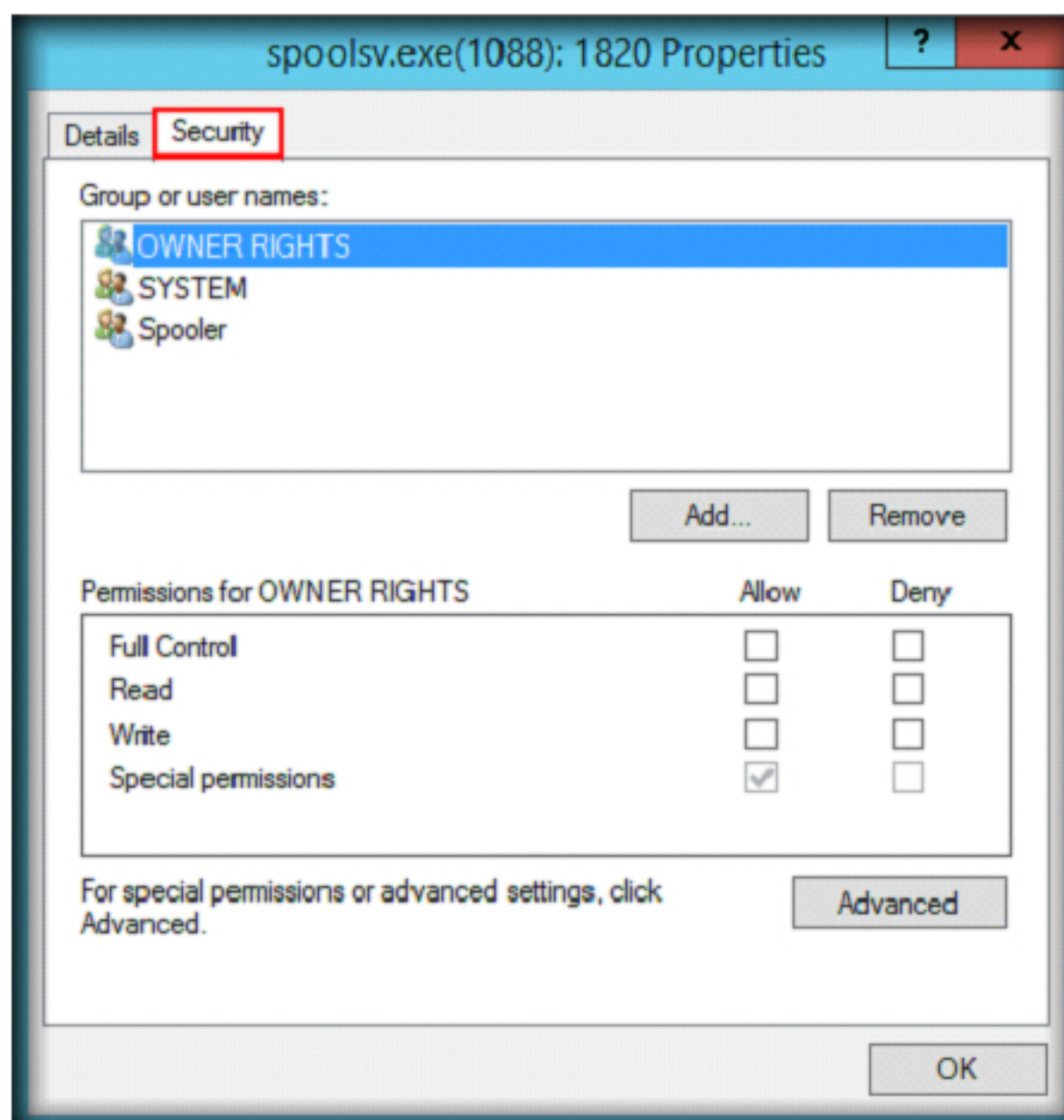


FIGURE 2.19: Process Explorer Handle Security tab

28. Click **OK** to close the **Properties** window.

Lab Analysis

Analyze the DLLs and handles in the process, and document the respective details.

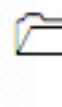
PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS
RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ iLabs

Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

Event Log Explorer is a software solution for viewing, monitoring, and analyzing events recorded in security, system, application, and other logs of Microsoft Windows OS.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

As an expert computer forensic investigator, to examine the security posture of a target network, you must know how to view, monitor, and analyze the events recorded in security, system, application, and other logs of the OS.

Lab Objectives

The objective of this lab is to help forensic investigators learn how to view, monitor, and analyze various events. Here we monitor and analyze:

- Security logs
- System logs
- Application logs
- Other logs of Microsoft Windows OS.

Lab Environment

This lab requires:

- Event Log Explorer located at **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Event Log Explorer**.
- You can also download the latest version of **Event Log Explorer** from **www.eventlogxp.com**.
- If you decide to download the latest version, then the screenshots shown in the lab might be slightly different.

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

- A computer running **Windows Server 2012**.
- Administrative privileges to install and run tools.

Lab Duration

Time: 15 Minutes

Overview of Viewing, Monitoring, and Analyzing Events Using the Event Log Explorer Tool

Event Log Explorer is a software solution for viewing, monitoring, and analyzing events recorded in security, system, application, and other logs of Microsoft Windows operating systems. It helps to quickly browse, find, and report on problems, security warnings and all other events that are generated within Windows.

Lab Tasks



TASK 1

Launching Event Log Explorer

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Event Log Explorer**.
2. Double-click **elx_setup.exe** to launch the setup, select the language as **English**, and follow the wizard-driven installation steps to install the application.

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

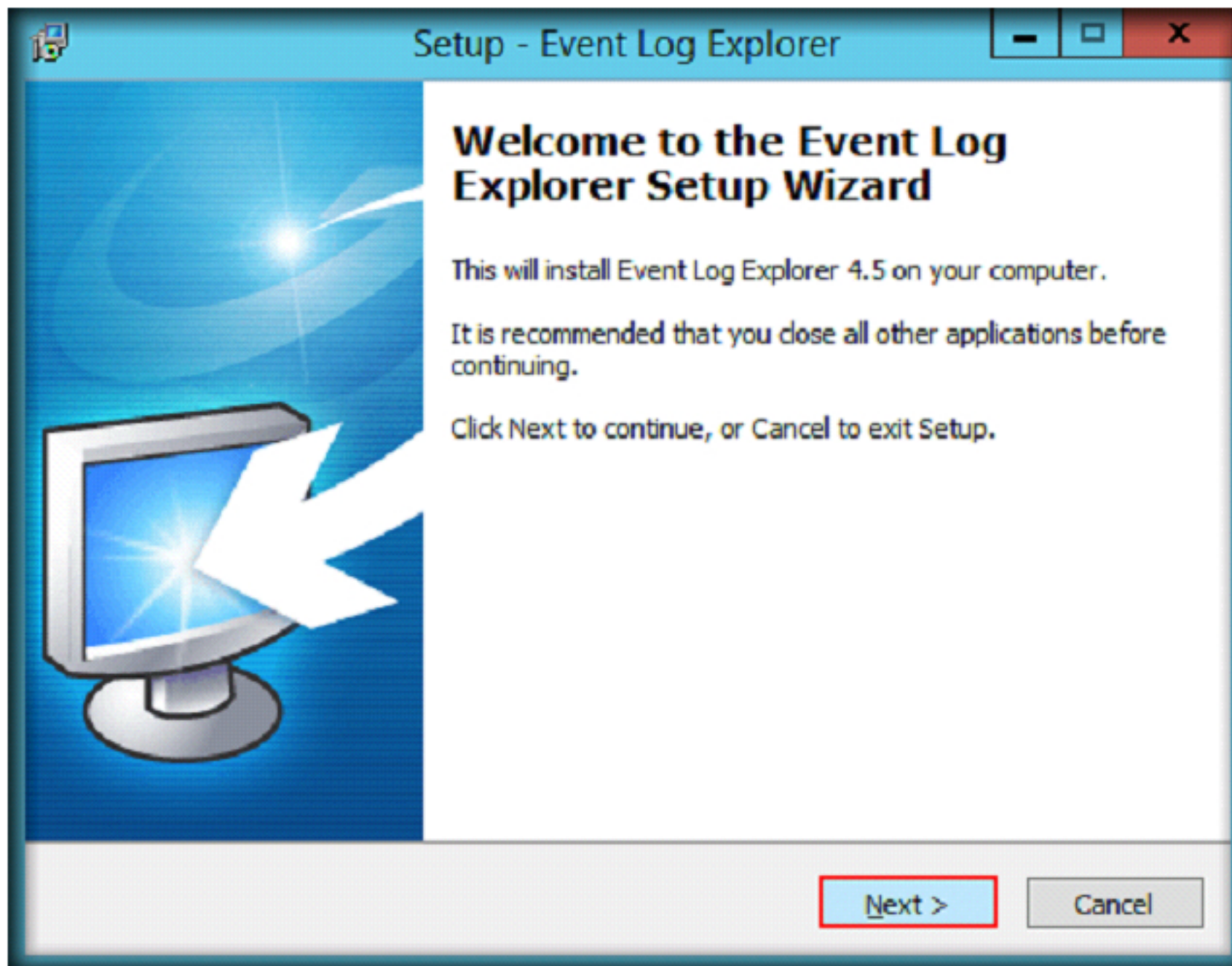


FIGURE 3.1: Event Log Explorer startup installer wizard

3. In the final step of installation, check **Launch Event Log Explorer** and click **Finish**.

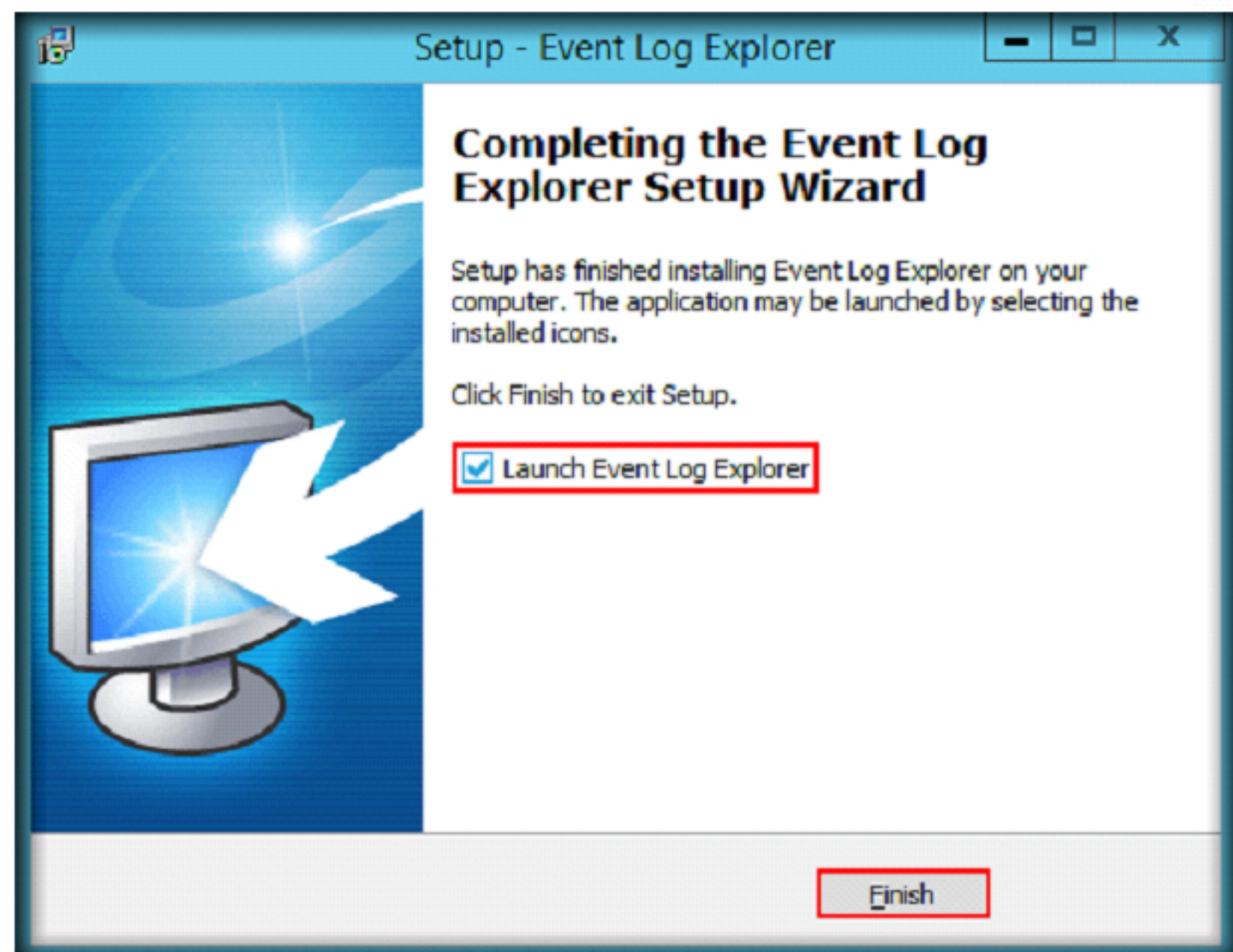


FIGURE 3.2: Event Log Explorer startup installer wizard

4. On completion of installation, a web page related to Event Log Explorer appears in a web browser. Close the web page.
5. An **Event Log Explorer** pop-up window appears, click **OK** to close it.

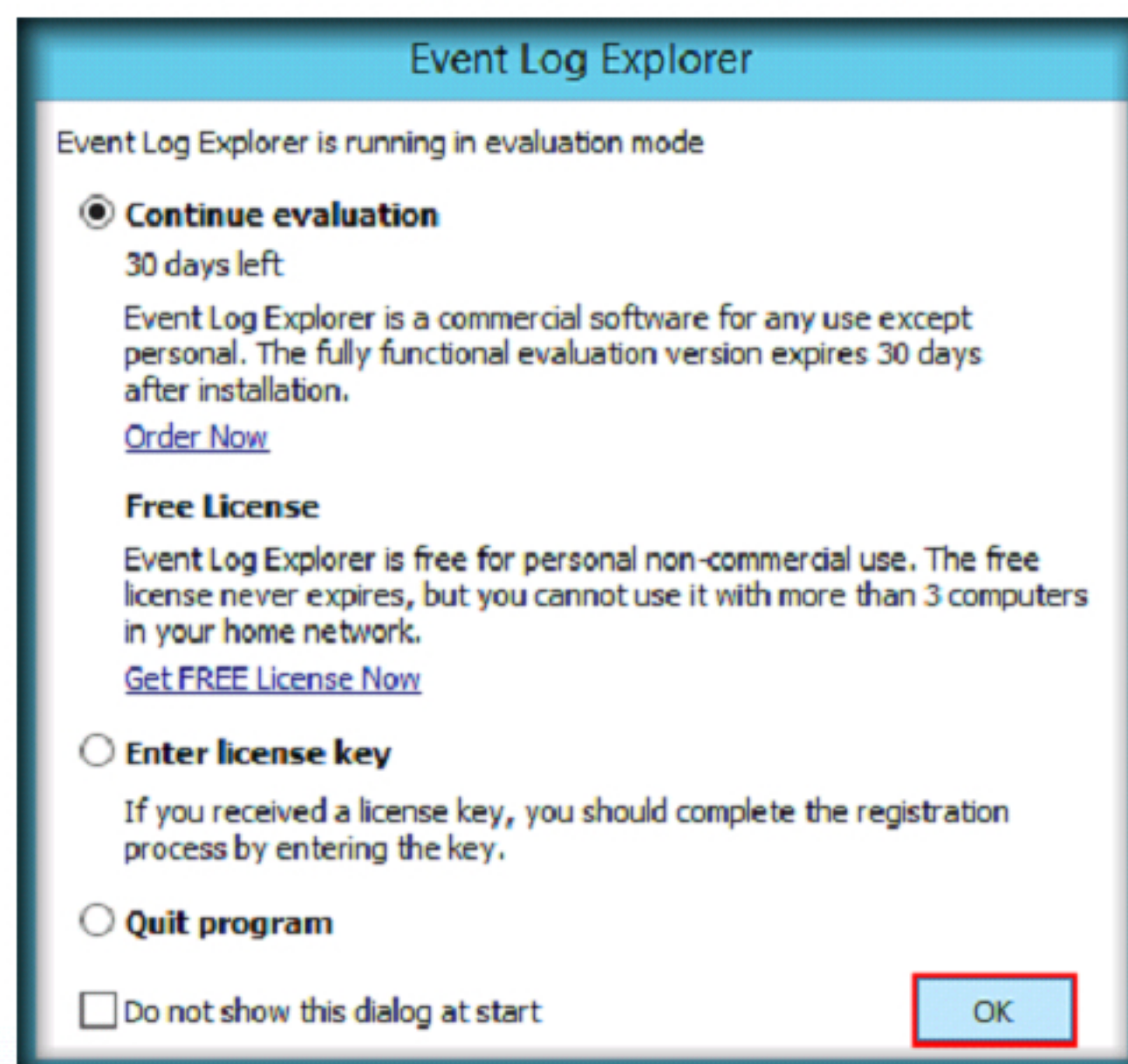


FIGURE 3.3: Event Log Explorer pop-up window

Event Log Explorer helps you to quickly browse, find, and report on problems, security warnings, and all other activities created within Windows.

TASK 2

Opening Event Log

Event Log Explorer provides a powerful event search and filtering engine.

6. **Event Log Explorer** main window appears, displaying an empty log view area and **Computer Tree** pane with Windows Server 2012 virtual machine's computer name.

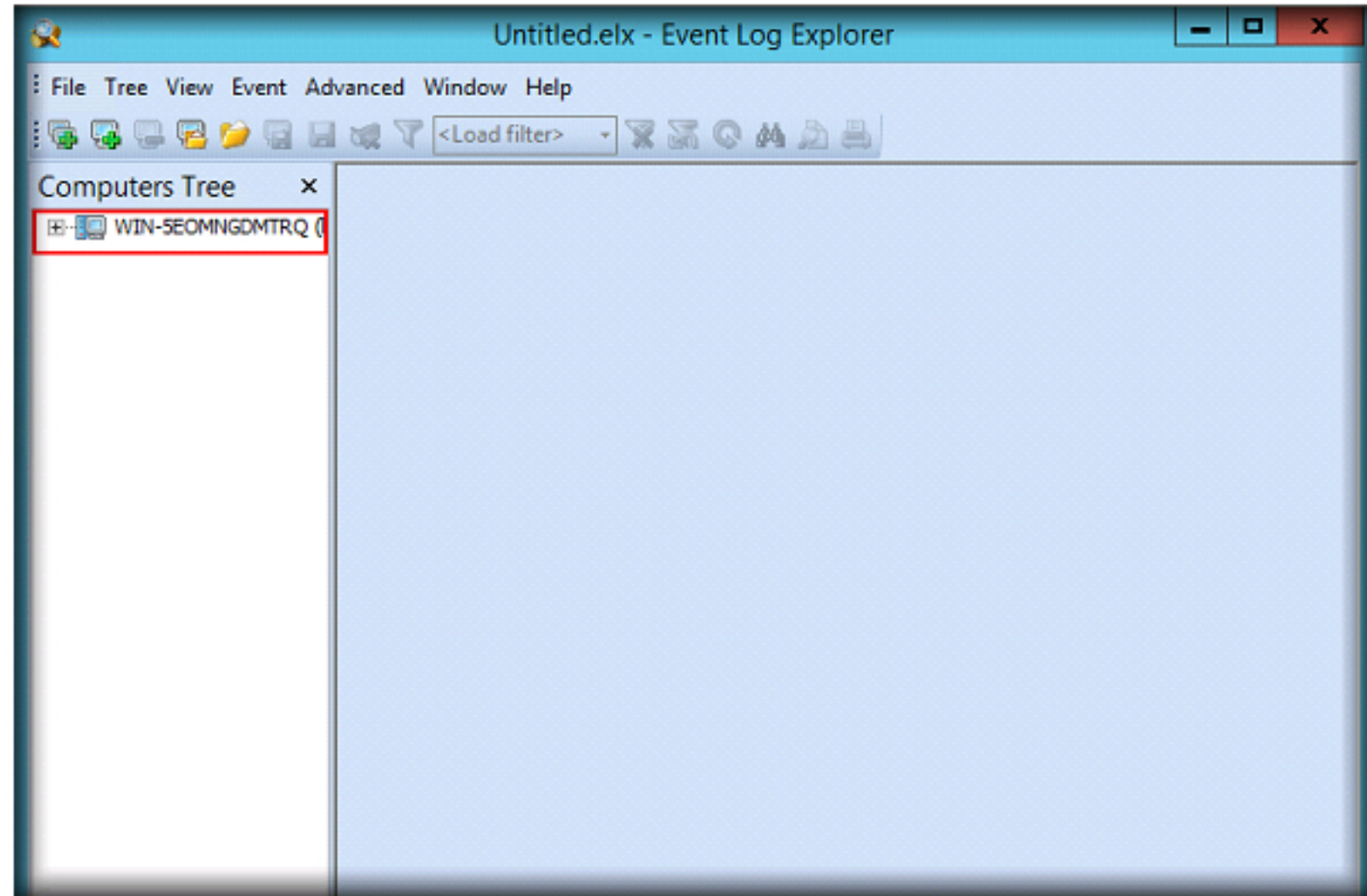


FIGURE 3.4: Event Log Explorer Main Window

7. If the local computer name does not appear in the **Computer Tree** pane, then choose **File → New Workspace**.

Every filter can be saved into a file. It saves your time when you want to reapply the filter in future.

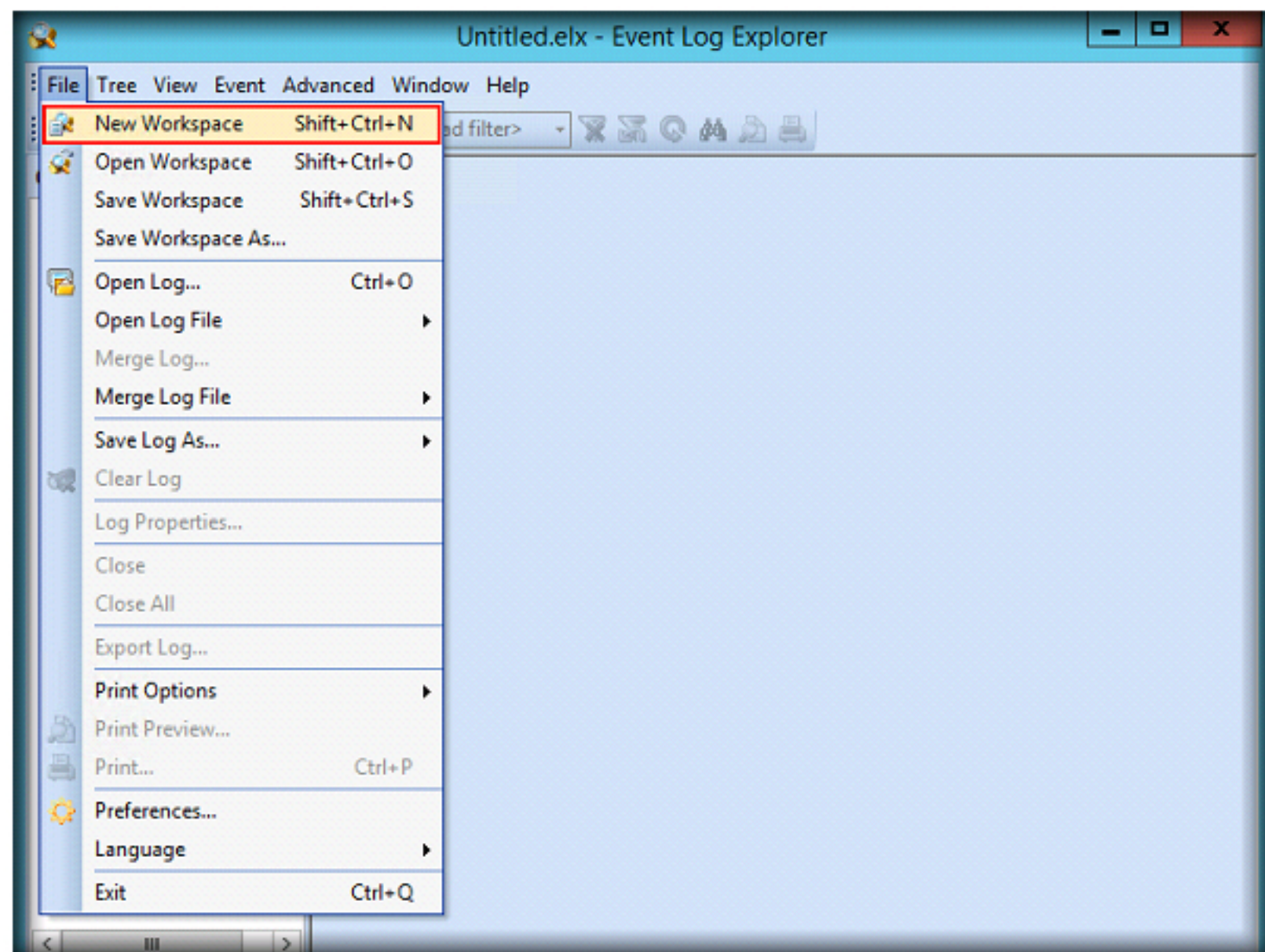


FIGURE 3.5: Event Log Explorer New Workspace

8. To open an event log of your local computer, click the  button near the computer name in the **Computers Tree** pane.

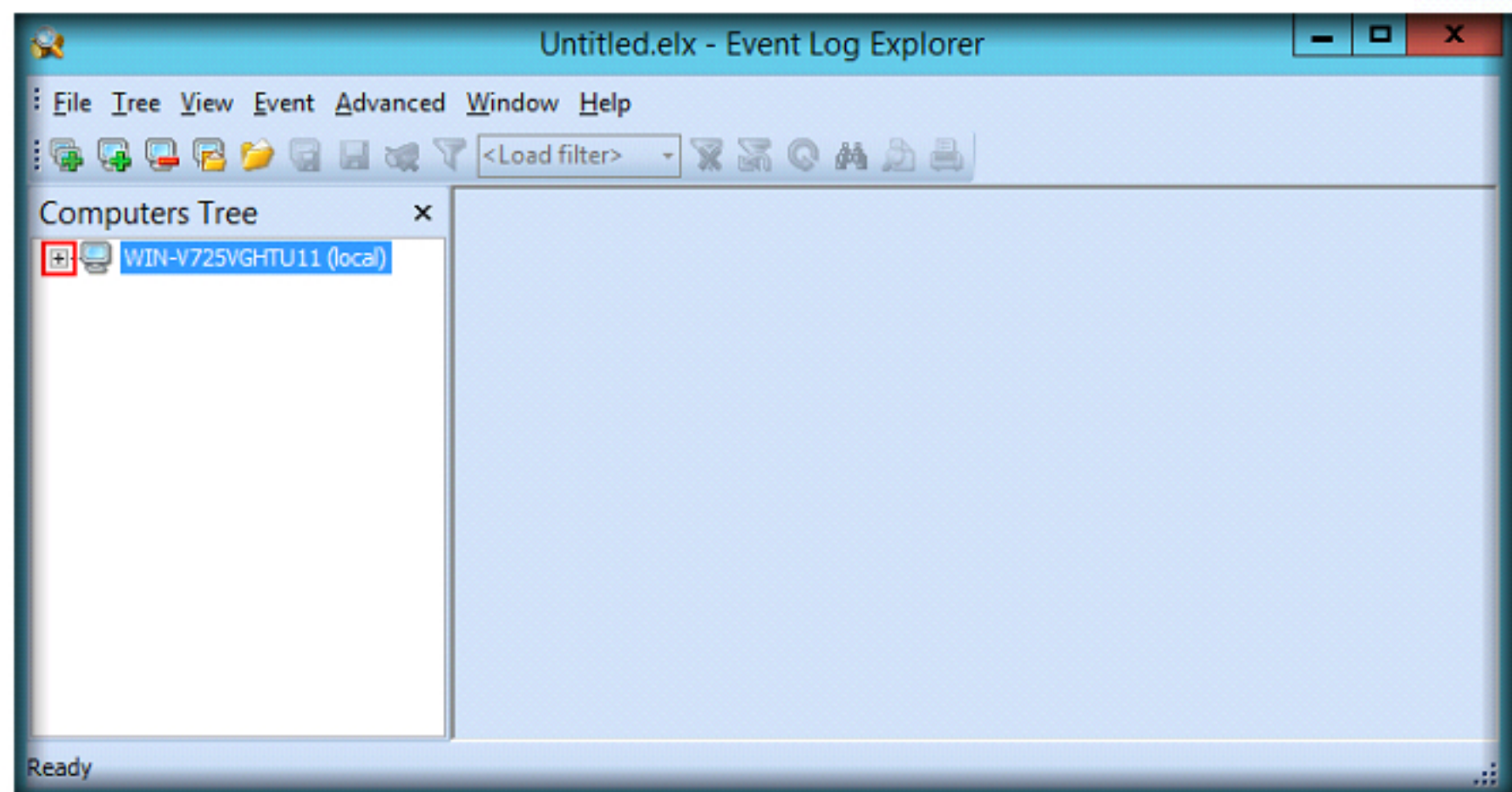


FIGURE 3.6: Event Log Explorer Computers Tree

9. It will expand the computer node to display all available event logs as shown in the following screenshot:

 Event Log Explorer can print event logs or even separate events. You can also export your event logs to other formats. At the time of writing, Event Log Explorer supports exports to HTML, Microsoft Excel, and tab-separated text files.

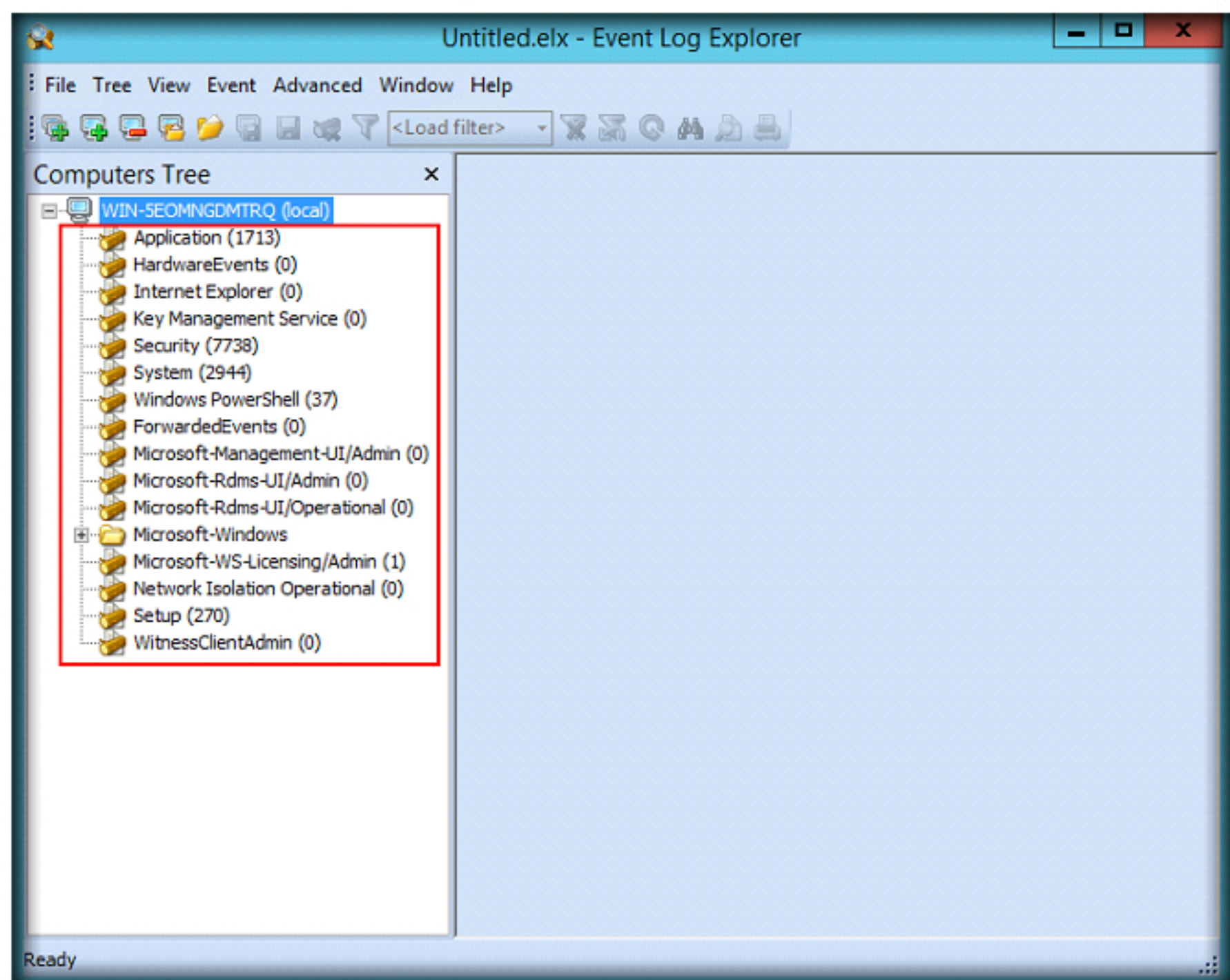


FIGURE 3.7: Expanding the Computers Tree of Event Log Explorer

10. Double-click **Application** in the **Computers Tree** pane to view the application events. The Application event logs will be displayed in the right pane of the window as shown in the screenshot:

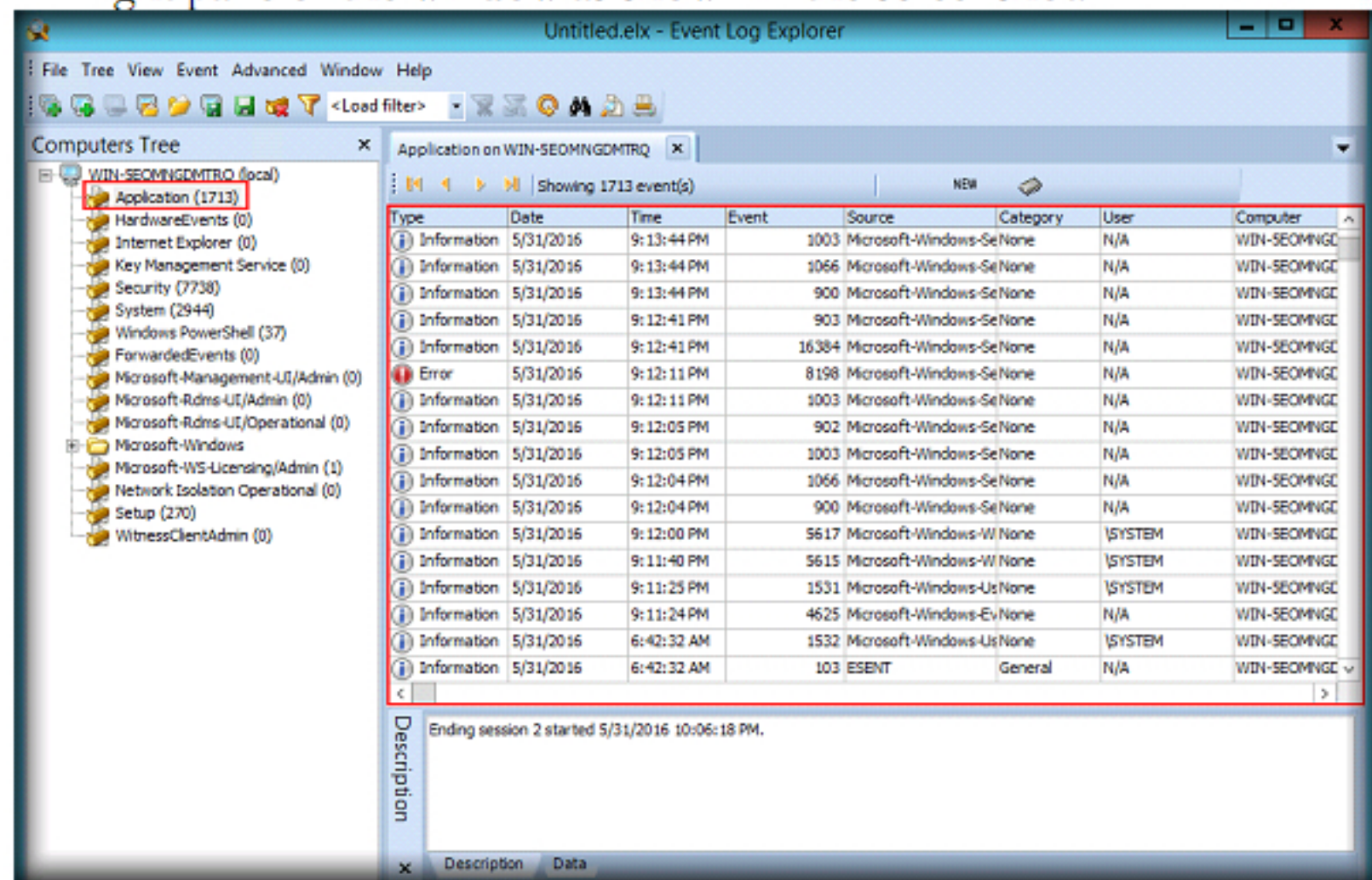


FIGURE 3.8: Event Log Explorer viewing the application events

Main features and benefits of Event Log Explorer at a glance:

- Favorite computers and their logs are grouped into a tree.
- Manual and automatic backup of event logs.
- Event descriptions and binary data are in the log window.
- Advanced filtering by any criteria, including event description text.
- Quick Filter feature allows you to filter an event log with a couple of mouse clicks.
- Log loading options pre-filter event logs.
- Color coding by Event ID.
- Print and export to different formats.
- Export logs to different formats.
- Read damaged EVT files and generate EVT files from event views.

11. Event Log Explorer also displays the events of Applicure DFS Replication, dotDefenderAudit, HardwareEvents, Key Management service, OAlerts, Security, System, Windows PowerShell.
12. Selecting any event displays the description of the event in the **Description** pane at the lower end of the window.

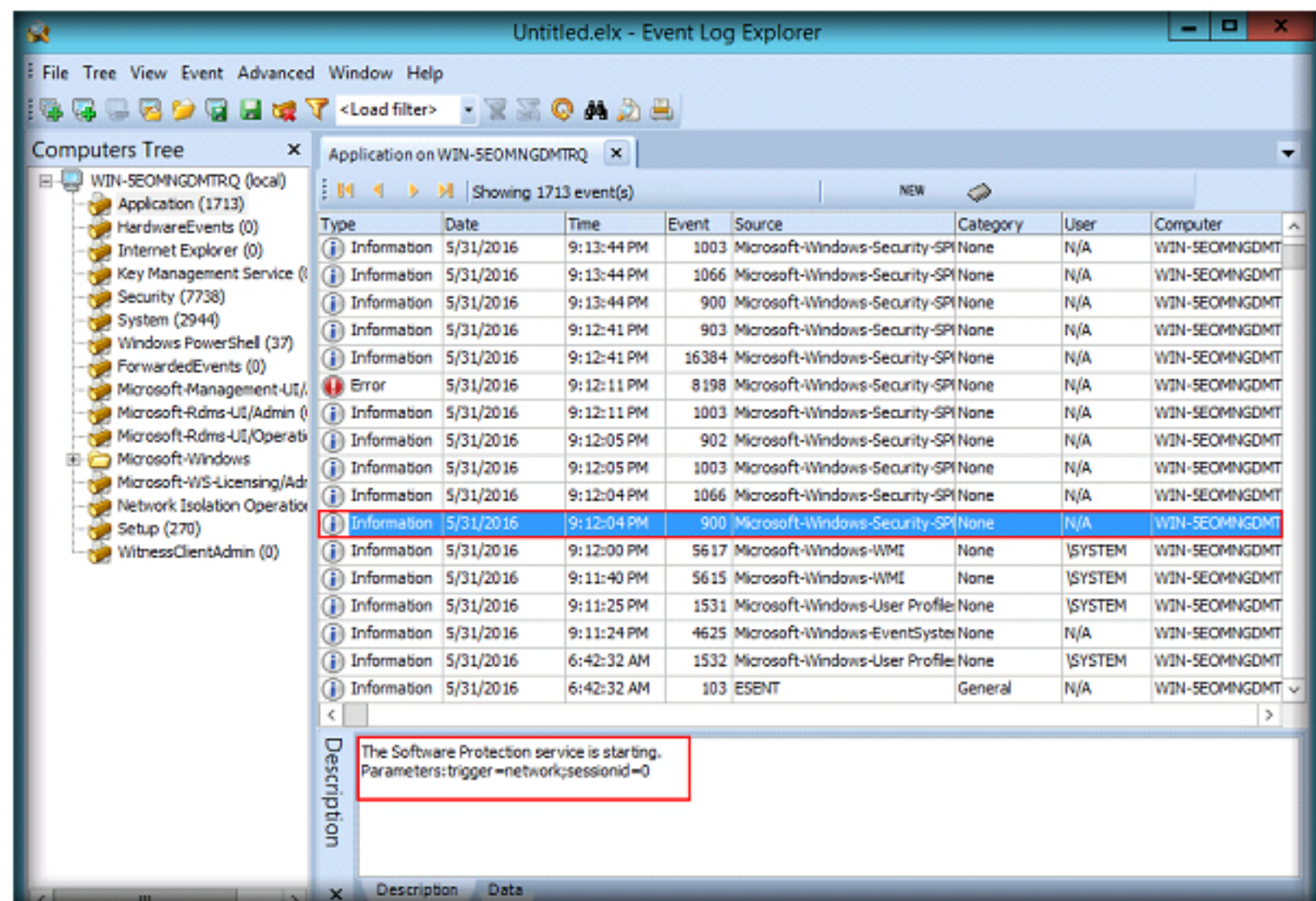
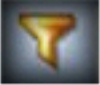


FIGURE 3.9: Event Log Explorer Description pane

13. You can also filter the events. To filter the events, click the filter icon  in the toolbar, or choose **View → Filter**.



TASK 3

Applying a Filter

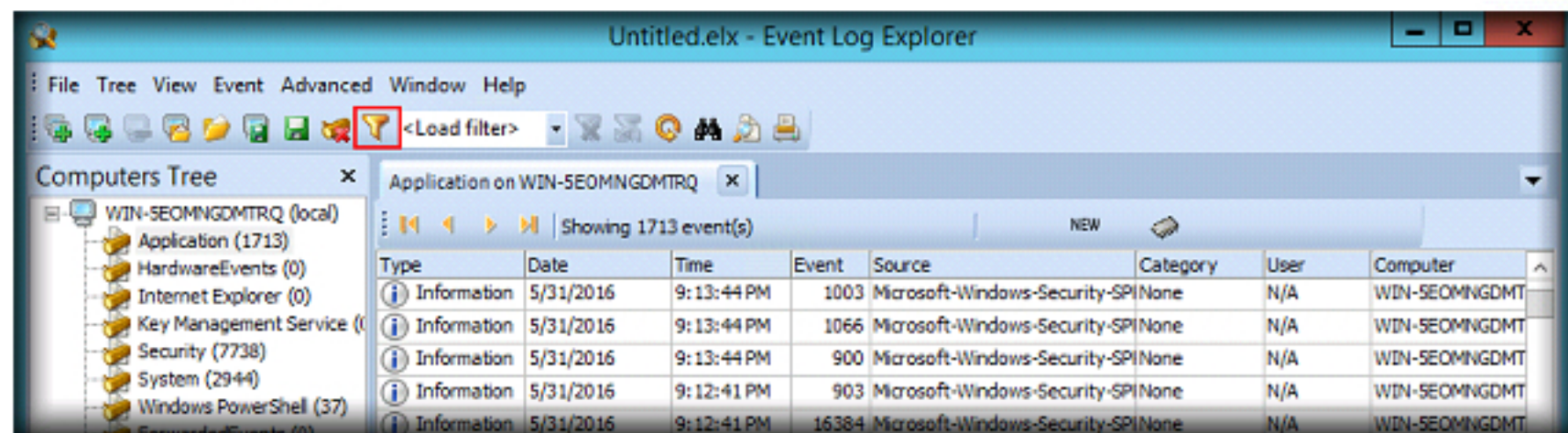


FIGURE 3.10: Event Log Explorer Filter option

14. It will pop up a new **Filter** window. Choose **Source**, **Category**, **User** and **Computer** and then, click **OK**.



Depending on the user interface style, log views are presented either as MDI child windows or as tabs.



Event Log Explorer allows sorting the list by a specified column. To sort the list, click the column header. Click a second time to reverse the sort order.

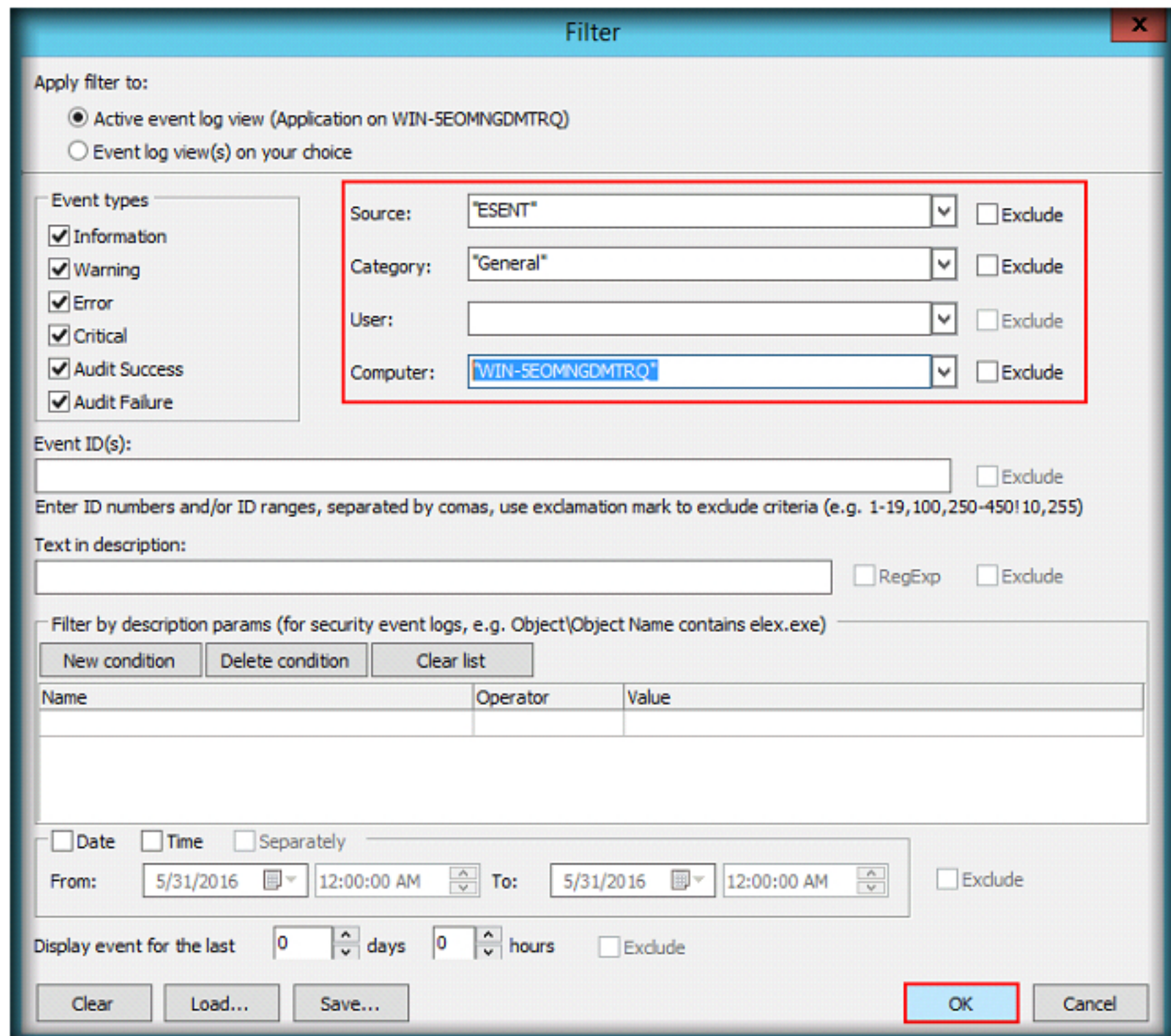


FIGURE 3.11: Event Log Explorer applying a filter

15. **Event Log Explorer** displays all the events related to your **Filter Settings**.

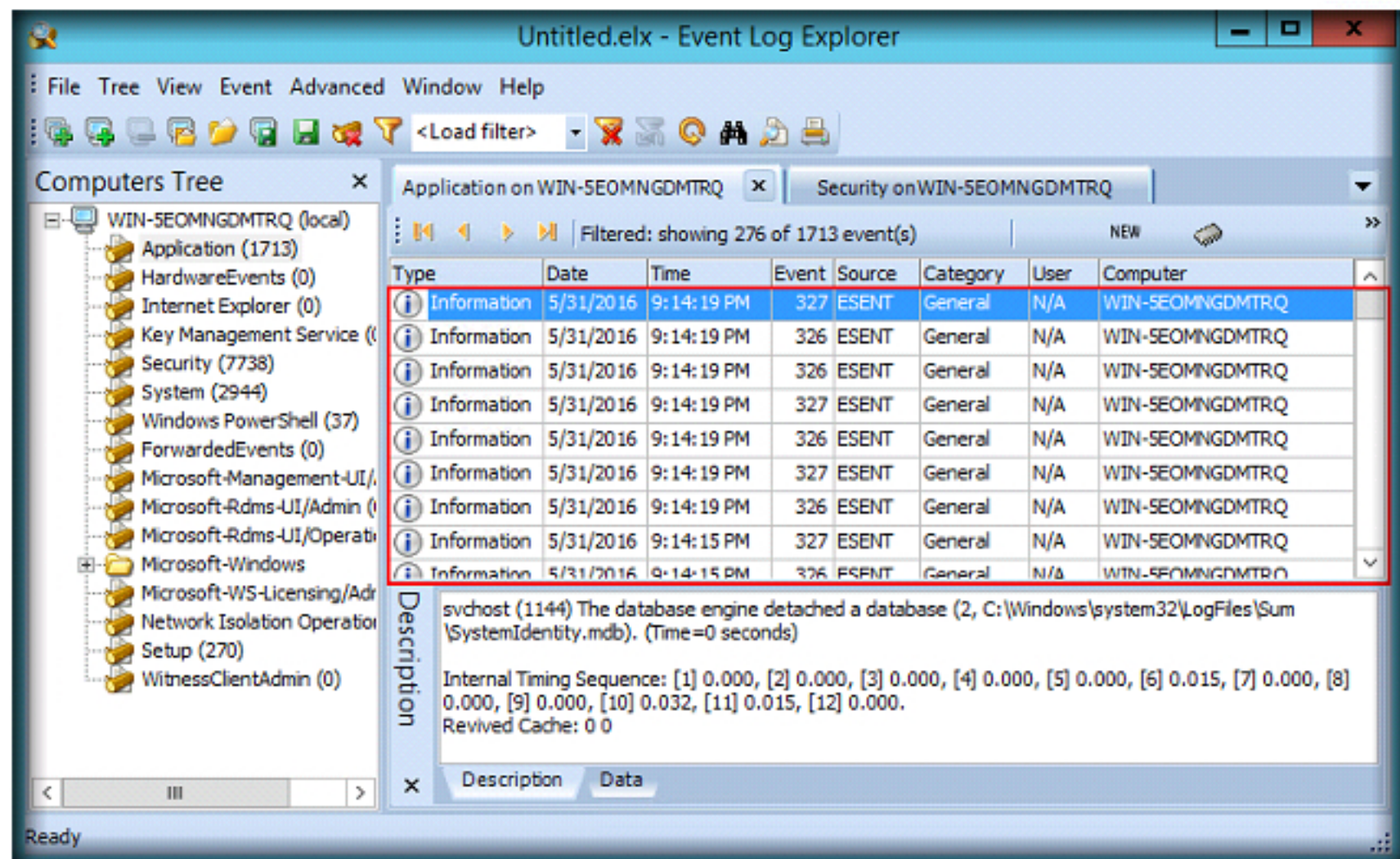


FIGURE 3.12: Event Log Explorer showing the filtered event logs

16. To clear the **Filter** settings, click on the clear filter  button on the toolbar, or go to **View → Clear Filter**.

