Understanding Hard Disks and File Systems

Module 03

Understanding Hard Disks and File Systems

A hard disk drive is a non-volatile, random access digital data storage device used in most computer systems. A file system is a set of data types that is employed for storage, hierarchical categorization, management, navigation, access, and recovery of data.

ICON KEY

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

Lab Scenario

Sam, a security professional at a company discovered that one of the company's employees was gathering crucial, confidential information about the company and saving it on his/her computer so that he/she could use it later for an illicit purpose. Sam immediately started checking each of his employee's computers in order to identify the dishonest employee. In order to escape from being caught, the culprit employee permanently deleted the gathered information.

Sam called a forensics investigator to launch an investigation. Sam explained the situation to the investigator. After listening to the story, the investigator decided to analyze the file systems and recover the deleted files to catch the dishonest employee.

Lab Objectives

The objective of this lab is to help the students understand how to:

- Recover files deleted from a hard disk.
- Analyze the file systems.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems

Lab Environment

This lab requires:

- A computer running **Windows Server 2012**.
- A web browser with an Internet connection.
- Administrative privileges to run tools.

Lab Duration

Time: 55 Minutes

Overview of Understanding Hard Disks and File Systems

While investigating a computer-based crime, it is most important to understand hard disks and file systems, as these are the major sources of data storage. People usually

delete their tracks after committing a crime using a computer in order to avoid being traced. Therefore, recovering the deleted files of hard disks and analyzing file systems is important when investigating a computer-based crime.

TASK 1

Lab Tasks

Overview

Recommended labs to assist you in understanding hard disks and file systems:

- Recovering Deleted Files from Hard Disks Using **WinHex**.
- Analyzing File system Types Using **The Sleuth Kit (TSK)**.
- Analyzing Raw image using **Autopsy**.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your expert opinion on the crime.

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

Lab 1

Recovering Deleted Files from Hard Disks Using WinHex

WinHex inspects and edits all kinds of files and recover deleted files or lost data from hard drives with corrupt file systems.

ICON KEY

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

Lab Scenario

The forensic investigators started scanning the computers for deleted data to catch the perpetrator, who has been collecting the company's private data for harmful purposes. To avoid identification, the perpetrator had deleted the data from the system. However, the investigators were able to trace the system used by the perpetrator by analyzing the file systems and recovering deleted data using the WinHex tool.

As a computer forensic investigator you should know how to recover files that have been permanently deleted and also the tools that can be used for recovering them.

Lab Objectives

The objective of this lab is to help you understand how to recover files that have been permanently deleted using the WinHex tool.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems

This lab requires:

- WinHex, which is located at **C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\WinHex.**
- A computer running **Windows Server 2012**.
- You can also download the latest version of **WinHex** from **https://www.x-ways.net/winhex/.**
- Kindly note that if you decide to download the **latest version**, then the screenshots shown in the lab might be slightly different.
- Administrative privileges to install and run tools.

- A web browser with an Internet connection.

Lab Duration

Time: 15 Minutes

Overview of WinHex

WinHex inspects and edits all kinds of files, recovers deleted files or lost data from hard drives with corrupt file systems, or from digital camera cards. It is a universal hexadecimal editor, particularly helpful in the realm of computer forensics, data recovery, low-level data processing, and IT security.

Lab Tasks

1. Navigate to **C:\CHFI-Tools\Evidence Files\Raw - DD Image** for the evidence files.

TASK 1

Launching WinHex

2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\WinHex**.
3. Double-click **setup.exe** to launch the setup and follow the wizard-driven installation instructions.
4. Once you complete the installation WinHex application launches automatically.

WinHex features application programming interface (API) and scripting.