Note: The **Clear Filter** option will be active only when a filter is applied.

17. You can save the event logs for future reference. To save the event logs choose **File → Save Log As...** and select any option according to your requirements. In this lab, **Save Event Log (Backup)...** option is selected.

TASK 4

Saving Event Logs

Event Log Explorer's friendly and powerful user interface lets you choose between two styles: multi-document or tabbed-document interface.

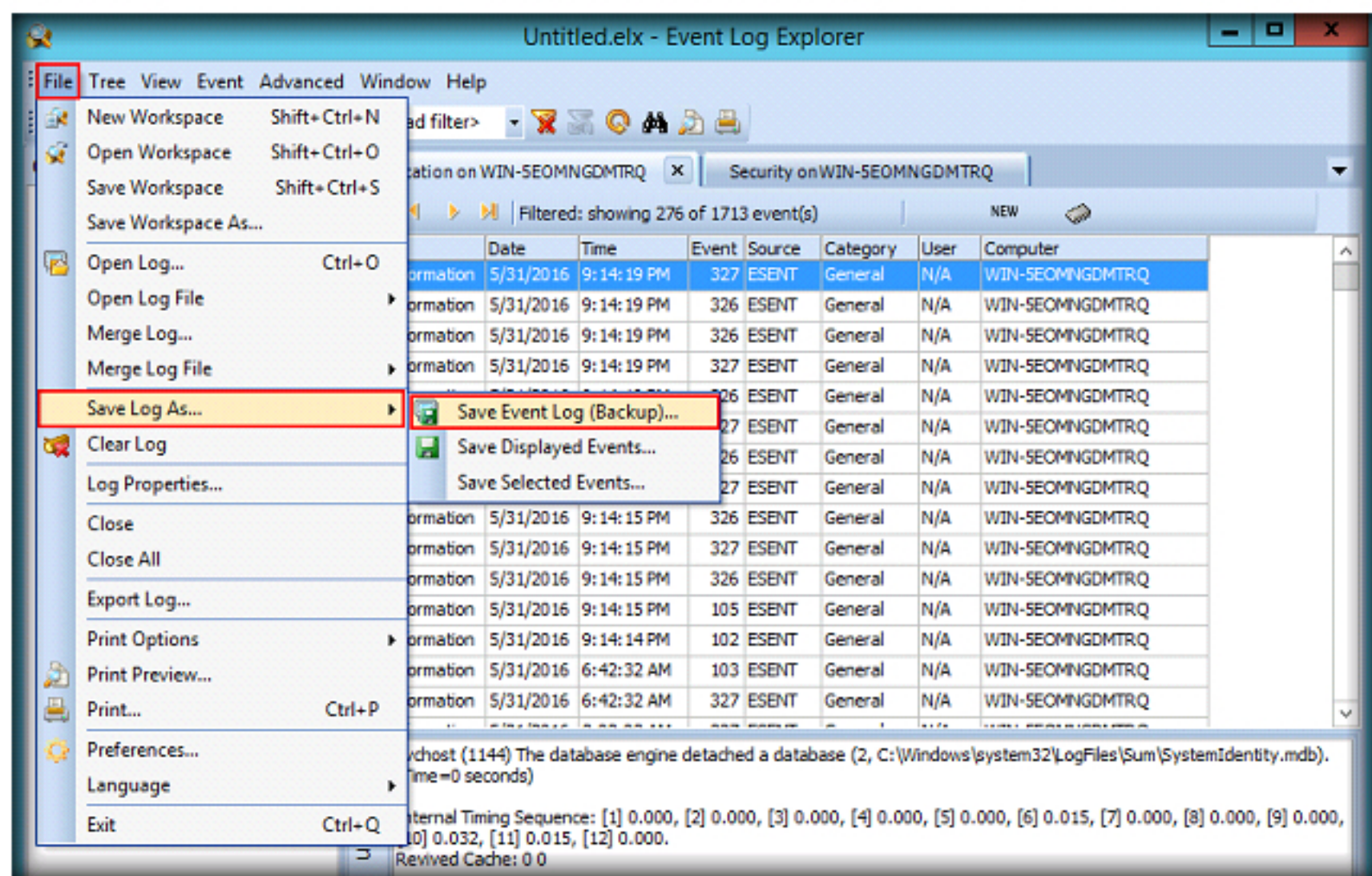


FIGURE 3.13: Event Log Explorer Save Log As options

18. Navigate to the location where you want to save the event logs (here we are saving the file to the Desktop), type the file name (here, **Application Events**) in the appropriate field, and then click **Save**.

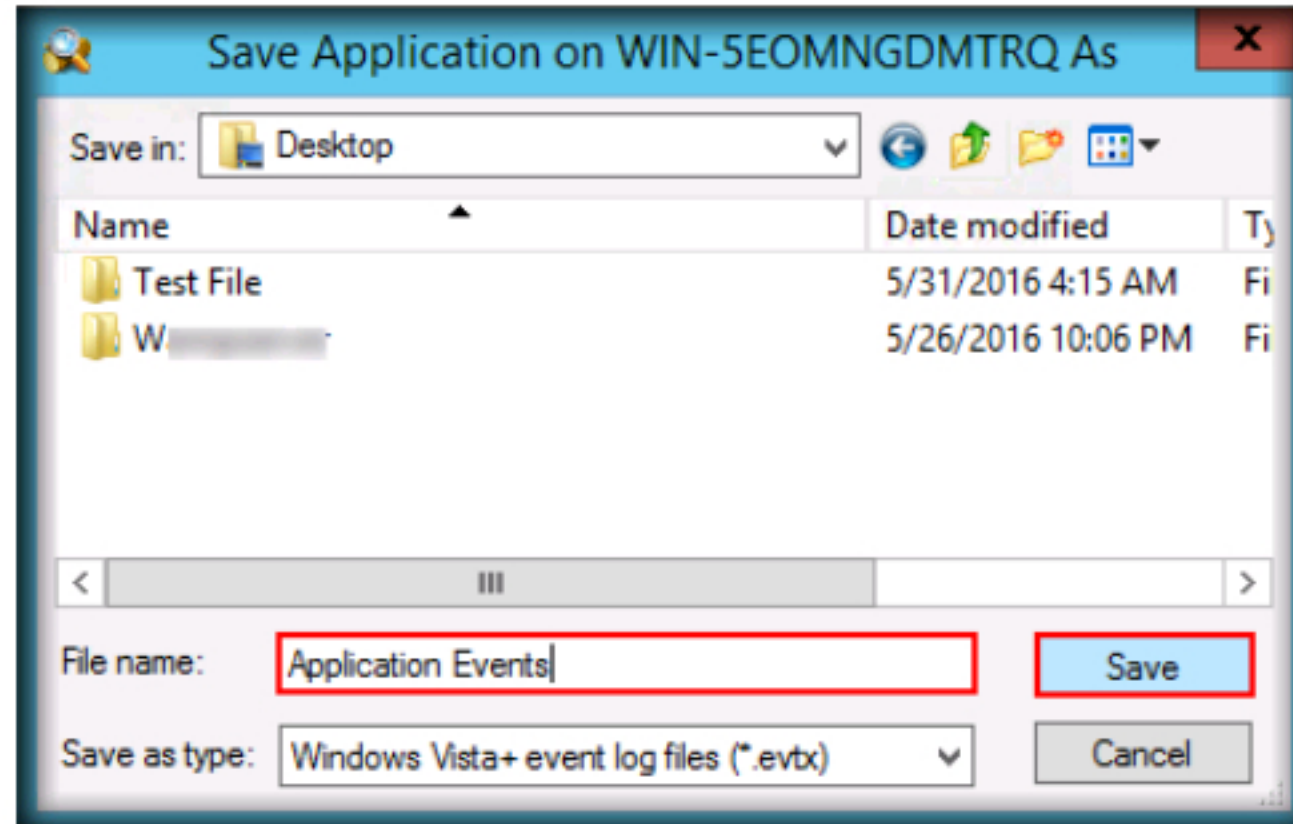


FIGURE 3.14: Event Log Explorer Save Log As window

Event Log Explorer
Supported OS: Windows
NT, 2000, XP, 2003, Vista,
2008, 7.

TASK 5

Opening Event Log Files

19. Navigate to the location where you saved the event logs and double-click on file to see the saved event logs.
20. The saved logs appear in the Event Viewer window as shown in the following screenshot:

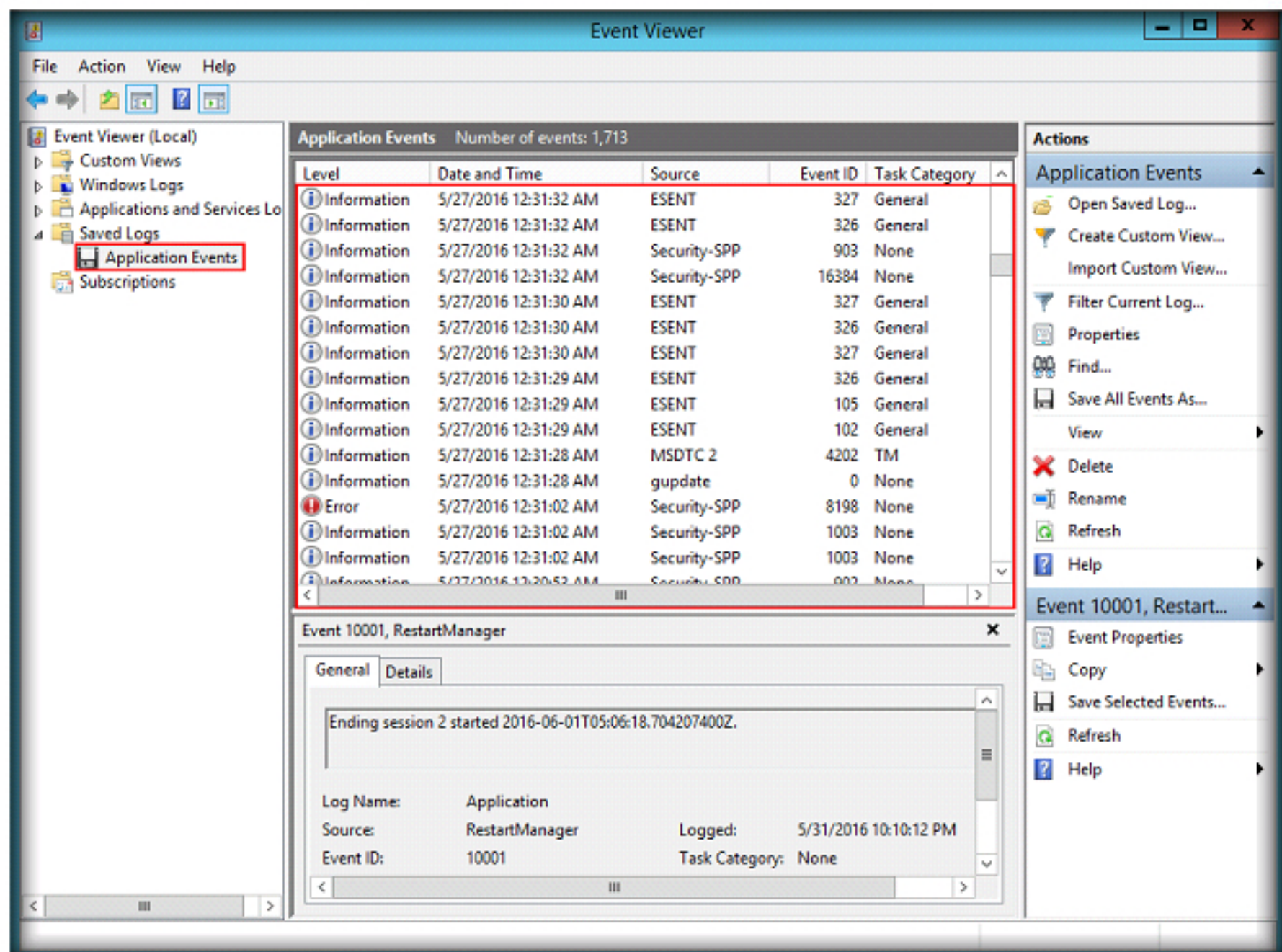


FIGURE 3.15: Event Log Explorer Event Viewer

Event Log Explorer
allows bookmarking.
Bookmarking is a handy
way to navigate between
events in the log view.

21. An alternative method for opening an event log file is to choose **File → Open Log File → Standard (or) File → Open Log File → Direct**.
22. In the pop-up window, click **Browse** to select the file and then click **OK**. It will open the saved file.

Event Log Explorer's backup file name has this format: LogName-year-month-day-hour-minute-seconds-millisecond.evt.

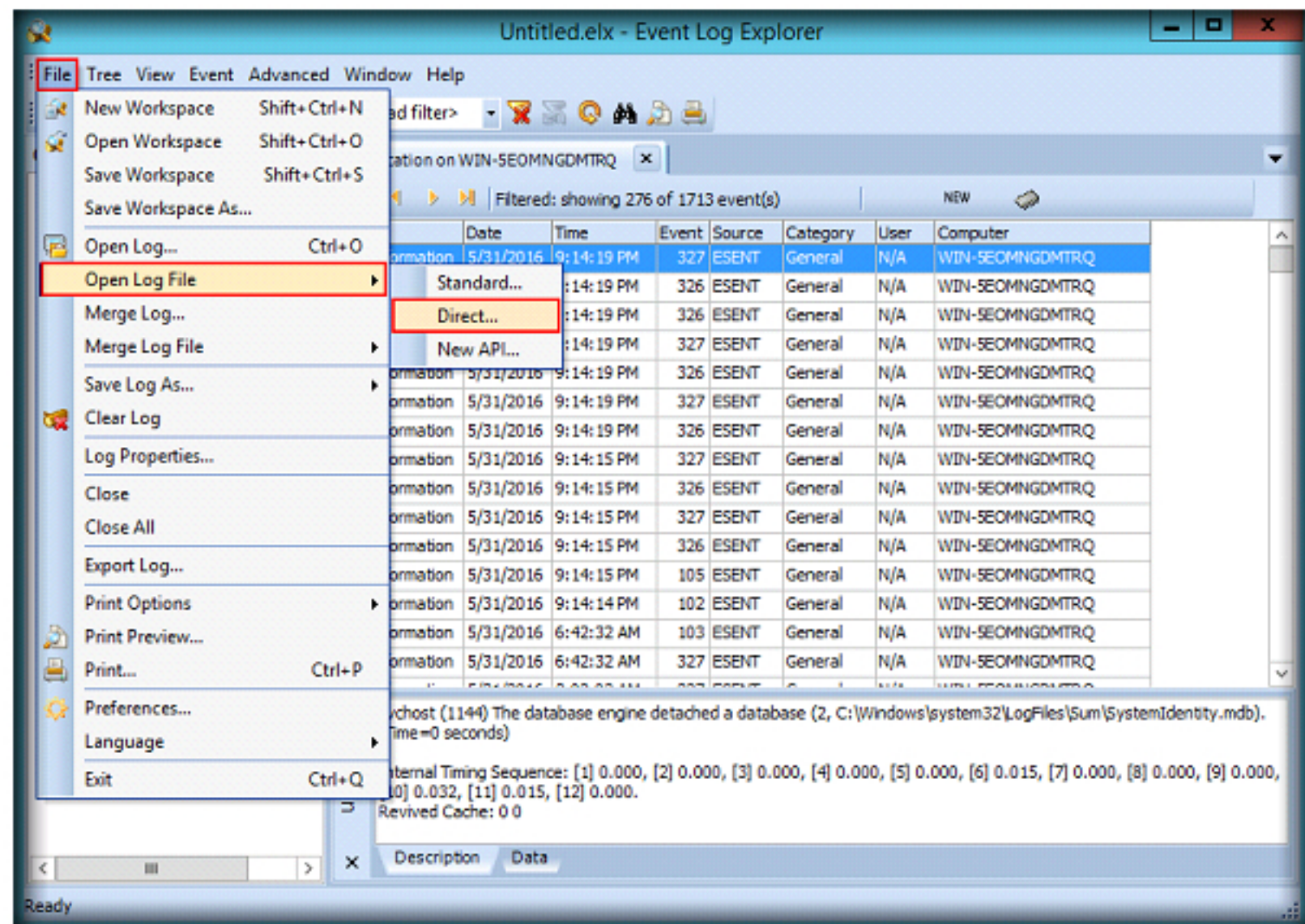


FIGURE 3.16: Event Log Explorer Direct

23. To clear the logs, select **File → Clear Log**.

Event Log Explorer's log view control toolbar displays log view status message (e.g. Loading, Filtering, Showing events), event list navigator buttons (First, Previous, Next, Last) and different status indicators.

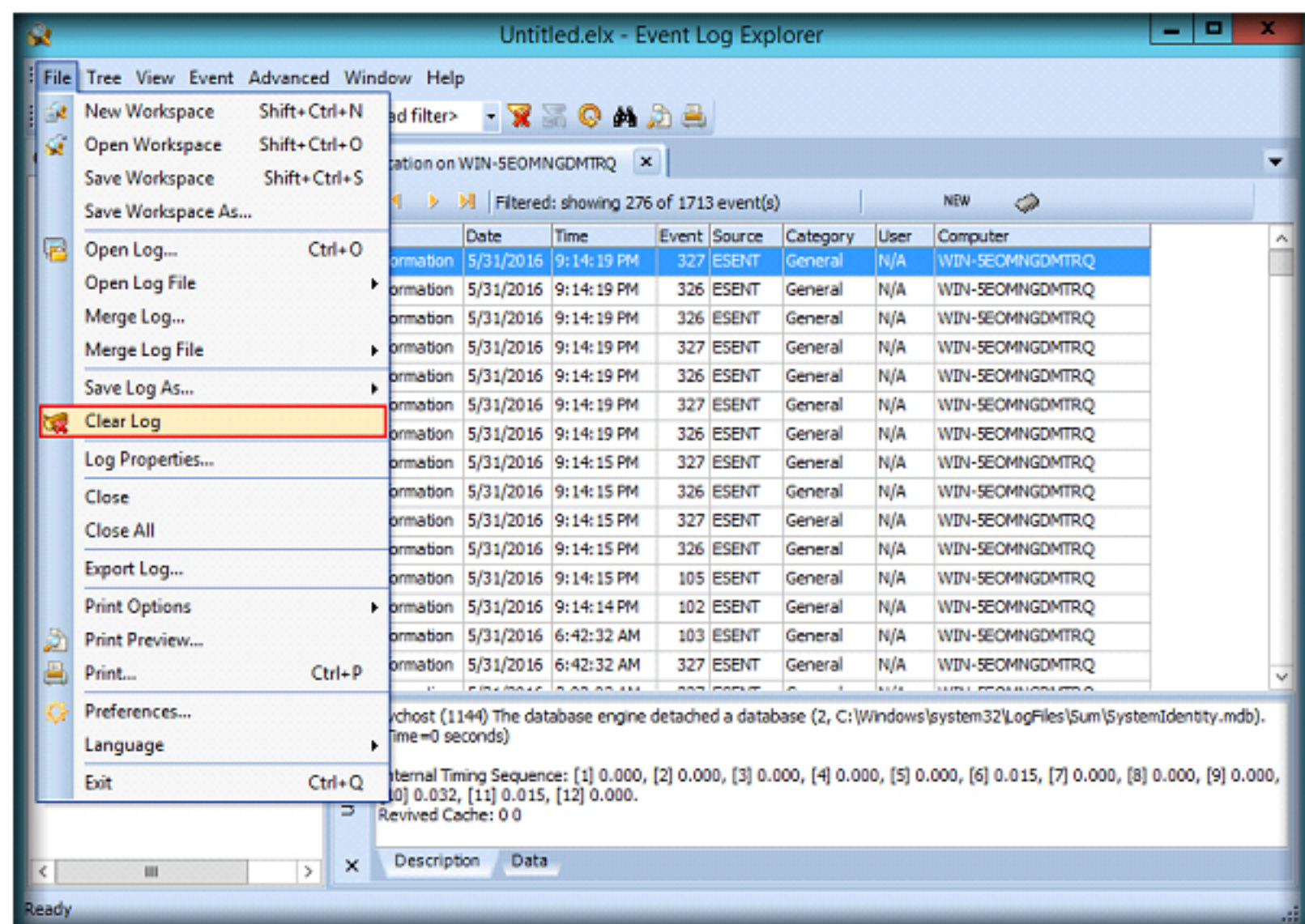


FIGURE 3.17: Event Log Explorer Clear Logs

24. A **Clear Log** pop-up appears; click **Yes** if you want to save the logs. If you do not want to save logs, click **No**. It will clear all the event logs of the selected category in the **Computers Tree** pane on the left.

Lab Analysis

Analyze the security, application, system, and other logs of the computer, and document the results related to the lab exercise. Give your opinion on the target computer's security situation and exposure.

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

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ iLabs

Lab

4

Performing a Computer Forensic Investigation Using the Helix Tool

Helix focuses on Incident response and forensics tools. It is meant to be used by individuals who have a sound understanding of Incident response and forensic techniques.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

In a company, when a cyber-security breach occurs, the network security admin should be able to aptly respond in the situation and take necessary steps to avoid further damage. In case, there is no proper person to take an action, the company would hire an investigator for Incident response. To be an expert computer forensic investigator, you must be able to offer Incident response activities. This lab discusses how an investigator can respond to the Incident using the Helix tool.

Lab Objectives

The objective of this lab is to help students learn how to investigate a computer-based crime using the Helix tool.

Lab Environment

To carry out the lab you need:

- The **Helix** tool, located at **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Helix**.
- A computer running **Windows Server 2012**.
- Administrative privileges to install and run tools.

Lab Duration

Time: 30 Minutes

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

Overview of Performing a Computer Forensic Investigation Using the Helix Tool

Helix uses software that is licensed under various additional licenses such as the GPL. Individual software maintains the original license for that prospective software. e-fense does not license, control, or support the individual software on the Helix CD. In no way does the title or copyright that e-fense holds on the name or packaging of Helix affect the additional third-party software included on the Helix CD. All rights and provisions for the additional third-party software included on Helix still apply.

Lab Tasks

Note: This lab is based on the free version of Helix 3.

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Helix**.
2. To launch **Helix**, double-click **helix.exe**.
3. It will display a warning message. Read it thoroughly and select your preferred language from the **Choose Your Language** drop-down menu.
4. Click **Accept** to continue.



FIGURE 4.1: Helix Warning message

5. After clicking the **Accept** button, Helix GUI appears as shown in the following screenshot:

 Helix is a fast and powerful live CD originally based on Knoppix which provides all necessary tools for live forensics, Incident response, and e-discovery.

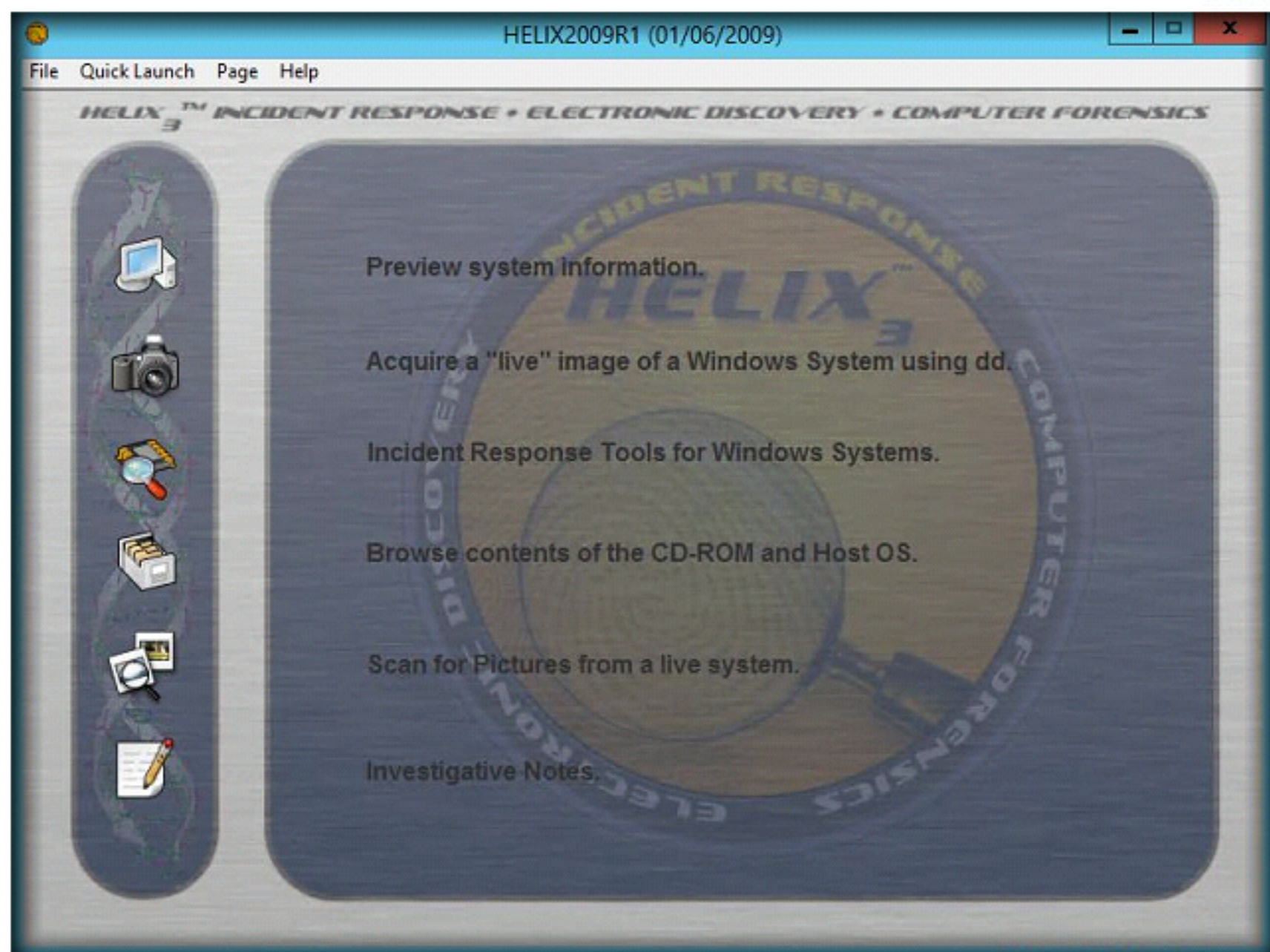


FIGURE 4.2: Helix Main Interface



TASK 1

Viewing System Information

 Helix is a customized version of Ubuntu Linux, allowing you to boot into a Linux environment containing customized Linux kernels, hardware detection, and a large number of applications designed for Incident response and forensics.

6. Click the **System Information** icon on the left side of the window to see the complete system information.

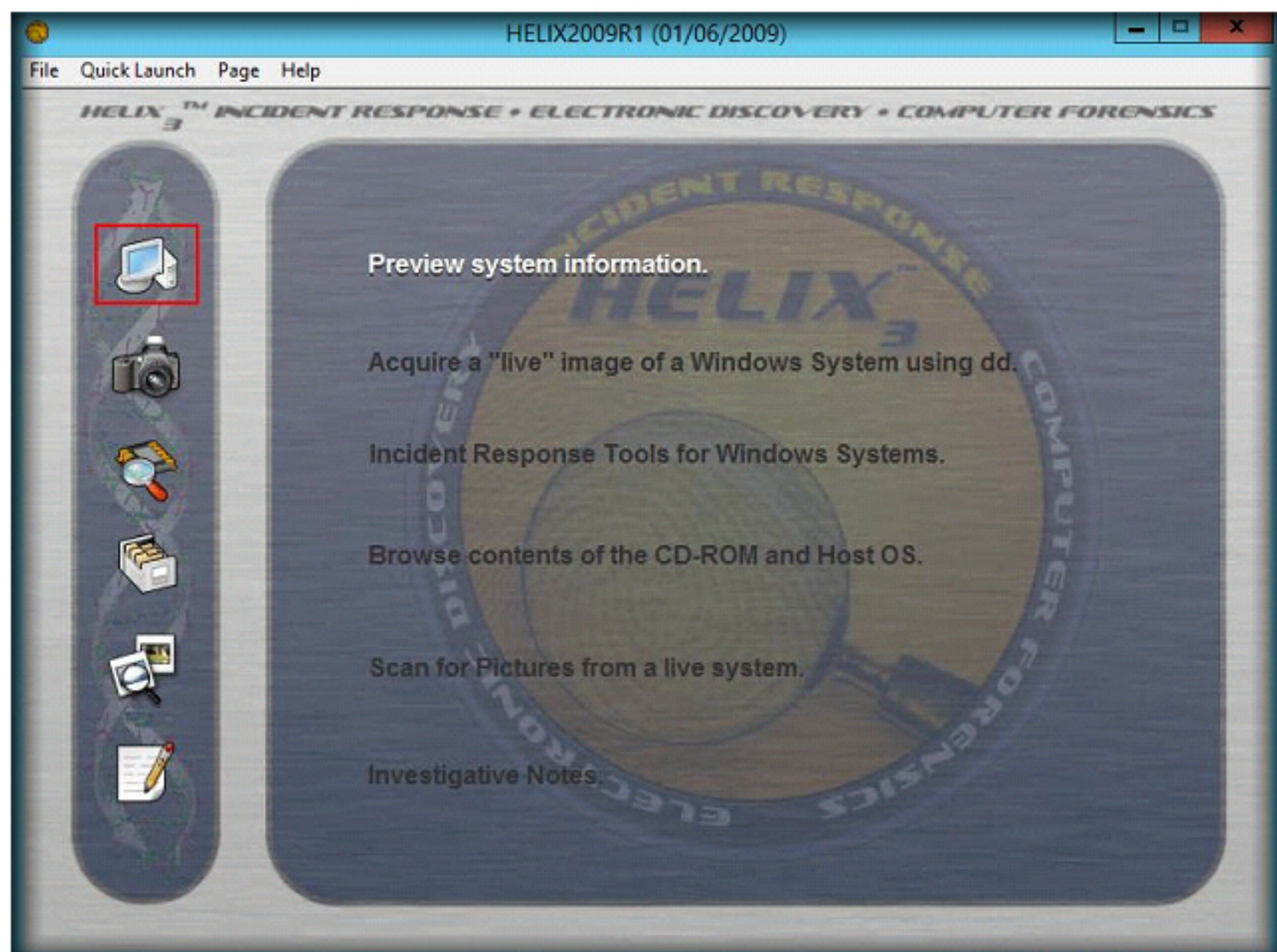


FIGURE 4.3: Helix System Information icon

7. It displays the OS information, owner information, network information, drives and their file types.

 Helix does not touch the host computer in any way and is forensically safe. It will not auto mount swap space or attached devices.

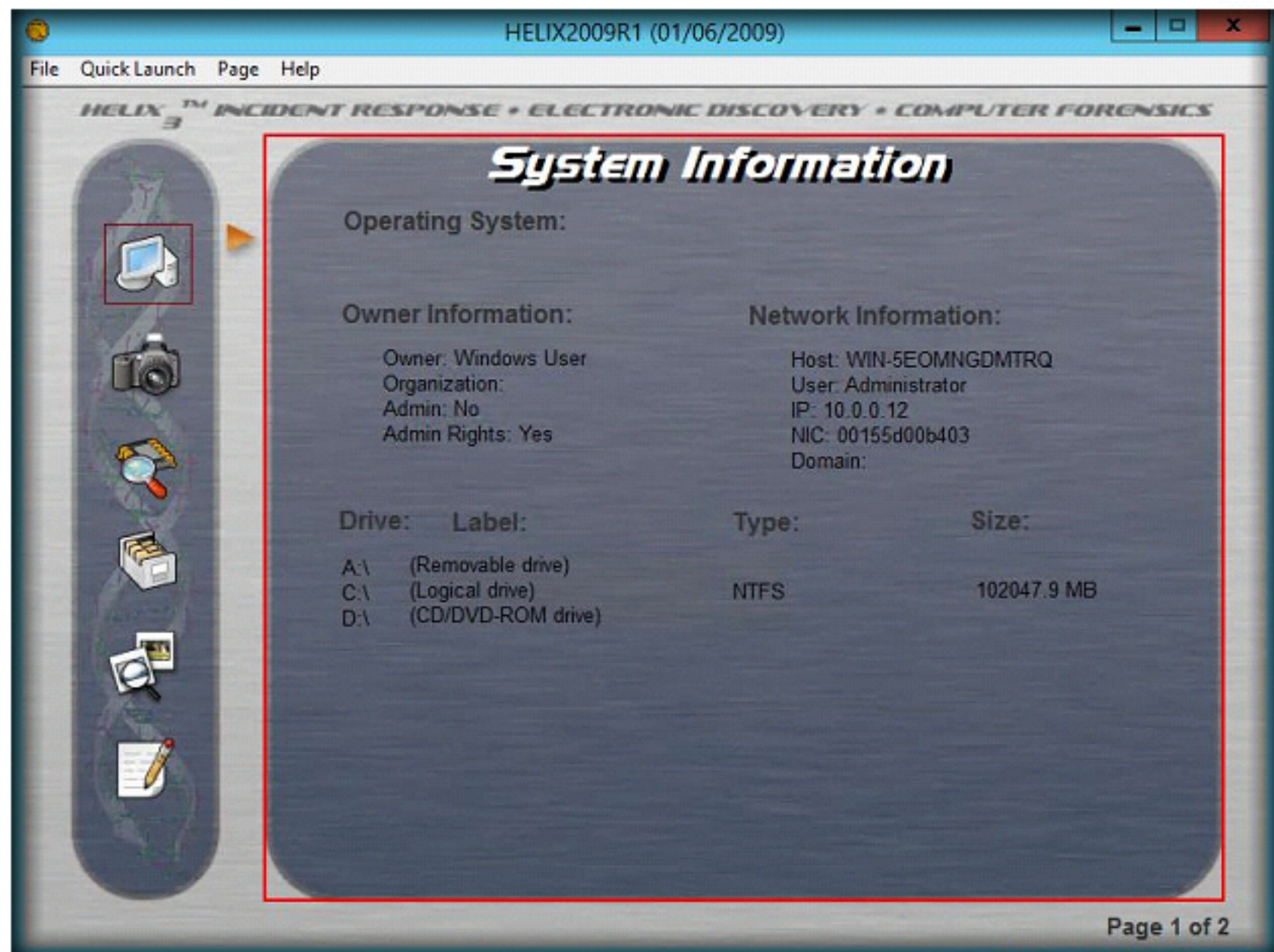


FIGURE 4.4: Helix System Information details

8. Click the  button to go to the second **System Information** page. This page displays the processes running on your system.

 Helix mainly provides Incident response and forensics tools, and is intended for users with solid knowledge of these techniques.

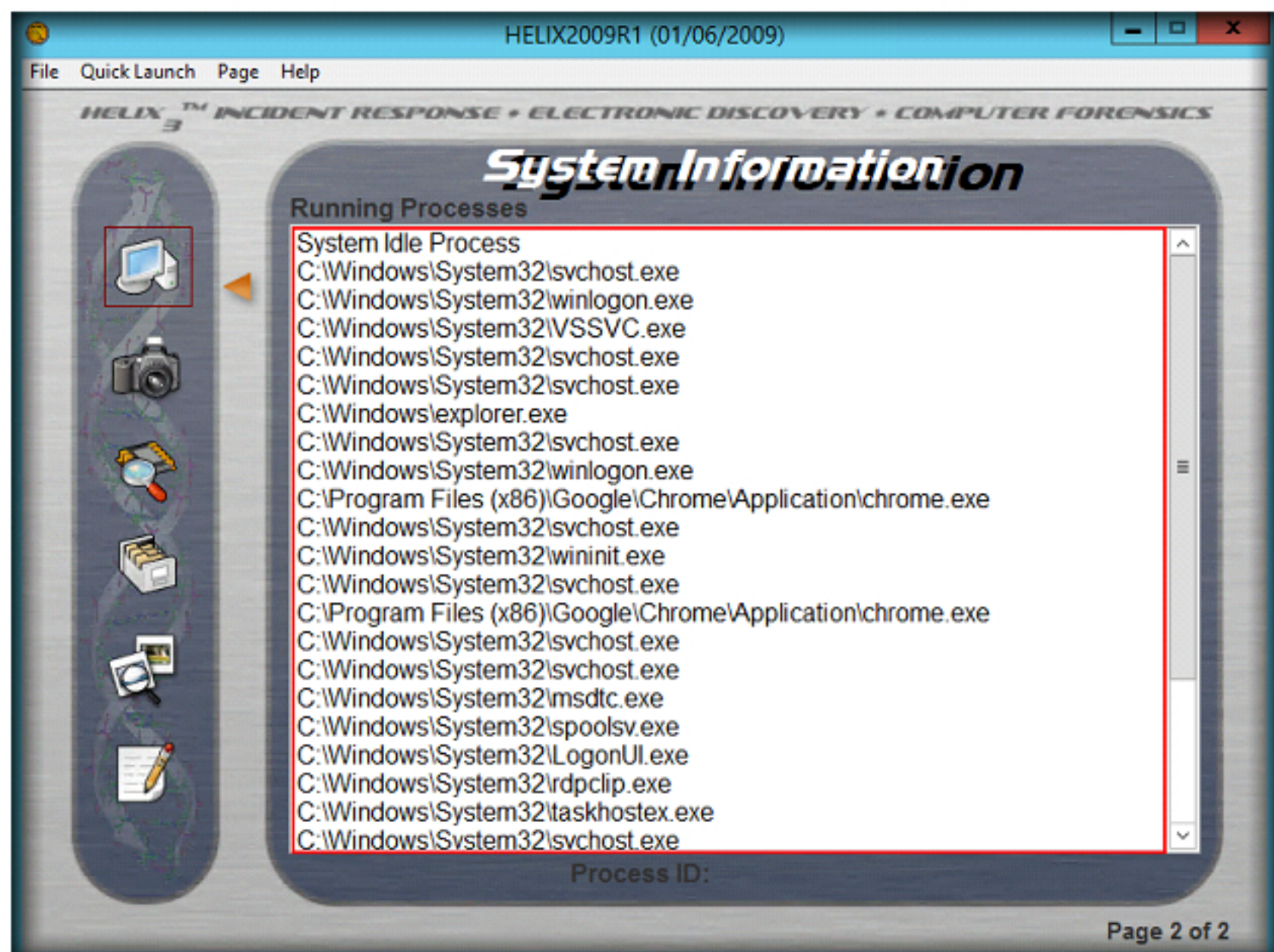


FIGURE 4.5: Helix System Information Running Processes

**TASK 2****Acquisition**

Security firm e-fence released a new version of their popular Linux-based forensics live CD, Helix. This new version is Ubuntu-based, which seems to be a popular choice among this genre of tools.

9. Click the **Acquisition** icon to acquire physical memory or disk drives.
10. Select the desired disk drive from the **Source** drop-down menu. In **Location Options**, choose any one option to save, give the destination path by clicking the **Folder** icon. Give the image a name and set the **DD Options** field to **default**, then click **Acquire**.

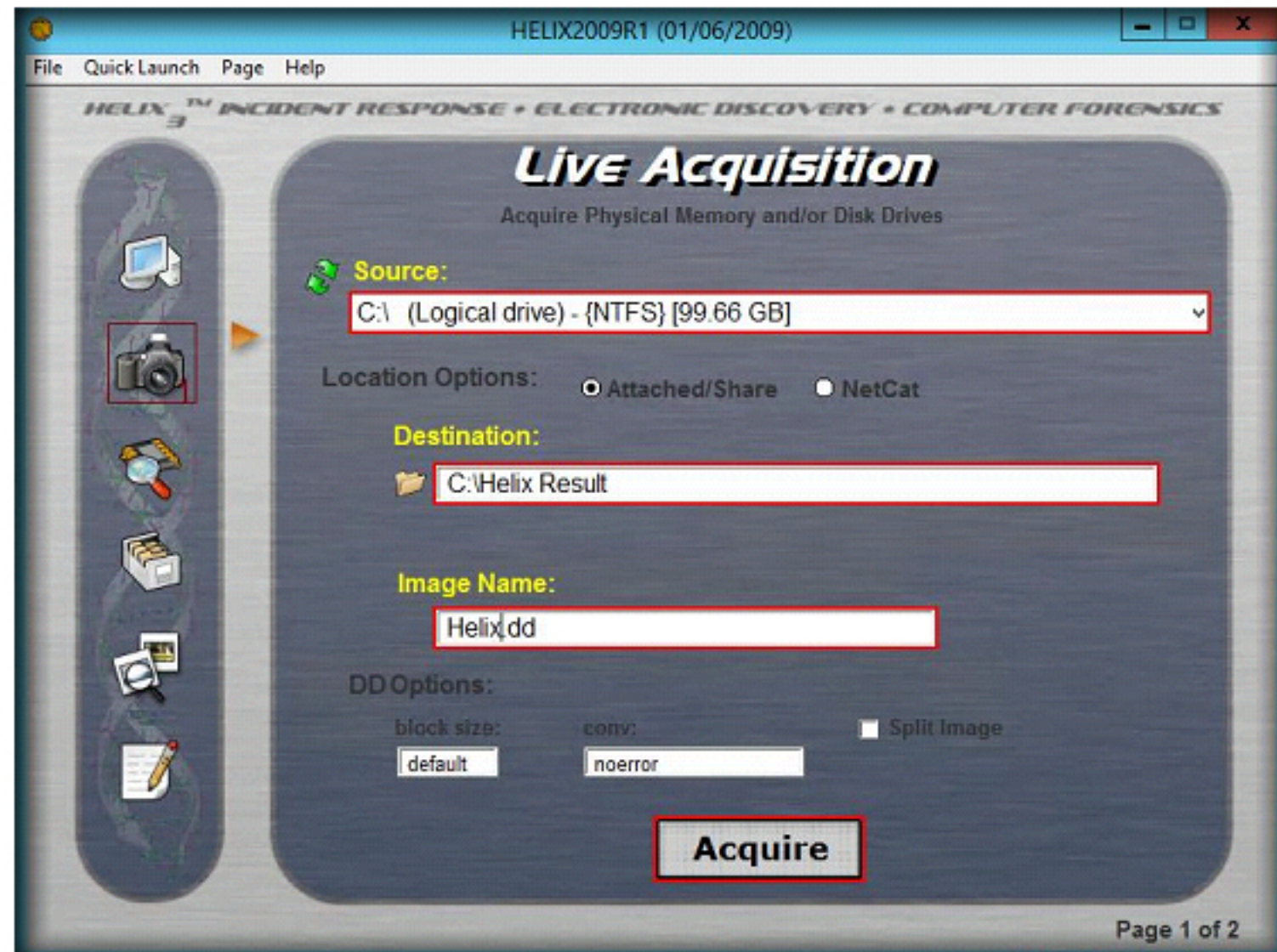


FIGURE 4.6: Helix Acquisition Step 1



11. To proceed to step 2 click the  button. To create an image of a folder with the help of AccessData FTK Imager, click **Imager**.



Helix is a customized distribution of Ubuntu Linux. Helix is more than just a bootable live CD. You can still boot into a customized Linux environment that includes customized Linux kernels, excellent hardware detection, and many applications dedicated to incident response and forensics.

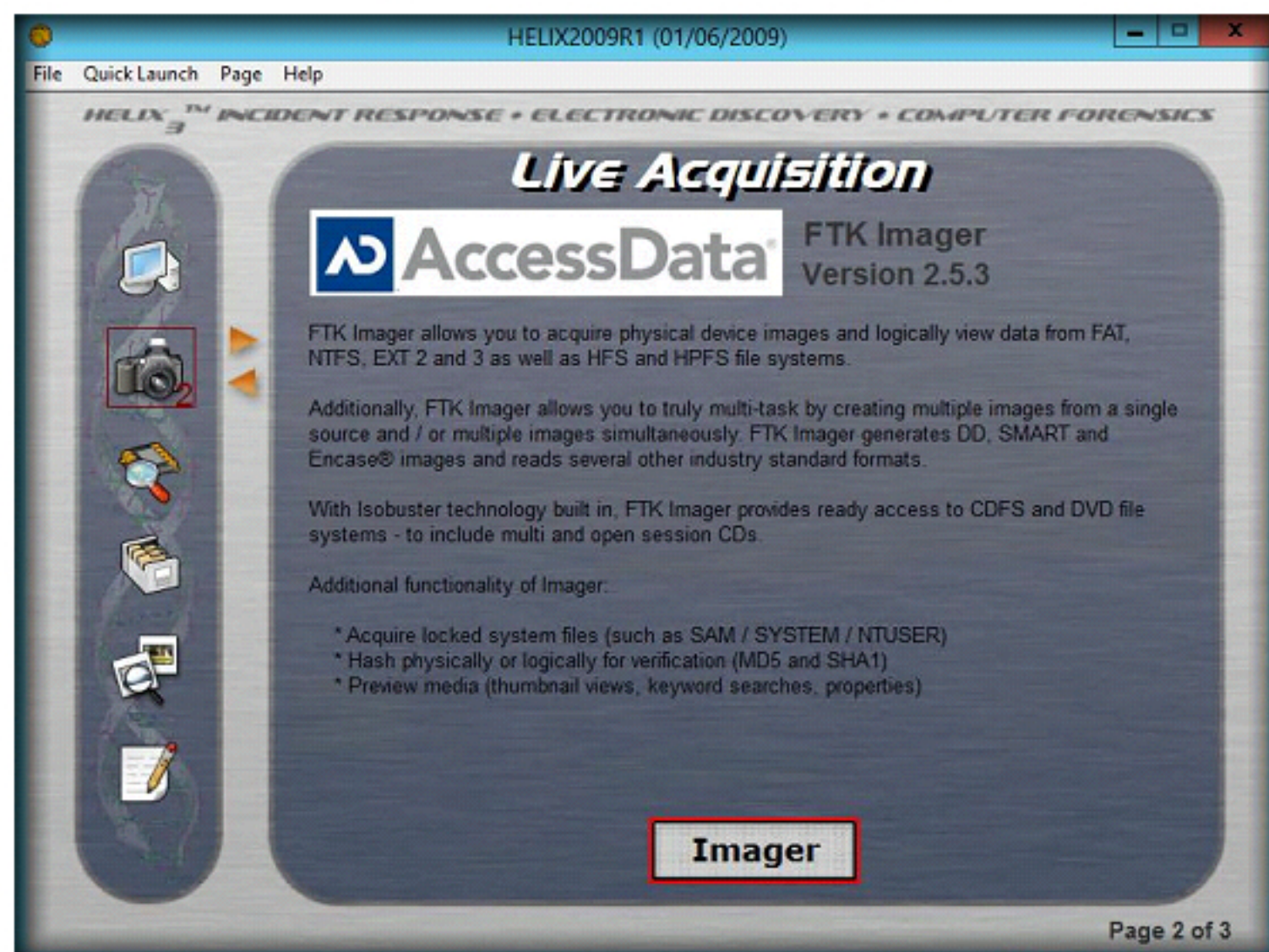


FIGURE 4.7: Helix Acquisition Step 2

TASK 3

Creating Disk Image

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

Note: We can also create an image of a physical drive, logical drive, image file, the contents of a folder, and a Fernico device (multiple CD/DVD).