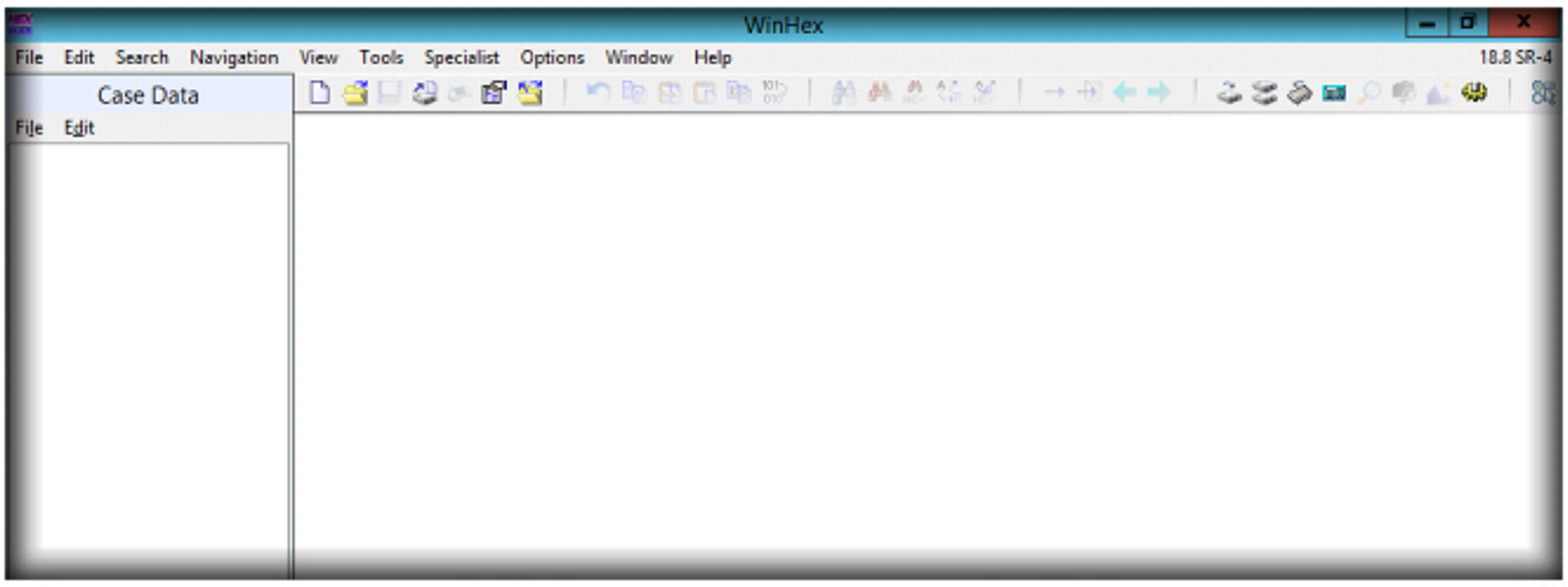


FIGURE 1.1: WinHexstartup window

TASK 2

Adding an Evidence File

5. Navigate to **File → Open** to add the evidence file.

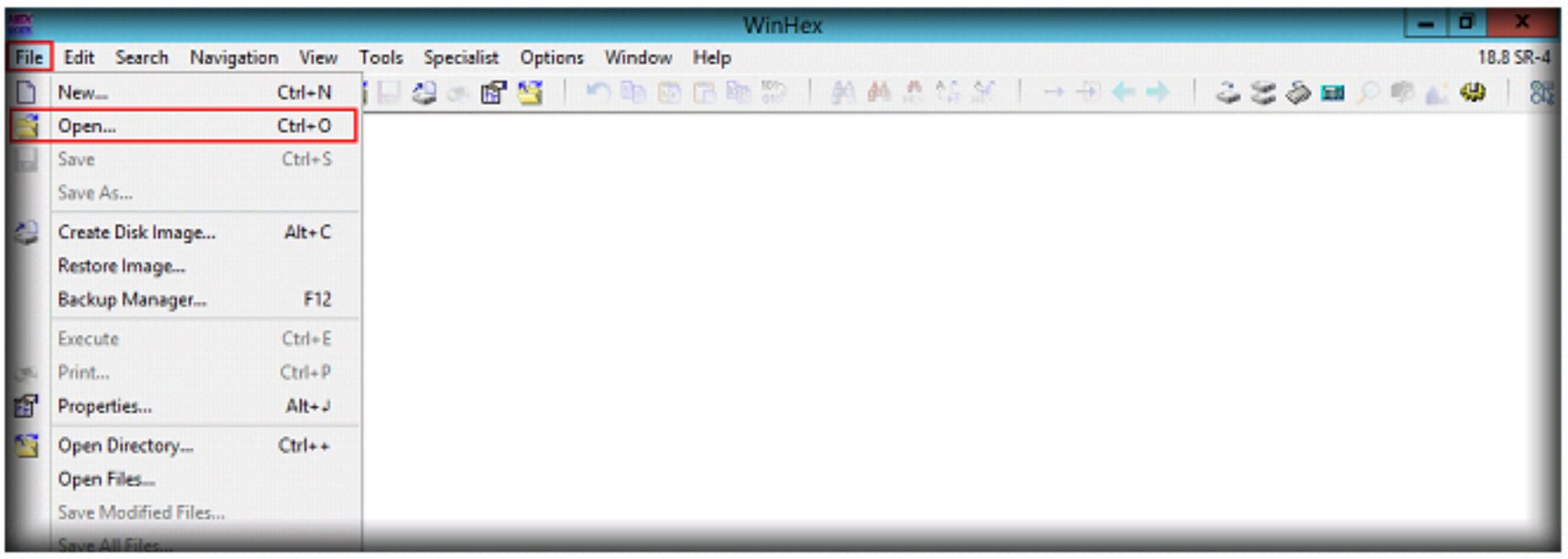


FIGURE 1.2: WinHex File menu

6. In the **Open Files** pop-up window, navigate to **C:\CHFI-Tools\Evidence Files\Raw - DD Image**, select **All Files** from the **Files of type** drop-down list, and then select **TestRawImage.dd**. Next Click **Open**.

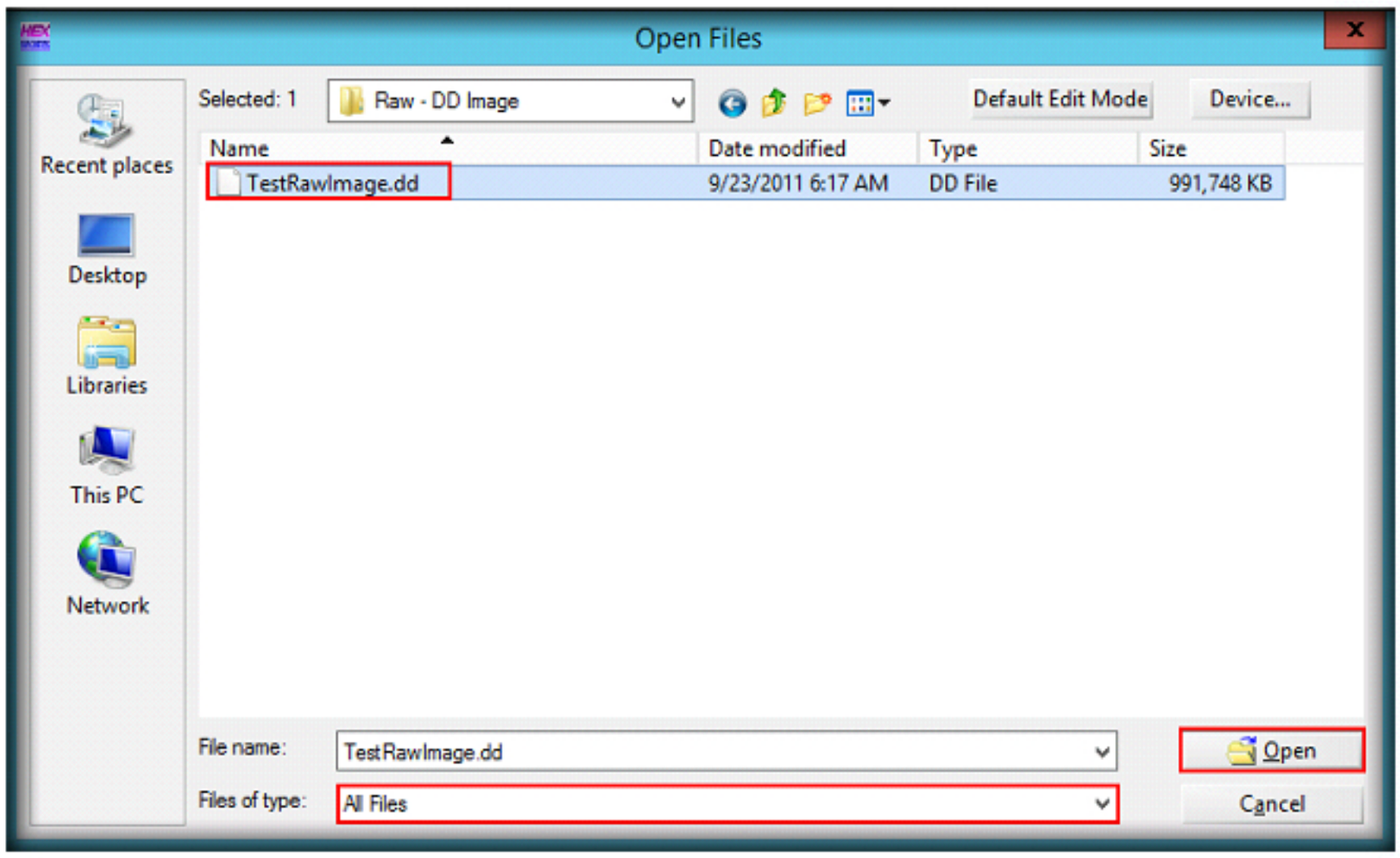


FIGURE 1.3:WinHex Open Files window

Import all clipboard formats, including ASCII hex values.

Erases (wipes) confidential files securely.Cleanses the hard drive to protect your privacy.

7. WinHex evaluation pop-up subsequently appears, click **OK**.

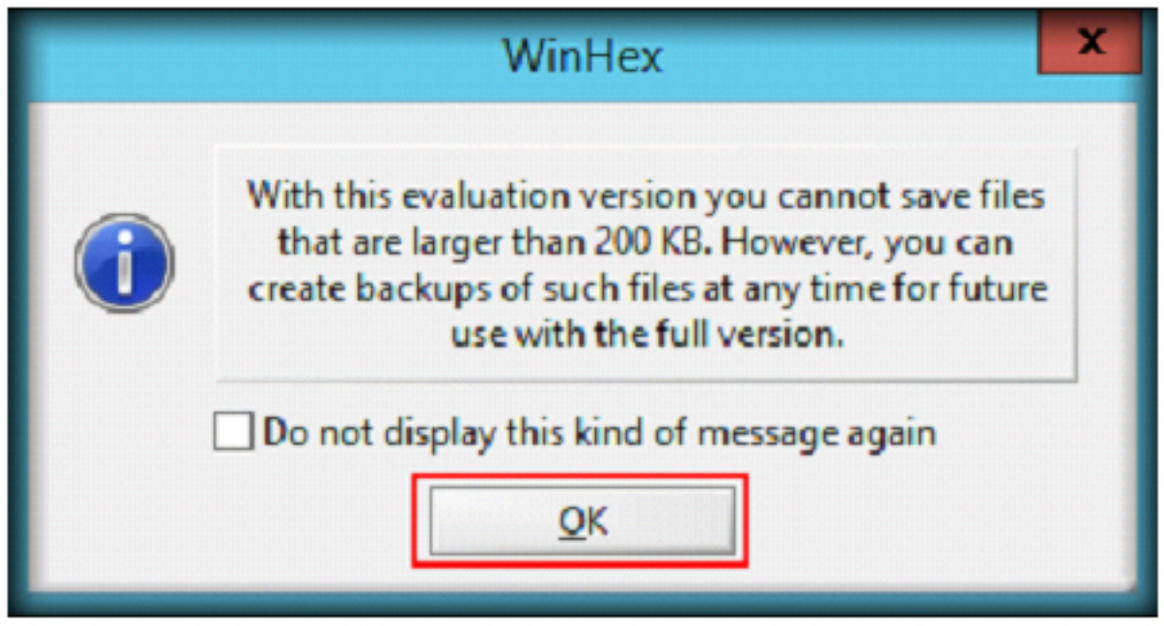


FIGURE 1.4:WinHex evaluation pop-up

Features character sets:

- ANSI ASCII
- IBM ASCII
- EBCDIC
- (Unicode)

8. WinHex will process the image file and display the following window with a **Data Interpreter** pop-up at the lower right corner of the window.