12. It will launch Access Data FTK Imager. Now go to the **File** menu from menu bar and click **Create Disk Image...**

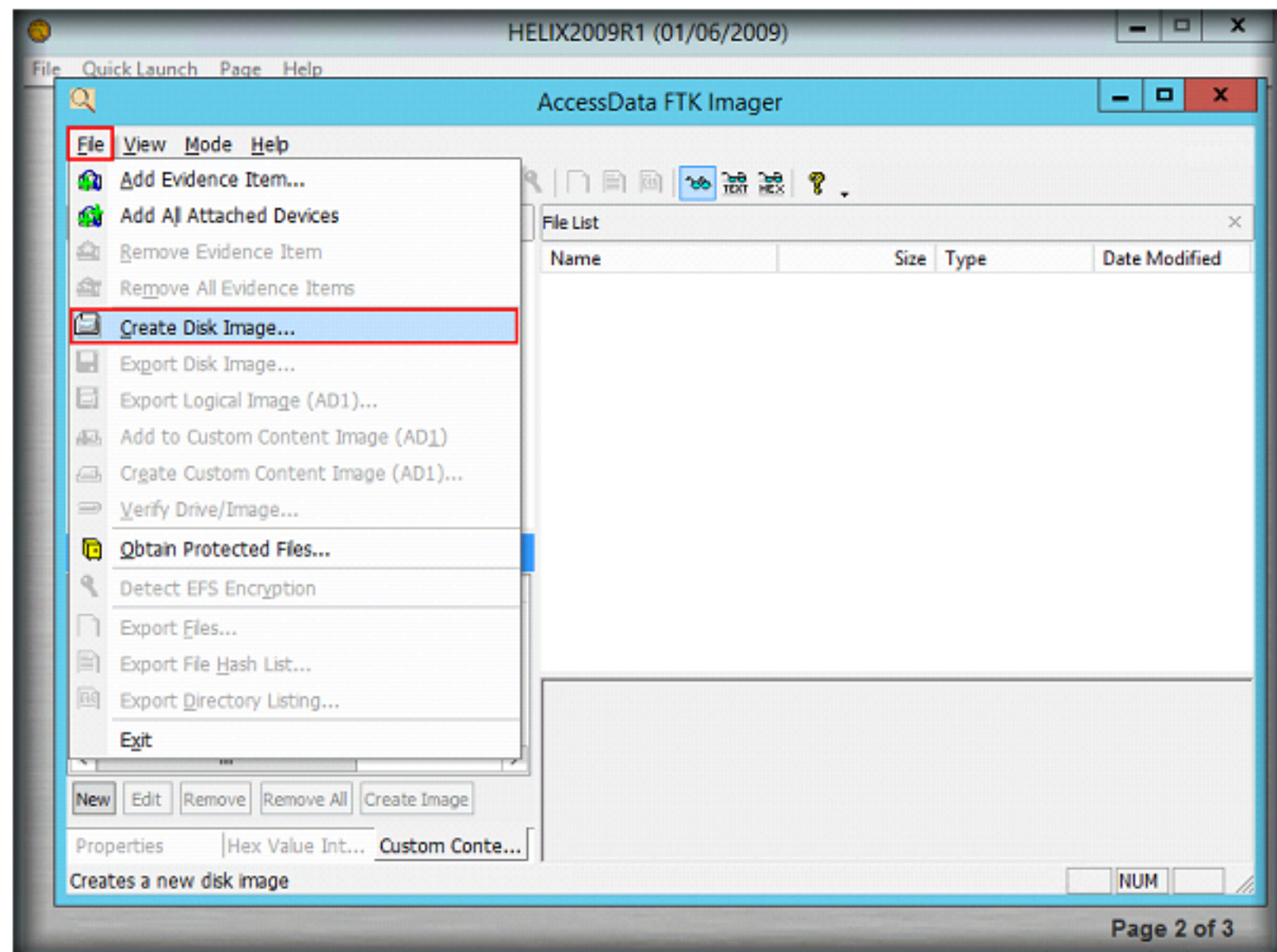


FIGURE 4.8: Helix Acquisition AccessData FTK Imager

13. Choose **Contents of a Folder** as the source evidence type, and then click **Next** to create an image.

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

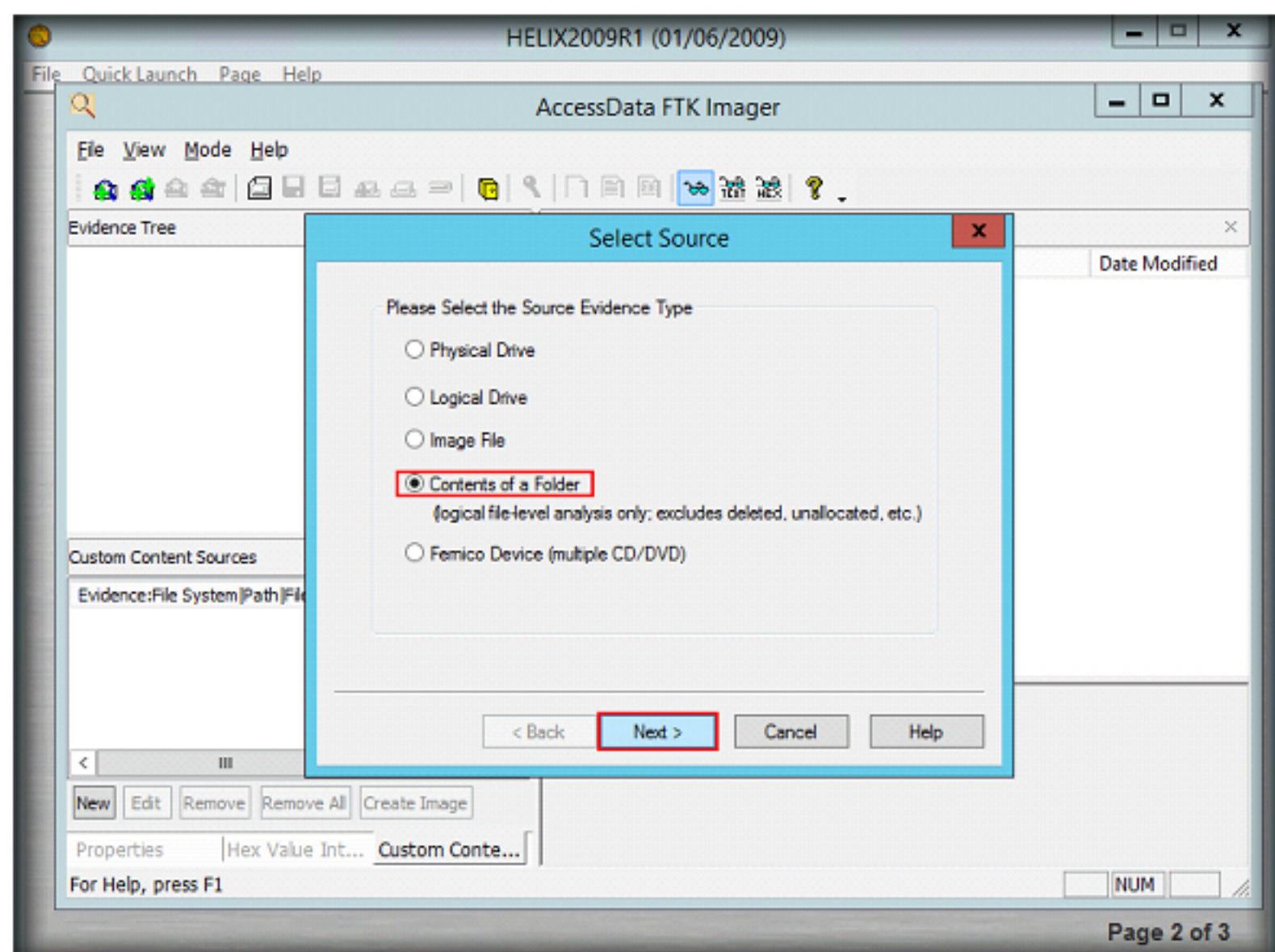


FIGURE 4.9: Helix Acquisition AccessData FTK Imager Select Source

14. AccessData FTK Imager will prompt you with a warning; if you want to continue click **Yes**.

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

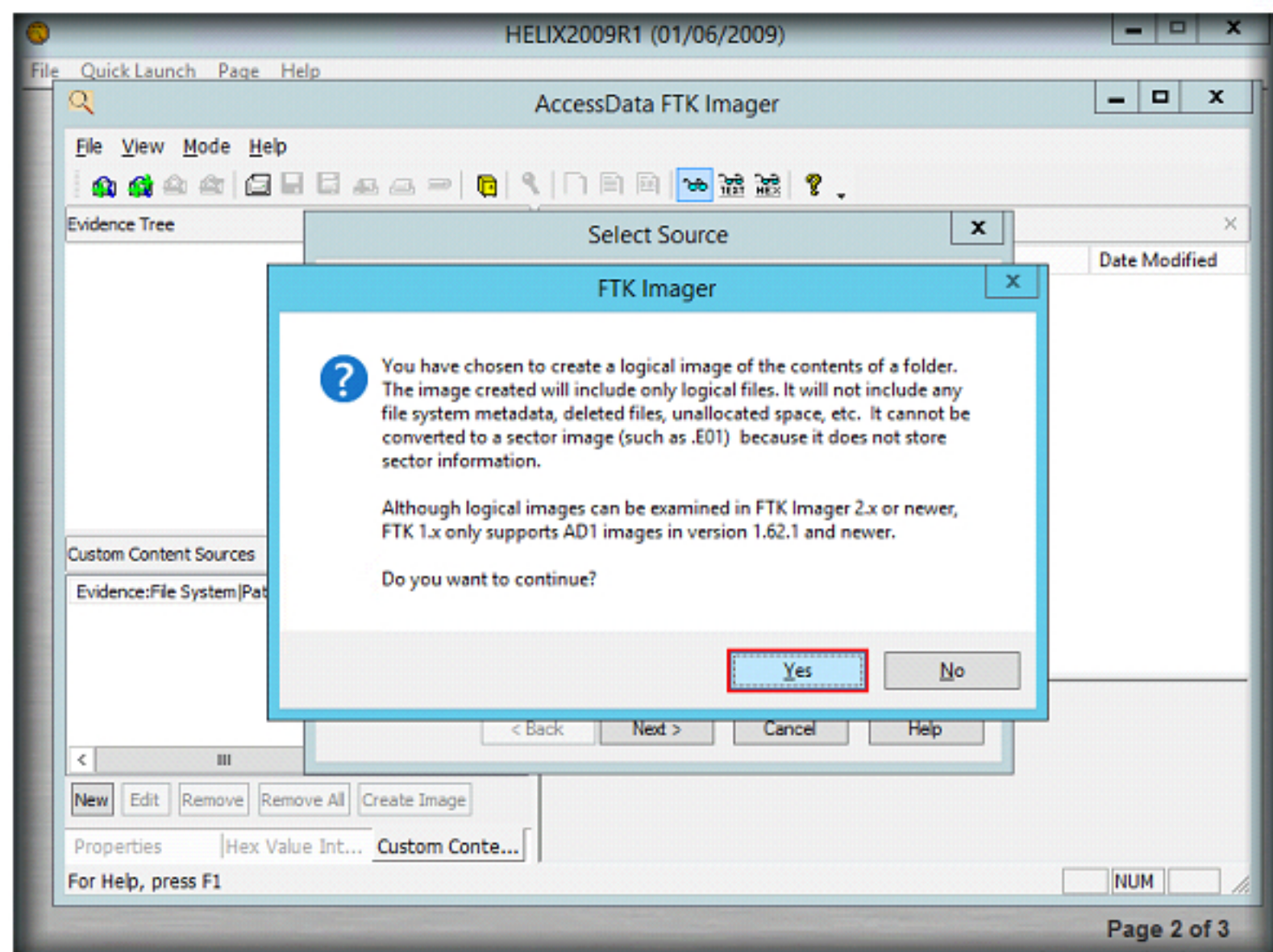


FIGURE 4.10: Helix Acquisition AccessData FTK Imager Warning

15. Now click **Browse** and select a folder, in this case, **C:\CHFI-Tools\Evidence Files\Image Files**, and then click **Finish**.

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

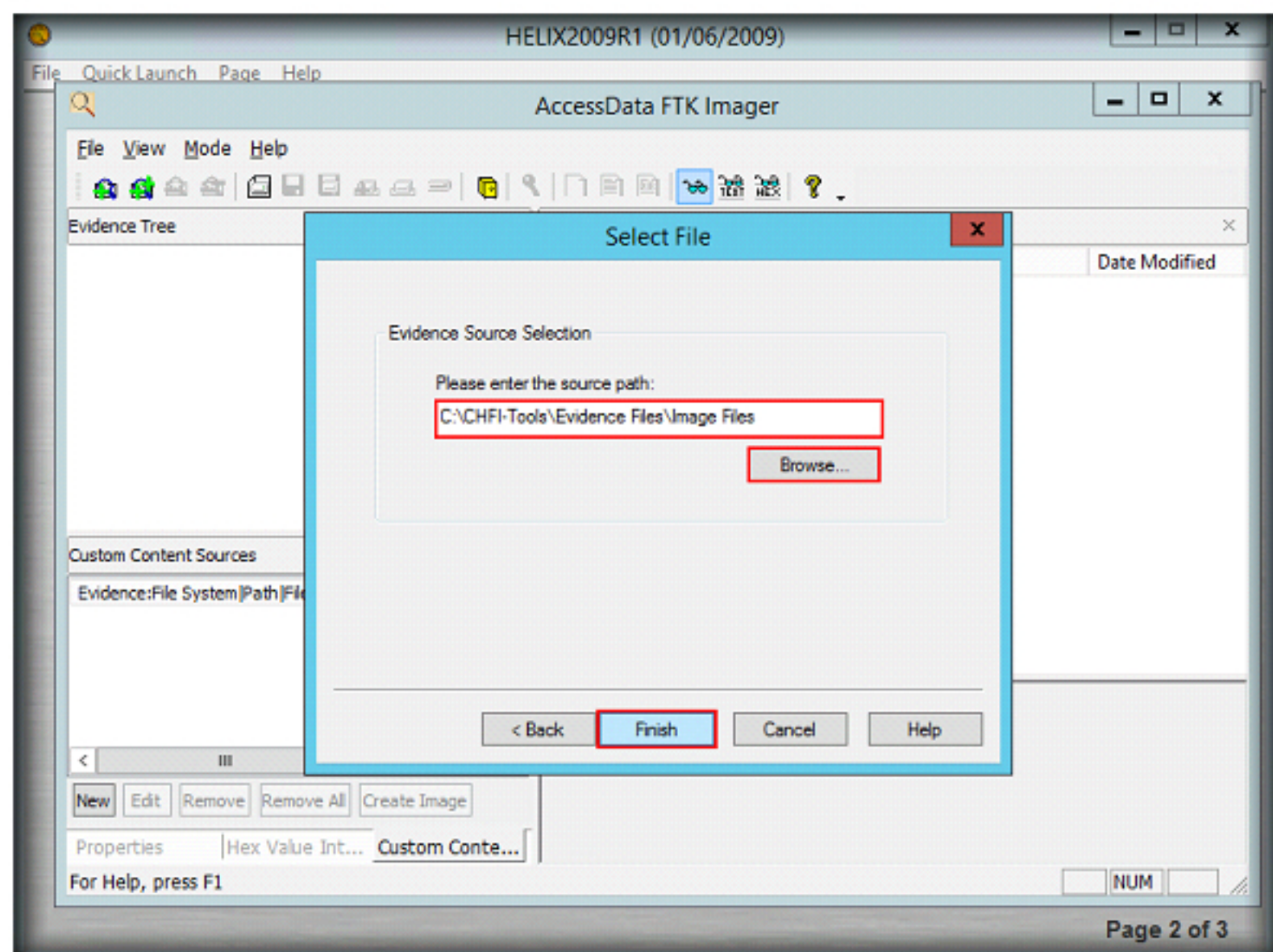


FIGURE 4.11: Helix Acquisition AccessData FTK Imager folder path to create an image

16. Click the **Add** button.

17. **Evidence Item Information** wizard appears, fill in the details, and click **Next**.

Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).

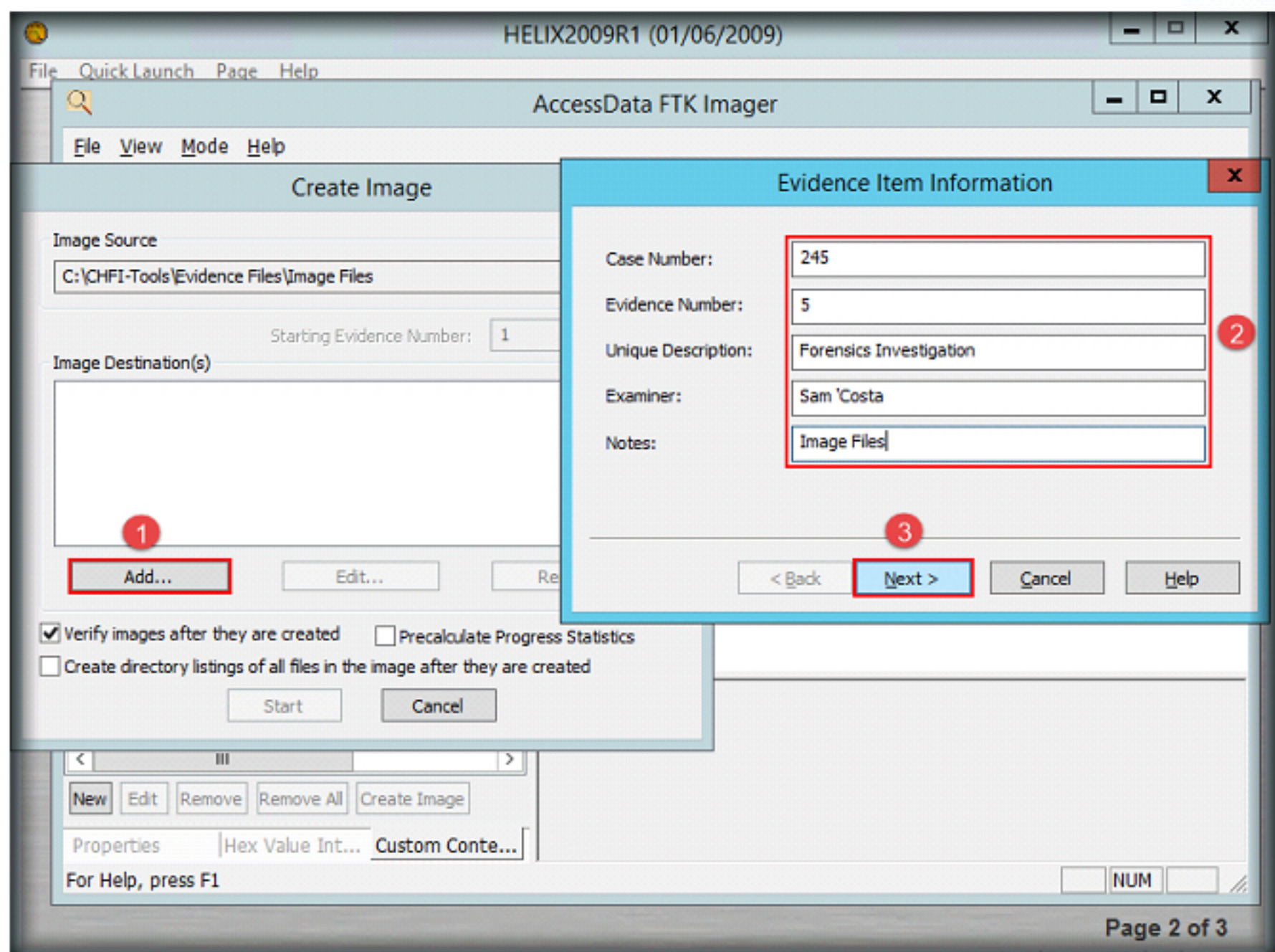


FIGURE 4.12: Helix Acquisition AccessData FTK Imager Evidence Item Imager

18. Now click the **Browse** button to give a destination path (in this lab we have created a folder named **Helix Result** in **C:** and saved the result in **C:\Helix Result**), enter an Image Filename excluding the extension, and click **Finish**.

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

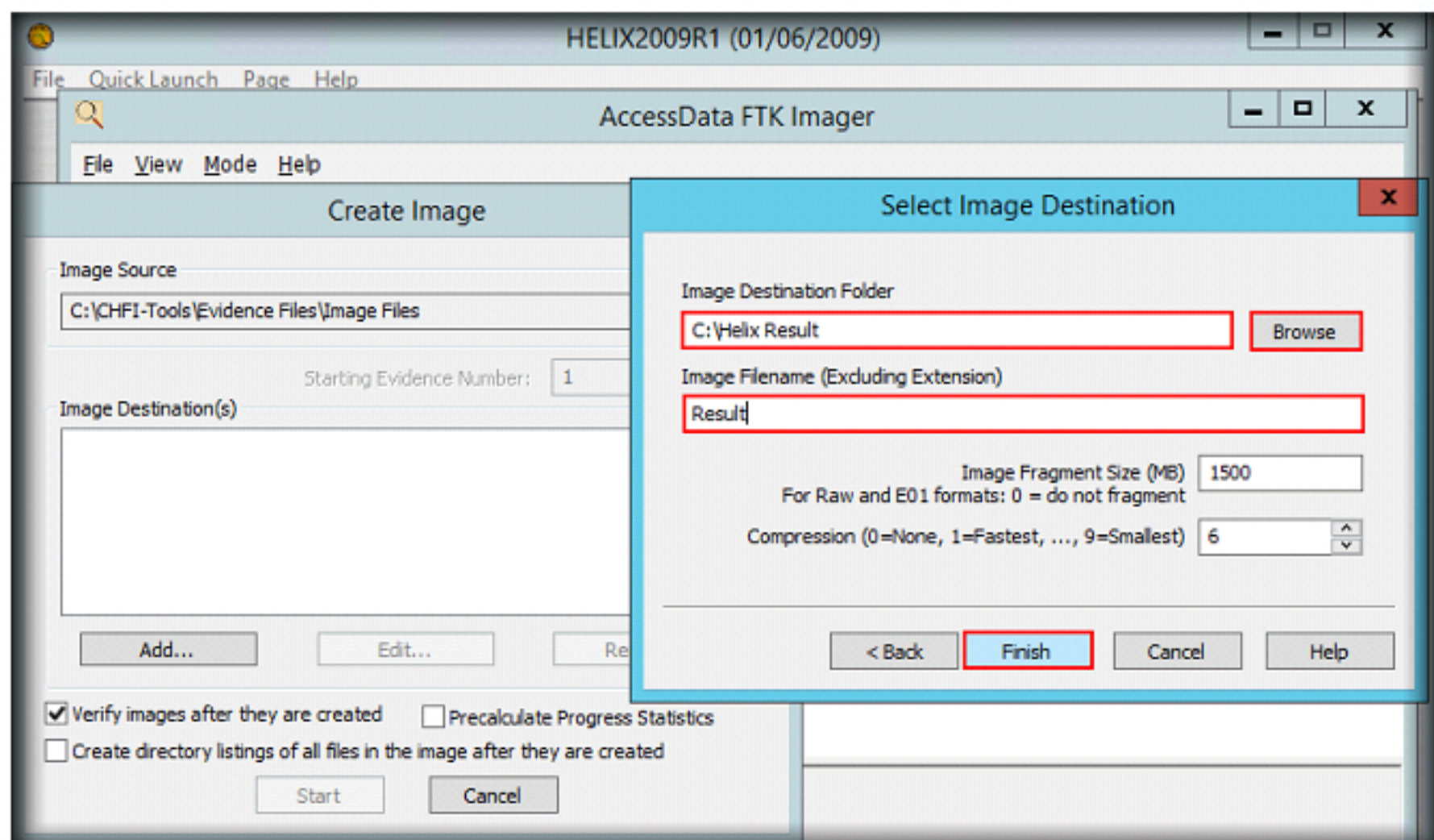


FIGURE 4.13: Helix Acquisition AccessData FTK Imager Select Image Destination

19. Now click the **Start** button in the **Create Image** wizard to create an image of the folder contents.

Helix is also unique in that it includes a Win32-based autorun toolset, giving users quick access to common forensic tools not found in Linux.

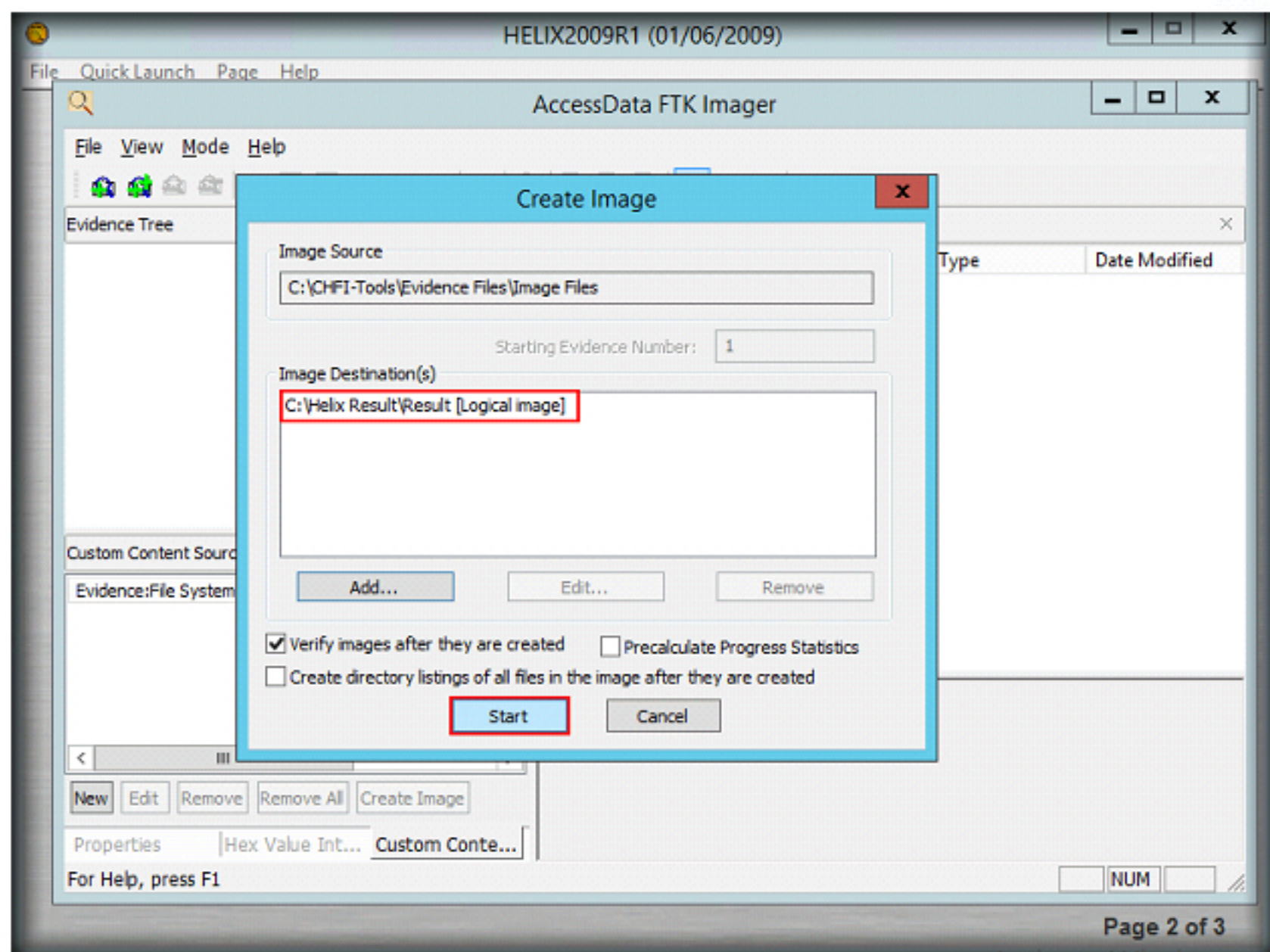


FIGURE 4.14: Helix Acquisition AccessData FTK Imager Create Image

20. After completion, the **Drive/Image Verify Results** summary will pop up. Click **Close** and then click **Close** in the **Create Image** wizard.

Helix is a customized distribution of the Knoppix Live Linux CD. Helix is more than just a bootable live CD.

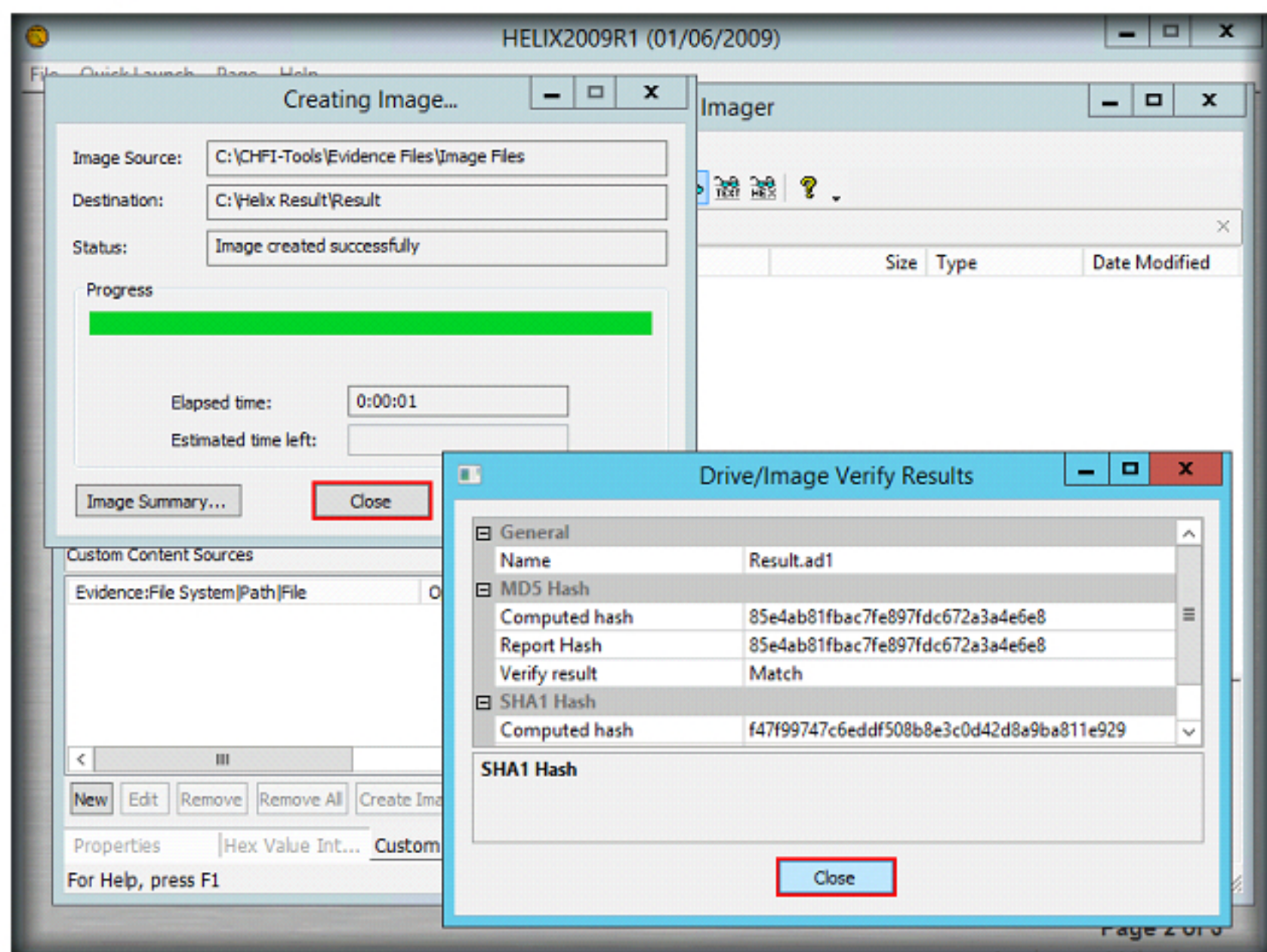


FIGURE 4.15: Helix Acquisition AccessData FTK Imager Drive/Image Result

21. Access Data FTK Imager created an image of a folder, to check this, navigate to the **C:\Helix Result** path mentioned in the destination.

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

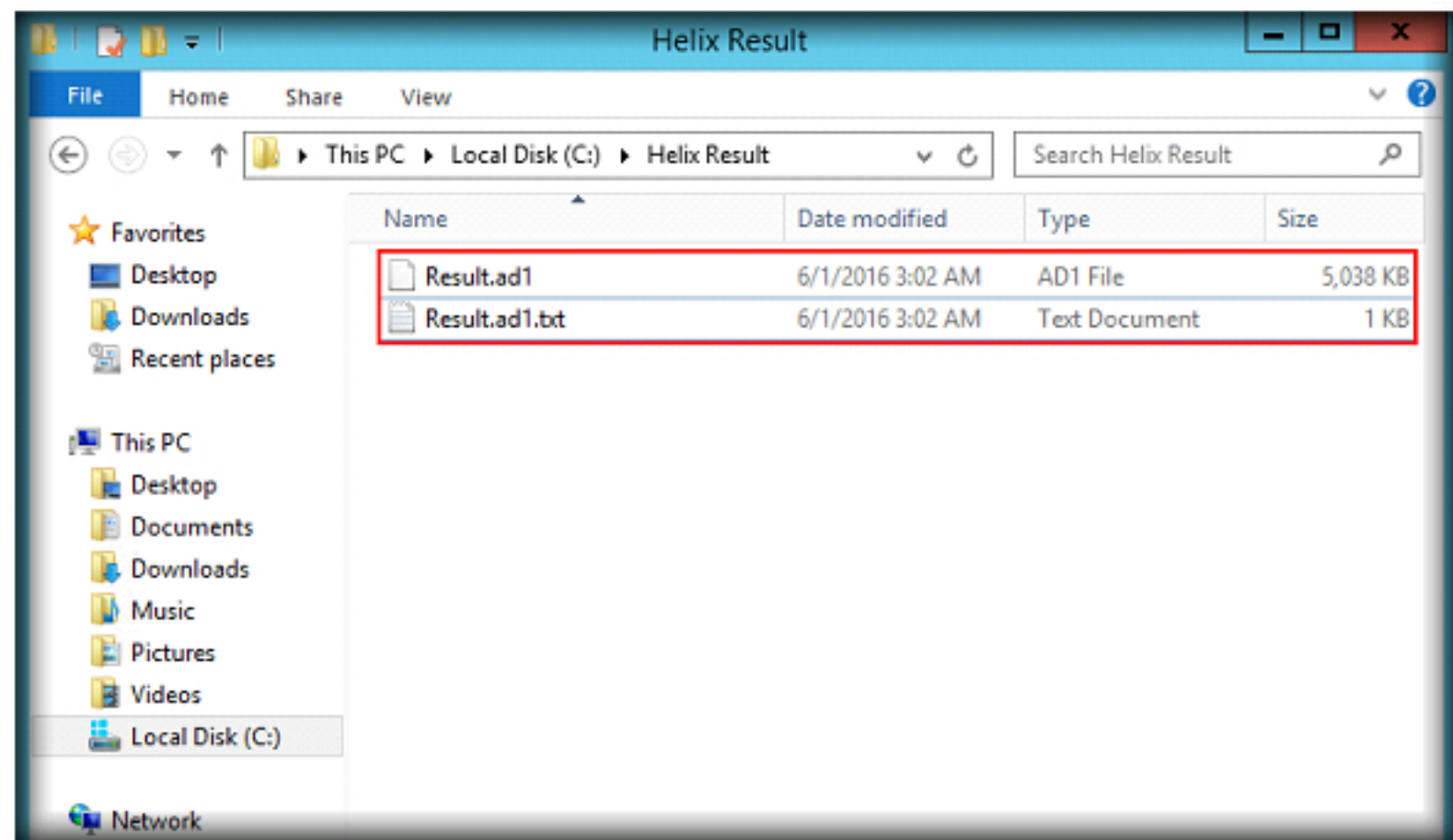


FIGURE 4.16: Helix Acquisition AccessData FTK Imager destination folder

22. Now, you can examine this image using Access Data FTK Imager. In this lab, we already have an evidence item/Disk Image located at **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image (DiskPartitionRawImage.dd)**, and we will be analyzing this image, instead of the one which we created in the previous steps.
23. Go to **File → Add Evidence Item** from the menu bar to add an evidence item for investigation.

To prevent accidental or intentional manipulation of the original evidence, FTK Imager makes a bit-for-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or drive free space.

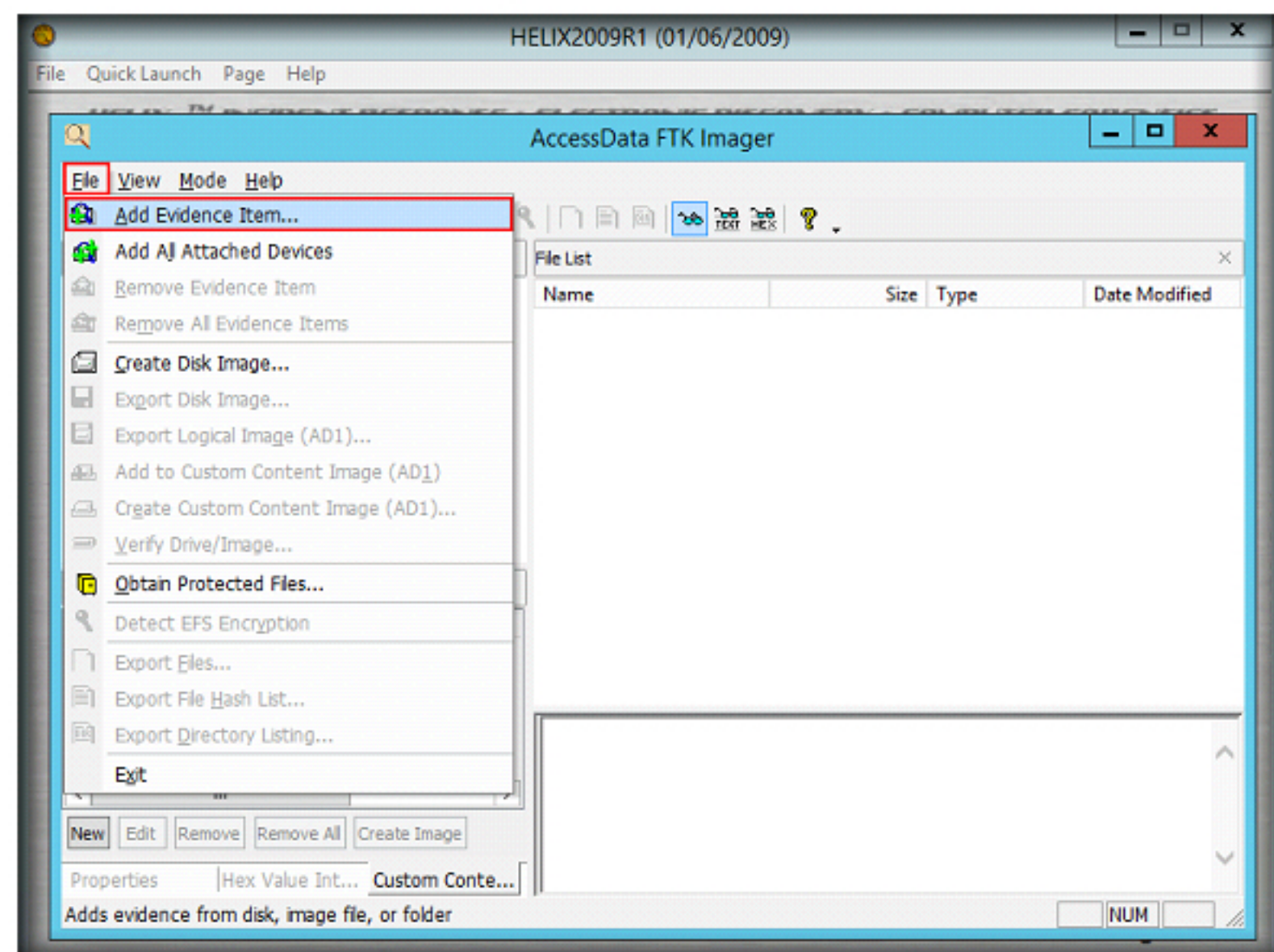


FIGURE 4.17: Helix Acquisition AccessData FTK Imager Add Evidence Item

24. Choose Image File option for investigating the image file, and click **Next**.

FTK Imager can be installed to the computer where it will be used, or it can be run from a portable device such as a USB thumb drive connected to a machine in the field, so there is no need to install it on a suspect's computer to capture its image.

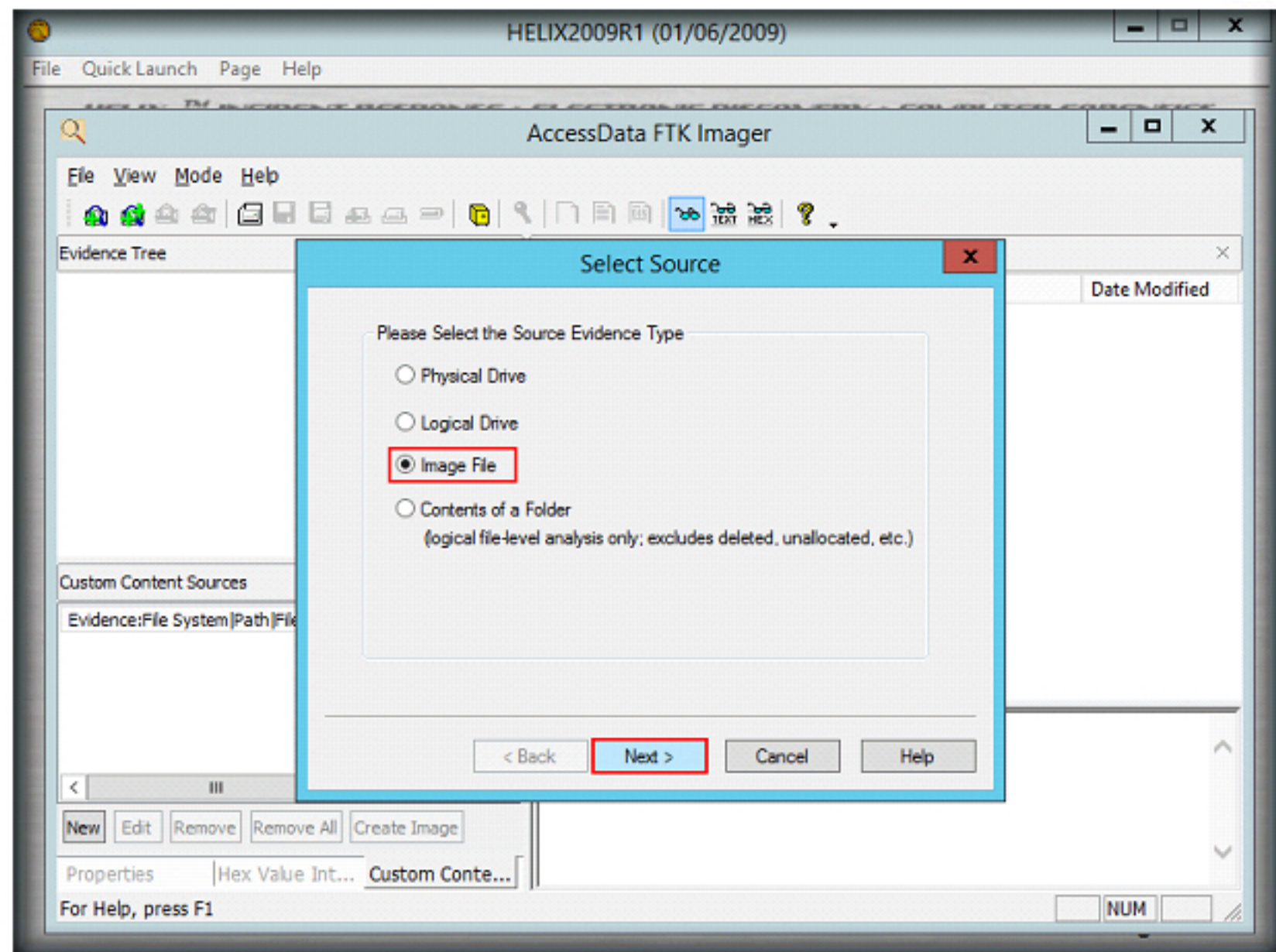


FIGURE 4.18: Helix Acquisition AccessData FTK Imager Select Source

25. Click **Browse**, navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd** and then, click **Finish**.

`/CreateDirListing=` creates a directory listing file in the folder where FTK Imager.exe is run from. `/VerifyImage=` verifies an image when you specify the image path and filename. `/EnableDebugLog=` enables logging to the FTKImageDebug.log file created in the folder you run FTK Imager.exe from.

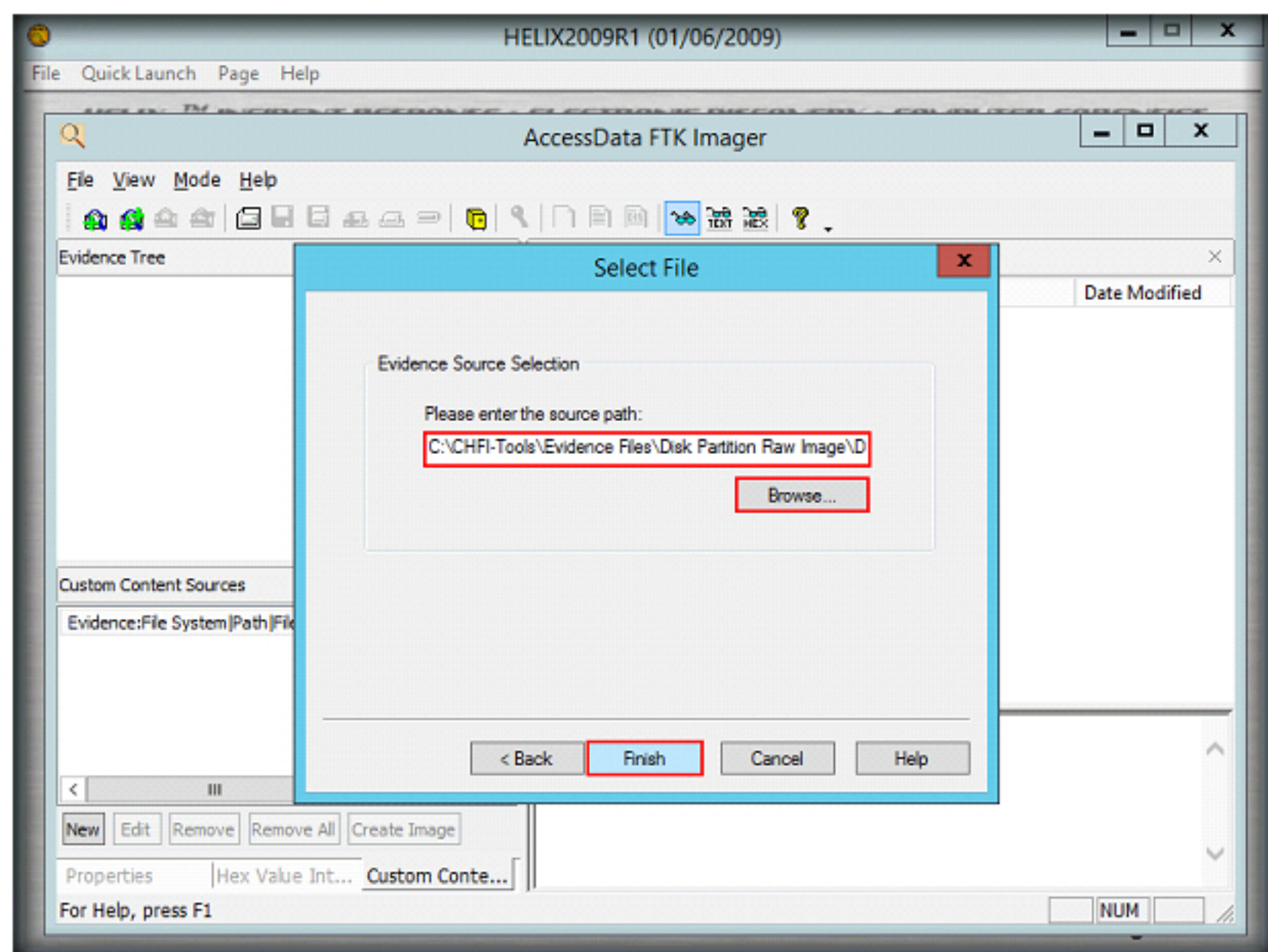


FIGURE 4.19: Helix Acquisition AccessData FTK Imager Selecting File

26. The image file is displayed in the **left pane** of the window. Now, expand **DiskPartitionRawImage.dd** → **Drive [NTFS]** → **[root]** and click on **Set of Images updated** folder. The contents of the folder are displayed in the right pane. Click on the desired image file to view the respective image in the lower section of the window.

Note: The application may not be able to open other file formats.

If you fail to specify an image when using the `/CreateDirListing=` or `/VerifyImage=` options, an error message appears indicating no image was found.

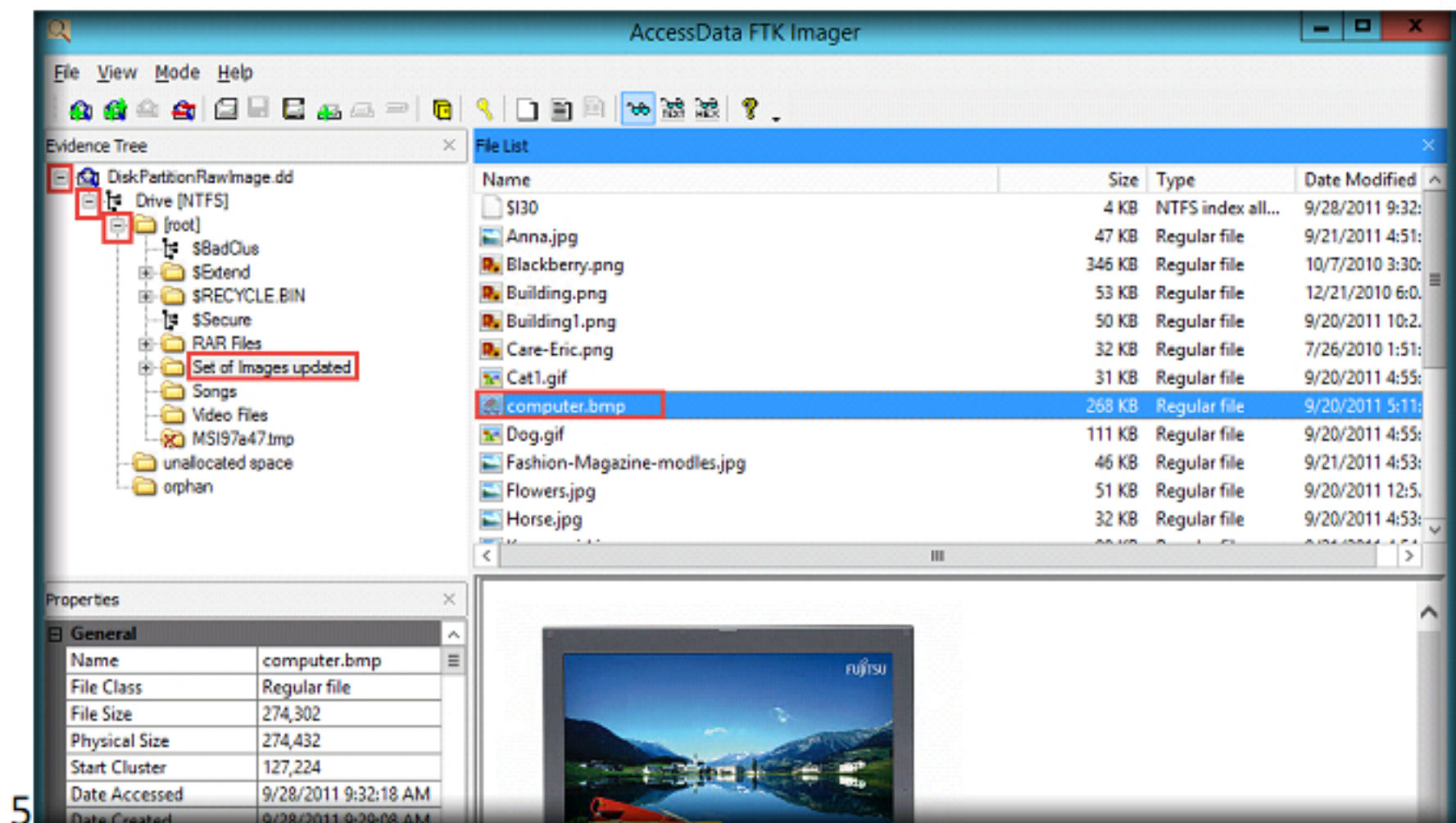


FIGURE 4.20: Helix Acquisition AccessData FTK Imager evidence content

27. The properties of the image file can be viewed by clicking the **Properties** tab in the lower left corner of Access Data FTK Imager GUI. Further details of the image file can be obtained by clicking other tabs besides the **Properties** tab.

The Evidence Tree pane (upper-left pane) displays added evidence items in a hierarchical tree. At the root of the tree are the selected evidence sources. Listed below each source are the folders and files it contains.