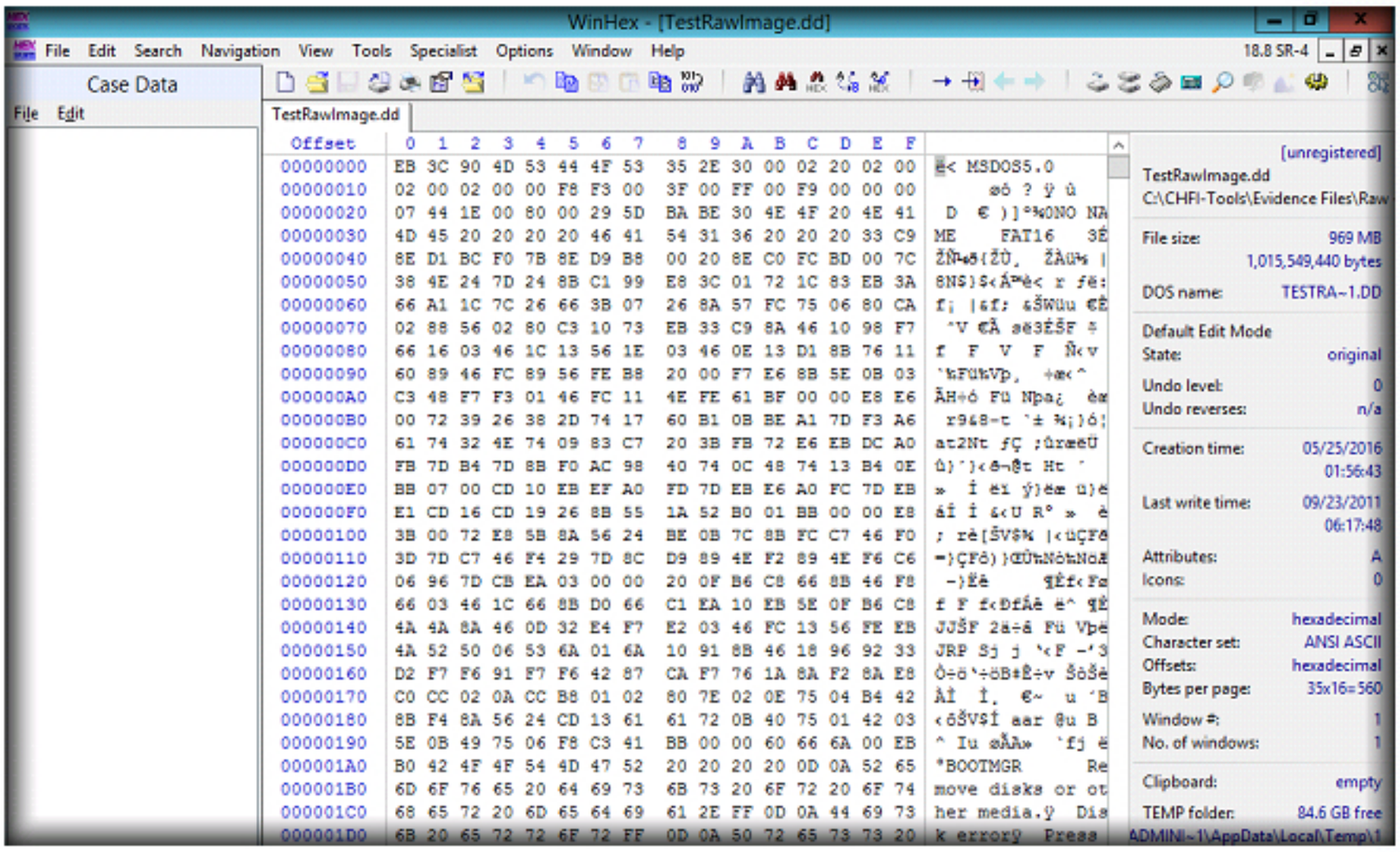


FIGURE 1.5: WinHex analyzing target DD image

WinHex converts between binary, hex ASCII, Intel Hex, and Motorola S.

TASK 3

Recovering Deleted Files

9. Navigate to **Tools → Disk Tools → File Recovery by Type...**

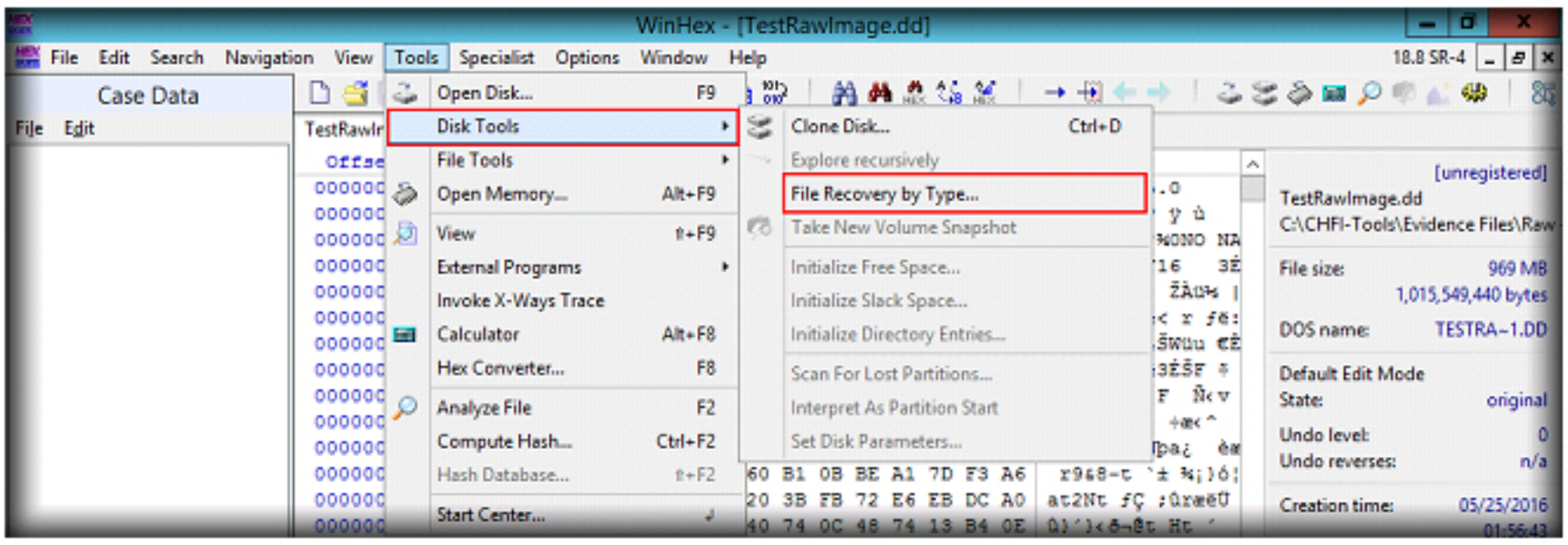


FIGURE 1.6: WinHex Tools menu

10. A WinHex pop-up appears, click **OK**

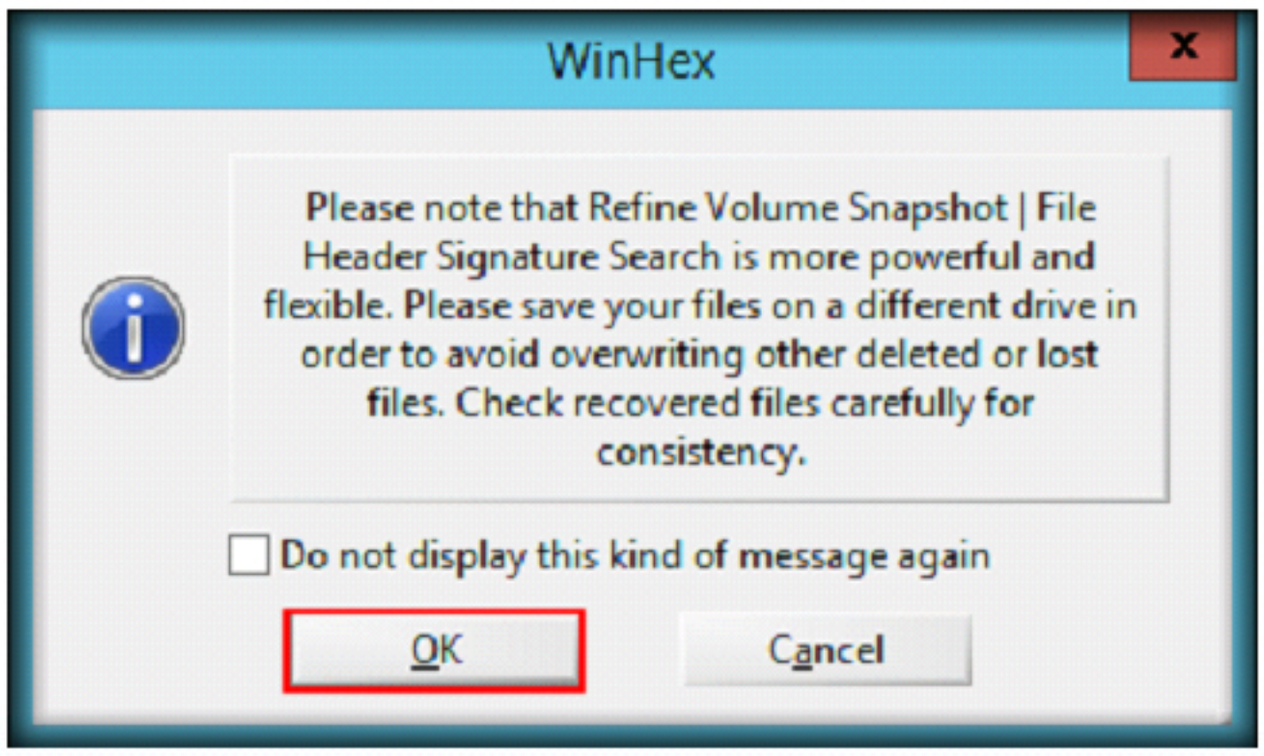


FIGURE 1.7: WinHex pop-up window

WinHex features a data interpreter that knows 20 data types.