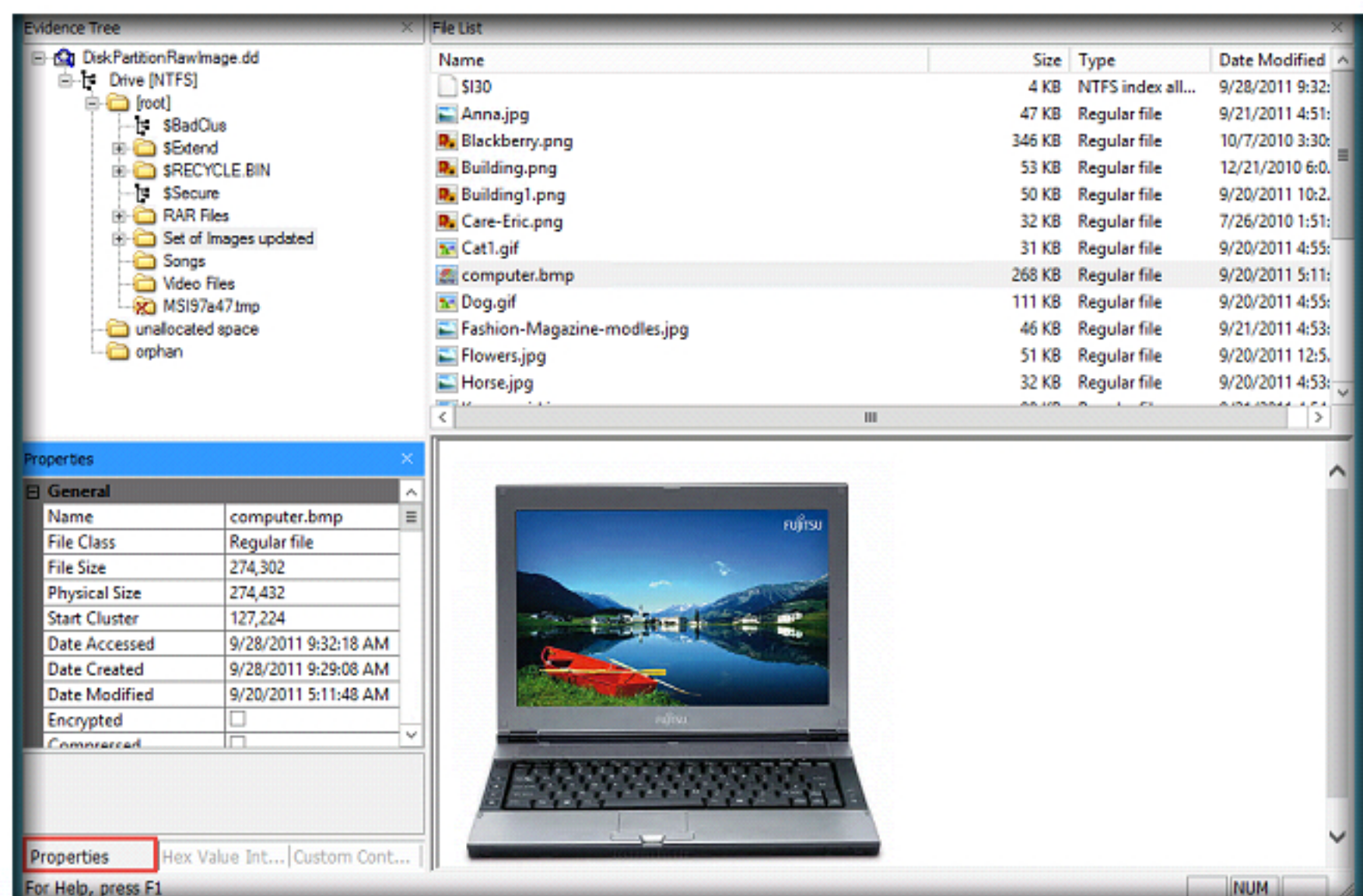


FIGURE 4.21: Helix Acquisition AccessData FTK Imager Properties tab

28. Now close the Access Data FTK Imager by clicking **Exit** in the **File** menu.

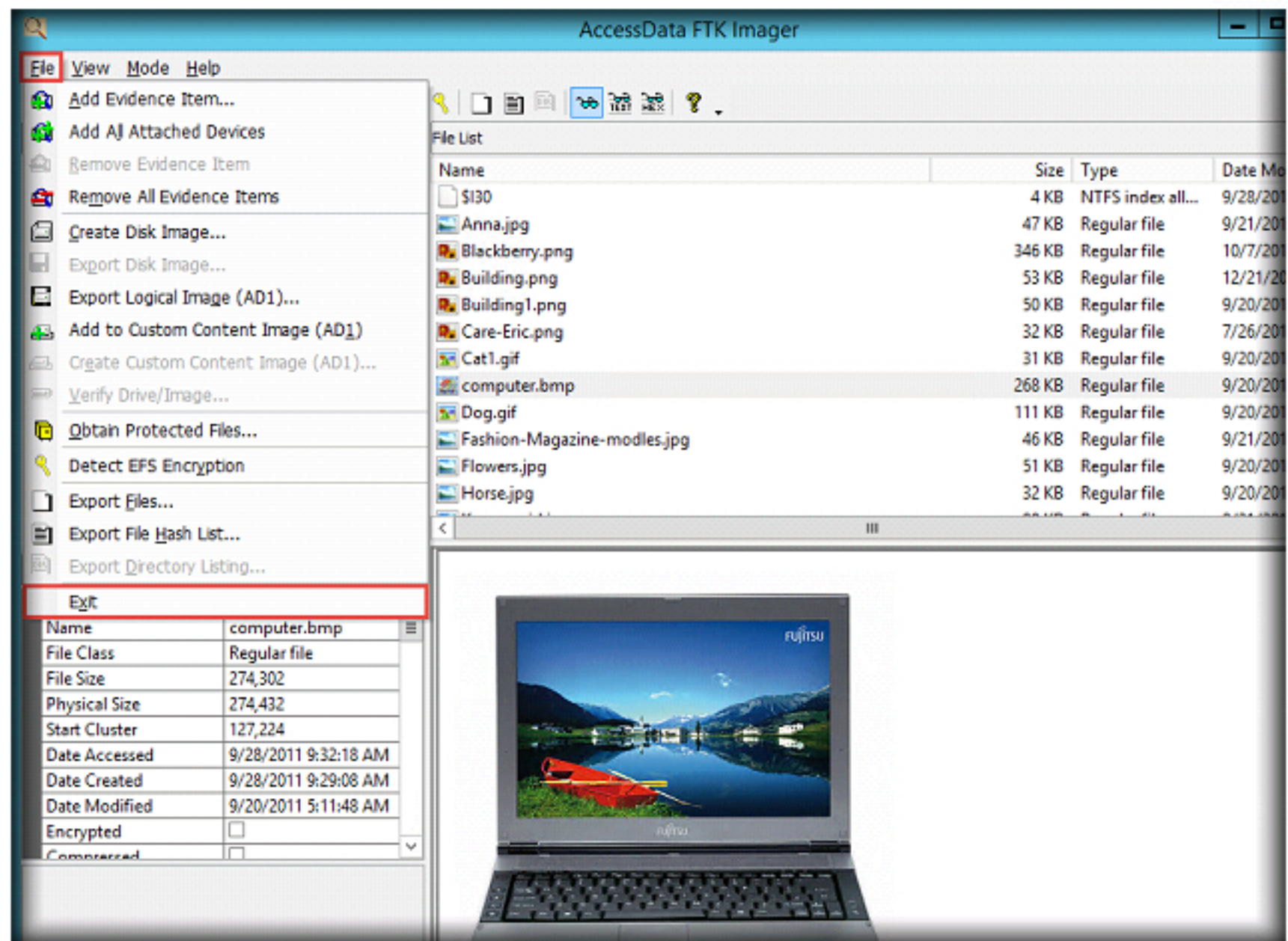


FIGURE 4.22: Helix Acquisition AccessData FTK Imager Closing

TASK 4

Disk Preview

29. Now click **Incident Response** icon in the left pane of Helix GUI.

30. Click **Agile Risk Management's Nigilant32** icon on Page 1.

Nigilant32 is an incident response tool designed to capture as much information as possible from a running system with the smallest potential impact.

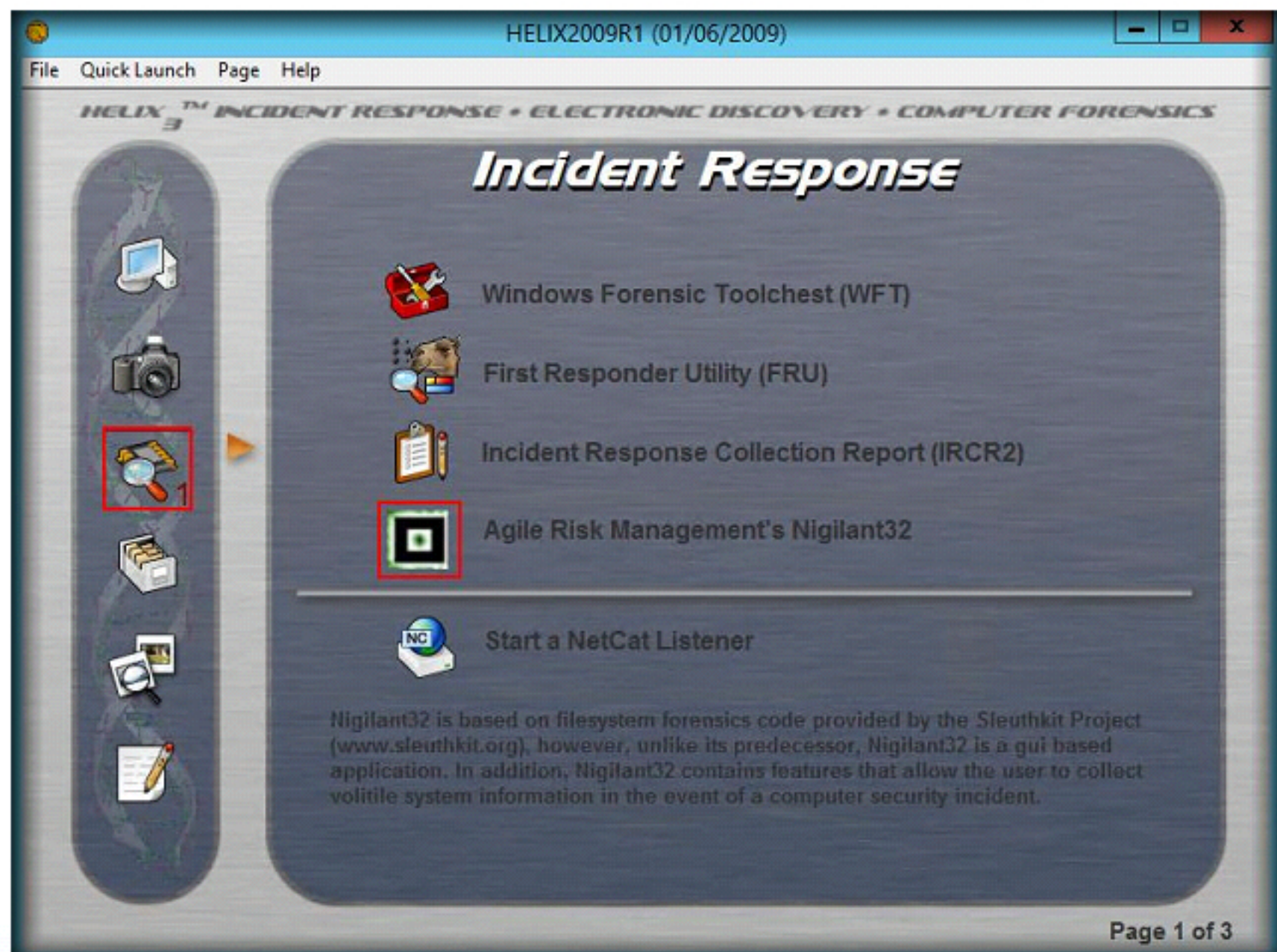


FIGURE 4.23: Helix Incident Response

31. It will prompt you with a **Notice**. Click **Yes**.

 Nigilant32 For First Responders: Using the SnapShot of Nigilant32, we can review and save a report of the running system that includes processes, services, user accounts, scheduled tasks, network ports, etc.

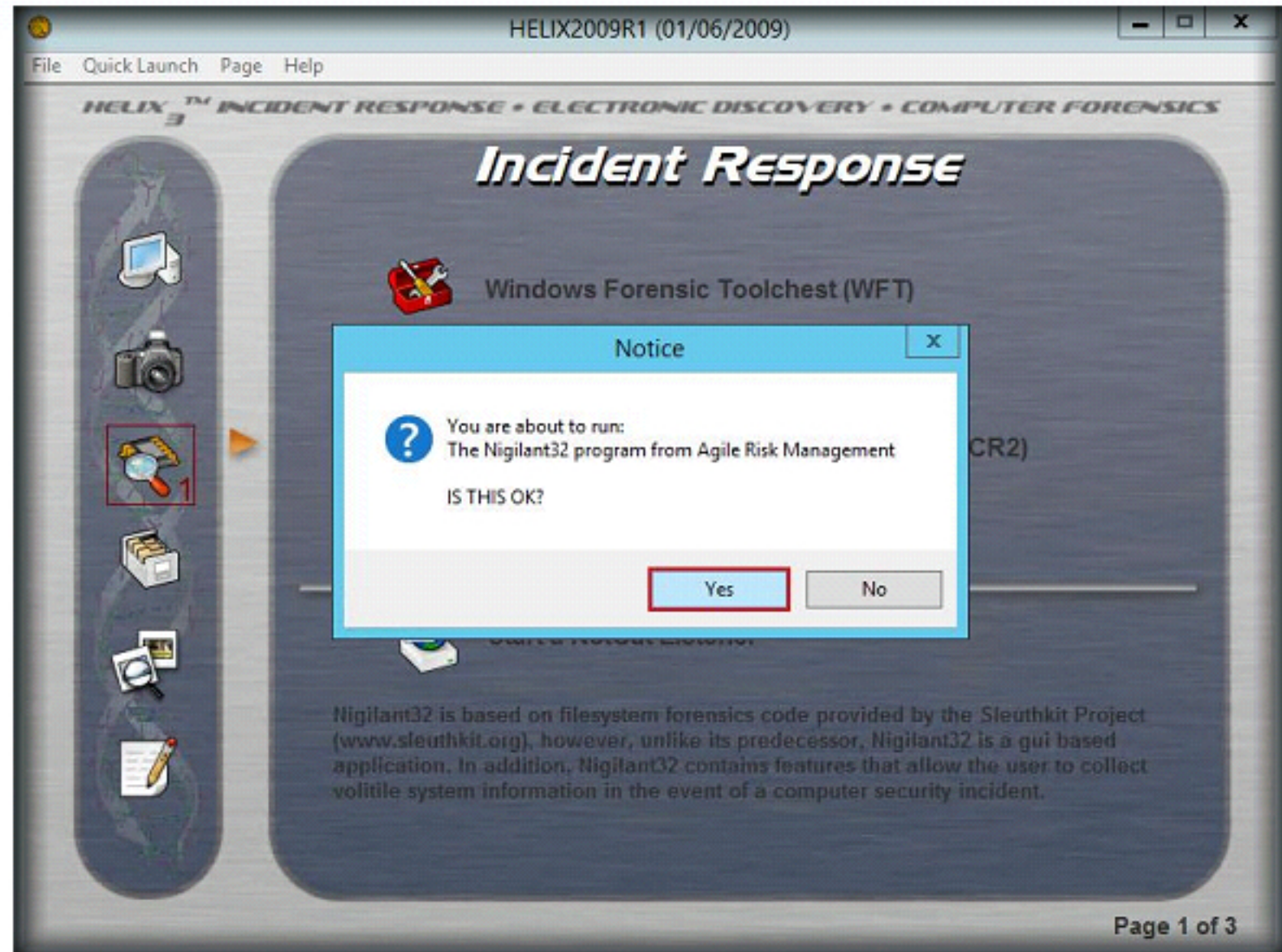


FIGURE 4.24: Helix Incident Response Nigilant32 notice

32. **Nigilant 32** pop-up appears, click the pop-up.

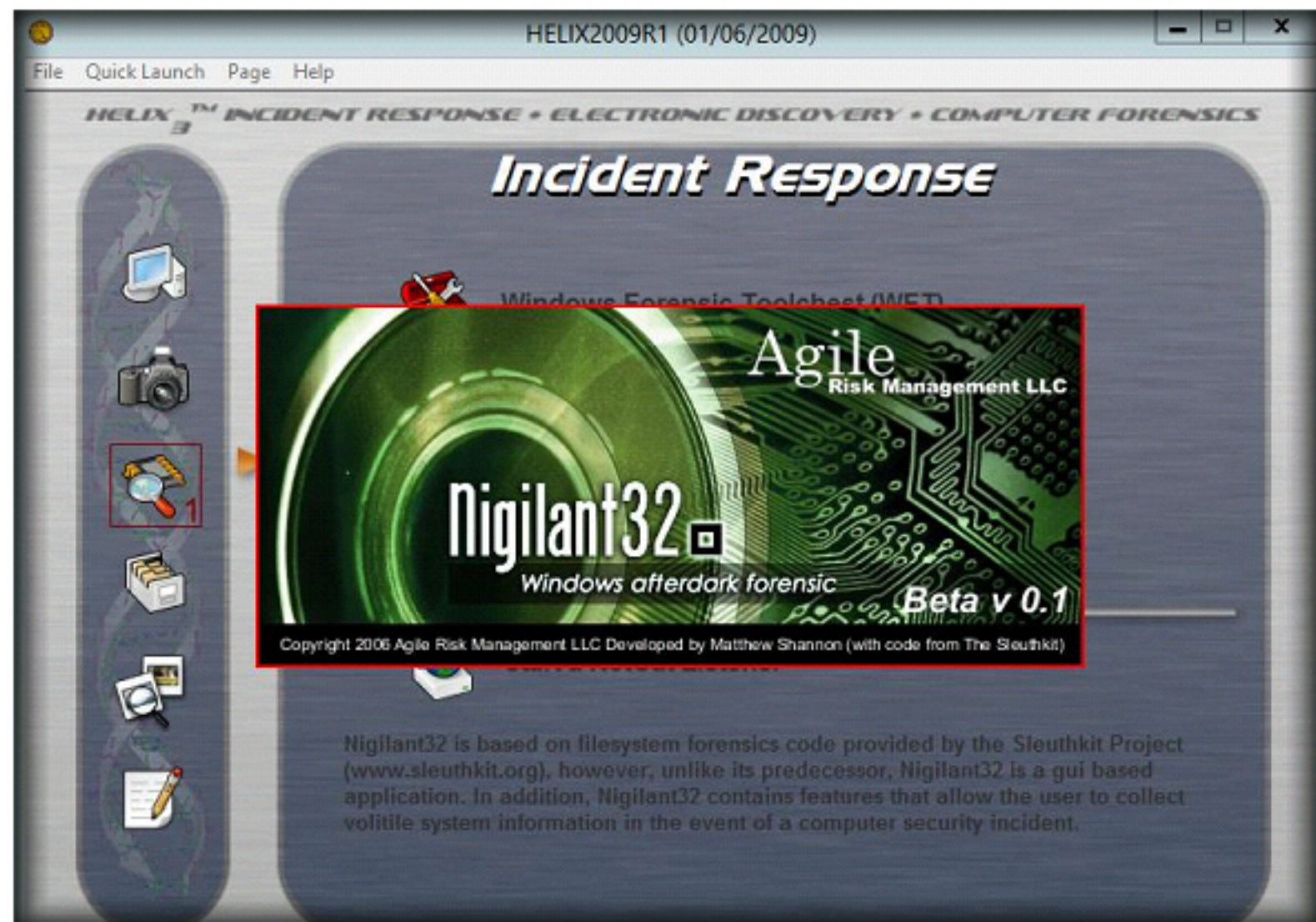


FIGURE 4.25: Helix Incident Response nigilant 32 pop-up

33. **Nigilant32 - Windows Afterdark Forensic** window appears as shown in the screenshot:

 **Nigilant32 For First Responders:** Filesystem Review: Using Nigilant32 we can explore the filesystem and possibly locate hidden files, folders, or recently deleted content, or extract files for offline analysis with limited risk of contamination.

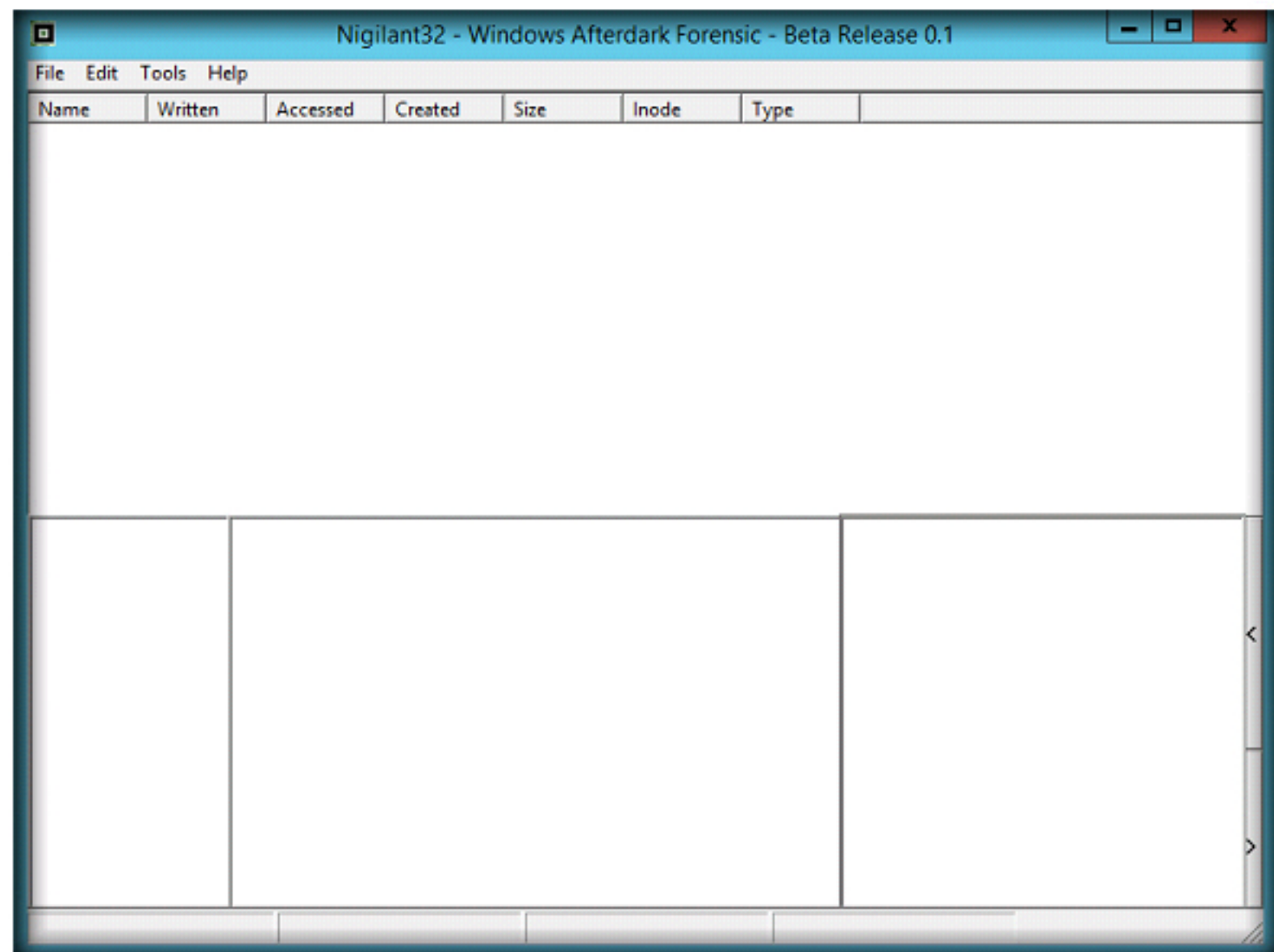


FIGURE 4.26: Helix Incident Response Nigilant32 main screen

34. Choose **File → Preview Disk...** to view the preview of the hard drives.

 **Nigilant32 For First Responders:** Using Active Memory Imaging: of Nigilant32, we can image the active physical memory (RAM) of the suspect workstation or server to secure portable media.

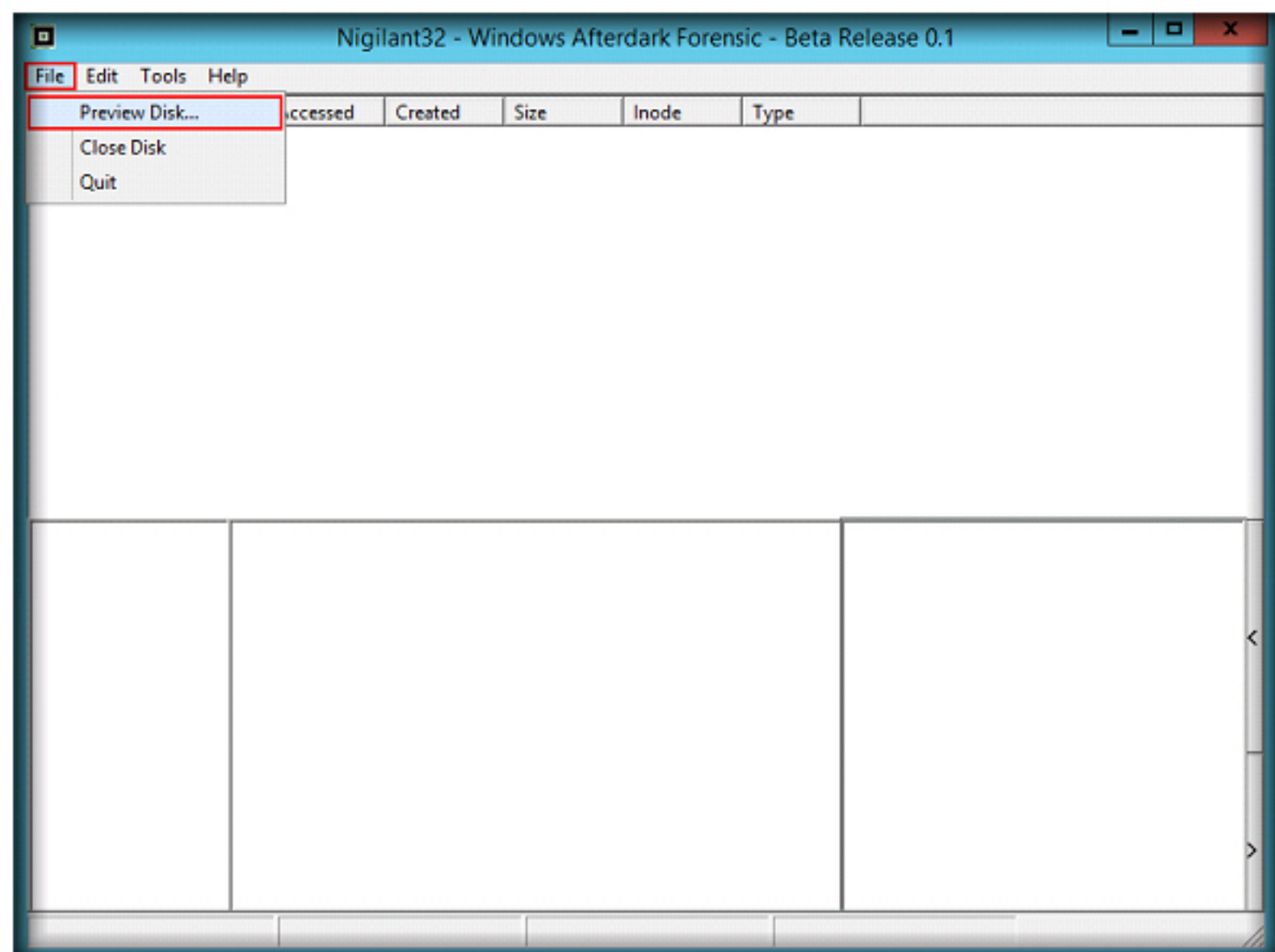


FIGURE 4.27: Helix Incident Response Nigilant32 Preview Disk

35. Select the drive to preview, and then click the **Apply** button.

Note: Do not select the **C Drive** (Contains system file).

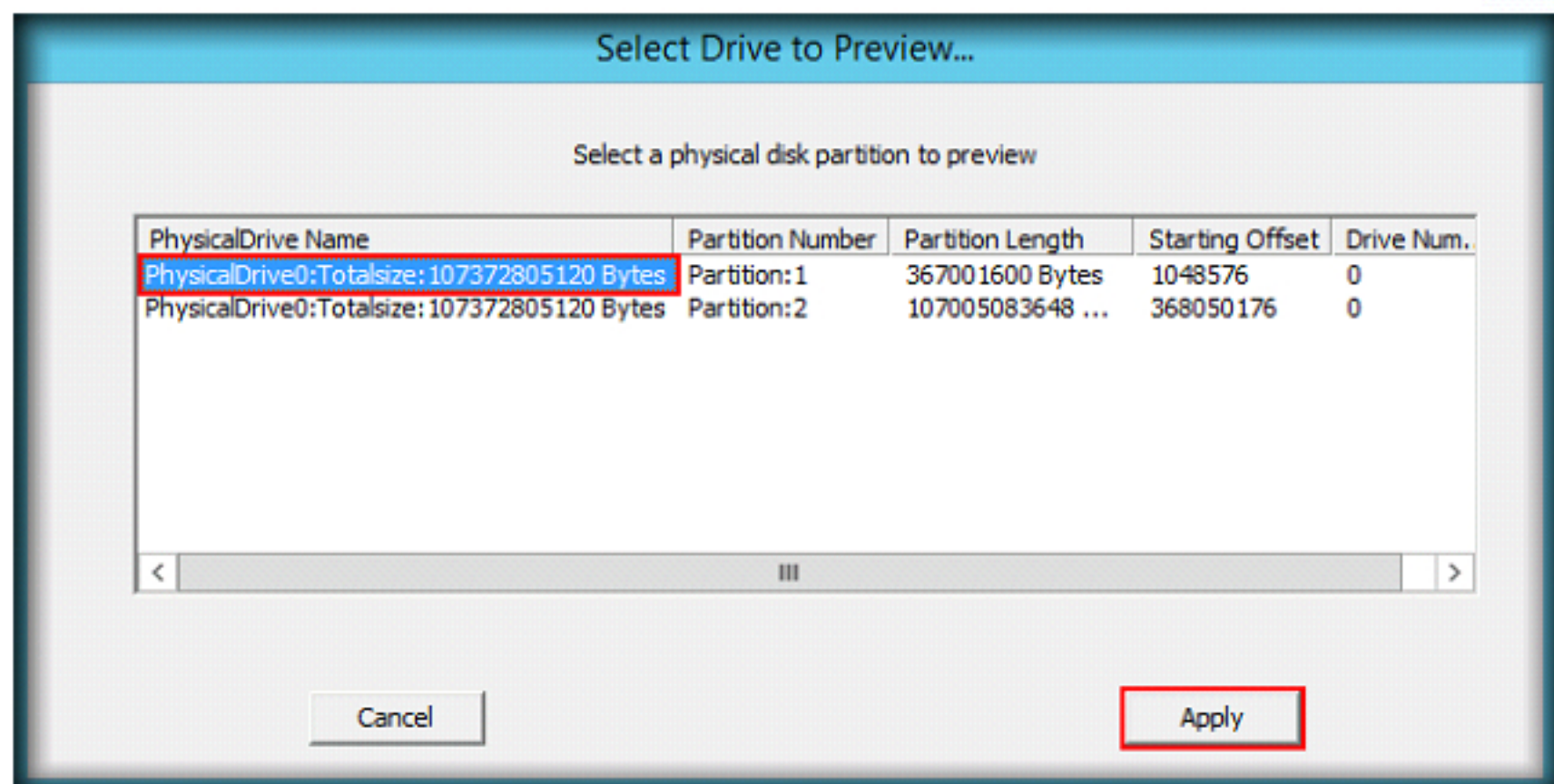


FIGURE 4.28: Helix Incident Response Nigilant32 selecting drive to preview

36. It displays the files and folders pertaining to the partition. Double-click on file to view the file content in the bottom pane of the window.

37. You may double-click a folder to view the contents in it.

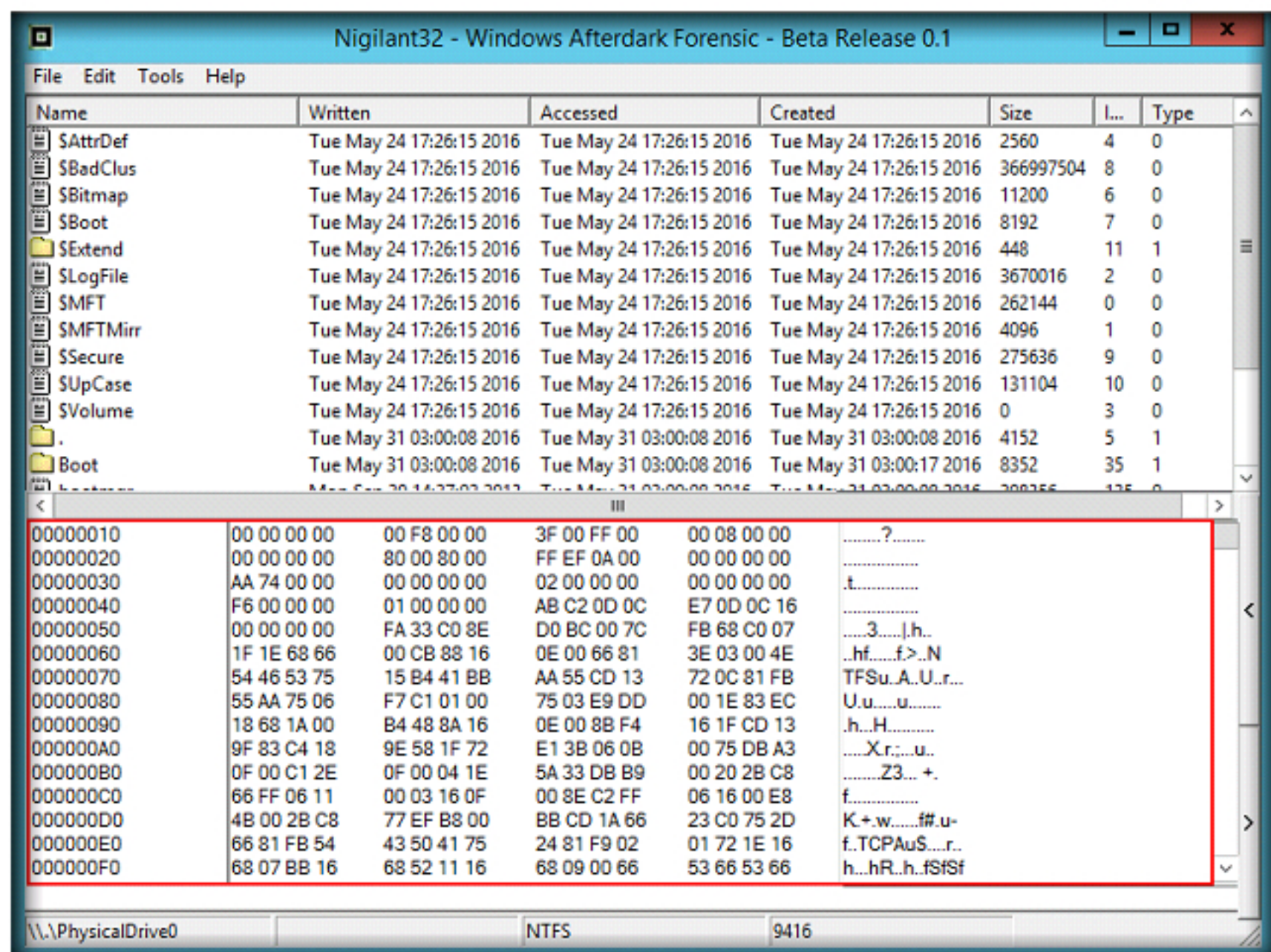


FIGURE 4.29: Helix Incident Response Nigilant32 Preview of the file

38. To take a snapshot of the computer, choose **Tools** → **Snapshot Computer**.

Helix also has a special Windows autorun side for Incident response and forensics.

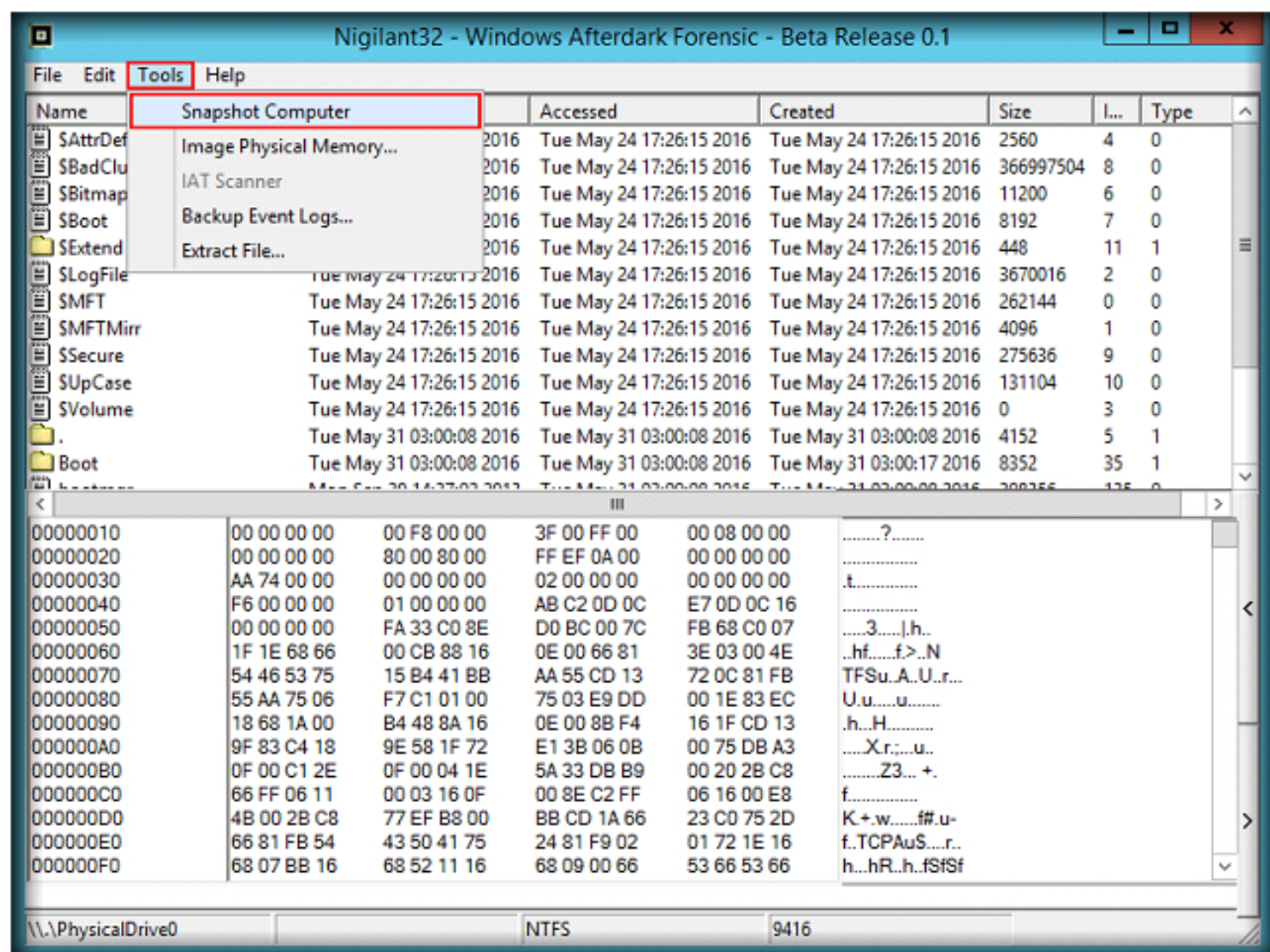


FIGURE 4.30: Helix Incident Response Nigilant32 Snapshot Computer

39. It will display the **Live Machine Snapshot** window. If you want to save the snapshot, click the **Save** button.

Helix focuses on Incident response and forensics tools. It is meant to be used by individuals who have a sound understanding of these techniques.

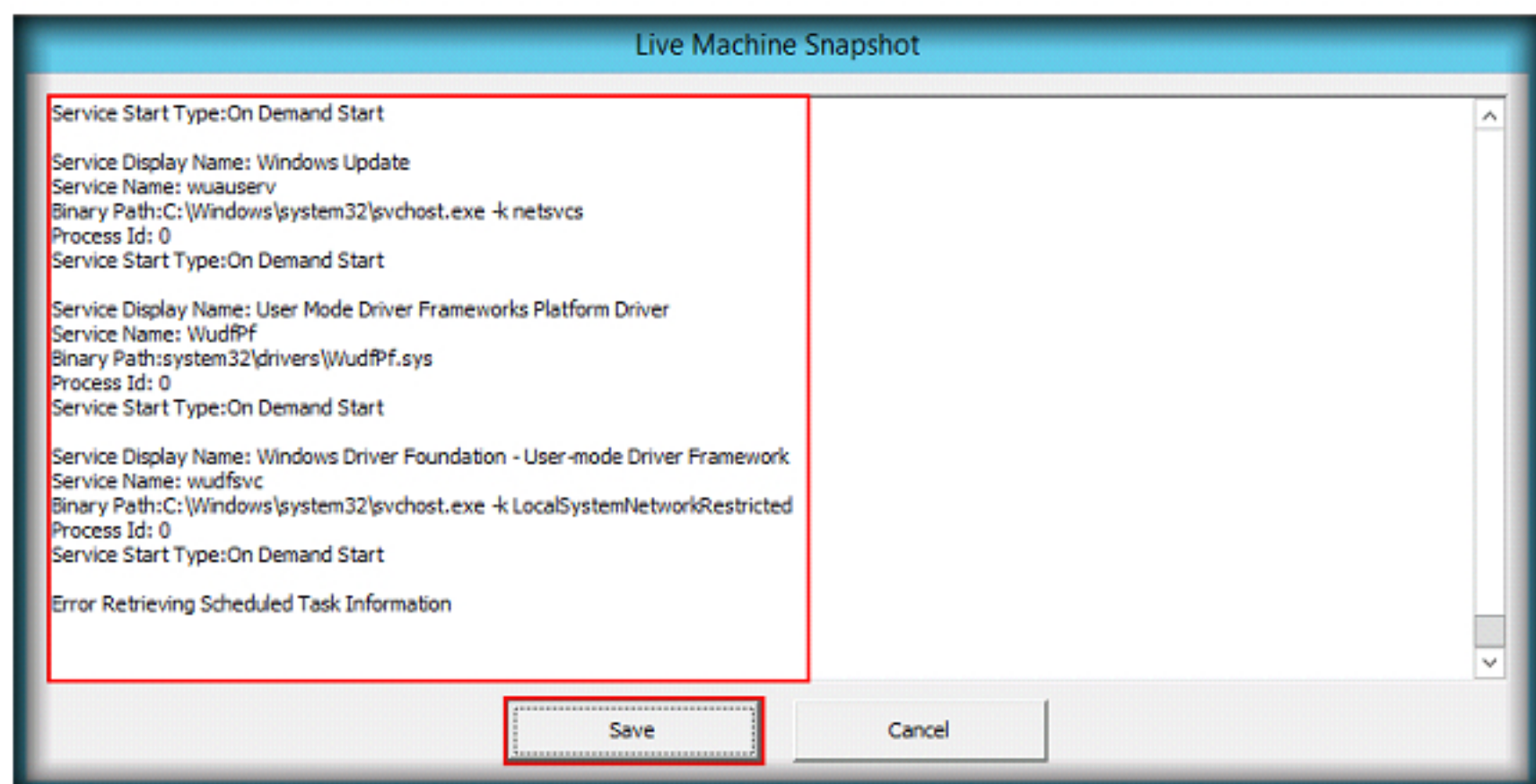


FIGURE 4.31: Helix Incident Response Nigilant32 Live Machine Snapshot

40. The **Save As** window appears, select the location in which the snapshot has to be saved and mention the file name in the **File Name** field and click **Save**.

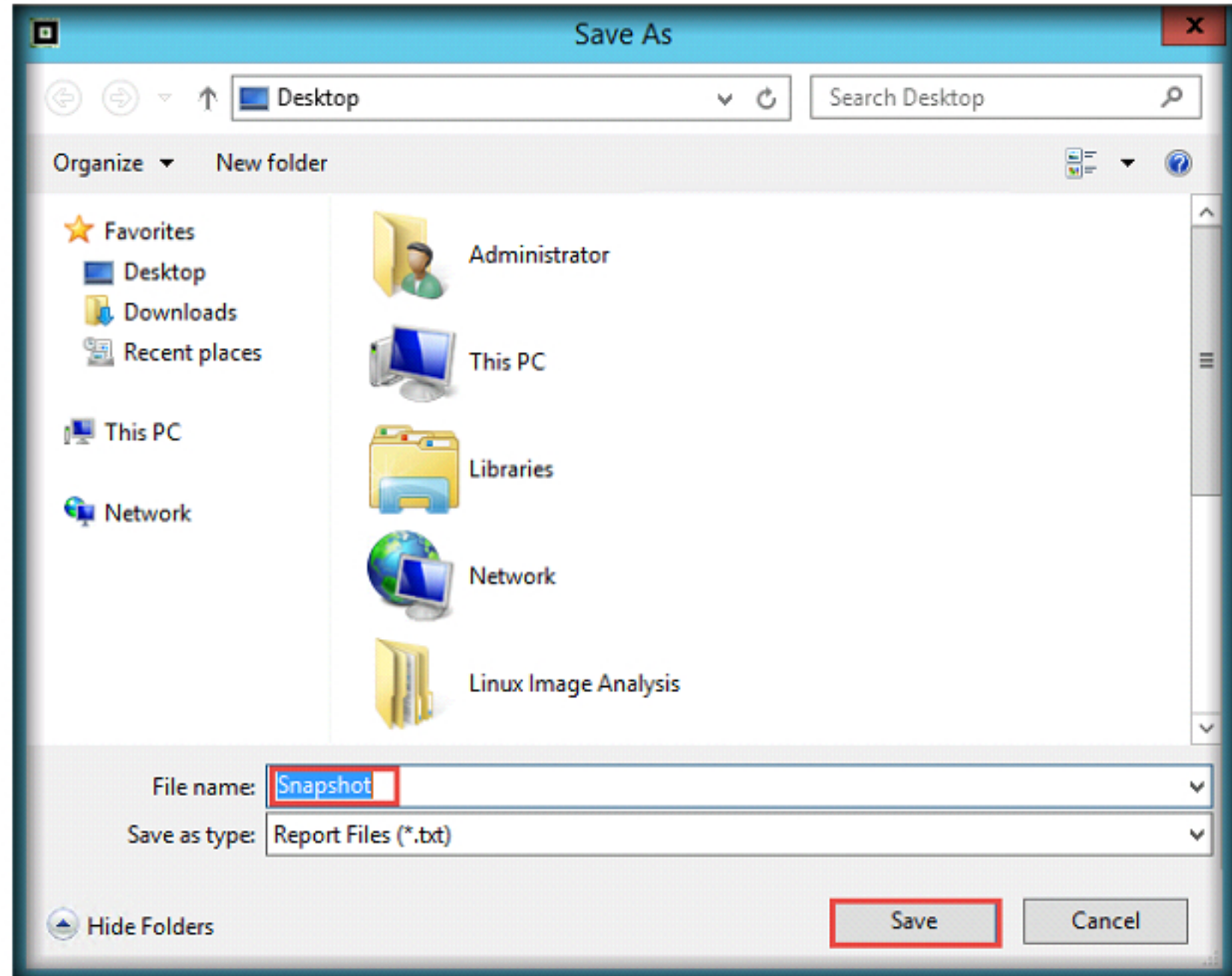


FIGURE 4.32: Helix Incident Response Nigilant32 Save As window

41. To create an image of physical memory, choose **Tools** → **Image Physical Memory**.

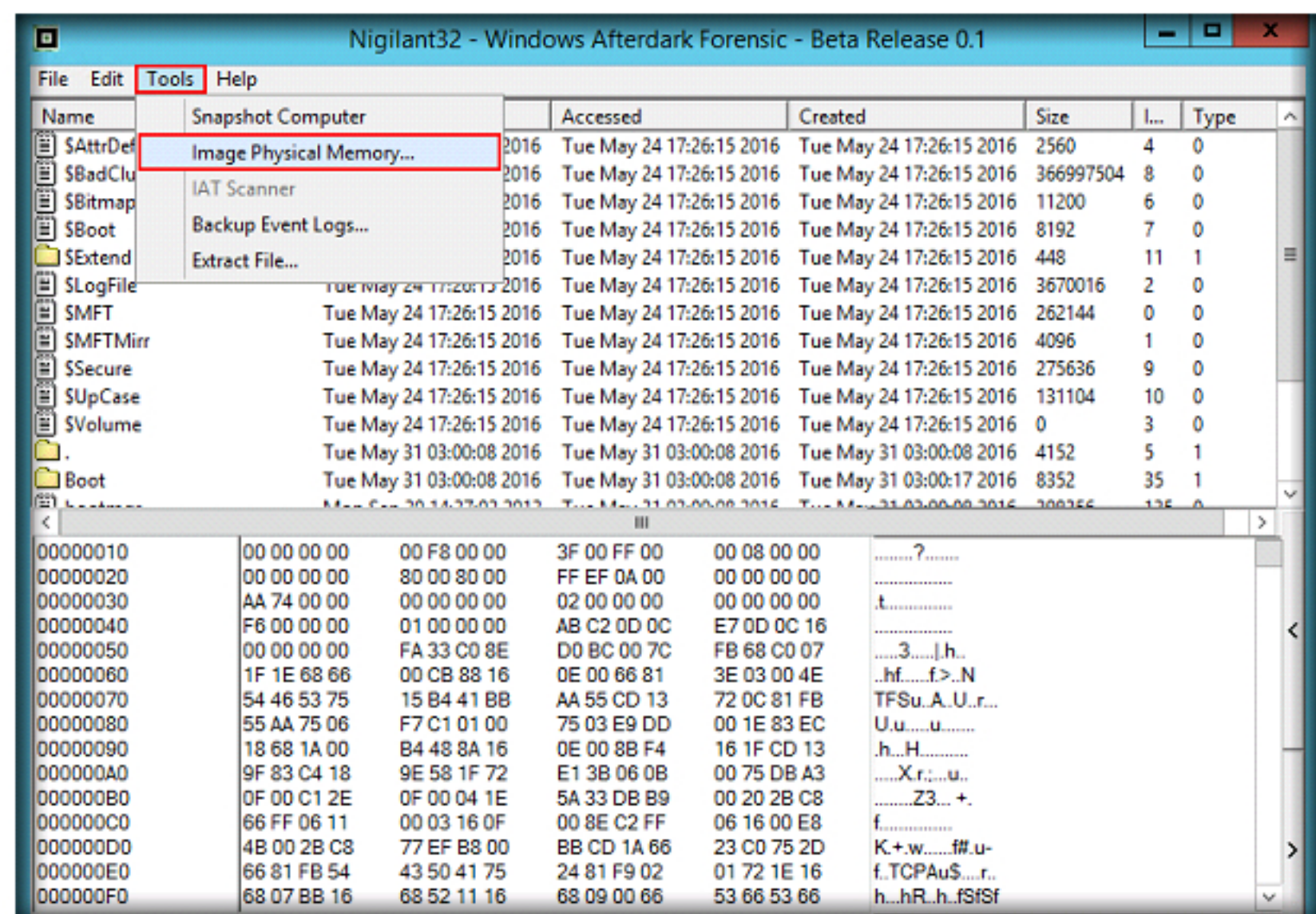


FIGURE 4.33: Helix Incident Response Nigilant32 Image Physical Memory

 Nigilant32: Free Windows Incident response tool. As such, we have recently released Nigilant32, a freeware Windows GUI.

42. Click **Start** to create an image of a Physical memory.

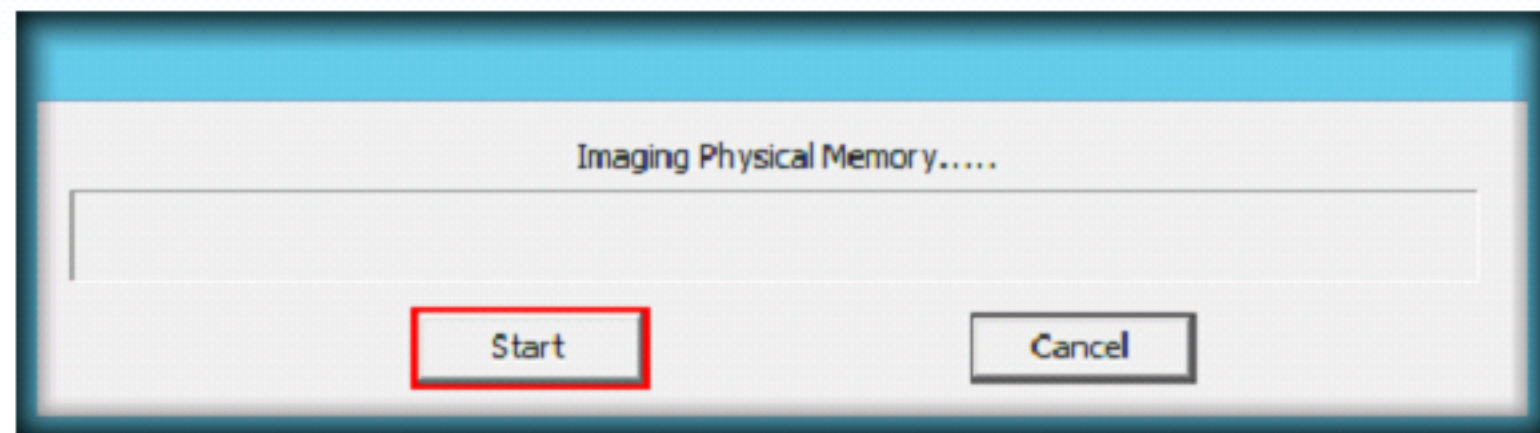


FIGURE 4.34: Helix Incident Response Nigilant32 Imaging Physical Memory

43. The **Save As** window appears, select the location in which the snapshot has to be saved, mention the file name in the **File Name** field, and click **Save**.

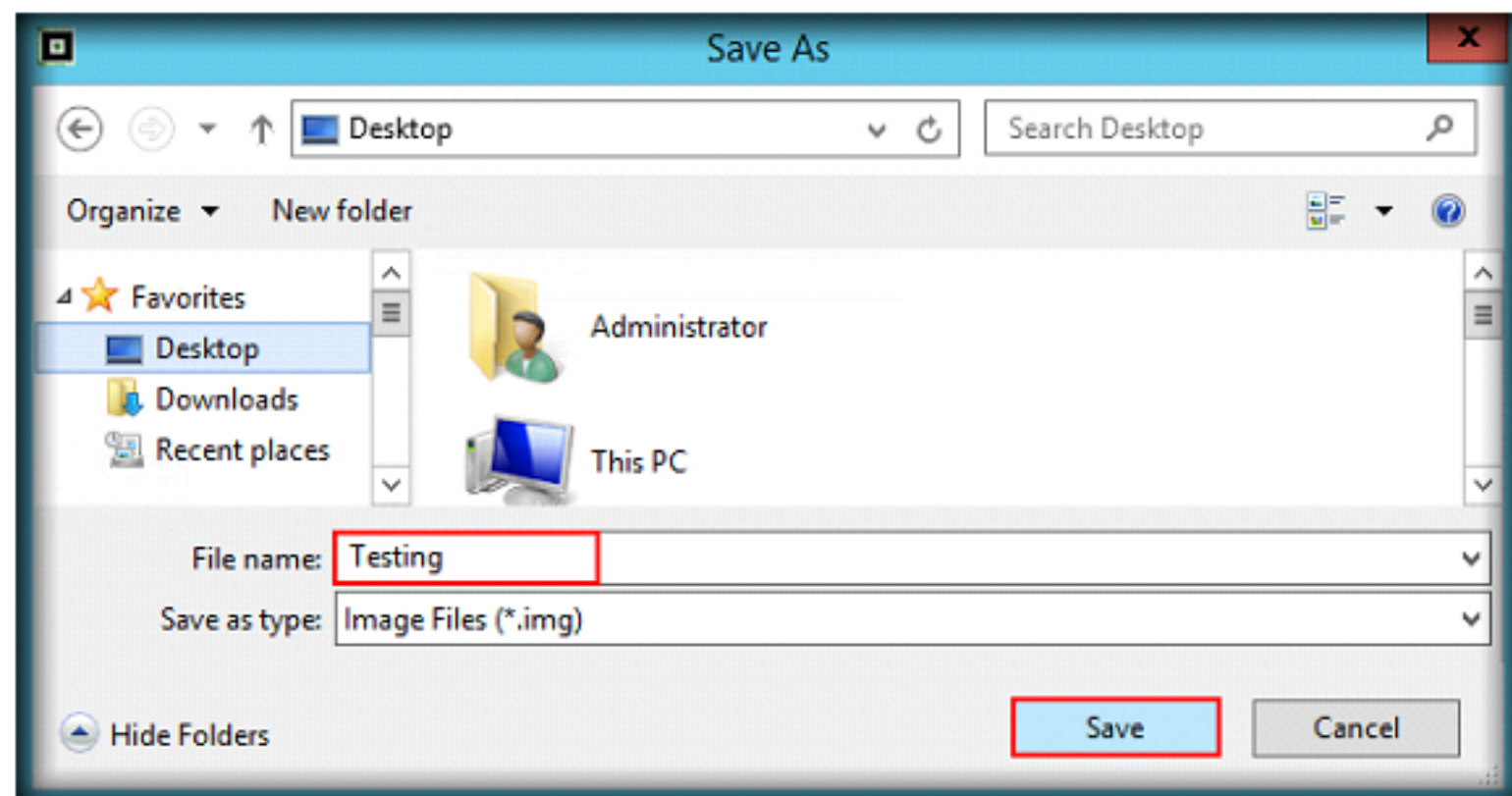


FIGURE 4.35: Helix Incident Response Nigilant32 destination path to save

44. Now go to Page 2 by clicking the  button.

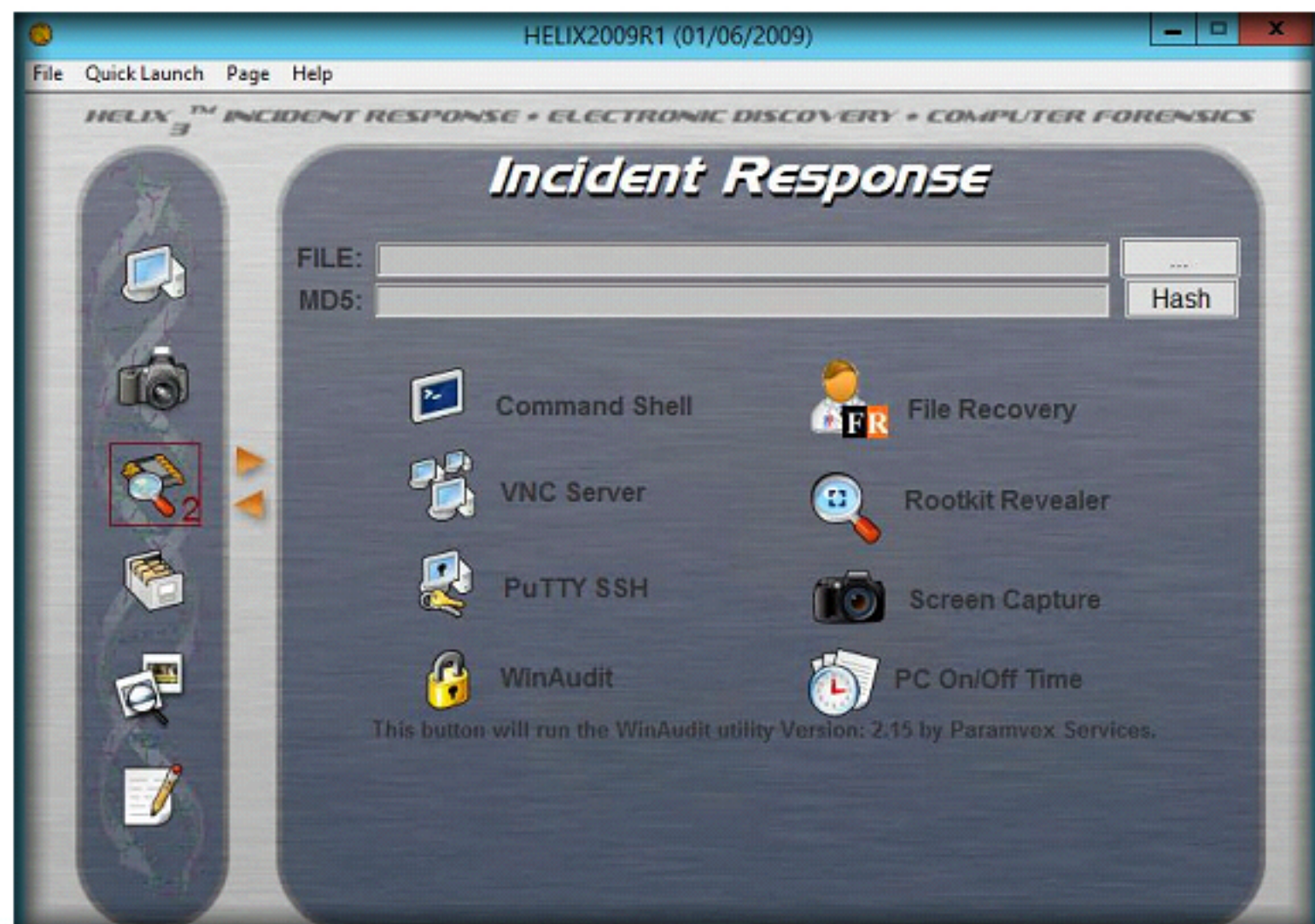


FIGURE 4.36: Helix Incident Response Page 2

TASK 5

MD5 Hash Calculation

The Message-Digest 5 (MD5) Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. It is specified in RFC 1321.

45. To generate an **MD5** hash value of a file, click the **Browse** button and select a file (in this case, **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Windows Forensics Tools\Helix\EULA.pdf**).
46. Click the **Hash** button to generate the hash value of the file.

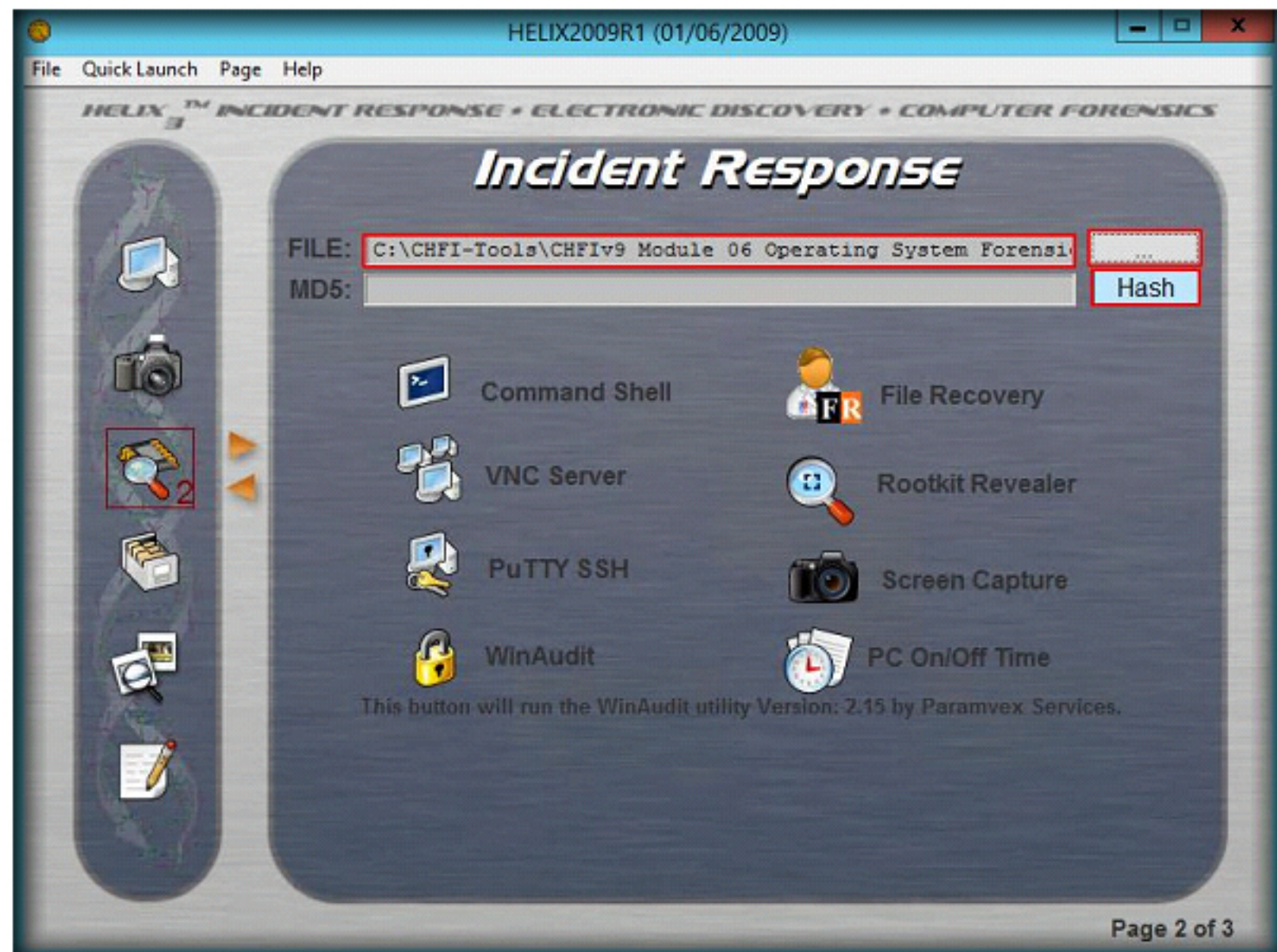


FIGURE 4.37: Helix Incident Response Page 2 MD5 calculation

47. A hash value is generated, as shown in the screenshot:

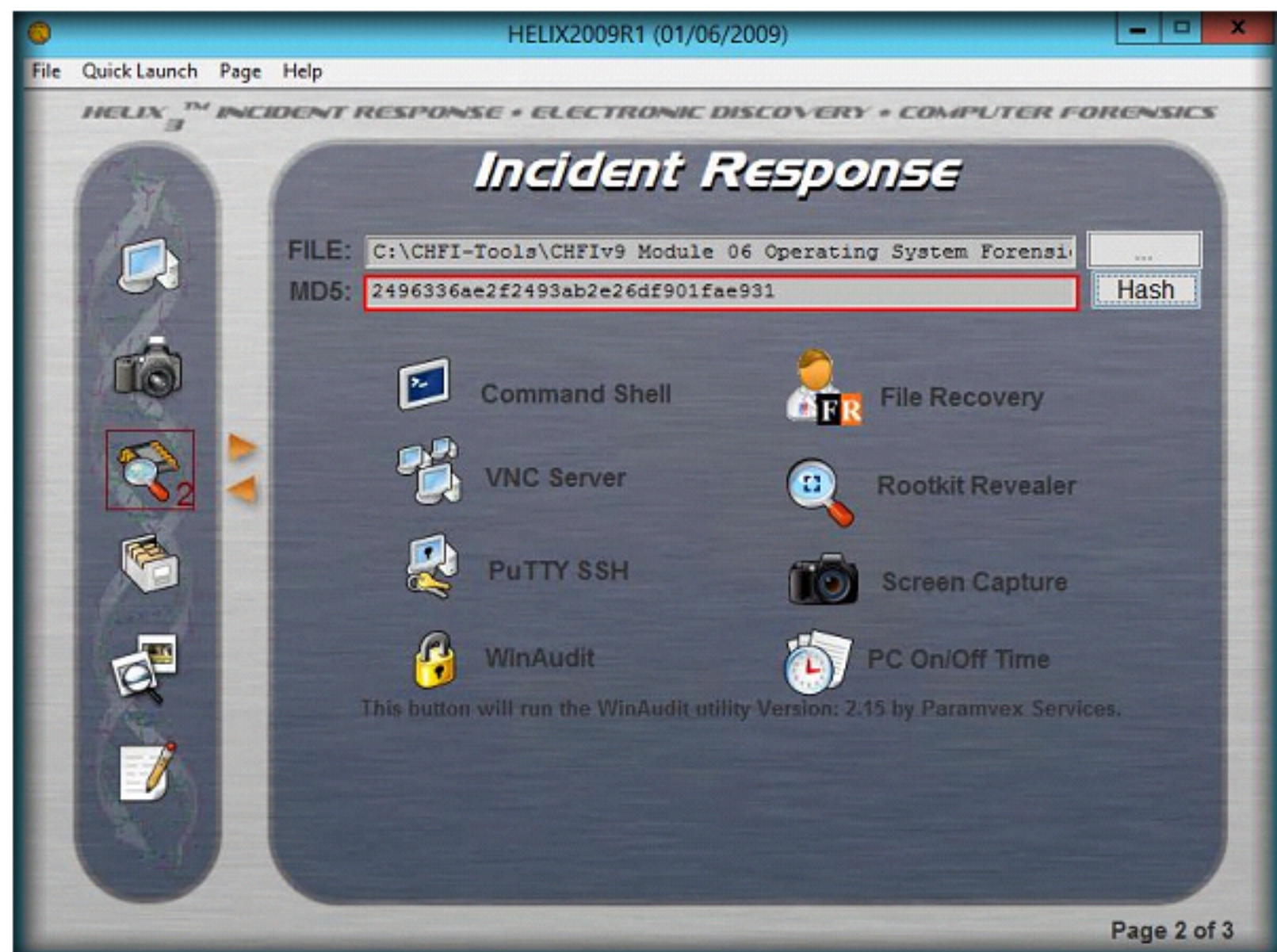


FIGURE 4.38: Helix Incident Response Page 2 MD5 value

MD5 has been employed in a wide variety of security applications and is also commonly used to check data integrity.

TASK 6

Recovering Deleted Files

48. Now click the **File Recovery** icon to recover the deleted files.

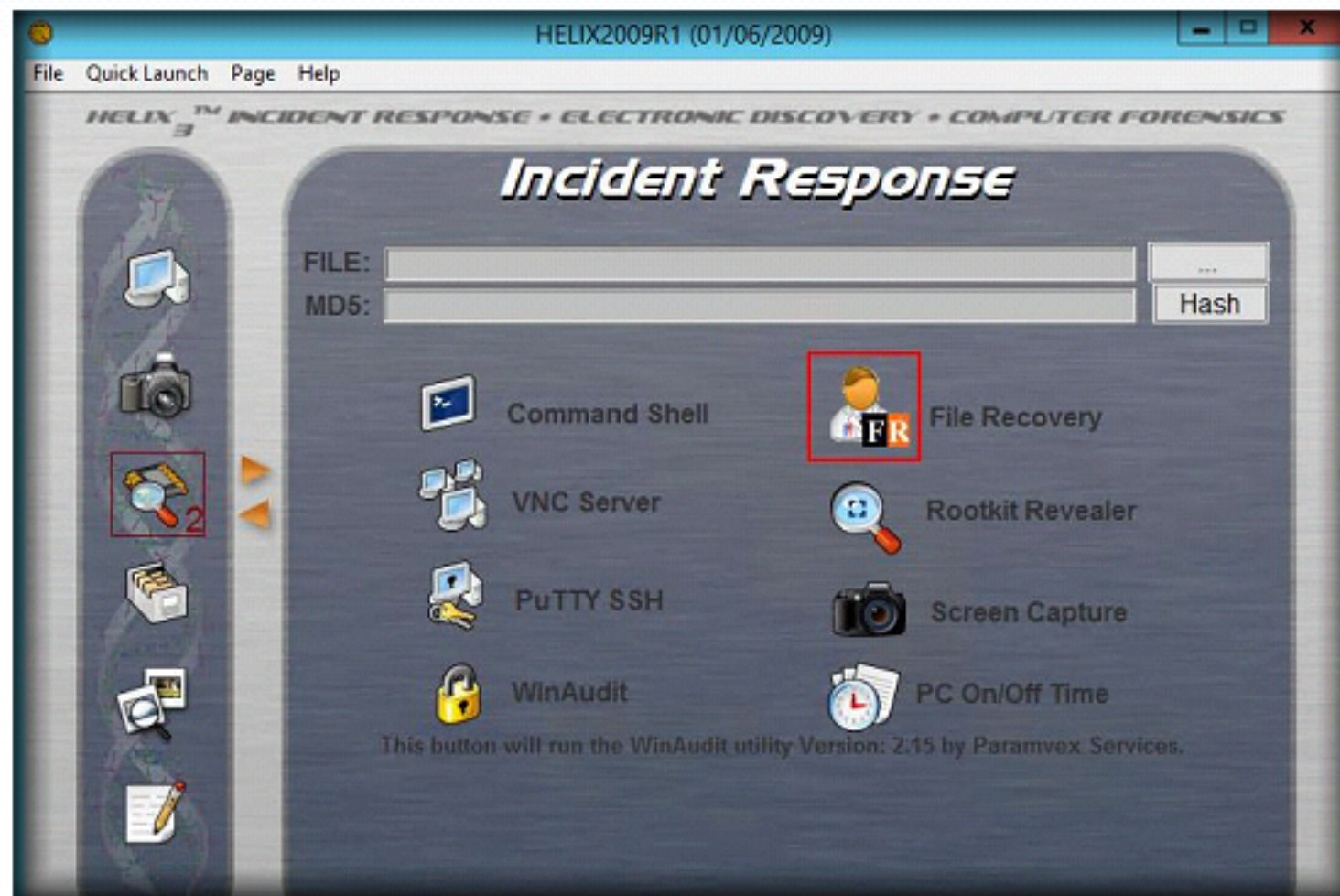


FIGURE 4.39: Helix Incident Response Page 2 File Recovery

49. It will prompt you with the **Notice** window. Click **Yes** to run **Filerecovery.exe**.

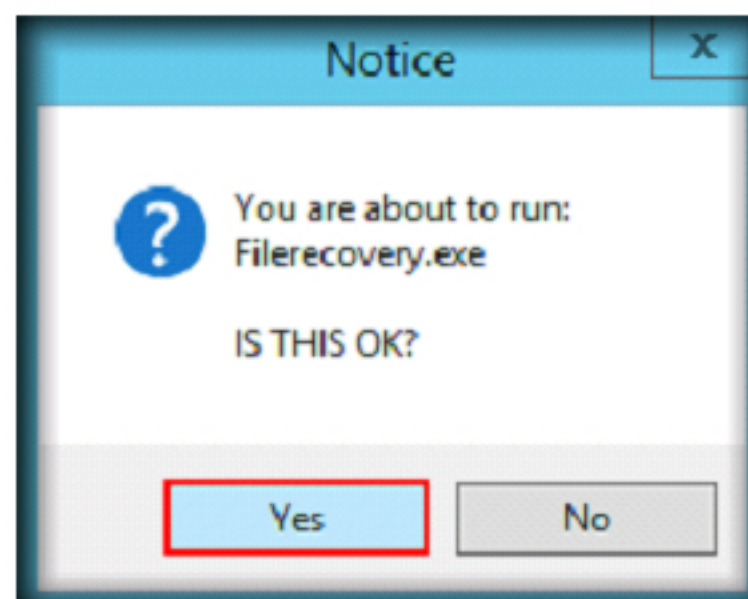


FIGURE 4.40: Helix Incident Response Page 2 File Recovery Notice

50. Select a language and click the  button in the **Choose Language** wizard.



FIGURE 4.41: Helix Incident Response Page 2 File Recovery language selection

 Supported file systems: FAT 12/16/32, NTFS (used by hard disks, disks, Smartmedia™, Compact Flash™, Memory Stick™ and others)

 Select your file (for several files use the **Ctrl** or **Shift** keys) and save it to another drive by selecting **Save to** from the **Object** menu.

Also, you can search for a deleted or lost file (or for several files) by selecting **Find** from **Object** menu.

51. Click the  button in the **Welcome** window of the **PC Inspector File Recovery** wizard.

 Select **Find lost data** from the **Tools** menu. The appearing dialog windows allow you to delimit the search (e.g. if you know the file/directory is situated more behind, move the track bar Start sector to the right).

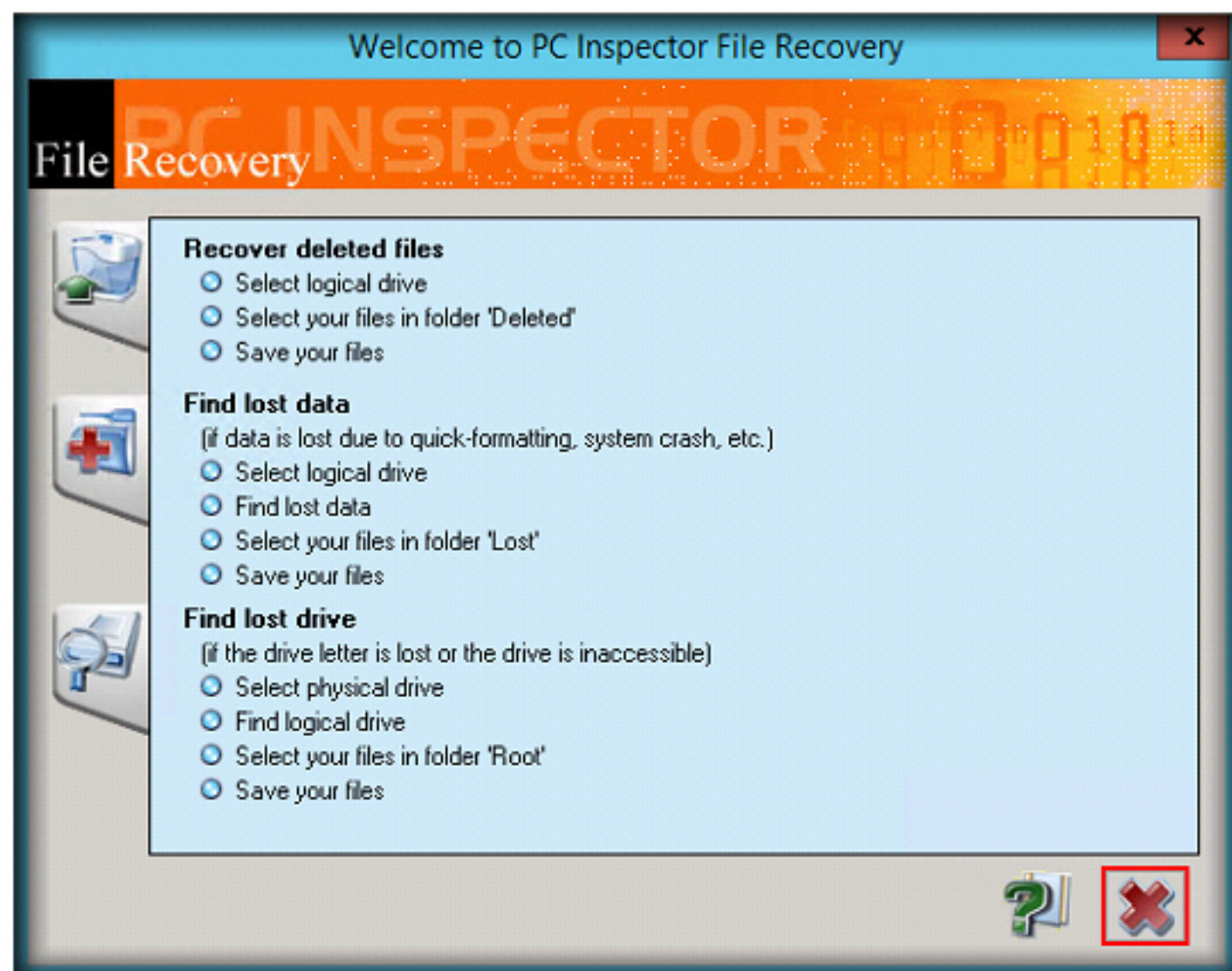


FIGURE 4.42: Helix Incident Response Page 2 File Recovery wizard Welcome window

52. Navigate to **Object** → **Drive**.

 Important: If a file is found with unknown name and size (e.g. cluster40.jpg), you can correct the name and size by choosing **Properties** from the **Object** menu. If the file is too small, simply change the file size to a higher value.

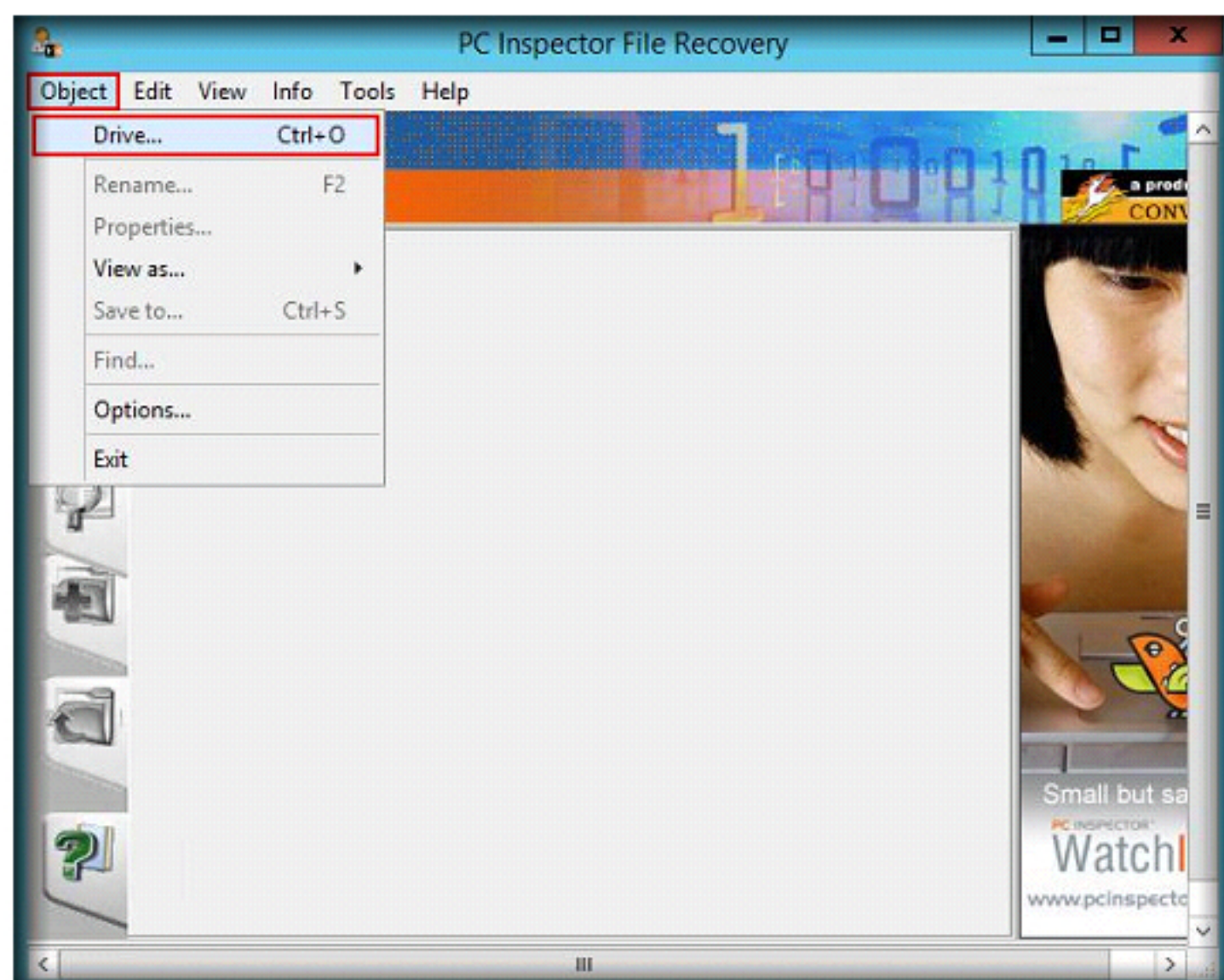


FIGURE 4.43: Helix Incident Response Page 2 File Recovery Object Menu

53. Now select a drive from the **Logical drive** or **Physical drive** tabs. In this lab, we are recovering files for logical drives.
54. Select any drive from the **Logical drive** tab and click the  button.

 In addition to the cluster scan, you can search for a deleted/lost file (or for several files) by selecting **Find** from the **Object** menu.

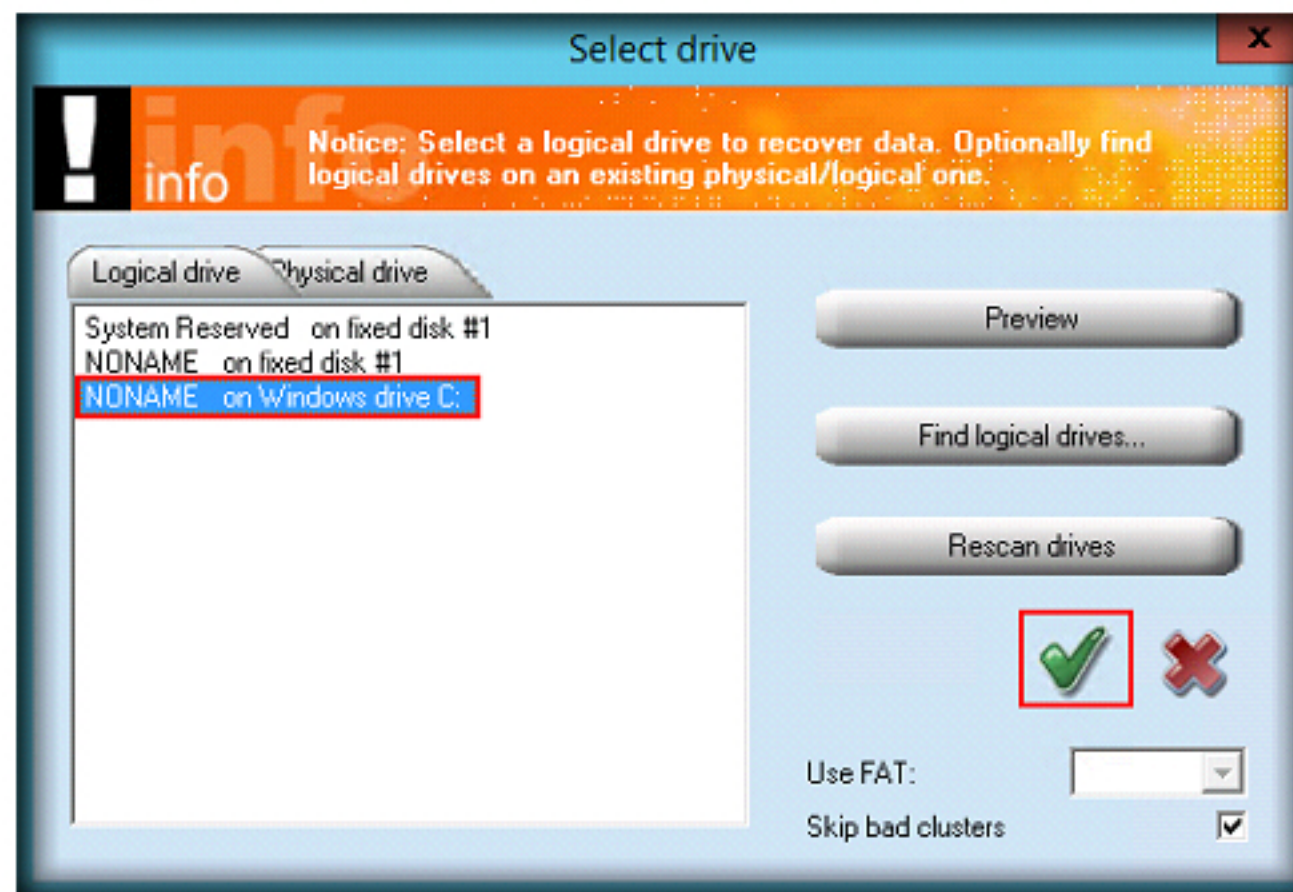


FIGURE 4.44: Helix Incident Response Page 2 File Recovery select drive

55. It will take some time to retrieve the files and folders of the drive, as shown in the screenshot:

 Important: To open the drive and to save your data, choose the option **no FAT (consecutive)** since the FAT has been deleted by quick-formatting.

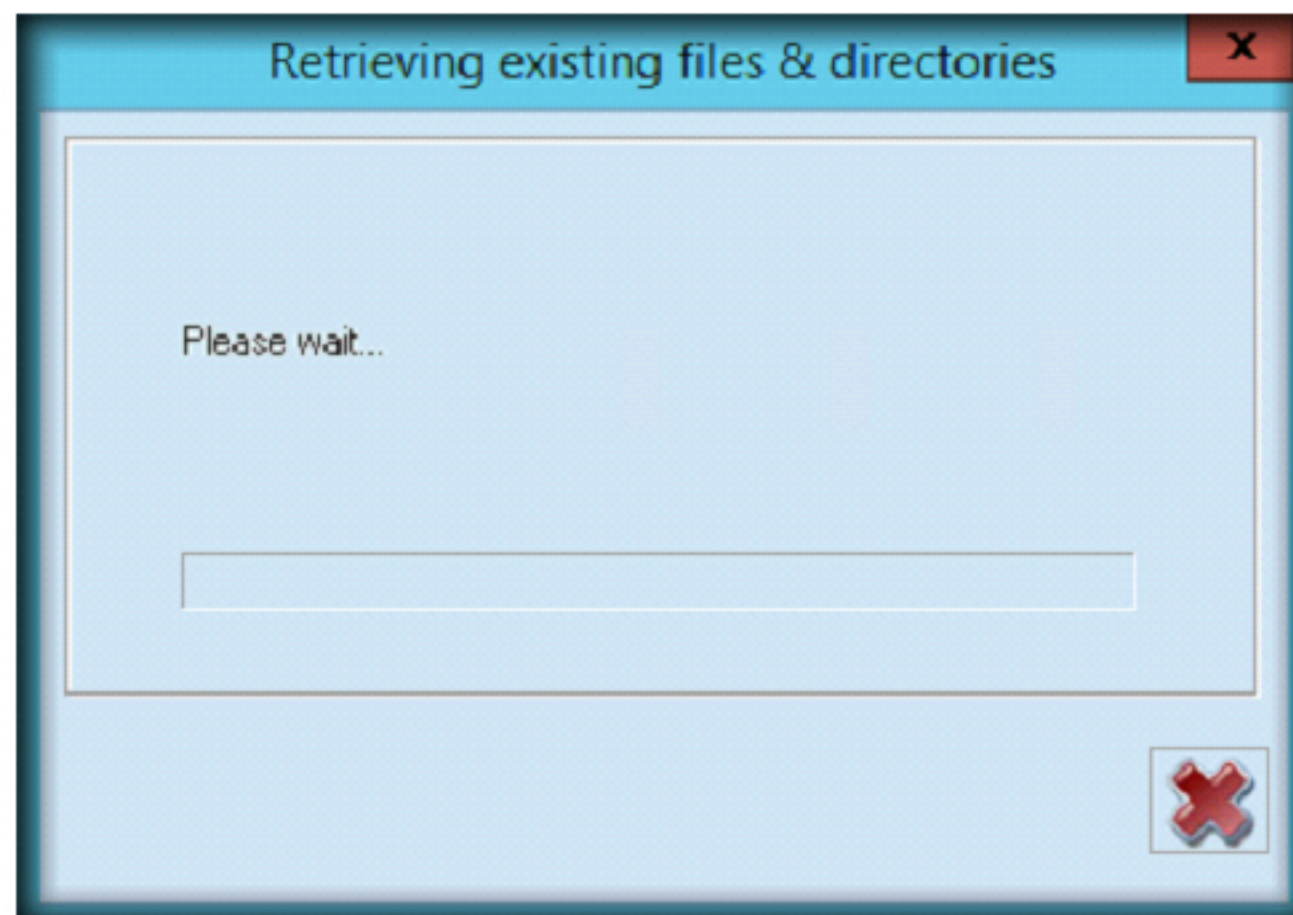


FIGURE 4.45: Helix Incident Response Page 2 File Recovery Retrieving files

56. In the **left pane** of the window, it will display a tree structure. In that structure, you can find a **Deleted** file string.
57. Expand the Deleted node; select a folder from the left pane. The contents of the folder appear in the right pane.

58. You can save those files to another hard drive or disk by right-clicking on the respective file and clicking **Save to**, and then, specifying the location to store the file.

After the search has been completed and a logical drive has been found select the drive under logical drive if the format seems to be correct. It is not exceptional if more drives are found than has been installed. The reason is that there are several copies of the boot sector on the hard disk (that's the unit that contains the information about a logical drive). So first use the function Preview to get the right logical drive.

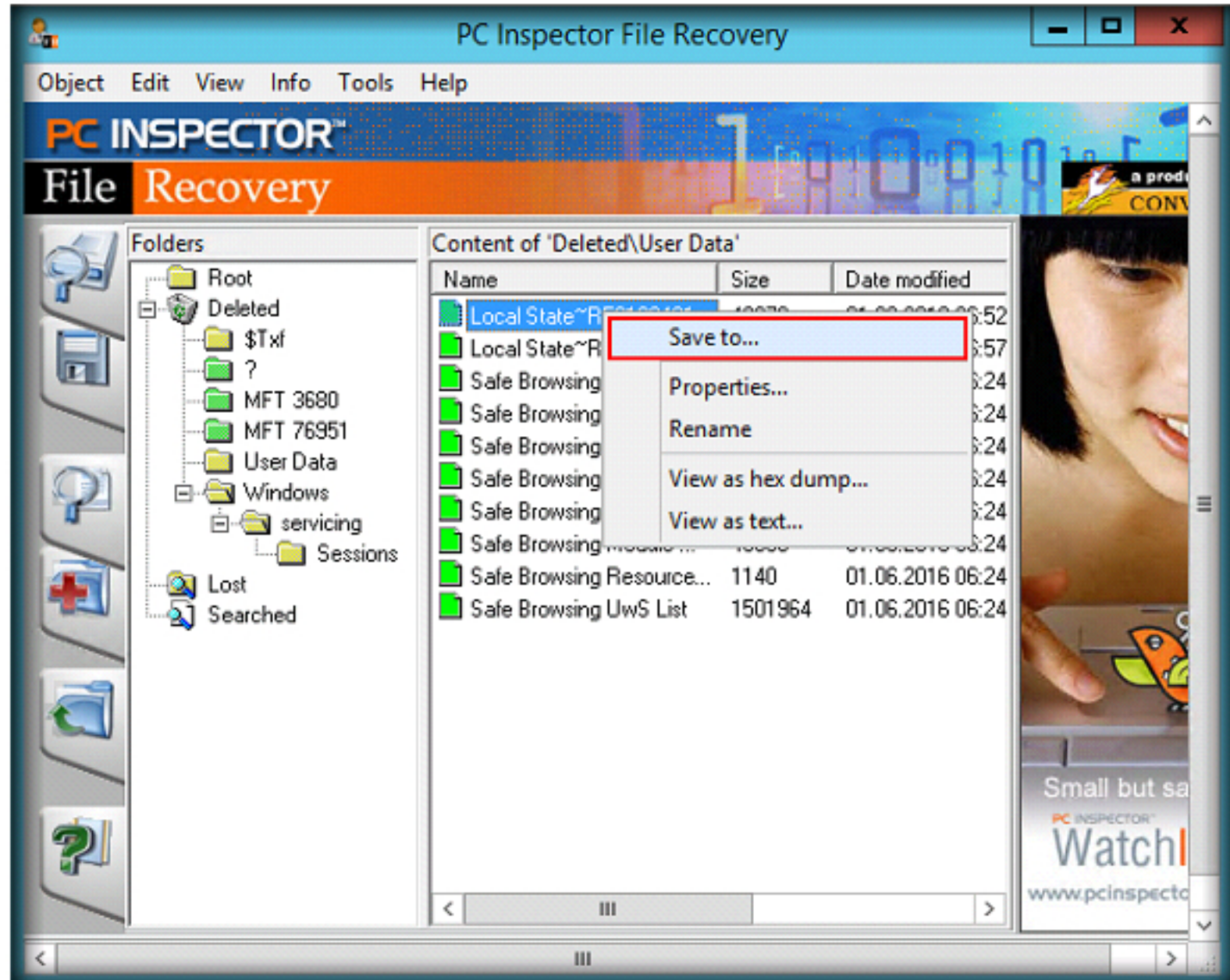


FIGURE 4.46: Helix Incident Response Page 2 File Recovery Save to option

59. Now click the  button to navigate to Page 3.

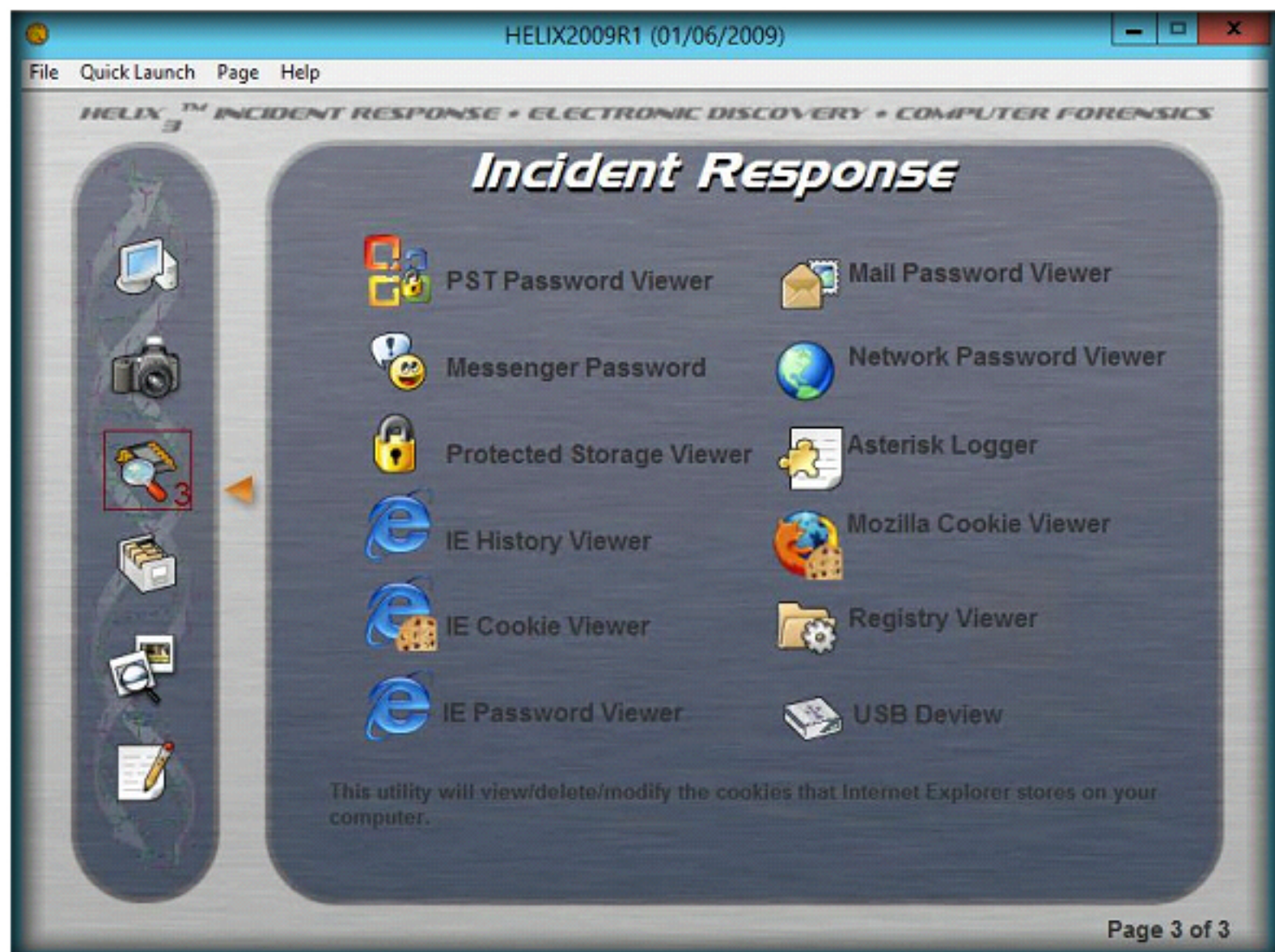


FIGURE 4.47: Helix Incident Response Page 3

TASK 7

Browsing
Contents in Hard
Drives

Helix is a customized version of Ubuntu Linux, allowing you to boot into a Linux environment containing customized Linux kernels, hardware detection and a large number of applications designed for incident response and forensics.