11. **File Header Search on TestRawImage.dd** window appears. In the left pane it will categorize the file types that you want to extract as shown in the screenshot.

12. In this lab we are going to extract the **Pictures** folder, click on **+** node to expand the pictures folder.

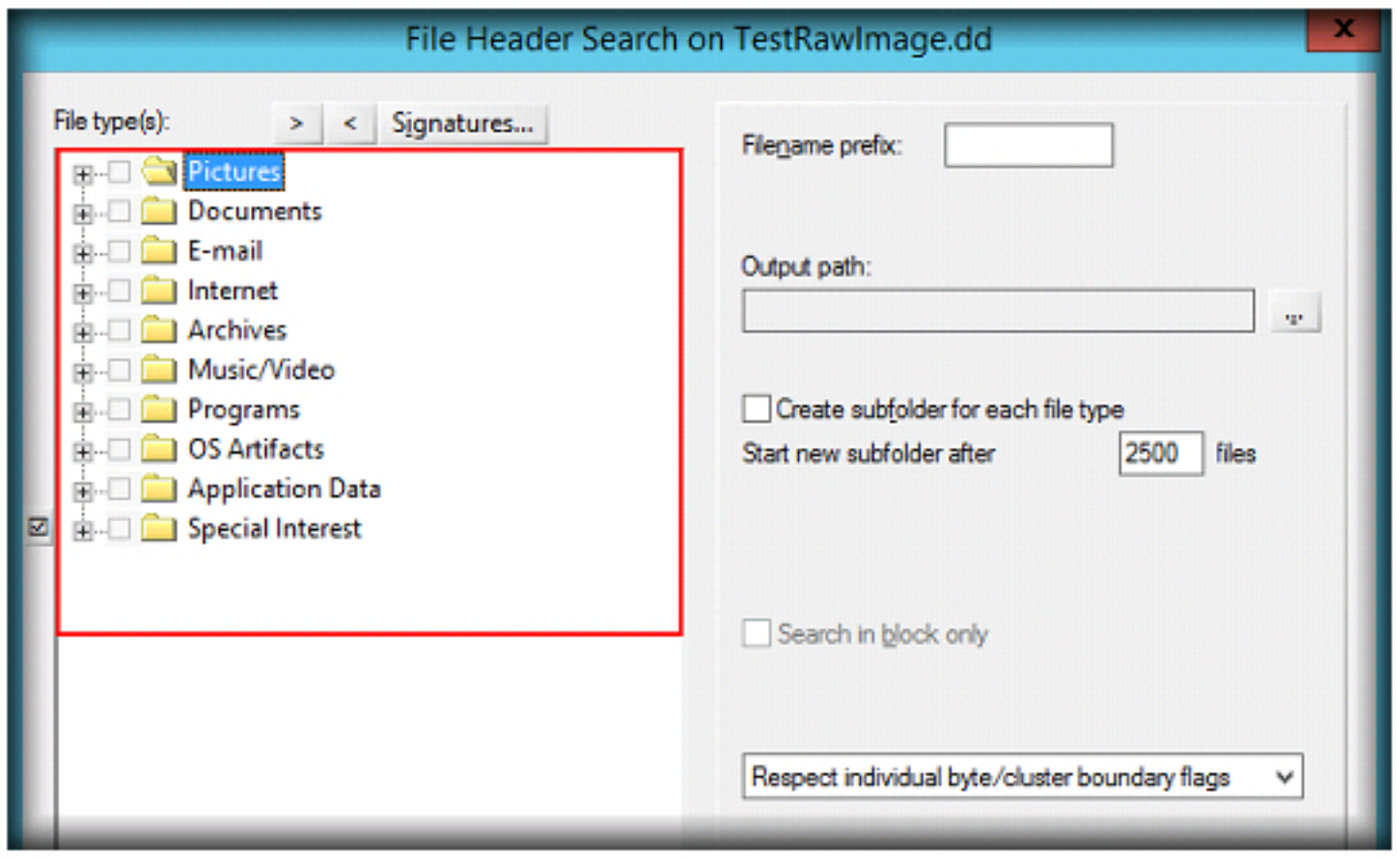


FIGURE 1.8: File Header Search on TestRawImage.dd window

13. Select the file types of the target files that you want to recover in Pictures folder from the left pane as shown in the screenshot and then click **OK.**

Note: Similarly, you can also choose other file types for the investigation process. Screenshot may differ if you have selected other file types.