60. To know the contents of your drives, click the **Browse** icon in the left pane. It displays all the drives in the middle pane of the window.
61. Expand the drive of your choice and expand the folders within the drive. It displays the files within the selected folder in the right pane.
62. Now, select a file in the right pane. The application displays the file properties in the lower right pane of the window as shown in the screenshot:

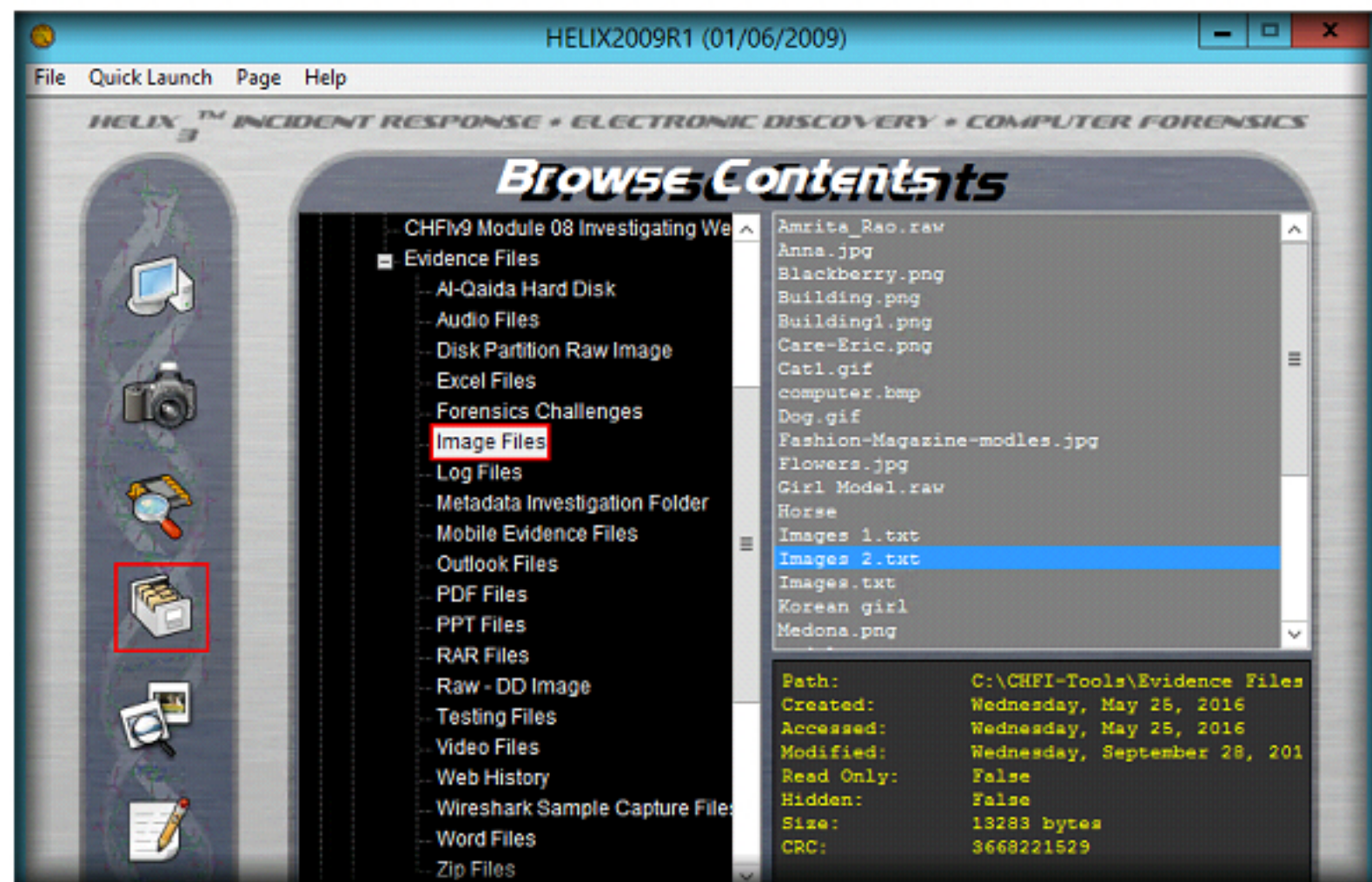


FIGURE 4.48: Helix Browsing Contents

TASK 8

Scanning for
Pictures

Helix is also unique in that it includes a Win32-based autorun toolset, giving users quick access to common forensic tools not found in Linux. Helix is a customized distribution of the Knoppix Live Linux CD. Helix is more than just a bootable live CD.

63. To scan images or pictures on the computer, click the **Scan for Pictures** icon, and then click **Load Folder** to view the images.

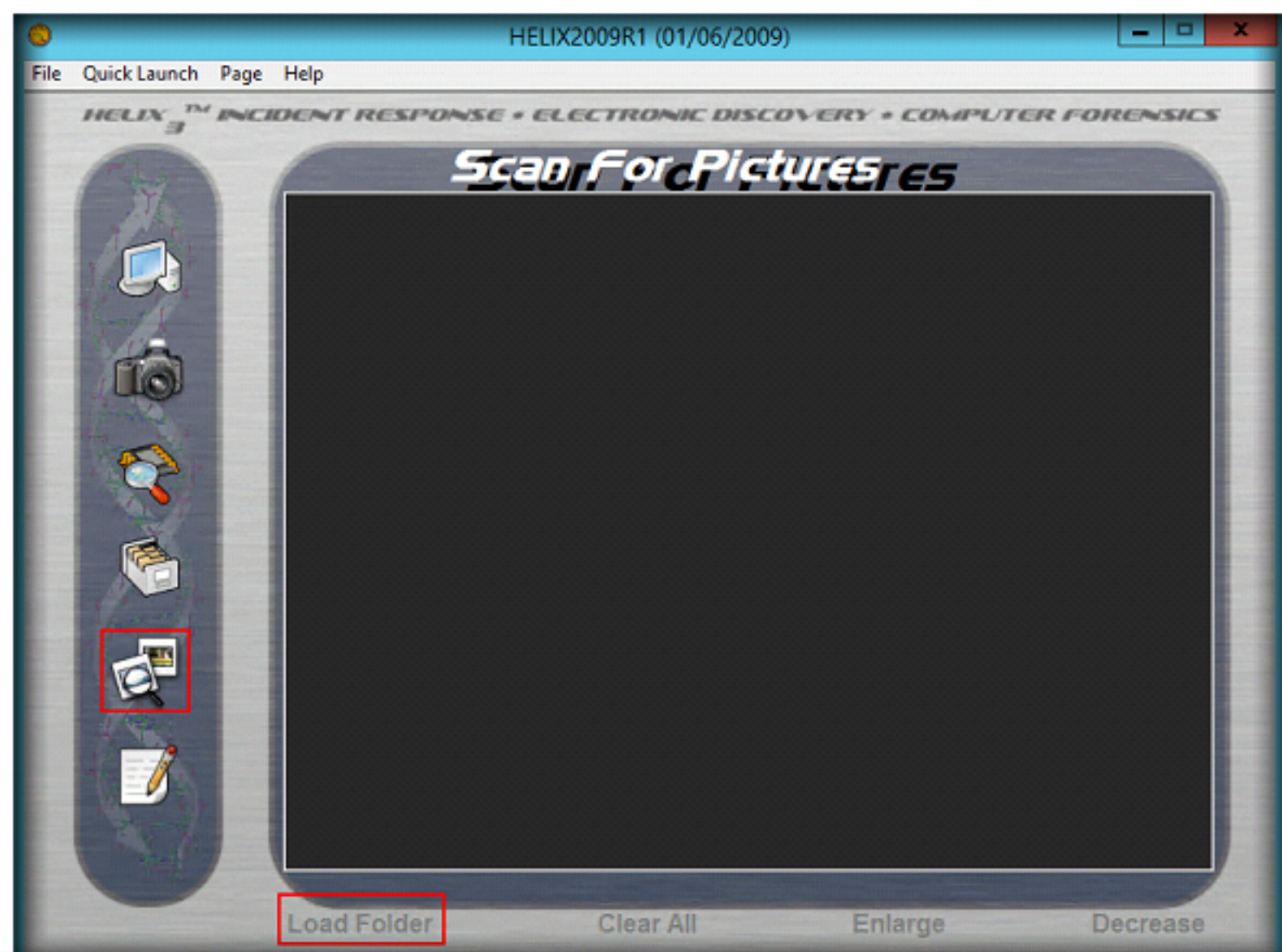


FIGURE 4.49: Helix Scan for Pictures

64. Navigate to **C:\CHFI-Tools\Evidence Files\Image Files** to load the pictures for scan then click **OK**.

Helix will not automount swap space, or automount any attached devices. Helix also has a special Windows autorun side for Incident response and forensics. Helix has been modified very carefully *not to* touch the host computer in any way, and it is forensically sound.

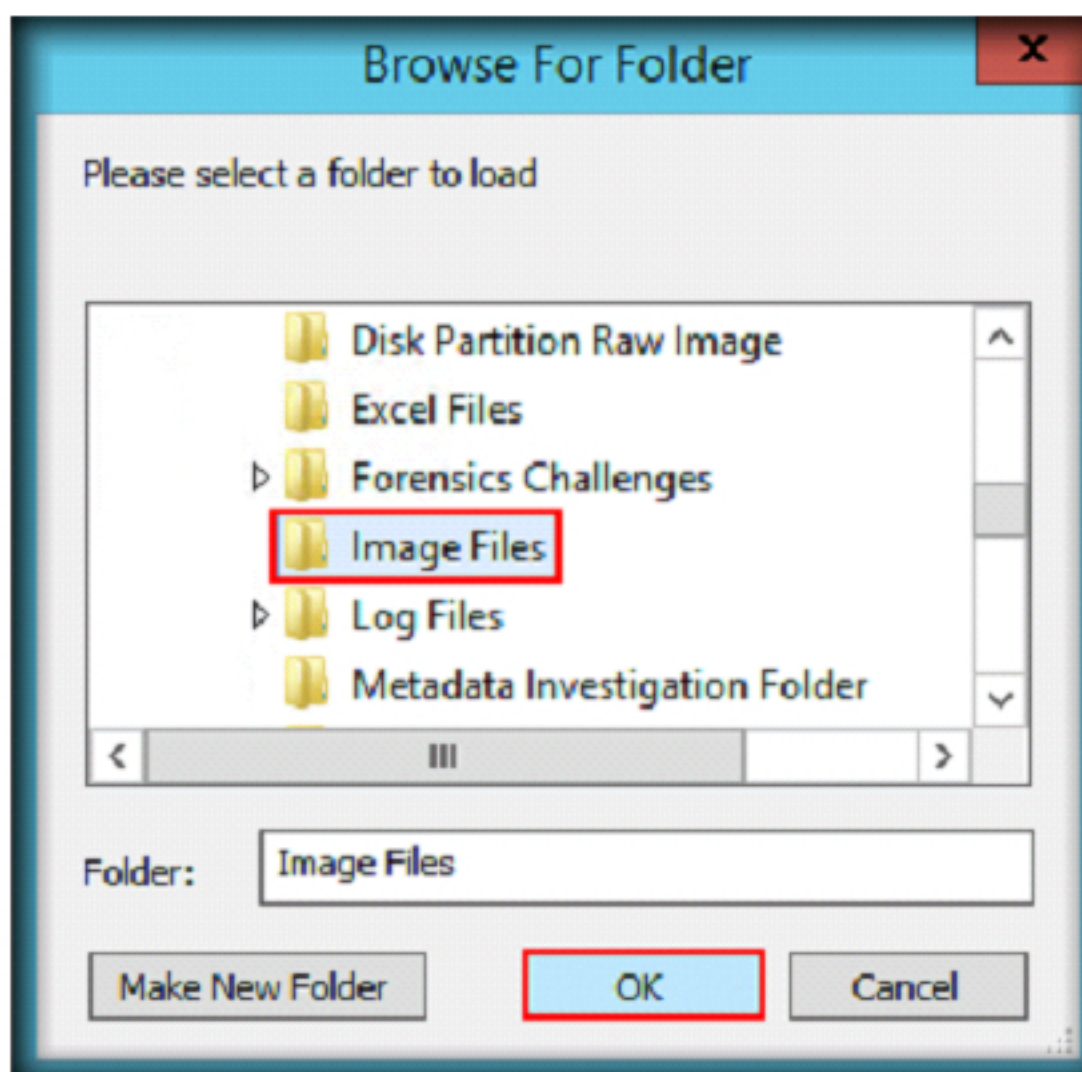


FIGURE 4.50: Helix Scan for Pictures location

65. It will prompt with a **Notice** window asking you to be patient. Click **OK**.

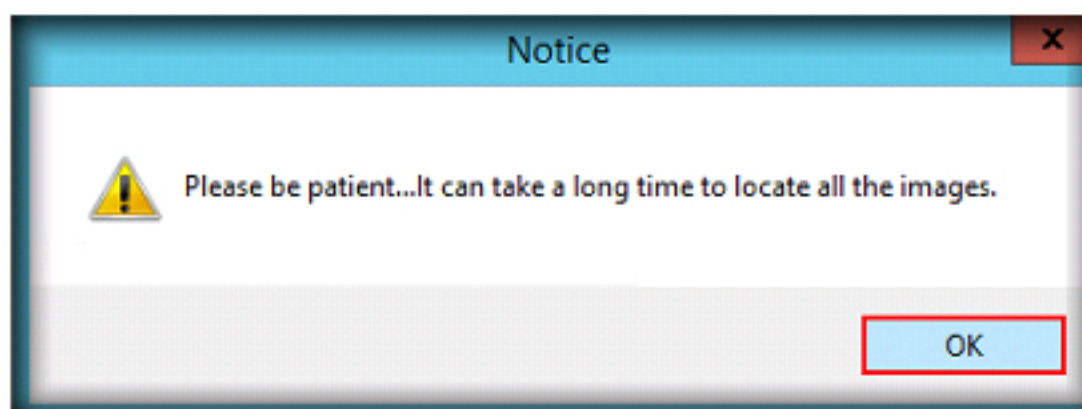


FIGURE 4.51: Helix Scan for Pictures Notice

66. You can view the images scanned by Helix as shown in the screenshot:

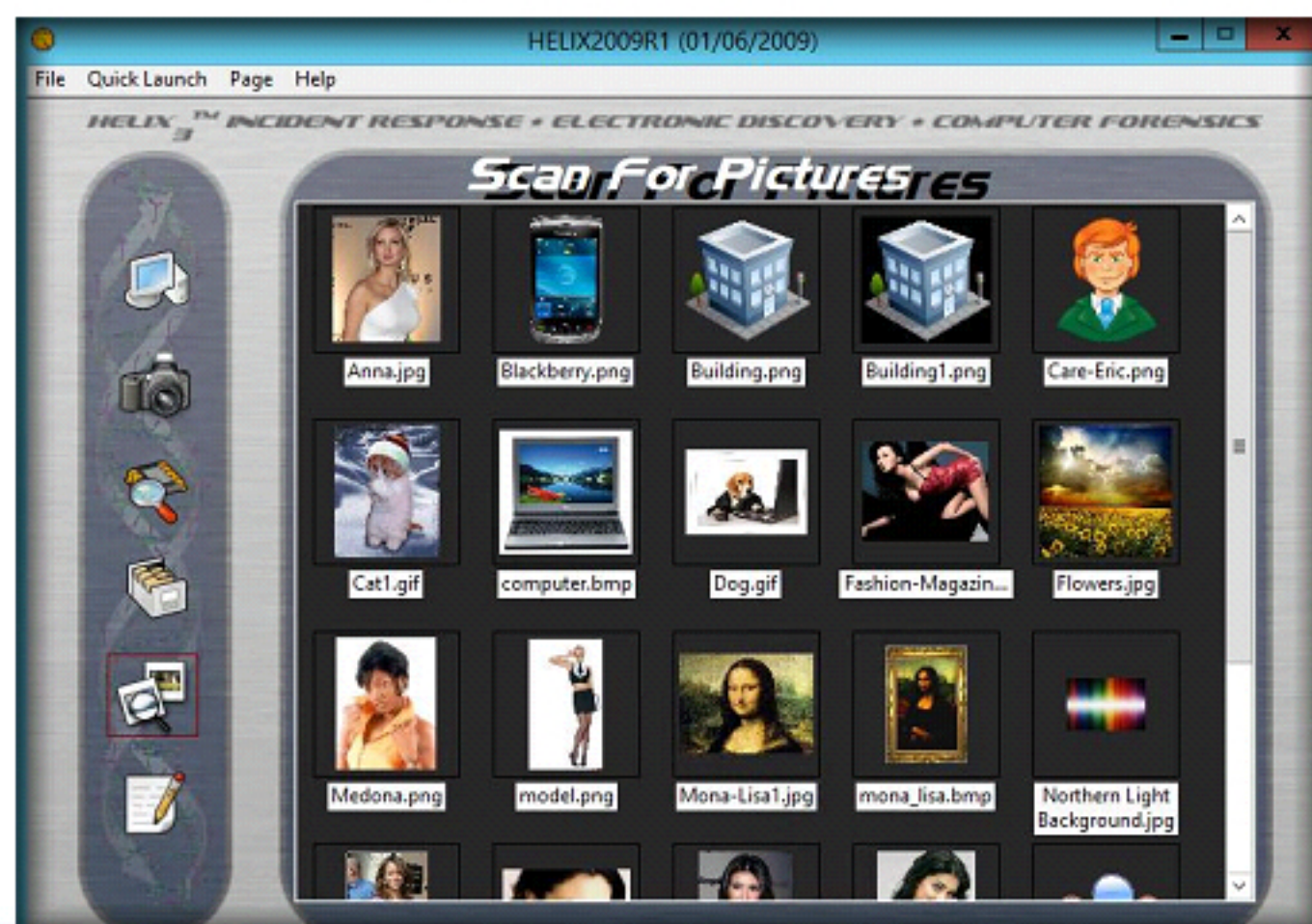


FIGURE 4.52: Helix scanned images

Lab Analysis

Analyze drive image creation and extraction, file recovery, and cookie viewing and document the respective details.

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

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ iLabs

Acquiring Volatile Data in Linux System

Linux OS stores user and session related data in RAM when the system is live.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

The data that changes when the system is turned off is volatile data. The investigator should possess skills to capture this data, analyze it and mine out the evidence from it. To be an expert **forensic investigator**, you must understand how to gather volatile data from a live Linux system and analyze it.

Lab Objectives

The objective of this lab is to help students learn to gather volatile data from a live Linux system and analyze it to find traces of attack to define the type, impact points, path as well as the perpetrator.

Lab Environment

To carry out the lab, you need:

- A computer running **Ubuntu OS (Linux Distro)**.
- Administrative privileges to run tools.
- A web browser with an **Internet** connection.

Lab Duration

Time: 15 Minutes

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

Lab Tasks



TASK 1

Launching Terminal in Linux

1. Launch a **Terminal** in the system

Note: Create a copy or image of the hard disk before acquiring any volatile data, as the commands and actions used to analyze it can make changes to the files in the system.

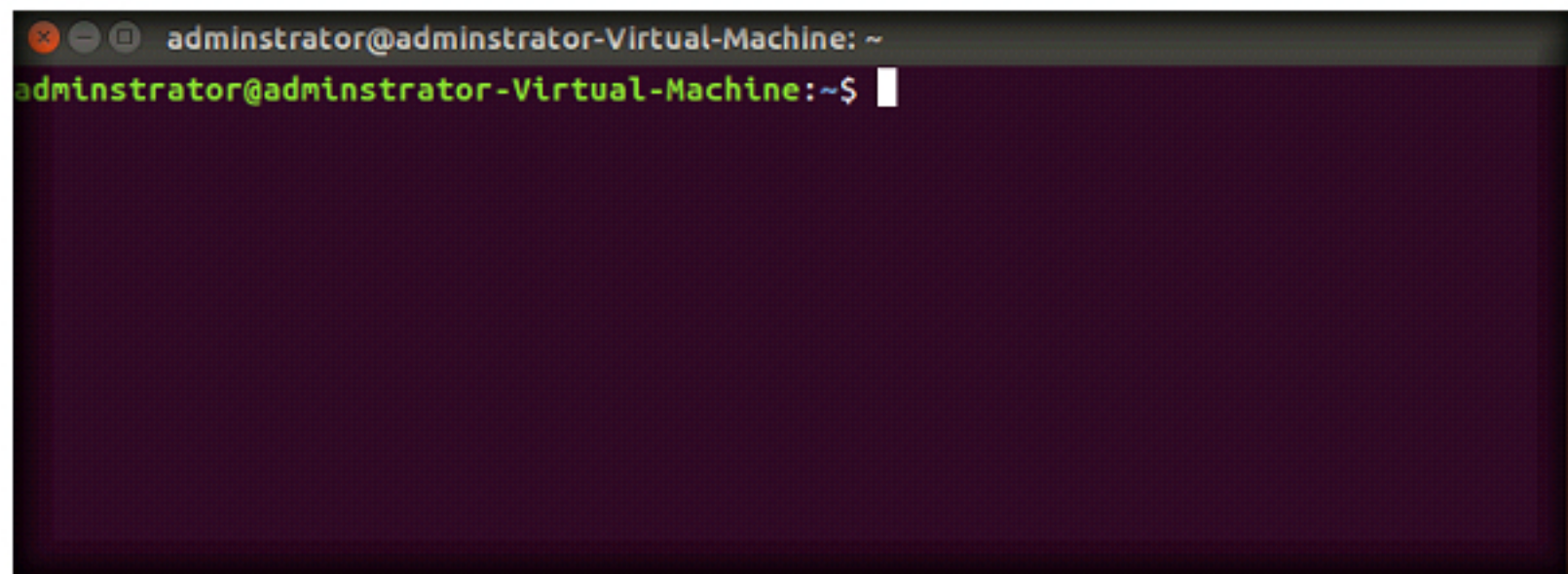


FIGURE 5.1: Ubuntu Terminal



TASK 2

Gather Volatile Data

2. Use the command **uname -a** to gather Linux system information in sequence including kernel name, hostname, kernel release and machine hardware name.

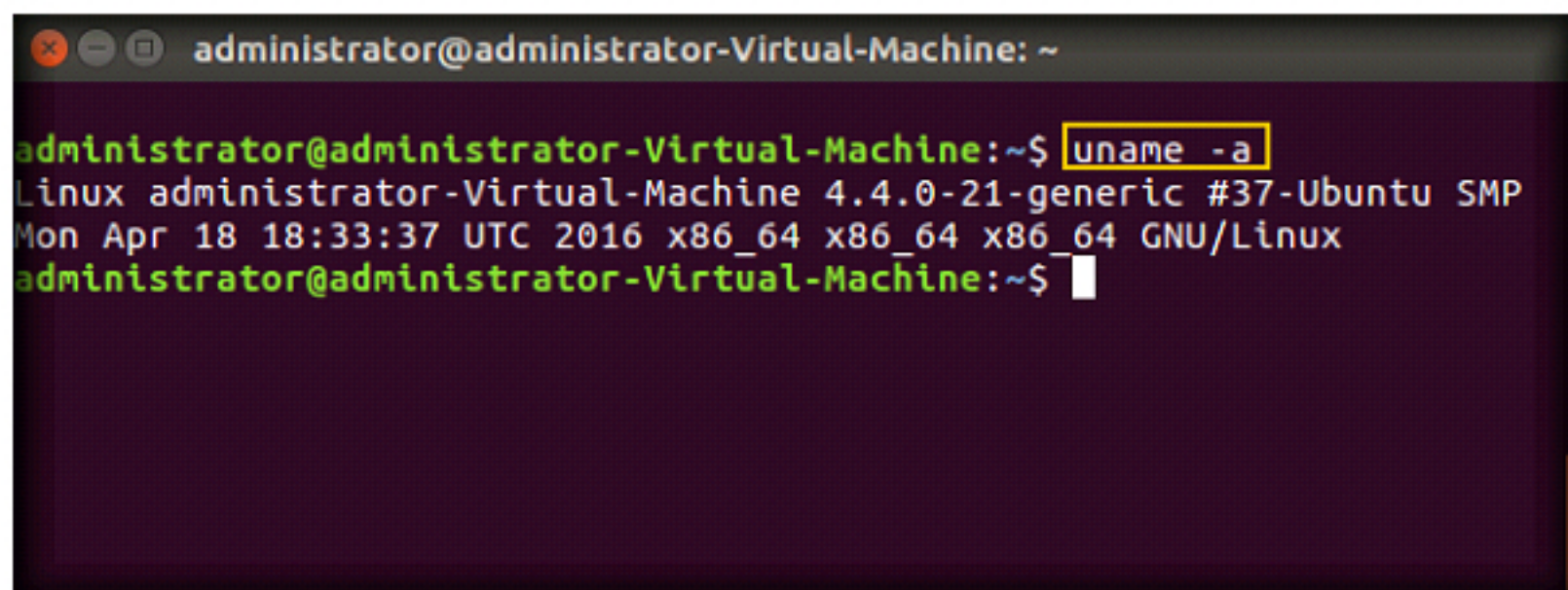


FIGURE 5.2: Ubuntu Terminal `uname -a` command

3. Type **sudo su** and press **Enter**. You will be prompted to enter a password. Type **toor** and press **Enter**.
4. The user will be changed from **jason** to **root** as shown in the screenshot:

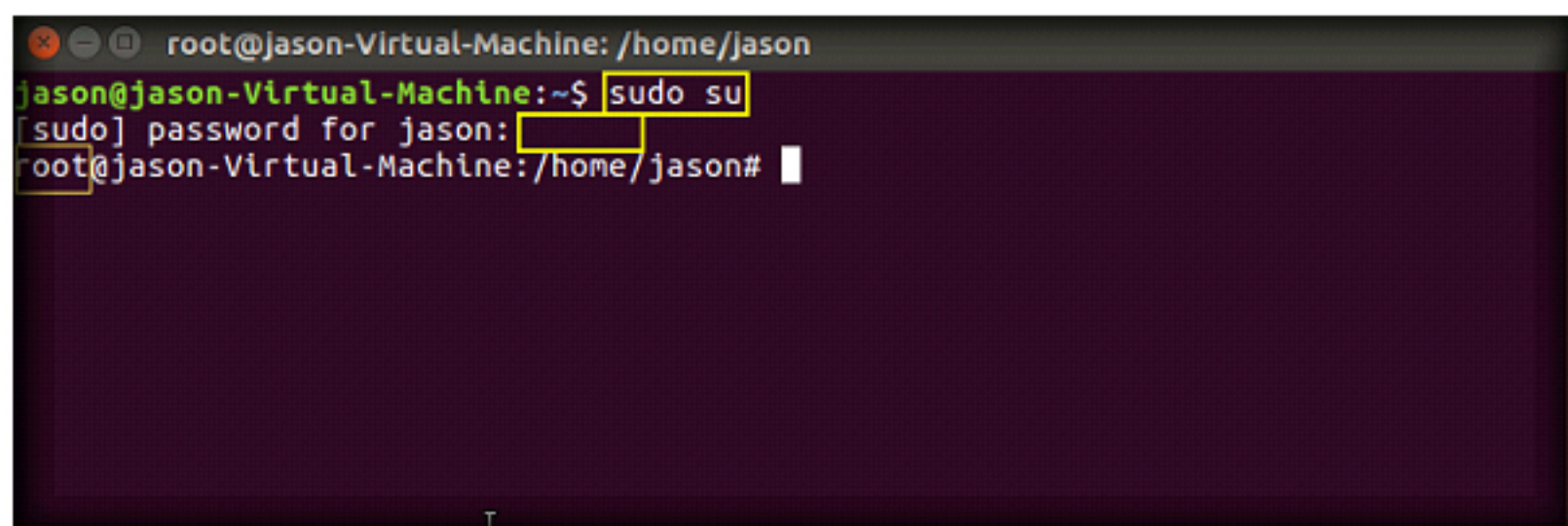
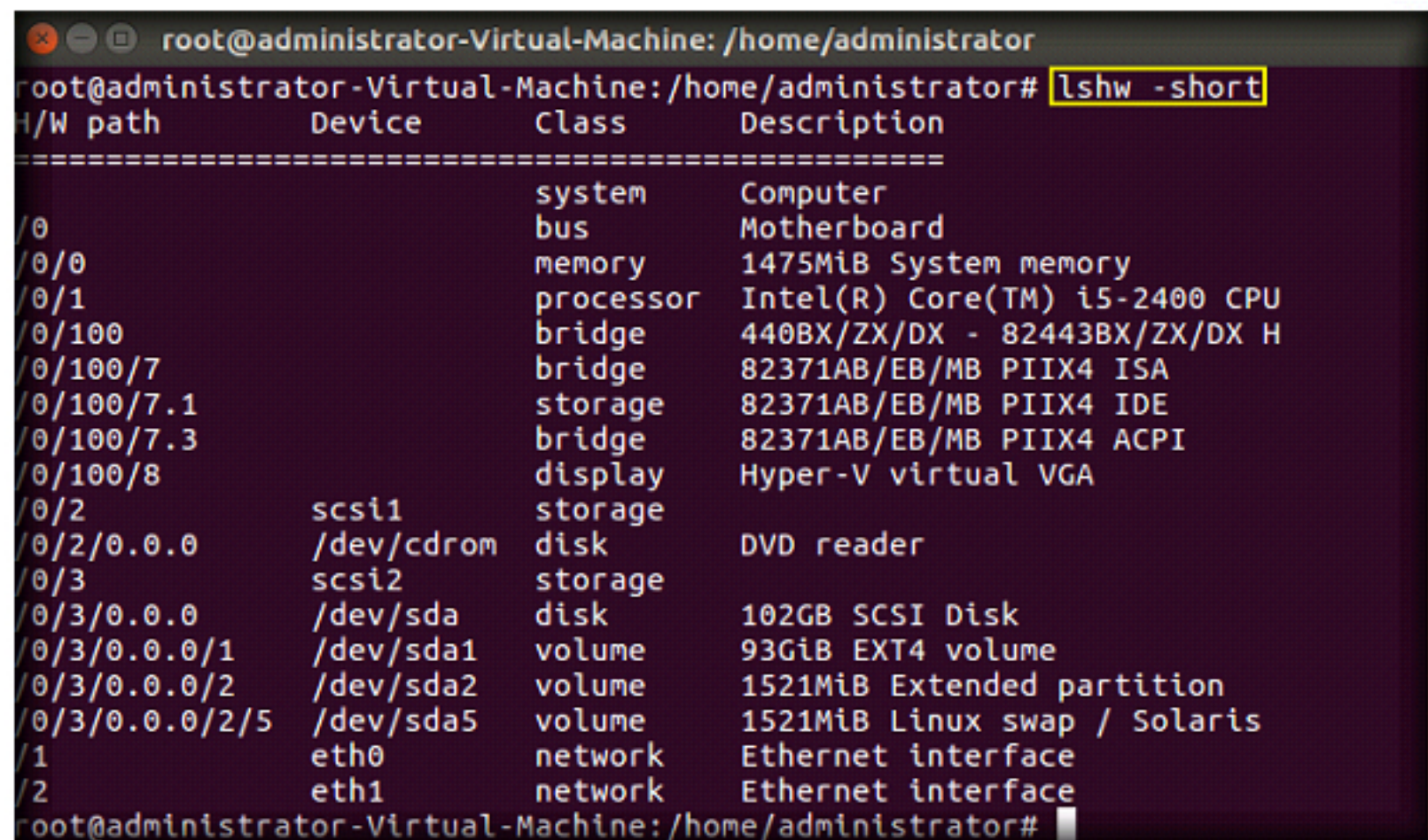


FIGURE 5.3: Ubuntu Terminal change user jason to root

5. The **lshw** command will help you in printing the **hardware details** of the system. Use **-short** option to print the summary of the information.



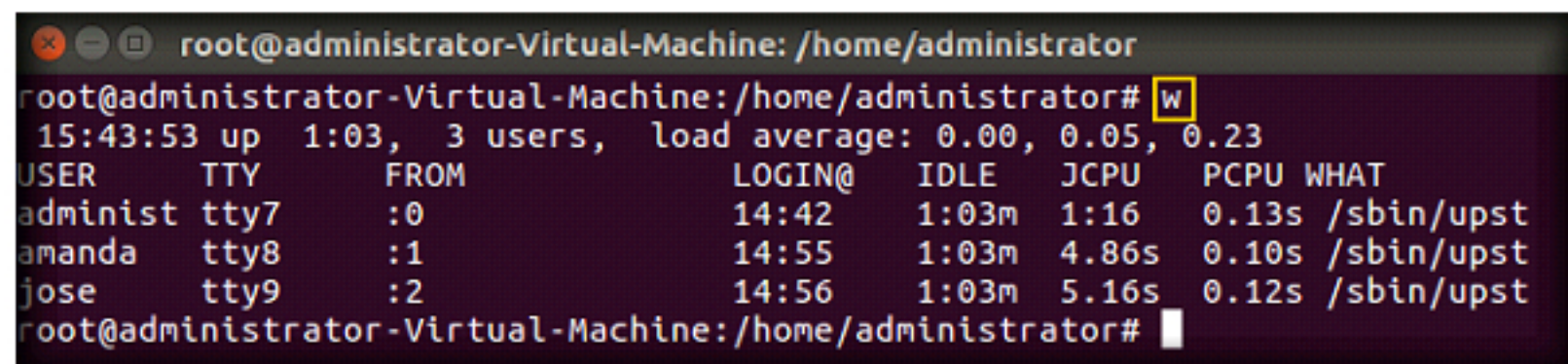
```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# lshw -short
H/W path      Device      Class      Description
-----
/0             system      Computer
/0             bus         Motherboard
/0/0           memory      1475MiB System memory
/0/1           processor   Intel(R) Core(TM) i5-2400 CPU
/0/100         bridge      440BX/ZX/DX - 82443BX/ZX/DX H
/0/100/7       bridge      82371AB/EB/MB PIIX4 ISA
/0/100/7.1     storage     82371AB/EB/MB PIIX4 IDE
/0/100/7.3     bridge      82371AB/EB/MB PIIX4 ACPI
/0/100/8       display     Hyper-V virtual VGA
/0/2           scsi1       storage
/0/2/0.0.0     /dev/cdrom  disk       DVD reader
/0/3           scsi2       storage
/0/3/0.0.0     /dev/sda    disk       102GB SCSI Disk
/0/3/0.0.0/1   /dev/sda1   volume     93GiB EXT4 volume
/0/3/0.0.0/2   /dev/sda2   volume     1521MiB Extended partition
/0/3/0.0.0/2/5 /dev/sda5   volume     1521MiB Linux swap / Solaris
/1            eth0        network     Ethernet interface
/2            eth1        network     Ethernet interface
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.4: Ubuntu Terminal system hardware details

6. To know uptime details, type **w** and press **Enter**.



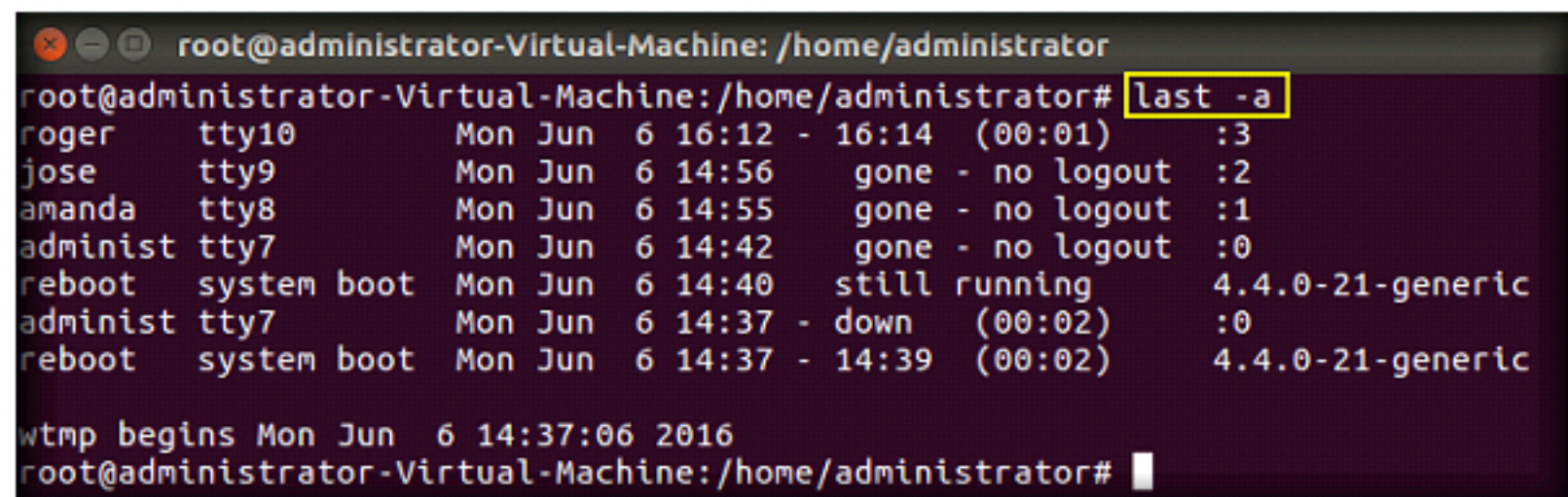
```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# w
 15:43:53 up 1:03, 3 users, load average: 0.00, 0.05, 0.23
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
administ  tty7     :0               14:42    1:03m  1:16   0.13s /sbin/upst
amanda    tty8     :1               14:55    1:03m  4.86s  0.10s /sbin/upst
jose      tty9     :2               14:56    1:03m  5.16s  0.12s /sbin/upst
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.5: Ubuntu Terminal uptime details

7. To gather the details of last login sessions, issue the command **last -a**.



```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# last -a
roger     tty10     Mon Jun 6 16:12 - 16:14 (00:01) :3
jose      tty9      Mon Jun 6 14:56   gone - no logout :2
amanda    tty8      Mon Jun 6 14:55   gone - no logout :1
administ  tty7      Mon Jun 6 14:42   gone - no logout :0
reboot    system boot Mon Jun 6 14:40   still running    4.4.0-21-generic
administ  tty7      Mon Jun 6 14:37 - down (00:02) :0
reboot    system boot Mon Jun 6 14:37 - 14:39 (00:02) 4.4.0-21-generic

wtmp begins Mon Jun 6 14:37:06 2016
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.6: Ubuntu Terminal last login session details

8. Use the **netstat** command to check network status of the system.

```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node    Path
unix  2      [ ]     DGRAM          State           34388     /run/user/1001/systemd/notify
unix  2      [ ]     DGRAM          State           30825     /run/user/1002/systemd/notify
unix  2      [ ]     DGRAM          State           17588     /run/user/1000/systemd/notify
unix  27     [ ]     DGRAM          State           9953      /run/systemd/journal/dev-log
unix  9      [ ]     DGRAM          State           9956      /run/systemd/journal/socket
unix  2      [ ]     DGRAM          State           10078     /run/systemd/journal/syslog
unix  3      [ ]     DGRAM          State           9948      /run/systemd/notify
unix  2      [ ]     STREAM         CONNECTED      41968     @/tmp/dbus-NrCx22x0nH
unix  3      [ ]     STREAM         CONNECTED      34835     @/tmp/dbus-mpuzYz0j5X
unix  3      [ ]     STREAM         CONNECTED      32667     @/tmp/dbus-mpuzYz0j5X
unix  3      [ ]     STREAM         CONNECTED      18318     @/tmp/dbus-AmGo3E2Gd8
unix  3      [ ]     STREAM         CONNECTED      35140     @/tmp/.X11-unix/X2
unix  3      [ ]     STREAM         CONNECTED      34624     @/com/ubuntu/upstart-session/1001/4582
unix  3      [ ]     STREAM         CONNECTED      18376     @/tmp/dbus-mpuzYz0j5X
unix  3      [ ]     STREAM         CONNECTED      18232     @/tmp/.X11-unix/X0
unix  3      [ ]     STREAM         CONNECTED      17694     /run/systemd/journal/stdout
unix  3      [ ]     STREAM         CONNECTED      36489     @/tmp/.X11-unix/X2
unix  3      [ ]     STREAM         CONNECTED      32922     @/tmp/dbus-GXFEppSuAf
unix  3      [ ]     STREAM         CONNECTED      32895     /run/systemd/journal/stdout
unix  3      [ ]     STREAM         CONNECTED      32171     @/tmp/dbus-GXFEppSuAf
unix  3      [ ]     STREAM         CONNECTED      32134     @/tmp/dbus-GXFEppSuAf
unix  3      [ ]     STREAM         CONNECTED      19610     @/tmp/dbus-mpuzYz0j5X
unix  3      [ ]     STREAM         CONNECTED      19607     /var/run/dbus/system_bus_socket
unix  3      [ ]     STREAM         CONNECTED      19204     @/tmp/dbus-mpuzYz0j5X
unix  3      [ ]     STREAM         CONNECTED      18542     /run/user/1000/pulse/native
unix  3      [ ]     STREAM         CONNECTED      35675     @/tmp/dbus-NrCx22x0nH
unix  3      [ ]     STREAM         CONNECTED      31308     @/tmp/dbus-NrCx22x0nH
unix  3      [ ]     STREAM         CONNECTED      31024     @/com/ubuntu/upstart-session/1002/3752
unix  3      [ ]     STREAM         CONNECTED      32958

```

FIGURE 5.7: Ubuntu Terminal system network status

9. You can review the current network settings using the command **ifconfig -a**.

```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:15:5d:00:b4:0d
          inet addr:192.168.0.152  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::3fdb:107f:f8c3:404c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:277219 errors:0 dropped:238 overruns:0 frame:0
          TX packets:5302 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:41649145 (41.6 MB)  TX bytes:530226 (530.2 KB)

eth1      Link encap:Ethernet  HWaddr 00:15:5d:00:b4:0e
          inet addr:10.0.0.9  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::b796:6523:ffcf:14bb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:8072 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6599 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:690522 (690.5 KB)  TX bytes:687777 (687.7 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8213 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8213 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:566270 (566.2 KB)  TX bytes:566270 (566.2 KB)

root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.8: Ubuntu Terminal current network settings review

10. The **lsof** (list open files) command will help you in finding all the open files associated with particular ports, services, and processes. Use the command **lsof > openfiles.txt** to save a text file in home directory, containing the result. The output contained in the text file is shown in the screenshot for reference.

The screenshot shows a terminal window with the command `lsof > openfiles.txt` executed. A warning message is displayed: `lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs Output information may be incomplete.` Below the terminal, a text editor window titled `openfiles.txt [Read-Only] (~/) - gedit` displays the output of the command as a table.

COMMAND	PID	TID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
systemd	1		root	cwd	DIR	8,1	4896	2	/
systemd	1		root	rtd	DIR	8,1	4096	2	/
systemd	1		root	txt	REG	8,1	1573136	1053358	/lib/
systemd/systemd									
systemd	1		root	mem	REG	8,1	18976	1053970	/lib/
x86_64-linux-gnu/libuuid.so.1.3.0			root	mem	REG	8,1	262408	1053778	/lib/
systemd	1		root	mem	REG	8,1	14608	1053810	/lib/
x86_64-linux-gnu/libblkid.so.1.1.0			root	mem	REG	8,1	456632	1053915	/lib/
systemd	1		root	mem	REG	8,1	1864888	1053786	/lib/
x86_64-linux-gnu/libdl-2.23.so			root	mem	REG	8,1	138744	1053932	/lib/
systemd	1		root	mem	REG	8,1	286824	1053862	/lib/
x86_64-linux-gnu/libpthread-2.23.so			root	mem	REG	8,1	64144	1053768	/lib/
systemd	1		root	mem	REG	8,1	92864	1053849	/lib/
x86_64-linux-gnu/libmount.so.1.1.0			root	mem	REG	8,1	117288	1053776	/lib/
systemd	1		root	mem	REG	8,1			
x86_64-linux-gnu/libapparmor.so.1.4.0			root	mem	REG	8,1			
systemd	1		root	mem	REG	8,1			
x86_64-linux-gnu/libbknod.so.2.3.0			root	mem	REG	8,1			
systemd	1		root	mem	REG	8,1			

FIGURE 5.9: Ubuntu Terminal open files

11. You can view the loaded modules in a Linux system using the command **lsmod**.

The screenshot shows a terminal window with the command `lsmod` executed. The output is a table listing loaded kernel modules, their sizes, and the processes using them.

Module	Size	Used by
crct10dif_pclmul	16384	0
crc32_pclmul	16384	0
aesni_intel	167936	0
aes_x86_64	20480	1 aesni_intel
lrw	16384	1 aesni_intel
gf128mul	16384	1 lrw
glue_helper	16384	1 aesni_intel
ablk_helper	16384	1 aesni_intel
cryptd	20480	2 aesni_intel,ablk_helper
i2c_piix4	24576	0
hyperv_fb	20480	4
8250_fintek	16384	0
input_leds	16384	0
hv_balloon	24576	0
serio_raw	16384	0
joydev	20480	0
mac_hid	16384	0
parport_pc	32768	0
ppdev	20480	0
lp	20480	0
parport	49152	3 lp,ppdev,parport_pc
autofs4	40960	2
hid_generic	16384	0
hv_netvsc	36864	0
hv_utils	24576	0
hyperv_keyboard	16384	0
hid_hyperv	16384	0

FIGURE 5.10: Ubuntu Terminal loaded modules

12. Install a Linux auditing tool called **auditd** to the system using the command **apt install auditd**.

Note: If Ubuntu is unable to download auditd, you need to update the repositories using the commands **apt-get update** and **apt-get upgrade**.

```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# apt install auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauparse0
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparse0
0 upgraded, 2 newly installed, 0 to remove and 209 not upgraded.
Need to get 227 kB of archives.
After this operation, 733 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/main amd64 libauparse0 amd64 1:2.4.5-1ubuntu2 [35.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial/main amd64 auditd amd64 1:2.4.5-1ubuntu2 [191 kB]
Fetched 227 kB in 0s (242 kB/s)
Selecting previously unselected package libauparse0:amd64.
(Reading database ... 172809 files and directories currently installed.)
Preparing to unpack .../libauparse0_1%3a2.4.5-1ubuntu2_amd64.deb ...
Unpacking libauparse0:amd64 (1:2.4.5-1ubuntu2) ...
Selecting previously unselected package auditd.

```

FIGURE 5.11: Ubuntu Terminal Linux auditing tool installation

13. The auditing tool consists of utilities that would help in creating records about the system information.
14. Gather details of all the login attempts made to the system by issuing the command **aureport**.

```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# aureport

Summary Report
=====
Range of time in logs: Monday 06 June 2016 17:19:05.365 - Monday
06 June 2016 17:24:44.355
Selected time for report: Monday 06 June 2016 17:19:05 - Monday
06 June 2016 17:24:44.355
Number of changes in configuration: 0
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 1
Number of terminals: 1
Number of host names: 1
Number of executables: 2
Number of commands: 1
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 3
Number of events: 7

```

FIGURE 5.12: Ubuntu Terminal login attempts details

15. Determine the User ID of a particular user using **id root** command, and then, track all the user events pertaining to the userid with **ausearch** command. Syntax of the command is **ausearch -ui <userID> --interpret**. In this lab, the user id is **0**.

```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine:/home/administrator# id root
uid=0(root) gid=0(root) groups=0(root)
root@administrator-Virtual-Machine:/home/administrator# ausearch -ui 0 --interpret
-----
type=SERVICE_START msg=audit(Monday 06 June 2016 17:19:05.382:25) : pid=1 uid=root auid=unset ses=unset
msg='unit=auditd comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_START msg=audit(Monday 06 June 2016 17:20:34.040:27) : pid=1 uid=root auid=unset ses=unset
msg='unit=cups comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_STOP msg=audit(Monday 06 June 2016 17:20:34.040:28) : pid=1 uid=root auid=unset ses=unset
msg='unit=cups comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_START msg=audit(Monday 06 June 2016 17:24:34.123:29) : pid=1 uid=root auid=unset ses=unset
msg='unit=NetworkManager-dispatcher comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_STOP msg=audit(Monday 06 June 2016 17:24:44.355:30) : pid=1 uid=root auid=unset ses=unset
msg='unit=NetworkManager-dispatcher comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_START msg=audit(Monday 06 June 2016 17:54:27.517:31) : pid=1 uid=root auid=unset ses=unset
msg='unit=NetworkManager-dispatcher comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=SERVICE_STOP msg=audit(Monday 06 June 2016 17:54:37.353:32) : pid=1 uid=root auid=unset ses=unset
msg='unit=NetworkManager-dispatcher comm=systemd exe=/lib/systemd/systemd hostname=? addr=? terminal=? res=success'
-----
type=USER_END msg=audit(Monday 06 June 2016 17:54:46.117:33) : pid=9736 uid=root auid=unset ses=unset
msg='op=PAM:session_close acct=root exe=/bin/su hostname=? addr=? terminal=/dev/pts/4 res=success'
-----
type=CRED_DISP msg=audit(Monday 06 June 2016 17:54:46.117:34) : pid=9736 uid=root auid=unset ses=unset
msg='op=PAM:setcred acct=root exe=/bin/su hostname=? addr=? terminal=/dev/pts/4 res=success'

```

FIGURE 5.13: Ubuntu Terminal User ID

16. Linux stores the scheduled tasks in **/var/spool/cron/** and **/etc/cron.daily** the system files. Find the scheduled tasks by verifying these files.

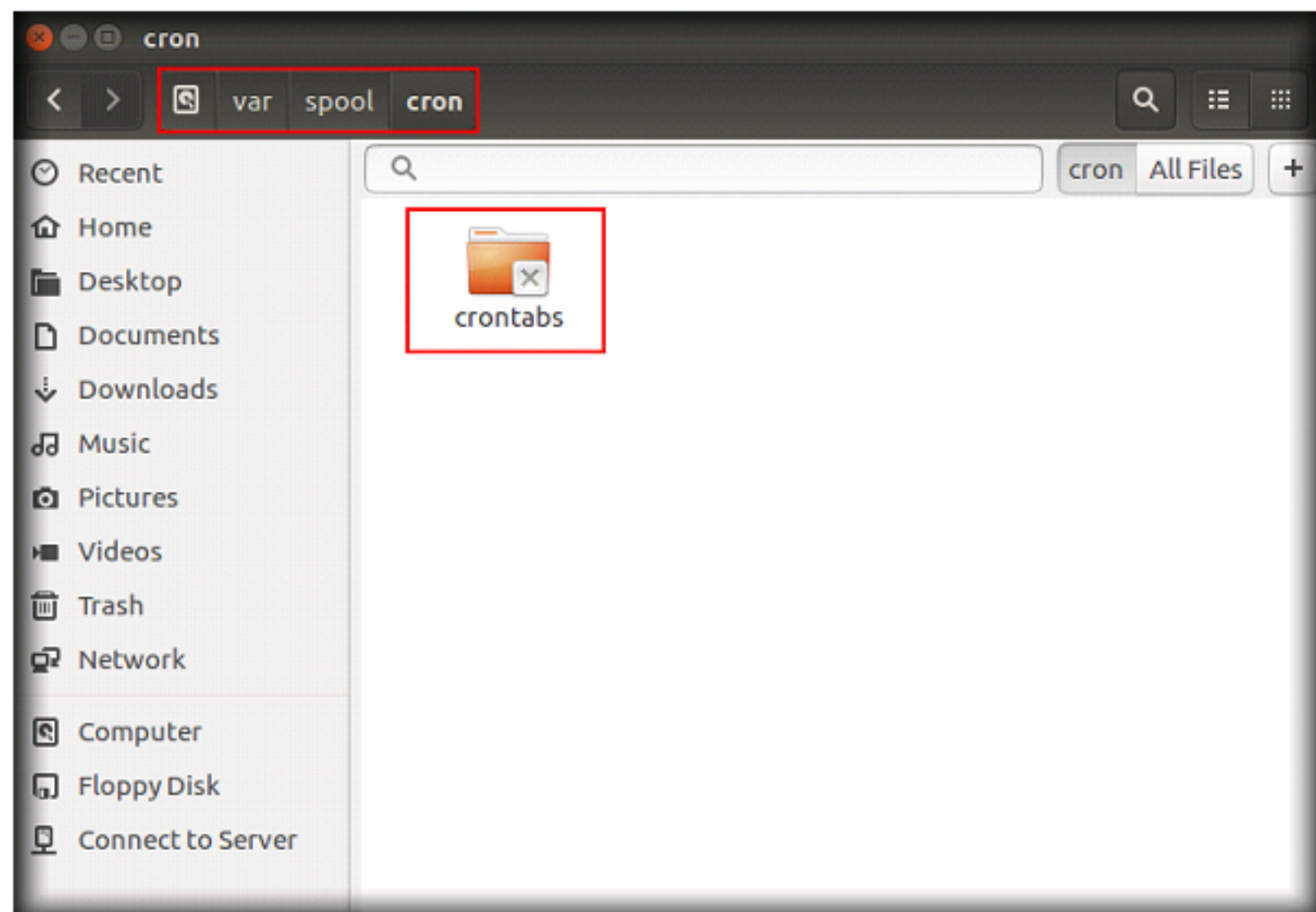


FIGURE 5.14: scheduled tasks location

17. The cron files also store data about the tasks scheduled hourly, daily, weekly and monthly. To view the daily scheduled task files go to **/etc/cron.daily**.

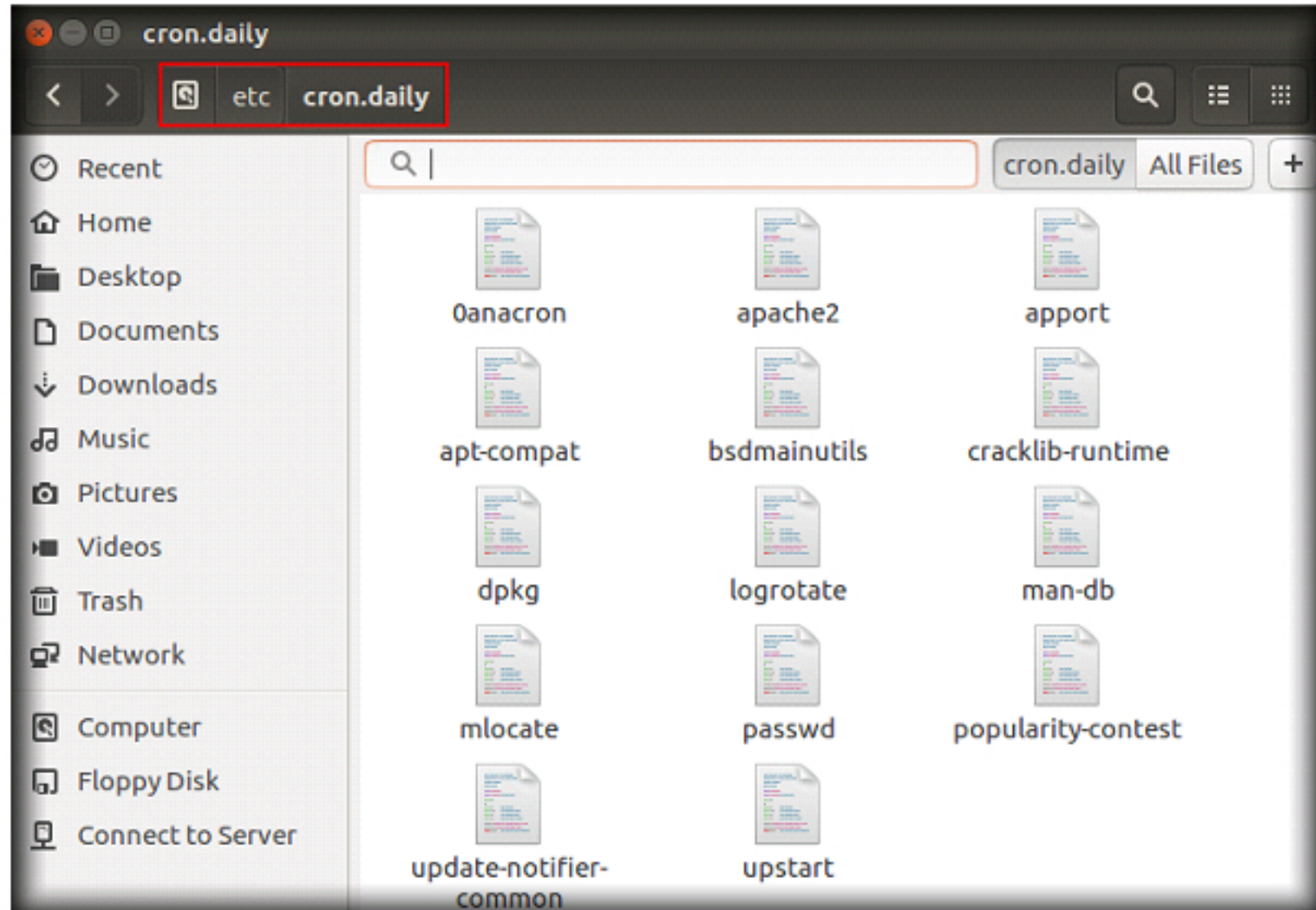


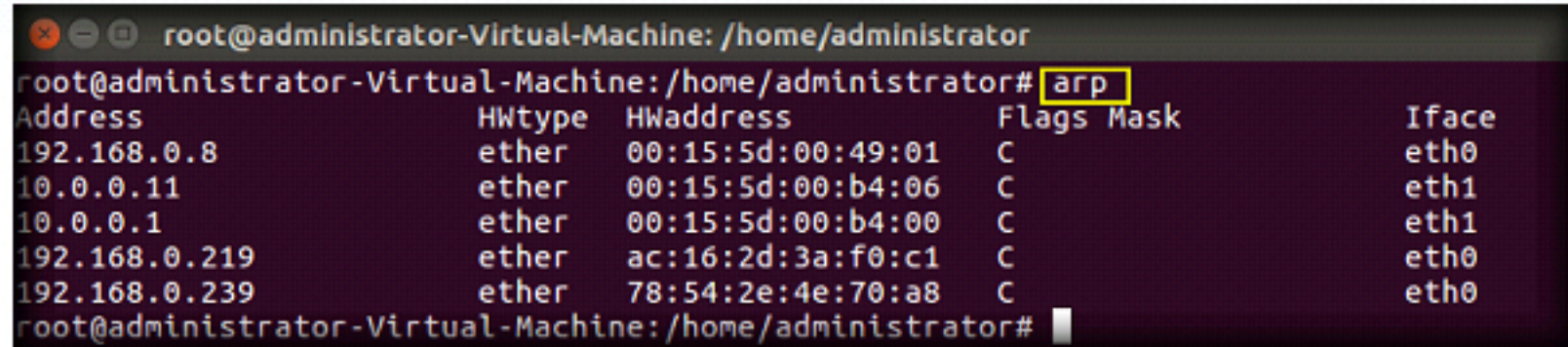
FIGURE 5.15: daily scheduled task files location

18. The **.bash_history** file contains the command history in the Linux system. To view the history, navigate to the **Home** directory and double-click **.bash_history** to view the entire bash history.



FIGURE 5.16: Linux system command history

19. Find the ARP Cache of the system using the **arp** command.



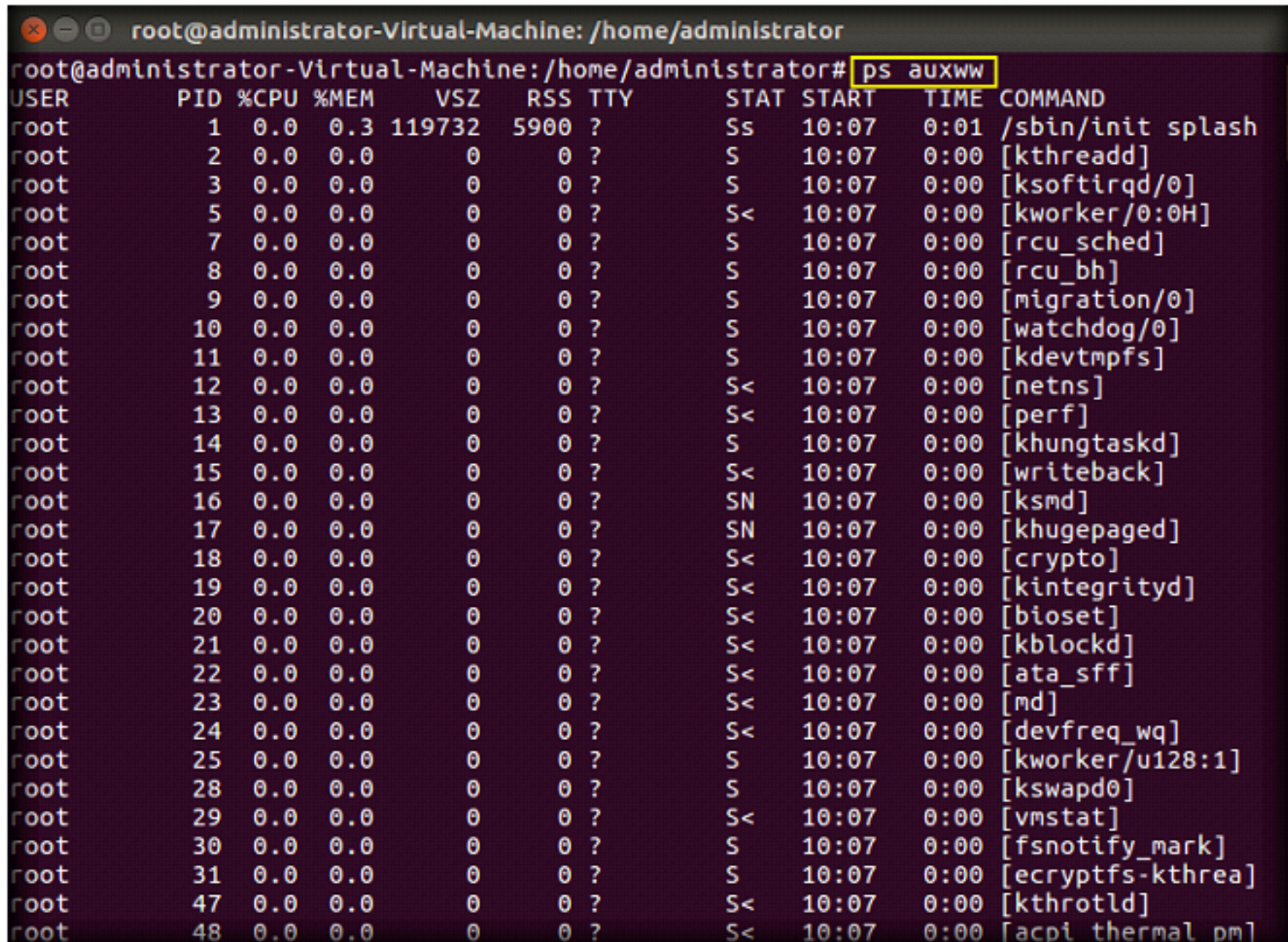
```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# arp
Address      HWtype  HWaddress  Flags Mask  Iface
192.168.0.8   ether    00:15:5d:00:49:01  C      eth0
10.0.0.11     ether    00:15:5d:00:b4:06  C      eth1
10.0.0.1      ether    00:15:5d:00:b4:00  C      eth1
192.168.0.219 ether    ac:16:2d:3a:f0:c1  C      eth0
192.168.0.239 ether    78:54:2e:4e:70:a8  C      eth0
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.17: Ubuntu Terminal Finding ARP Cache

20. Use the **ps** command to view the running processes in the system. You can use the option **auxww** to view all details of the running processes.



```

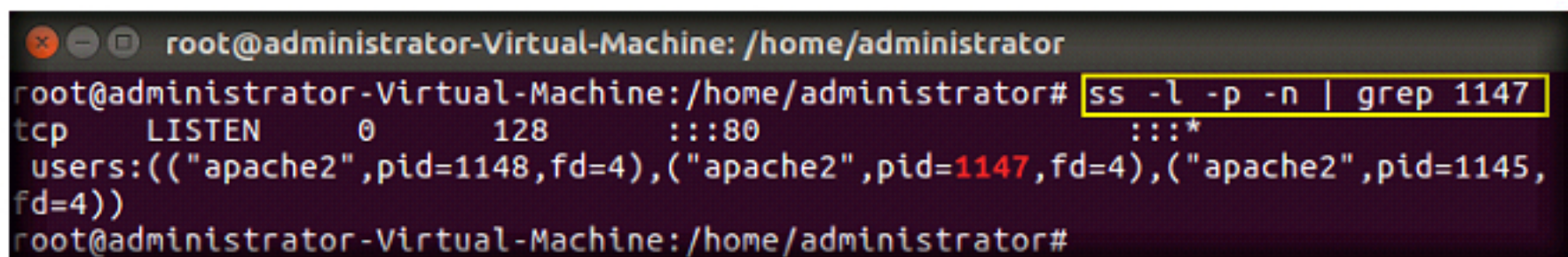
root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# ps auxww
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3 119732  5900 ?        Ss   10:07   0:01 /sbin/init splash
root         2  0.0  0.0      0     0 ?        S    10:07   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    10:07   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   10:07   0:00 [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    10:07   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    10:07   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    10:07   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S    10:07   0:00 [watchdog/0]
root        11  0.0  0.0      0     0 ?        S    10:07   0:00 [kdevtmpfs]
root        12  0.0  0.0      0     0 ?        S<   10:07   0:00 [netns]
root        13  0.0  0.0      0     0 ?        S<   10:07   0:00 [perf]
root        14  0.0  0.0      0     0 ?        S    10:07   0:00 [khungtaskd]
root        15  0.0  0.0      0     0 ?        S<   10:07   0:00 [writeback]
root        16  0.0  0.0      0     0 ?        SN   10:07   0:00 [ksmd]
root        17  0.0  0.0      0     0 ?        SN   10:07   0:00 [khugepaged]
root        18  0.0  0.0      0     0 ?        S<   10:07   0:00 [crypto]
root        19  0.0  0.0      0     0 ?        S<   10:07   0:00 [kintegrityd]
root        20  0.0  0.0      0     0 ?        S<   10:07   0:00 [bioset]
root        21  0.0  0.0      0     0 ?        S<   10:07   0:00 [kblockd]
root        22  0.0  0.0      0     0 ?        S<   10:07   0:00 [ata_sff]
root        23  0.0  0.0      0     0 ?        S<   10:07   0:00 [md]
root        24  0.0  0.0      0     0 ?        S<   10:07   0:00 [devfreq_wq]
root        25  0.0  0.0      0     0 ?        S    10:07   0:00 [kworker/u128:1]
root        28  0.0  0.0      0     0 ?        S    10:07   0:00 [kswapd0]
root        29  0.0  0.0      0     0 ?        S<   10:07   0:00 [vmstat]
root        30  0.0  0.0      0     0 ?        S    10:07   0:00 [fsnotify_mark]
root        31  0.0  0.0      0     0 ?        S    10:07   0:00 [ecryptfs-kthrea]
root        47  0.0  0.0      0     0 ?        S<   10:07   0:00 [kthrotld]
root        48  0.0  0.0      0     0 ?        S<   10:07   0:00 [acpi_thermal_pm]

```

FIGURE 5.18: Ubuntu Terminal view system running processes

21. You can find the ports related to a particular process using the command **ss -l -p -n | grep <PID>**.

Note: If any error related to grep appears, you need to install grep on the machine. Issue the command, **apt-get install grep** to install grep on Ubuntu.



```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# ss -l -p -n | grep 1147
tcp    LISTEN  0      128      :::80      :::*
users: (("apache2",pid=1148,fd=4),("apache2",pid=1147,fd=4),("apache2",pid=1145,fd=4))
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.19: Ubuntu Terminal finding particular process ports

22. You can collect the current state data of the system by viewing the state of processes running in the **/proc** file system.

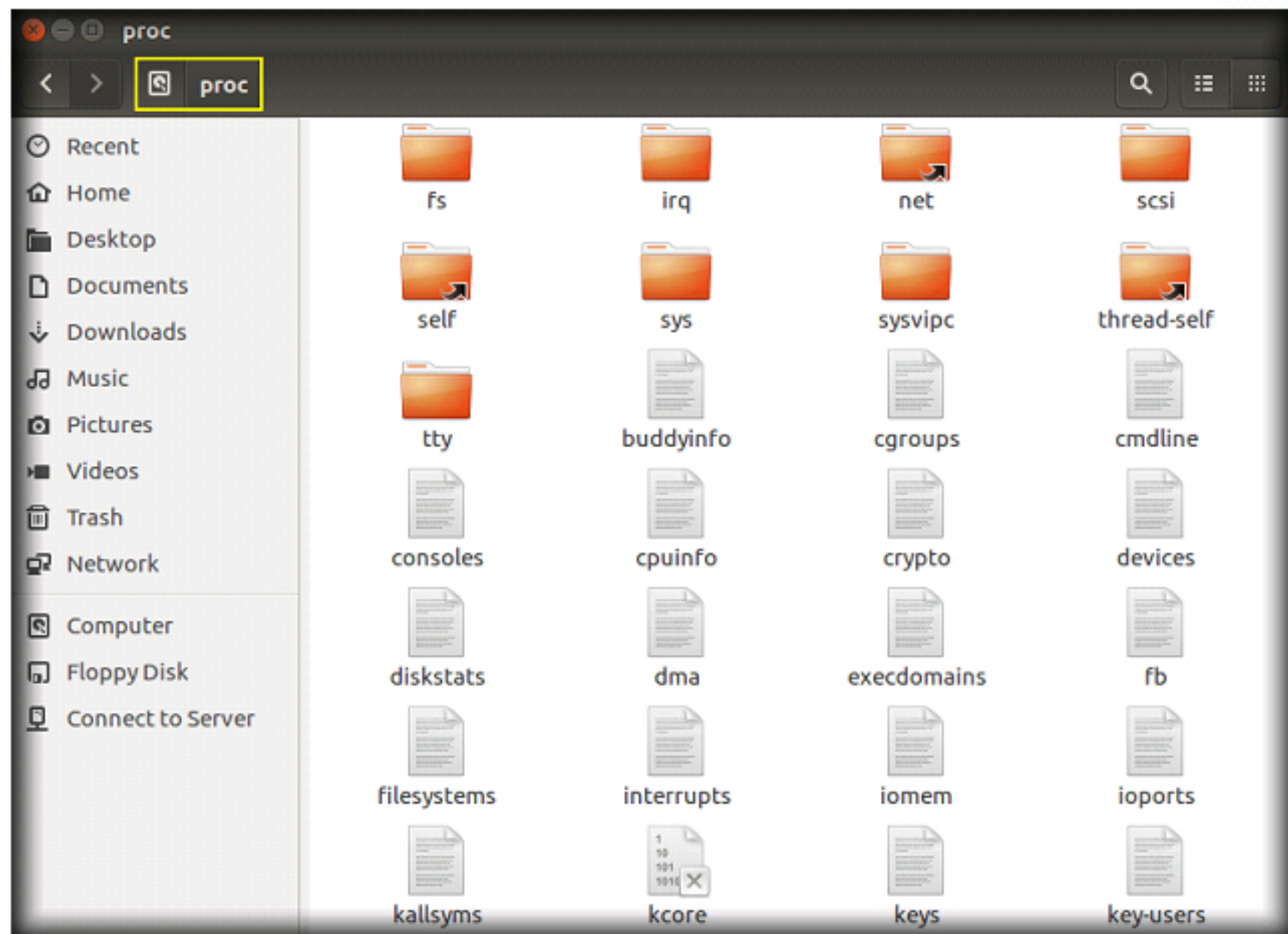


FIGURE 5.20: Current state data of the system

23. Clipboard stores the details of files or text copied recently. Copy and review the clipboard contents using the **xclip** command.

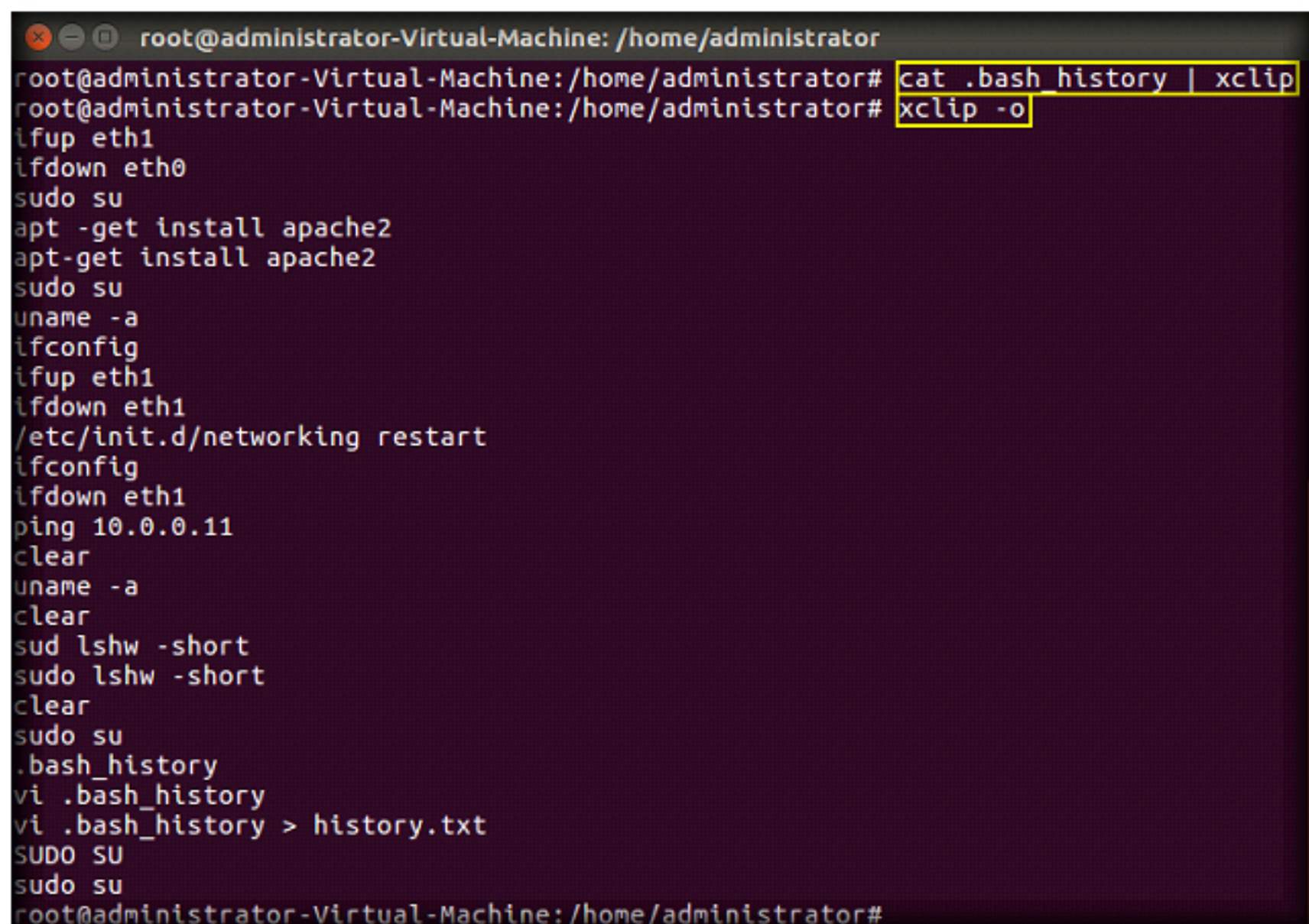
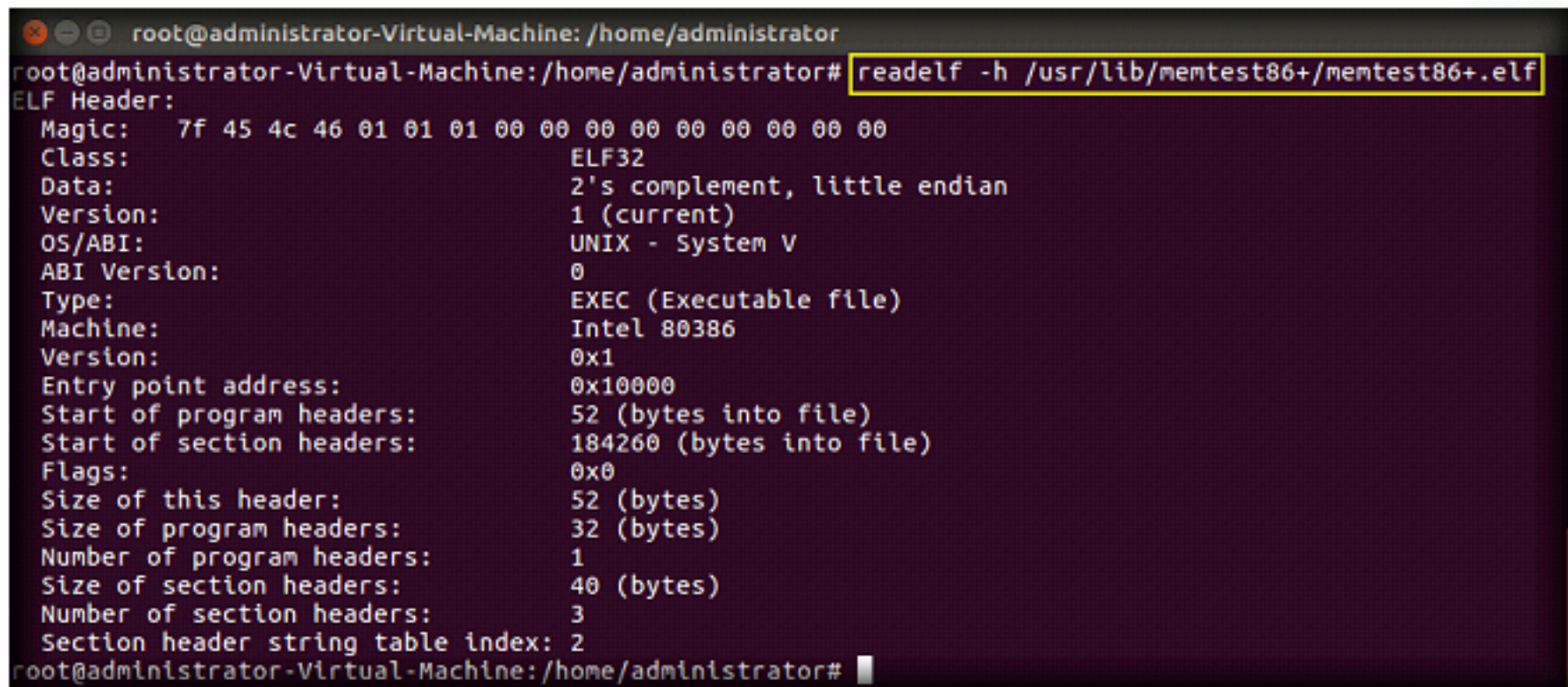


FIGURE 5.21: Ubuntu Terminal copy clip board contents

24. You can analyze the headers and sections of ELF files using the **readelf** command. Syntax of the command is **readelf option <elf file>**.



```

root@administrator-Virtual-Machine: /home/administrator
root@administrator-Virtual-Machine: /home/administrator# readelf -h /usr/lib/mentest86+/mentest86+.elf
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                                ELF32
  Data:                                      2's complement, little endian
  Version:                               1 (current)
  OS/ABI:                                UNIX - System V
  ABI Version:                           0
  Type:                                  EXEC (Executable file)
  Machine:                               Intel 80386
  Version:                               0x1
  Entry point address:                   0x10000
  Start of program headers:              52 (bytes into file)
  Start of section headers:             184260 (bytes into file)
  Flags:                                  0x0
  Size of this header:                   52 (bytes)
  Size of program headers:              32 (bytes)
  Number of program headers:             1
  Size of section headers:              40 (bytes)
  Number of section headers:             3
  Section header string table index:     2
root@administrator-Virtual-Machine: /home/administrator#

```

FIGURE 5.22: Ubuntu Terminal analyze the headers and sections of ELF files

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Internet Connection Required

☐ Yes

☒ No

Platform Supported

☒ Classroom

☒ iLabs

Lab

6

Analyzing Non-volatile Data in Linux System

Non-volatile data is the information that does not change when you switch off the system. Mostly, investigators collect non-volatile data from the image of a system hard disk.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

The non-volatile data remains the same even if the system is turned off. This data includes system files, applications, and permanent files an application creates during installation. Analysis of these files can provide the investigator with numerous evidences. To be an expert **forensic investigator**, you must understand the changes happening to a system when turned off and the process of collecting information from it.

Lab Objectives

The objective of this lab is to help students learn how to analyze an image of a Linux hard disk and gather required evidence from it.

Lab Environment

To carry out the lab, you need:

- Autopsy located at **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Linux Forensics Tools\Autopsy**
- A computer running **Windows Server 2012**
- Administrative privileges to run tools
- A web browser with an **Internet** connection

Lab Duration

Time: 20 Minutes

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics**

Overview of Autopsy

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. This tool helps investigators to view the file system, retrieving deleted data, performing timeline analysis and web artifacts, etc., during a forensic investigation.

Lab Tasks

1. Before beginning this lab, navigate to **C:\CHFI-Tools\Evidence Files\Linux Image**, right-click on **Linux_disk1.7z** and select **Extract Here**. On extracting the file, delete **Linux_disk1.7z**.
2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 06 Operating System Forensics\Linux Forensics Tools\Autopsy**.
3. Double-click **autopsy-4.0.0-64bit.msc** to launch the setup, and follow the wizard-driven installation instructions to install the application.
4. Double-click **Autopsy 4.0.0** shortcut icon located on the Desktop to launch the application.
5. The main window of **Autopsy** will appear.

Note: You can also launch the tool from **Apps** screen.

6. Click the **Create New Case** option.

 T A S K 1

Select the Forensics Image



FIGURE 6.1: Autopsy Create New Case option

7. In the **New Case Information window**, provide **Case Name**, **Base Directory** and click the **Next** button.

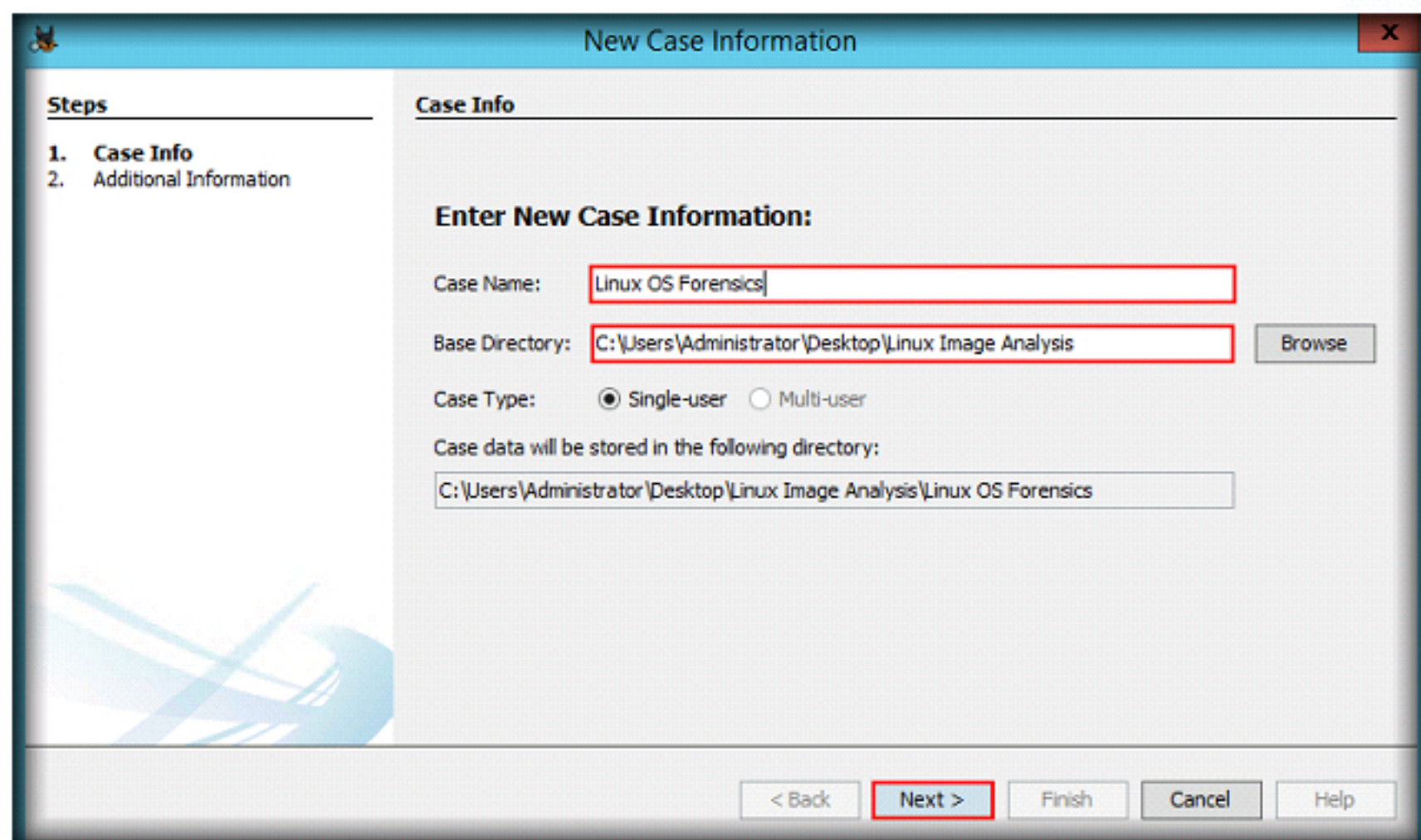


FIGURE 6.2: Autopsy New Case Information window

8. Provide the **Case Number** and **Examiner details**, and click **Finish** button.

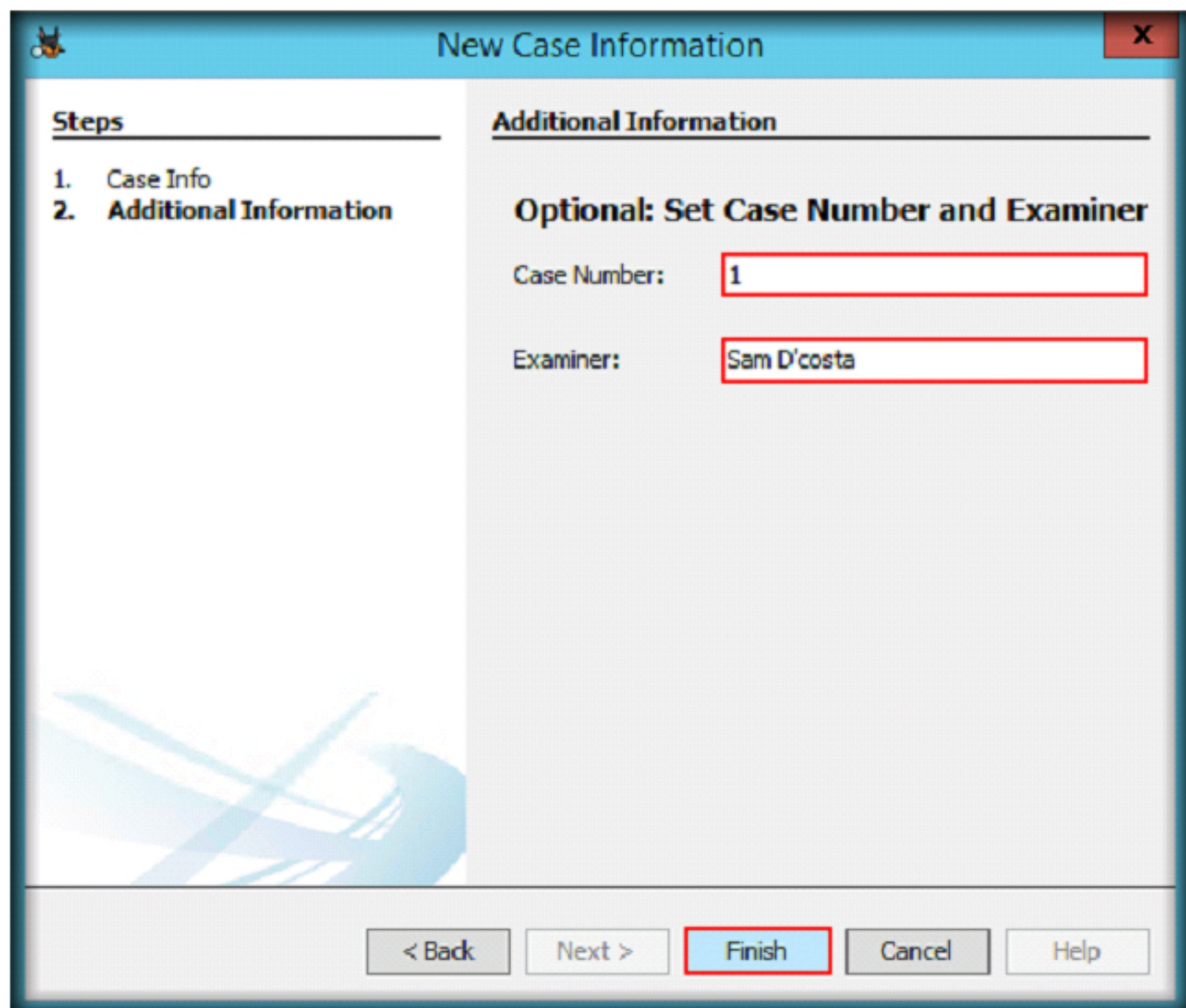


FIGURE 6.3: Autopsy New Case Information window

- Click the **Browse** button.

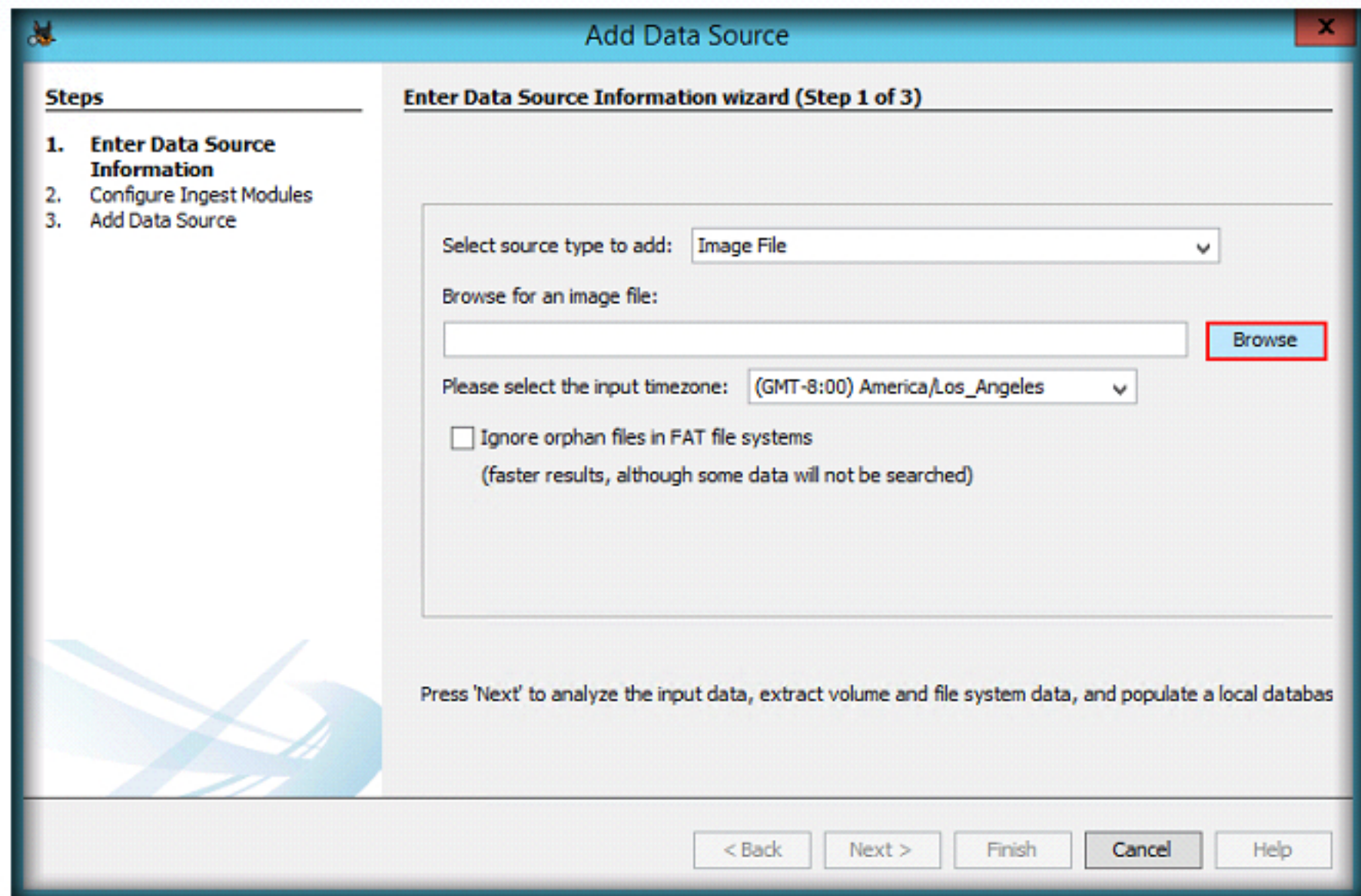


FIGURE 6.4: Autopsy Enter Data Source Information wizard

- Navigate to the location, **C:\CHFI-Tools\Evidence Files\Linux Image**, select the **Linux_Image1.img** file and click the **Open** button.

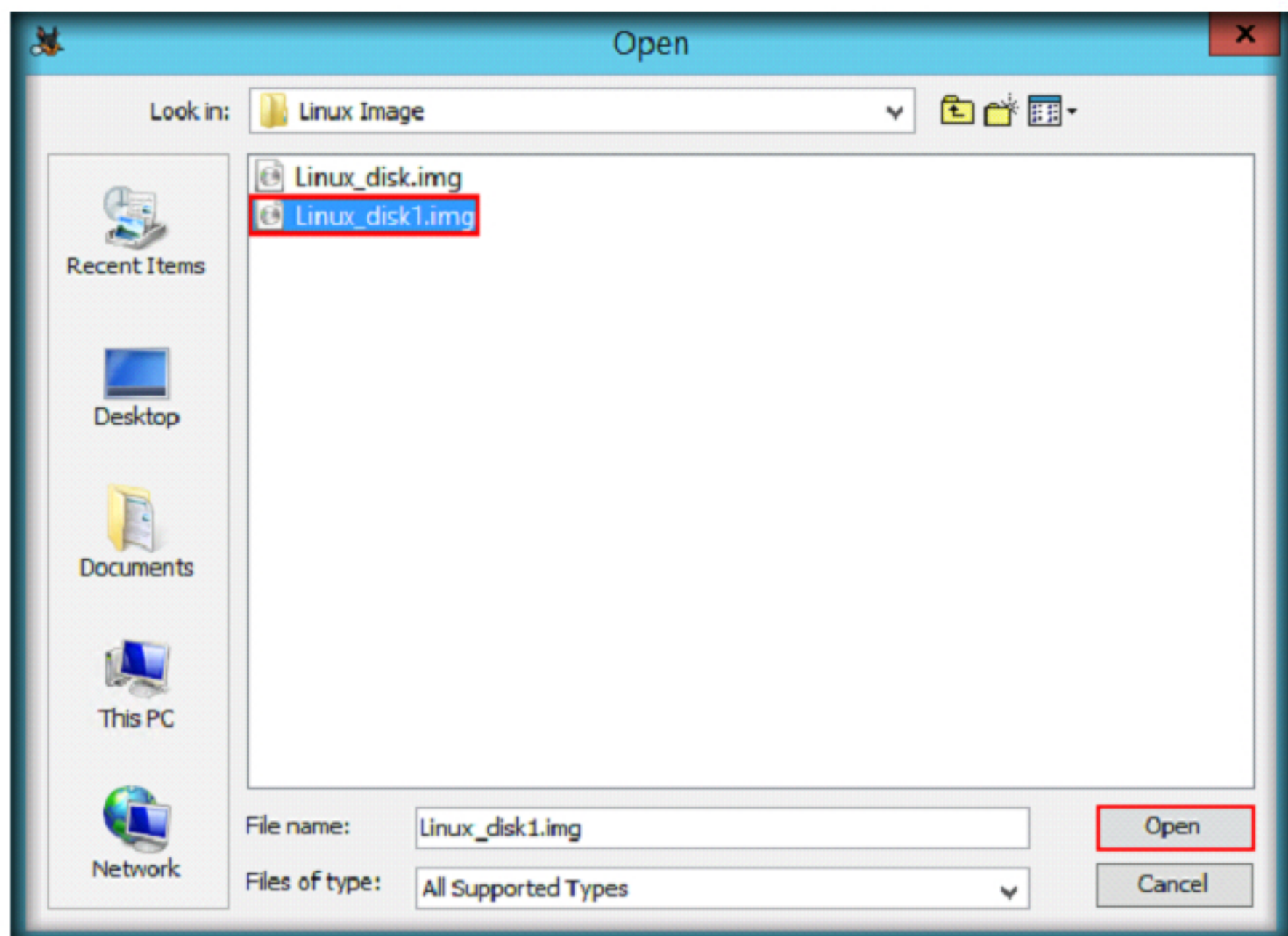


FIGURE 6.5: Autopsy open Linux Image

11. Click the **Next** button.

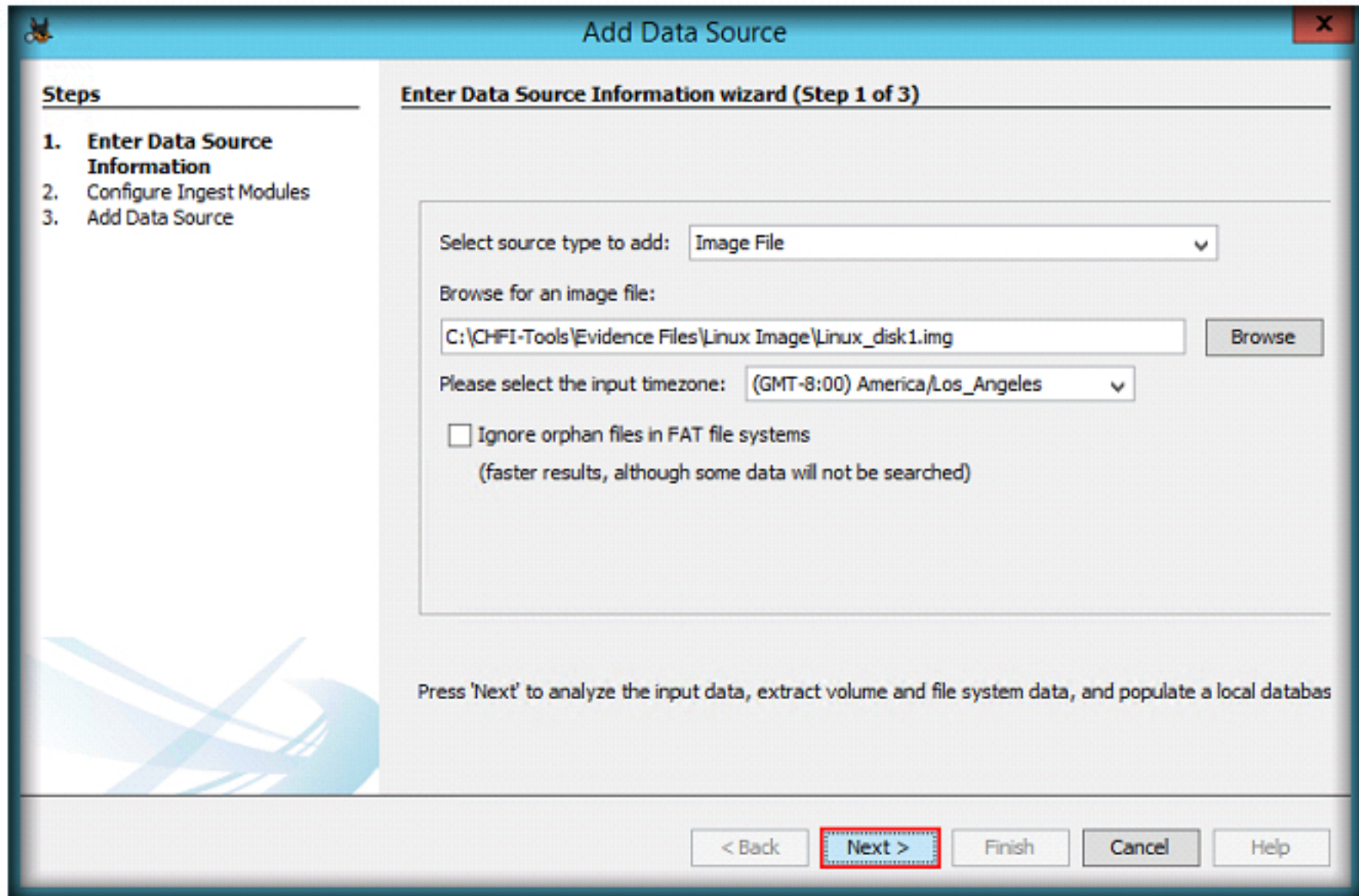


FIGURE 6.6: Autopsy Enter Data Source Information wizard

12. Check the required boxes and click the **Next** button.

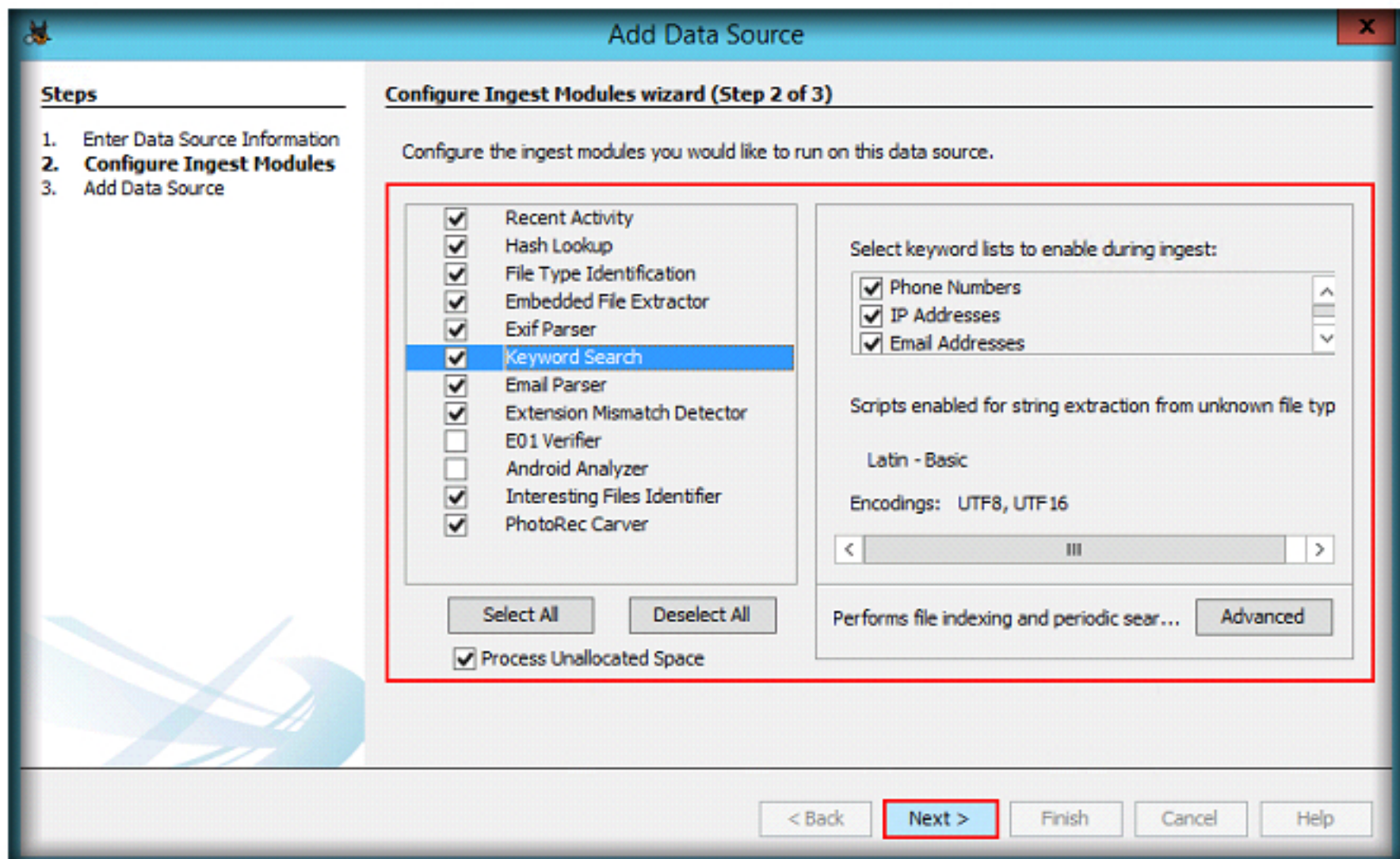


FIGURE 6.7: Configure Ingest Modules wizard

13. Click the **Finish** button.

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

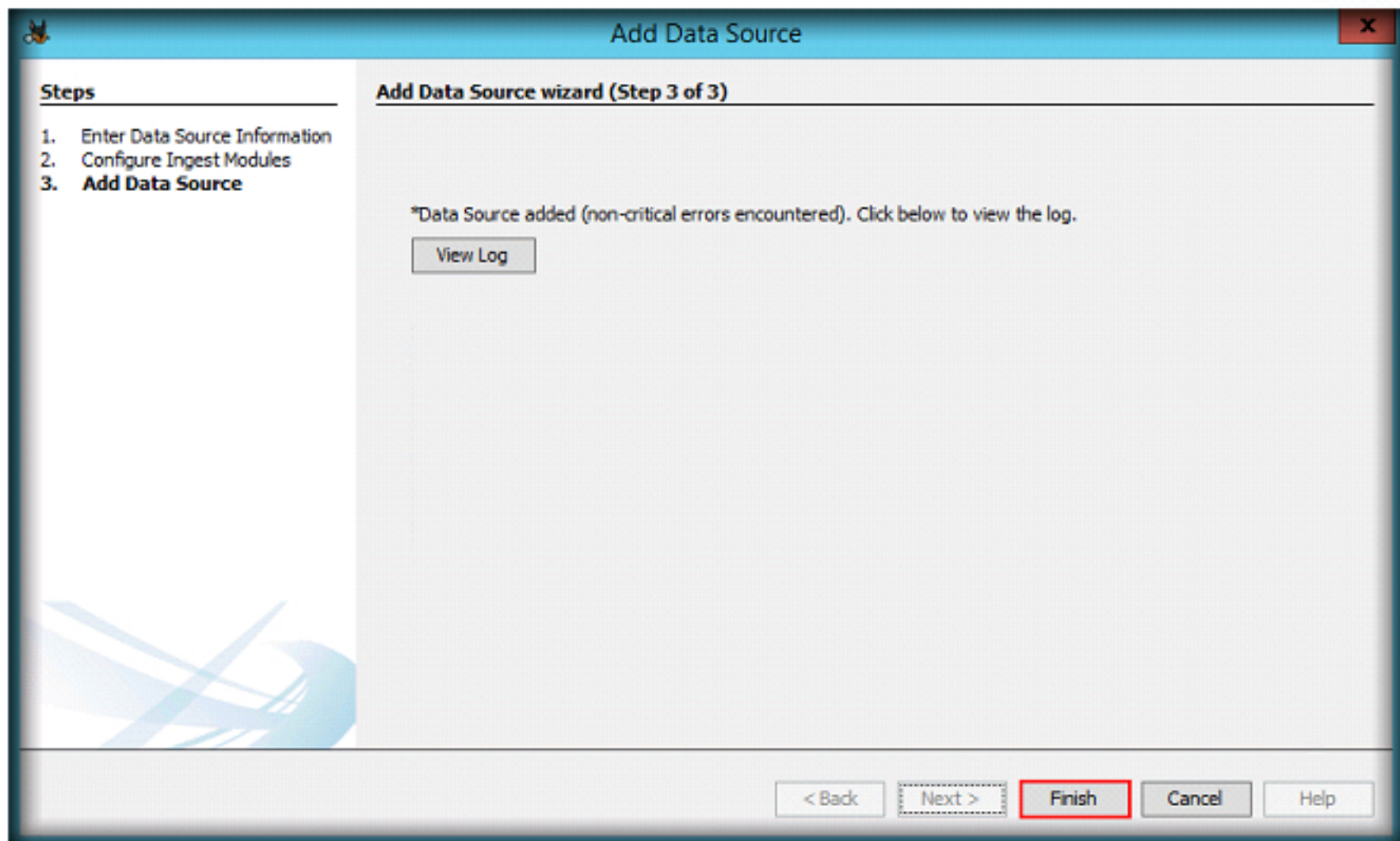


FIGURE 6.8: Add Data Source wizard

14. The tool will display the result after analysis. Expand the **Data Sources** node in the left pane. The Data Sources option will include the name of the image file you have analyzed.

15. Click the image name, here **Linux_disk1.img**, to expand and see its contents. It will include all the necessary operating systems data.



TASK 2

Examine the Forensic Image

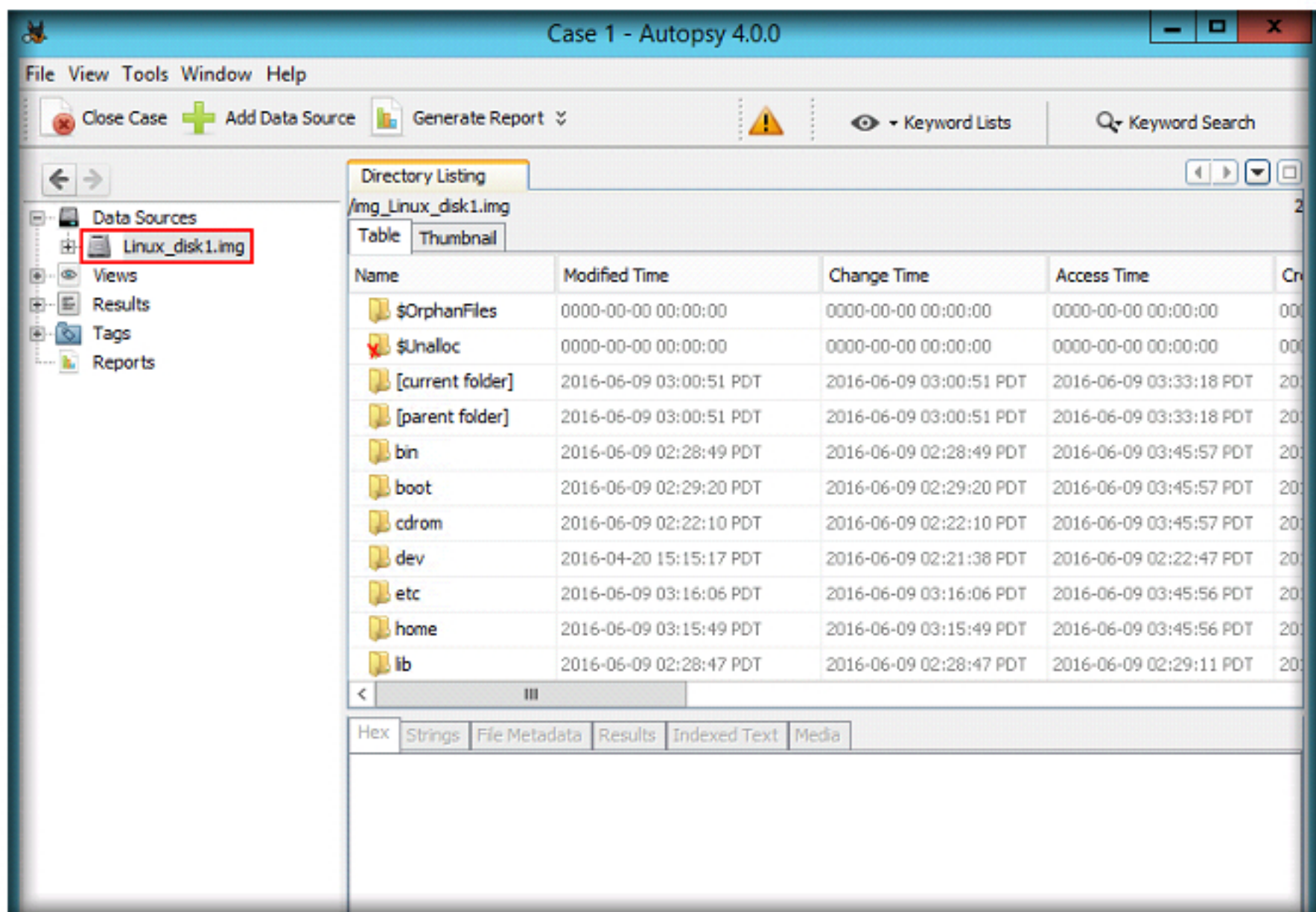


FIGURE 6.9: Autopsy Case 1

16. The image contains folders each of which stores data related to files, process, services, tools and commands used on the Linux system.
17. The **bin** contains command binaries of all users. Click the **bin** option to see its content. Click the option you want to verify and review.
18. Select the **auto partition-loop** file option from the menu. Click the **Strings** tab to view all the strings present in a selected file. You can observe that the file contains **Syslog** information that stores **Linux log data**.

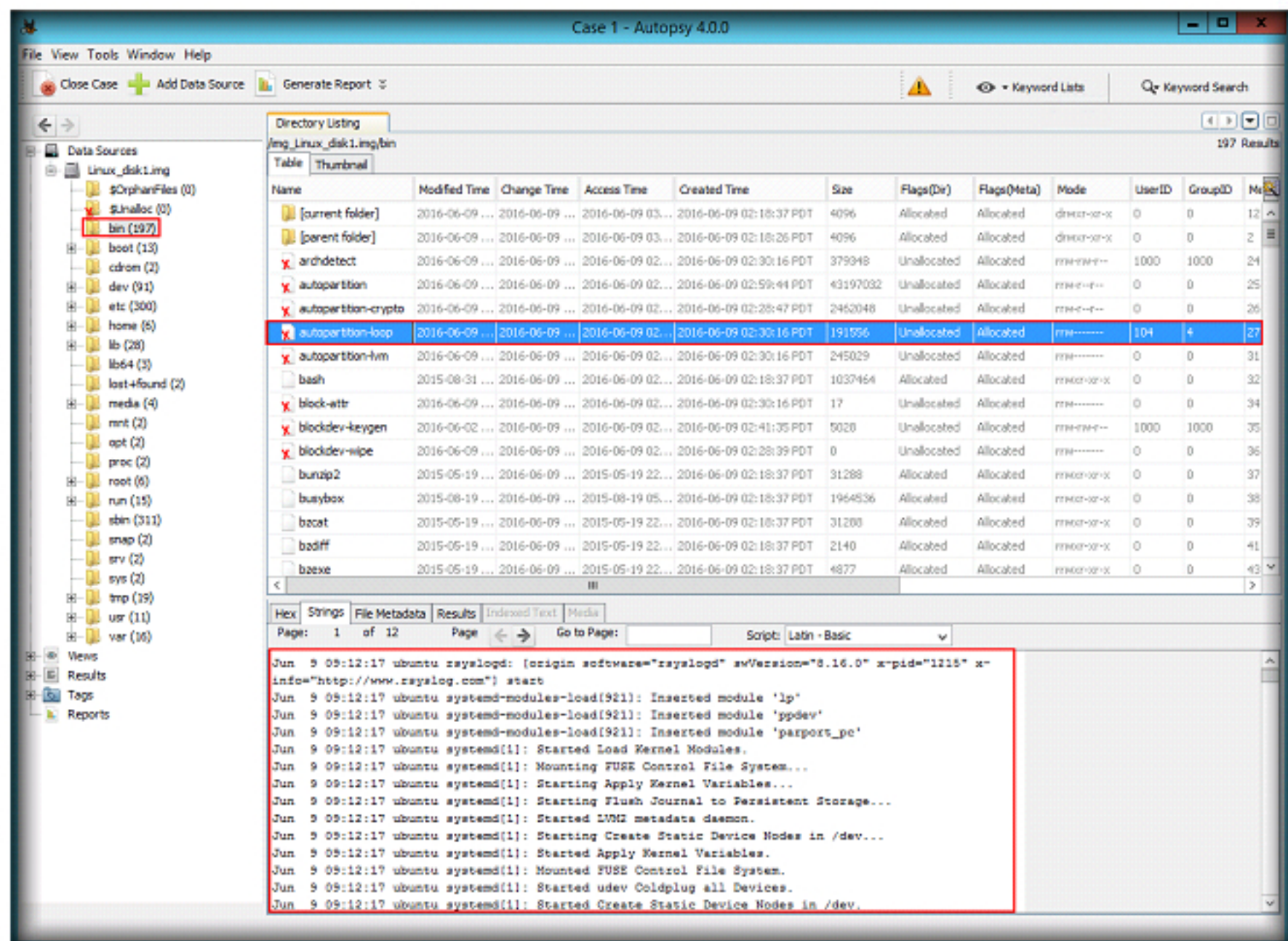


FIGURE 6.10: Autopsy Case 1 auto partition-loop file option

Note: The files that are marked with a red cross are the deleted files, which have been recovered by Autopsy. Analyze the deleted files to find any suspicious activities. It may also help in finding if the attacker has used any anti-forensic techniques that delete files and folders after completion of given task.

19. The **update-dev** file stores data about login sessions of different users in the Linux system. Select the **update-dev** file and click on **Strings** tab to view the file information in textual format.

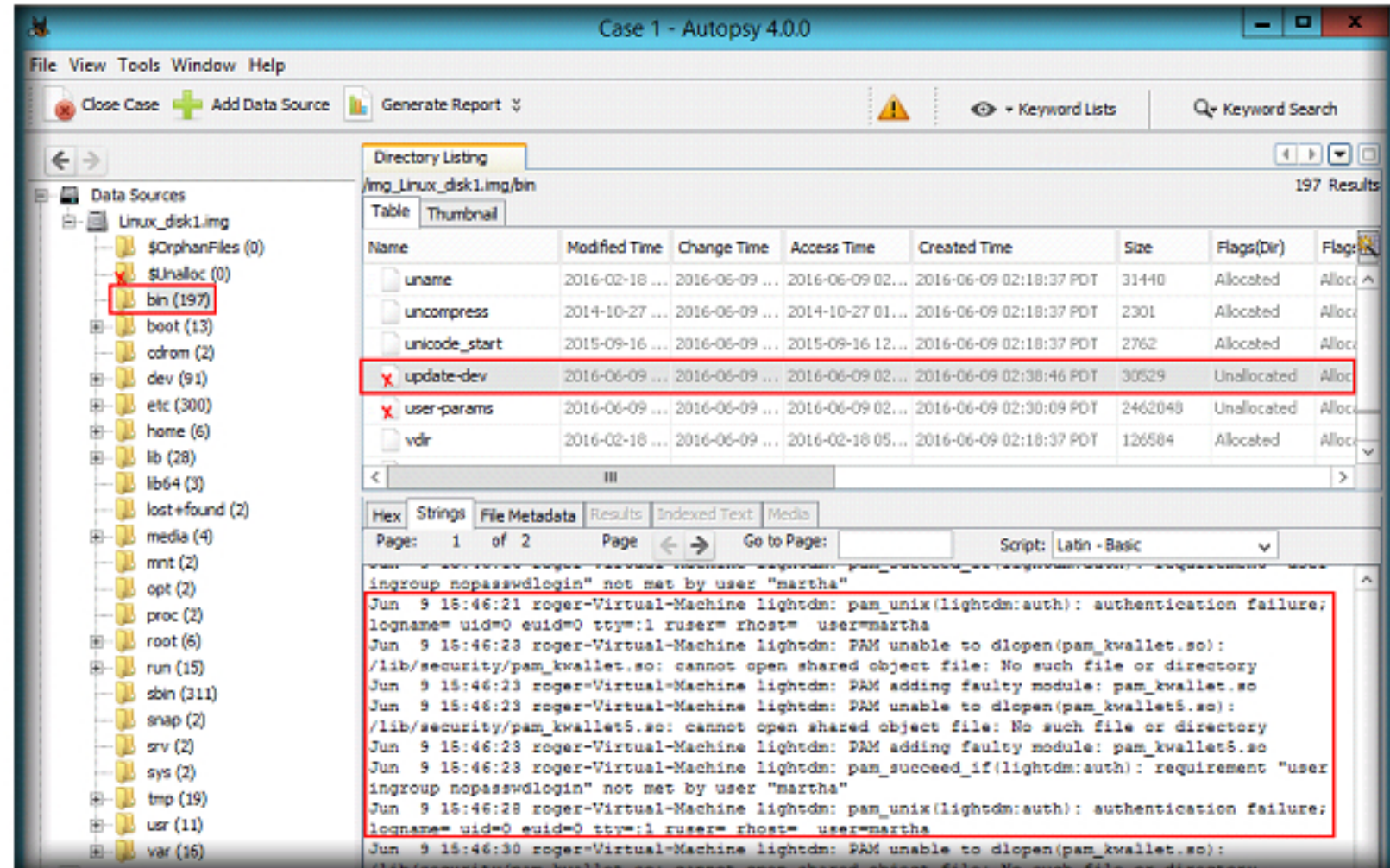


FIGURE 6.11: Autopsy Case 1 update-dev file information in textual format

20. Click the **boot** menu option to view the **bootloader files** of the Linux operating system present on the hard disk image.
21. Verifying these files helps you in finding the presence of any boot based malware.

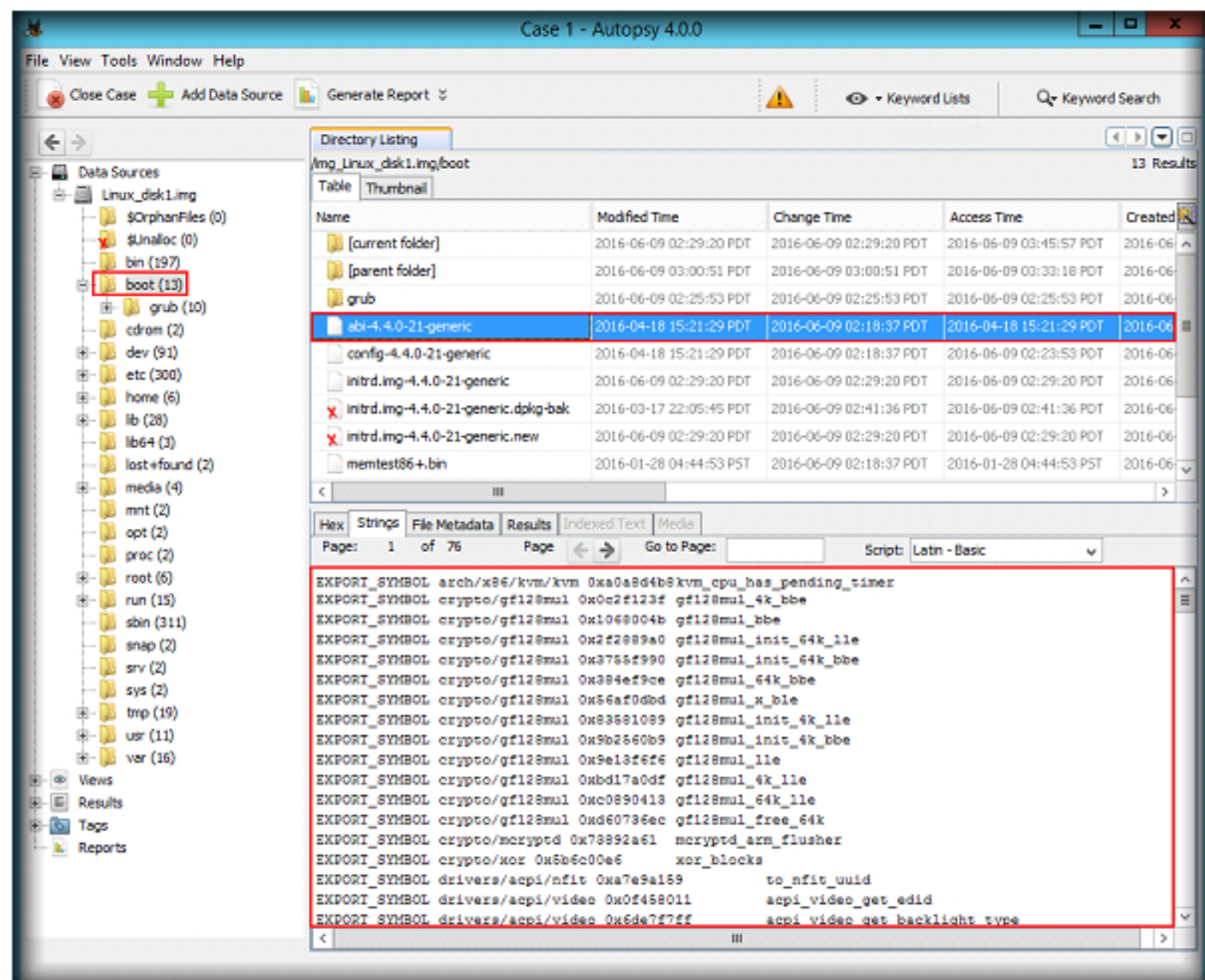


FIGURE 6.12: Autopsy Case 1 bootloader files

22. The **dev** file stores information about devices connected to the system. Click the option to see information about different audio, media, etc., files connected to the system.

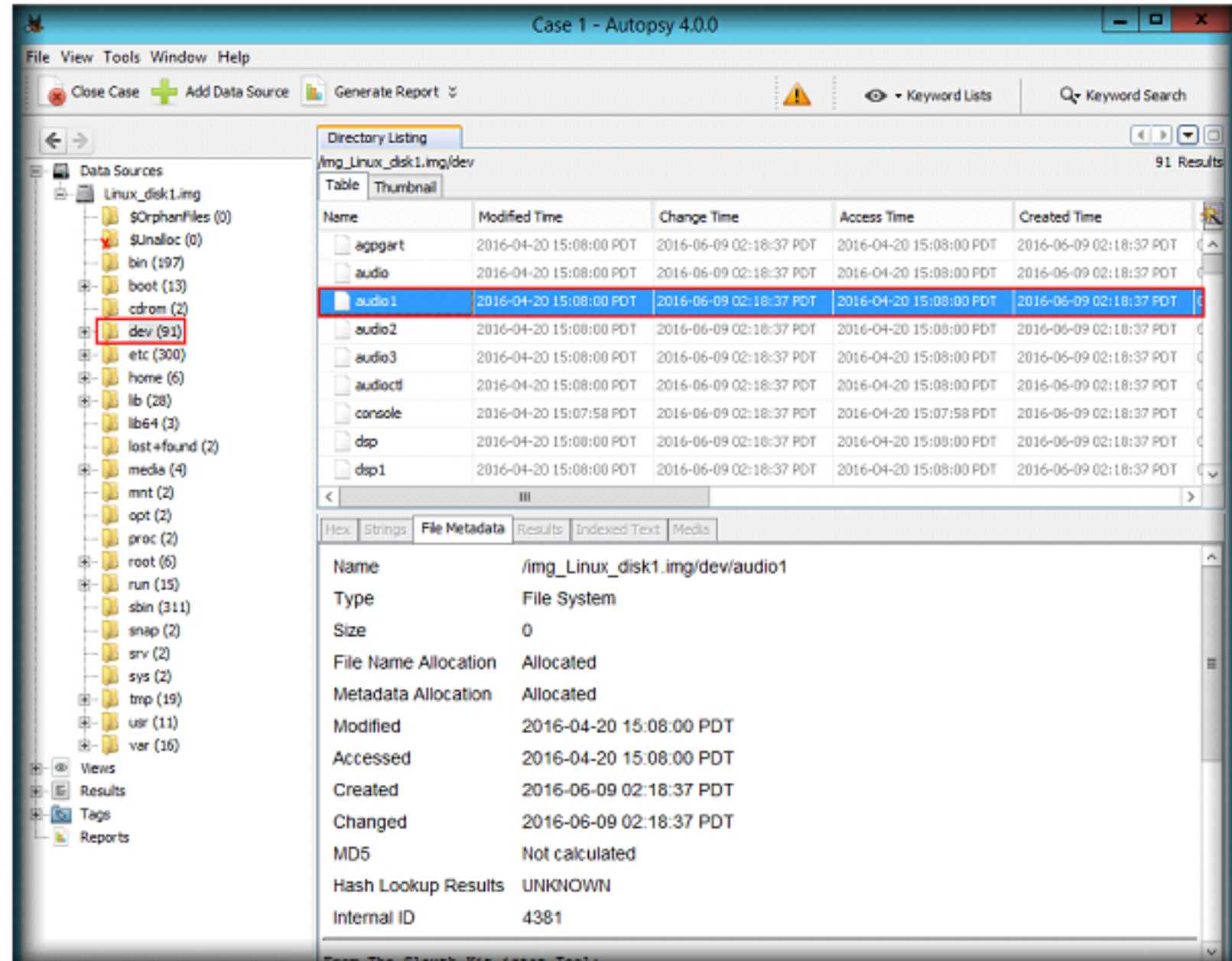


FIGURE 6.13: Autopsy Case 1 dev files

23. The **etc** folder contains system configuration files. Expand the etc node and click on it to view internal files.

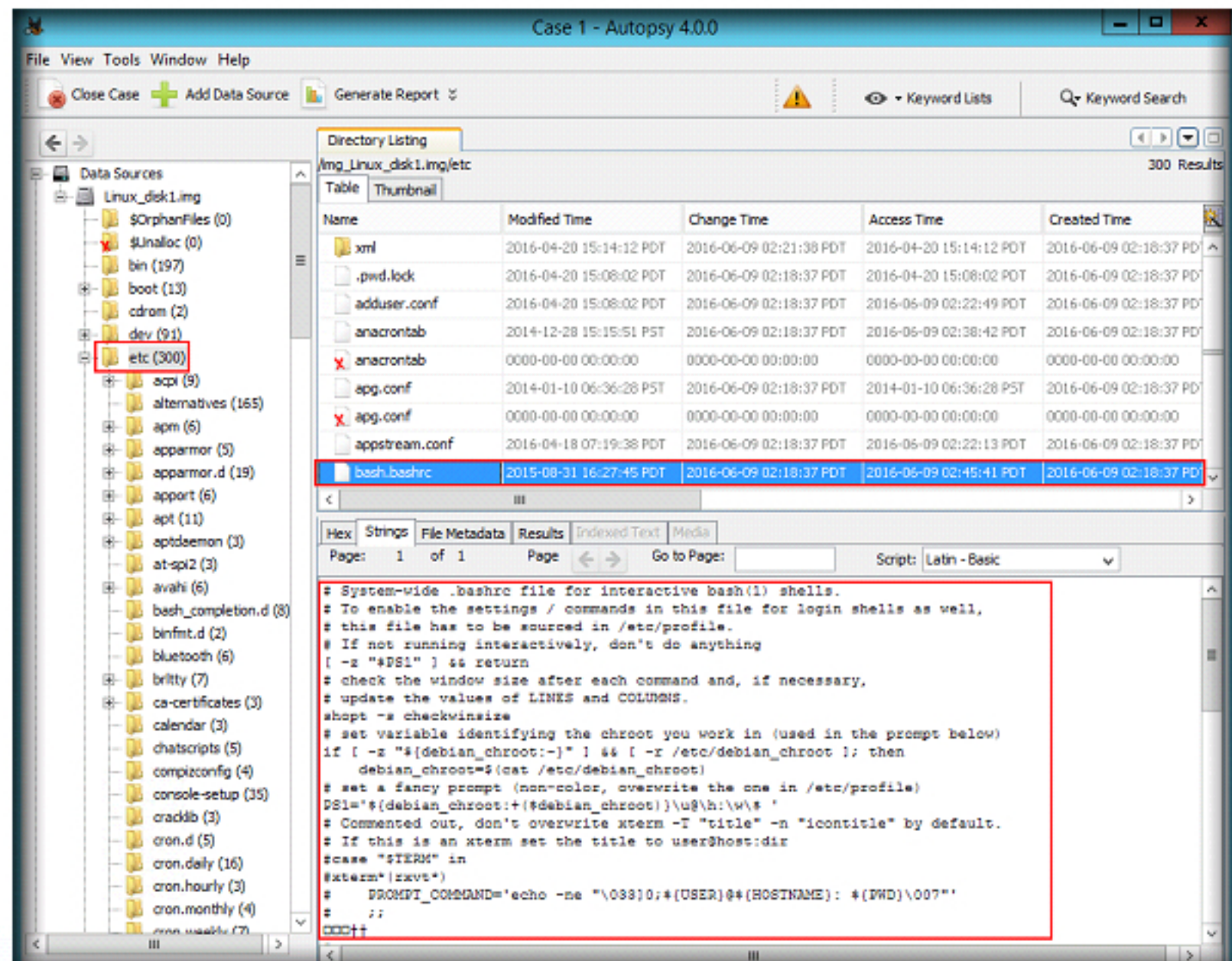


FIGURE 6.14: Autopsy Case 1 etc folder files

24. The **home** file stores details of user home directories. It helps users to view the files and folders stored on the system. It also consists of details of other user accounts present on the system.

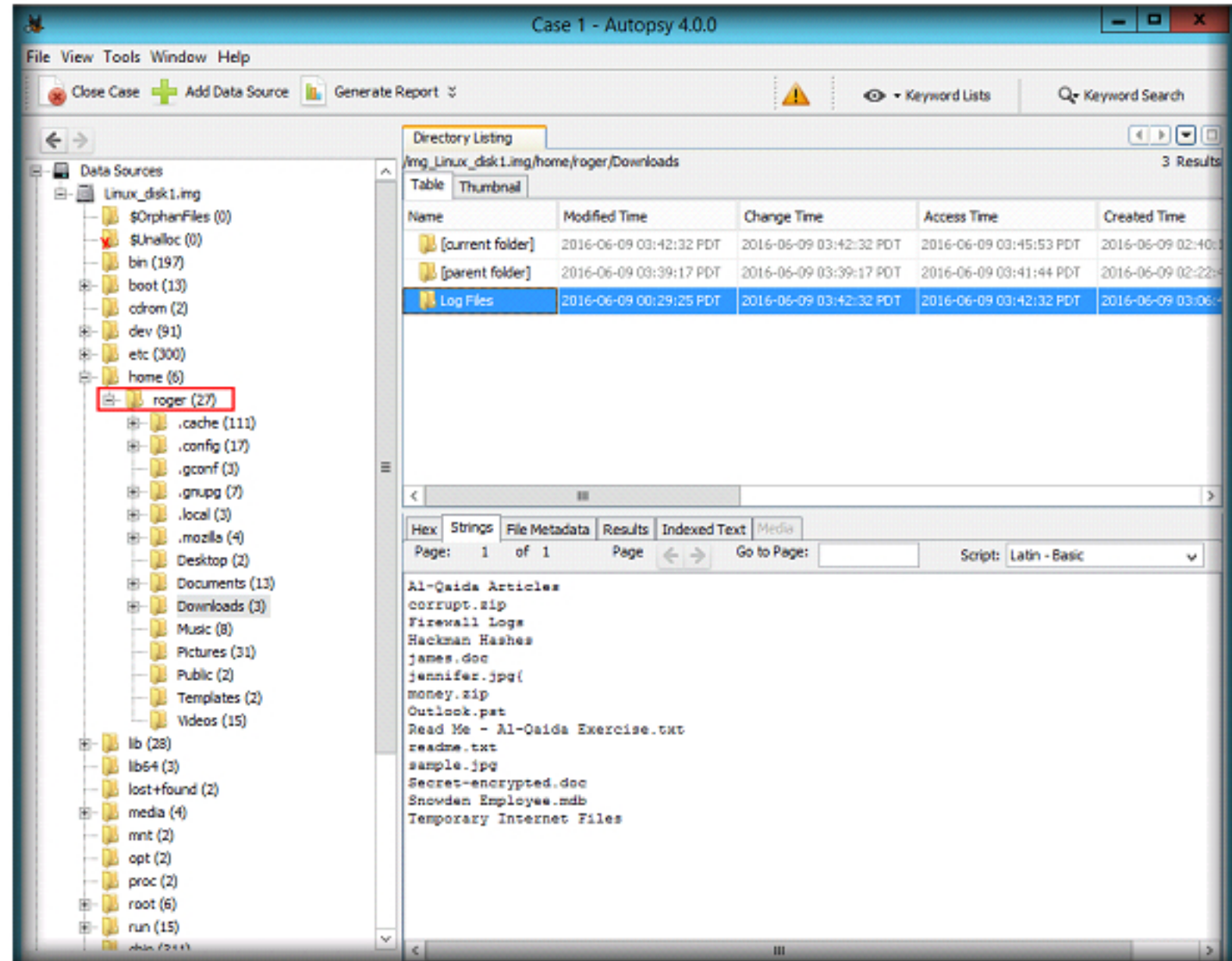


FIGURE 6.15: Autopsy Case 1 home file

25. Select the **var** folder from the left side menu. Expand the **log** folder from the sub menu and select **apt** folder under it. The apt folder contains **history.log** file that stores history of actions performed.

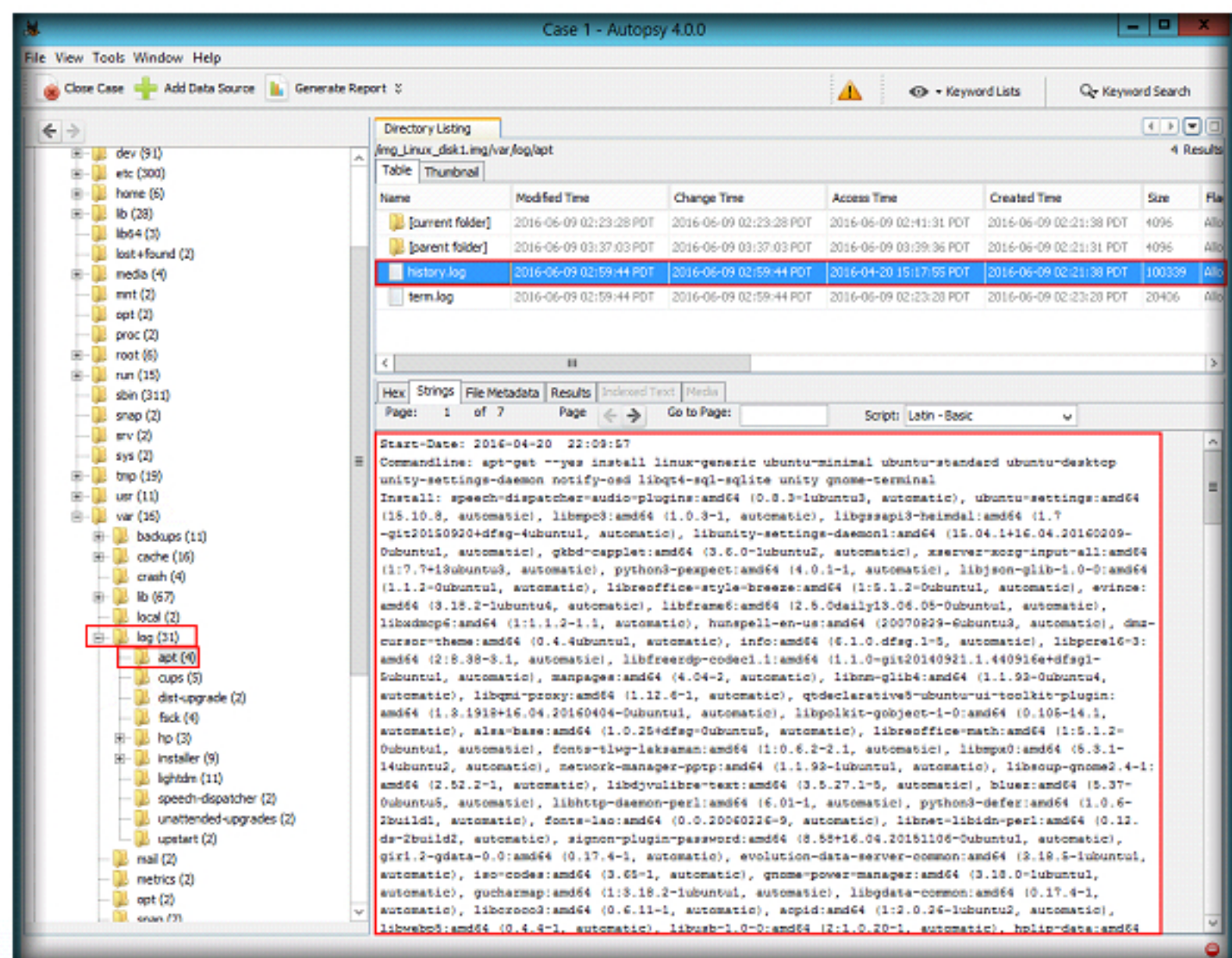


FIGURE 6.16: Autopsy Case 1 var file

26. Select the **cups** folder. It stores access logs, error logs, and page logs. Select the access log option in the Table tab to view the logs.

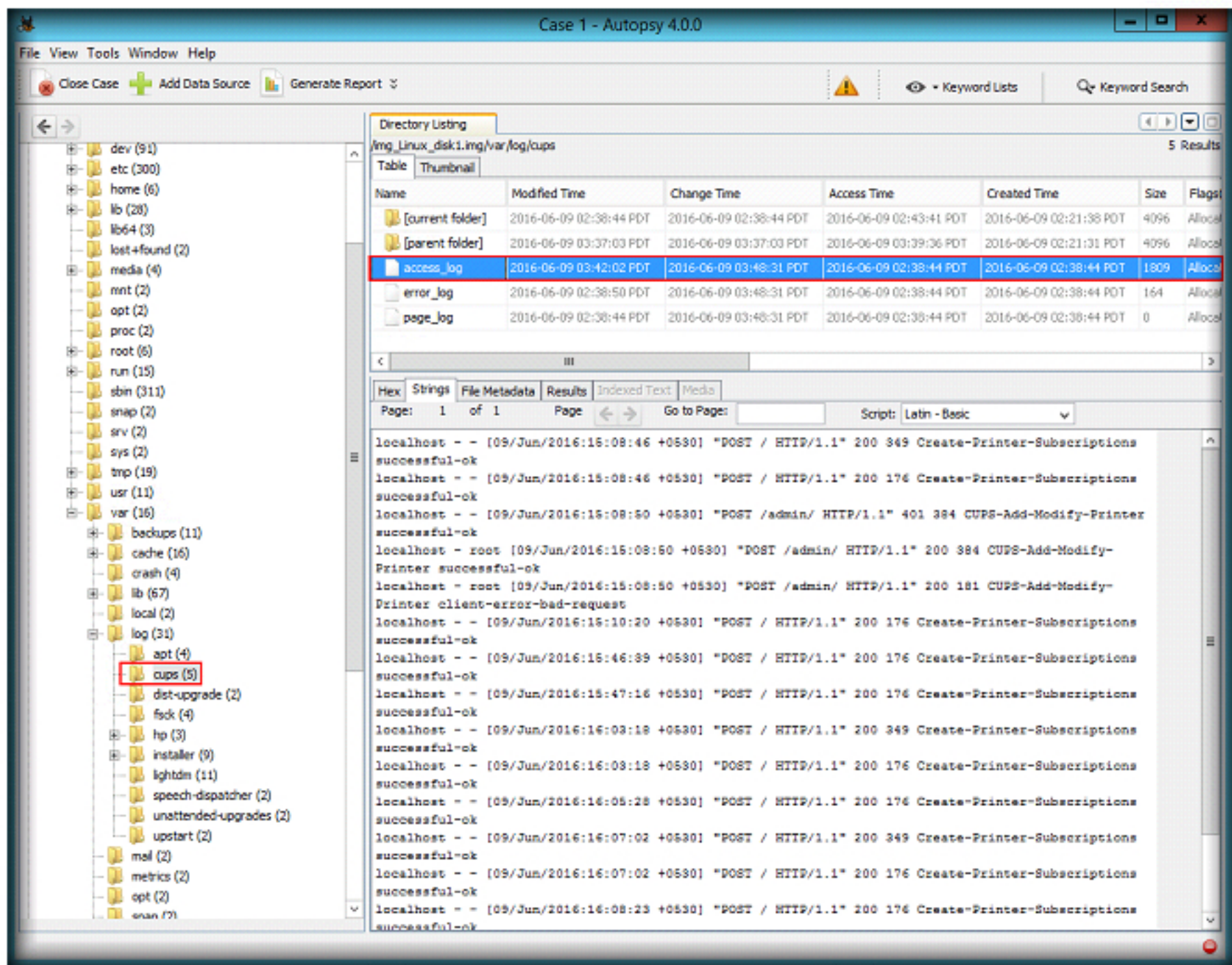


FIGURE 6.17: Autopsy Case 1 cups file

27. The tool also displays deleted files. Expand **Views** option from the left menu list, expand **Deleted Files** option and click **All** to view all the deleted files.

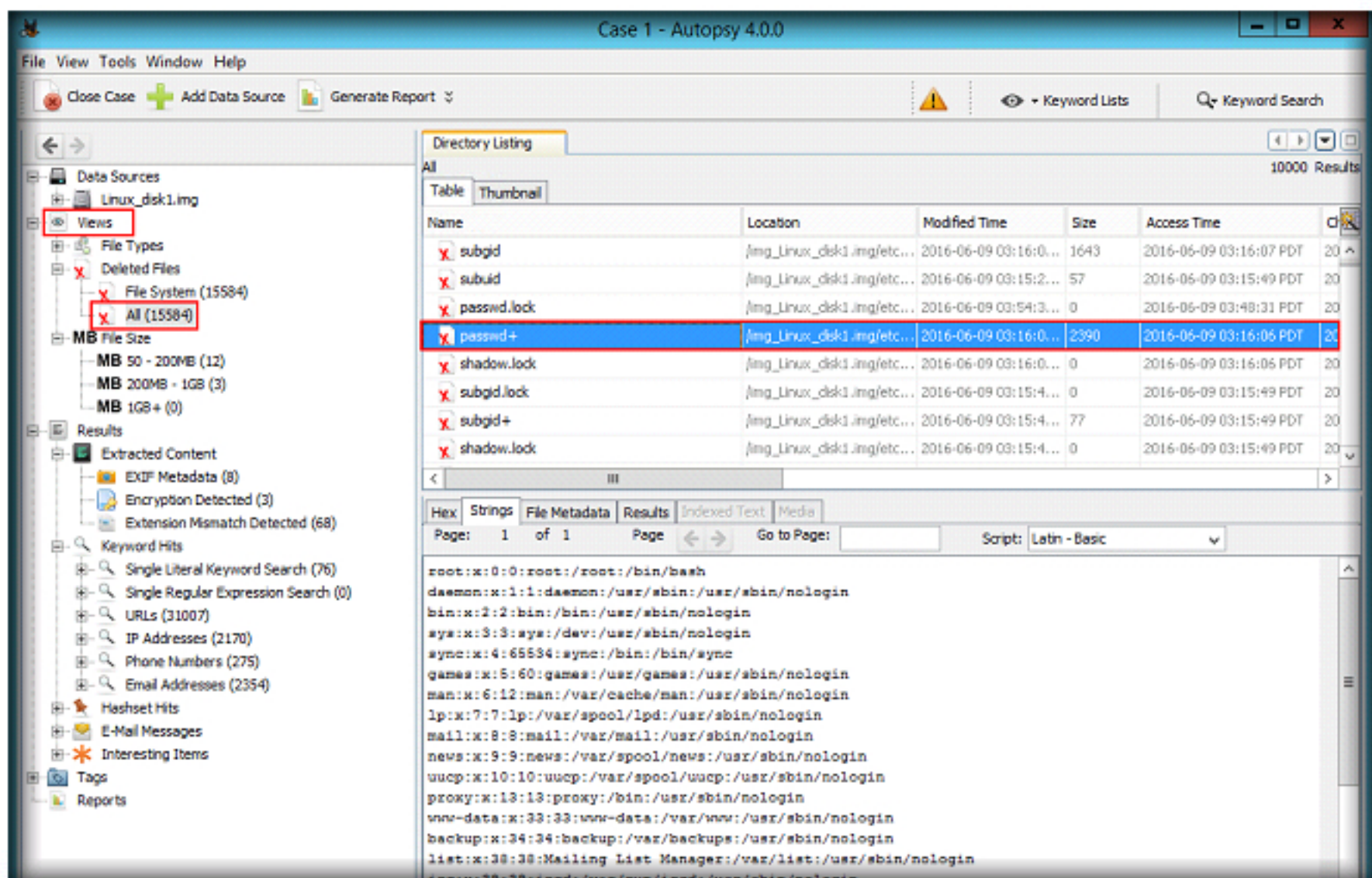


FIGURE 6.18: Autopsy Case 1 deleted files

28. Select the **Results** folder from left pane. It contains sections such as EXIF Metadata files, Encrypted Content and Extension Mismatch Detected. Analyze these files to look obfuscated malware files as well as metadata files.

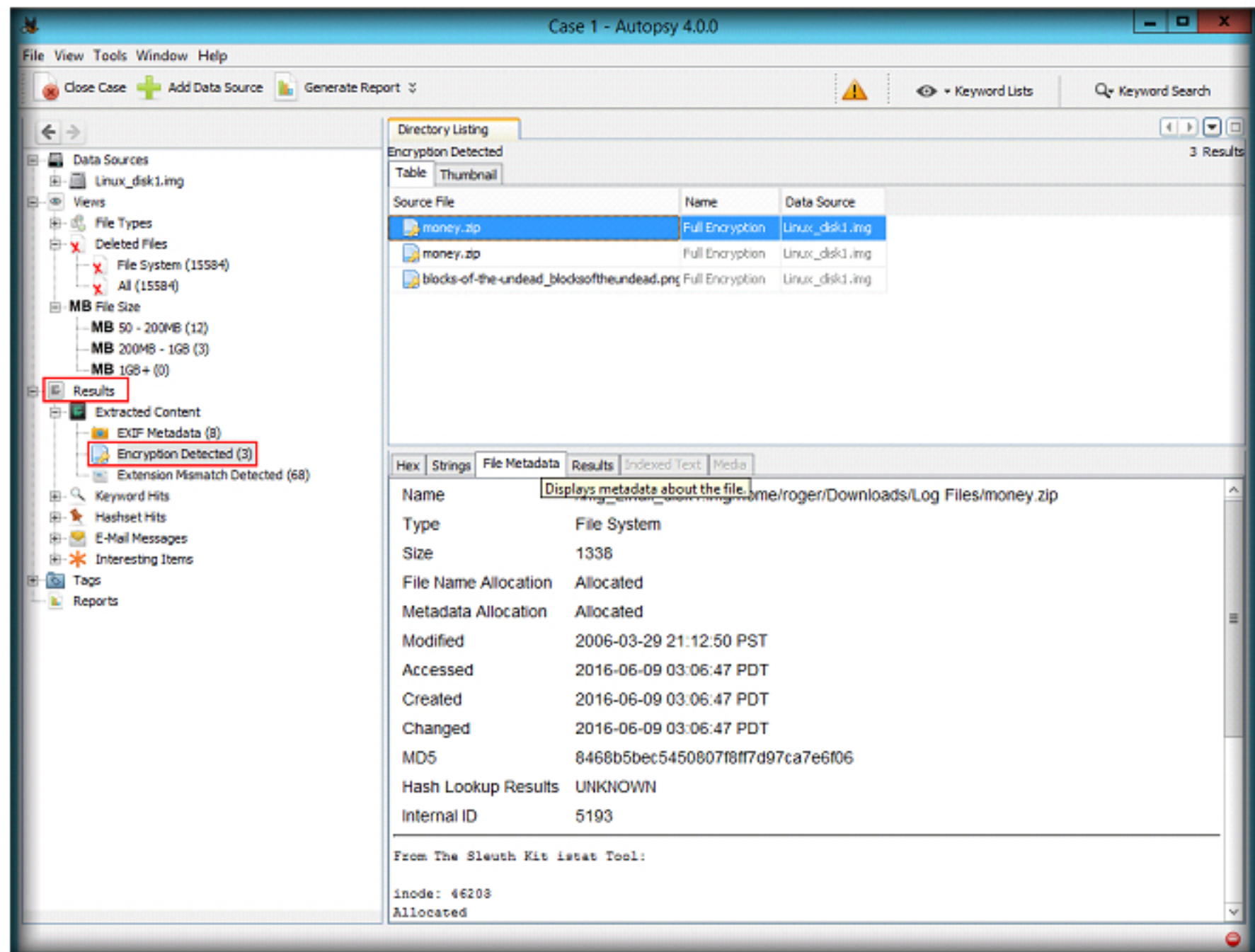


FIGURE 6.19: Autopsy Case 1 Results option

29. Similarly, analyze lib, media, mnt, opt, root, sbin, and tmp folders to analyze libraries and kernel modules, mount points of removable media, temporary mount points, add-on application packages, root user's home directory, system binaries and temporary files respectively.
30. Other system files include srv containing data for services provided, usr file with secondary hierarchy and user commands, var file with variable data such as log files, mail spools, caches and lock files.

Lab Analysis

Analyze and document the results related to the lab exercise.

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

Internet Connection Required	
☐ Yes	☒ No
Platform Supported	
☒ Classroom	☒ iLabs