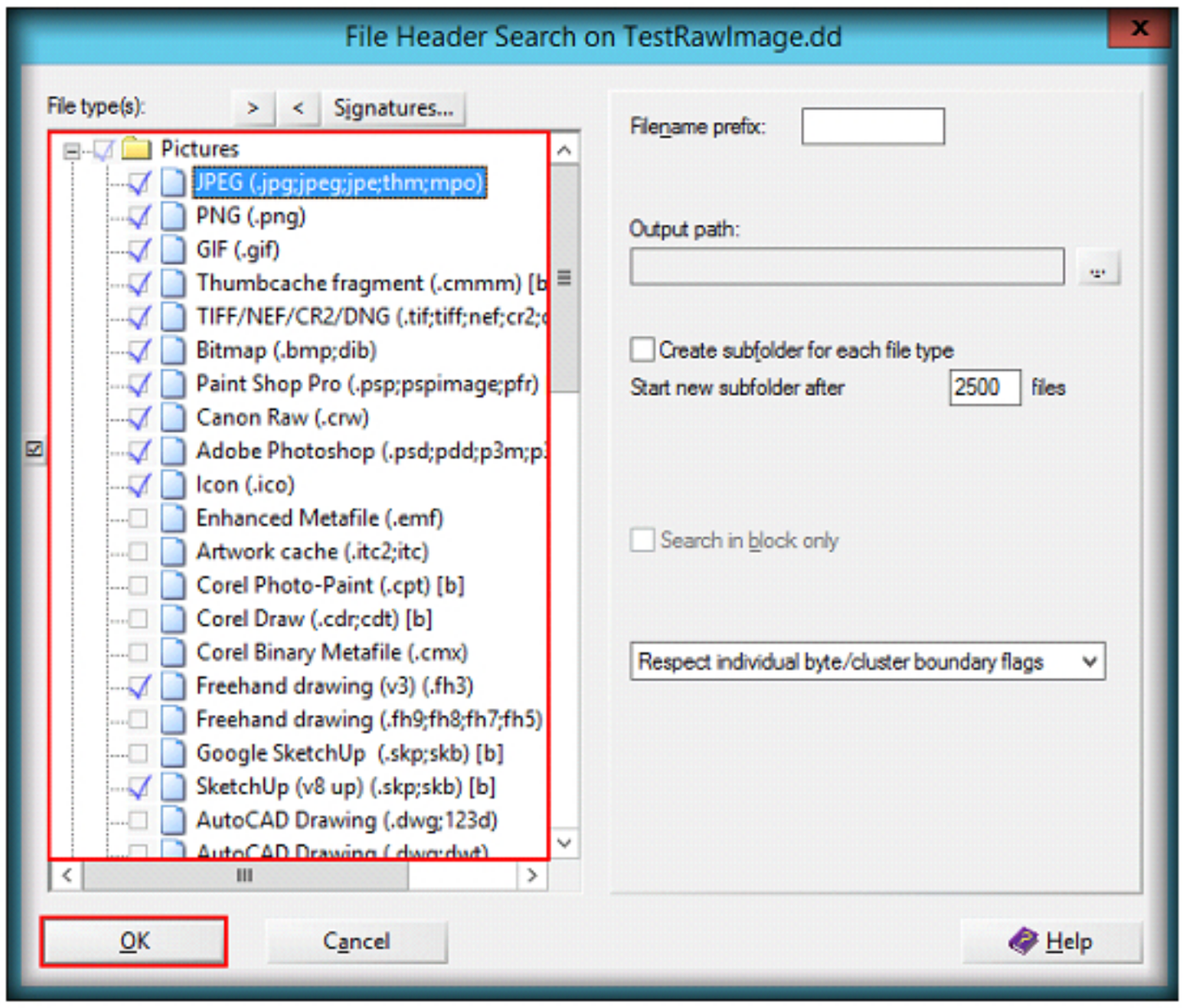


FIGURE 1.9: WinHex file header search

Capable of cloning disks.

Built-in interpretation of RAID systems and dynamic disks

WinHex concatenates and splits files, unifying and dividing odd and even bytes and words.

TASK 4

Selecting the Target Folder

14. It will display a new **Select Target Folder** window. Navigate to the location where you want to save the retrieved files. Create a folder, give it a name, select the folder, and then click **OK.** (Here we created a new folder called **Retrieved Files** on the Desktop.)

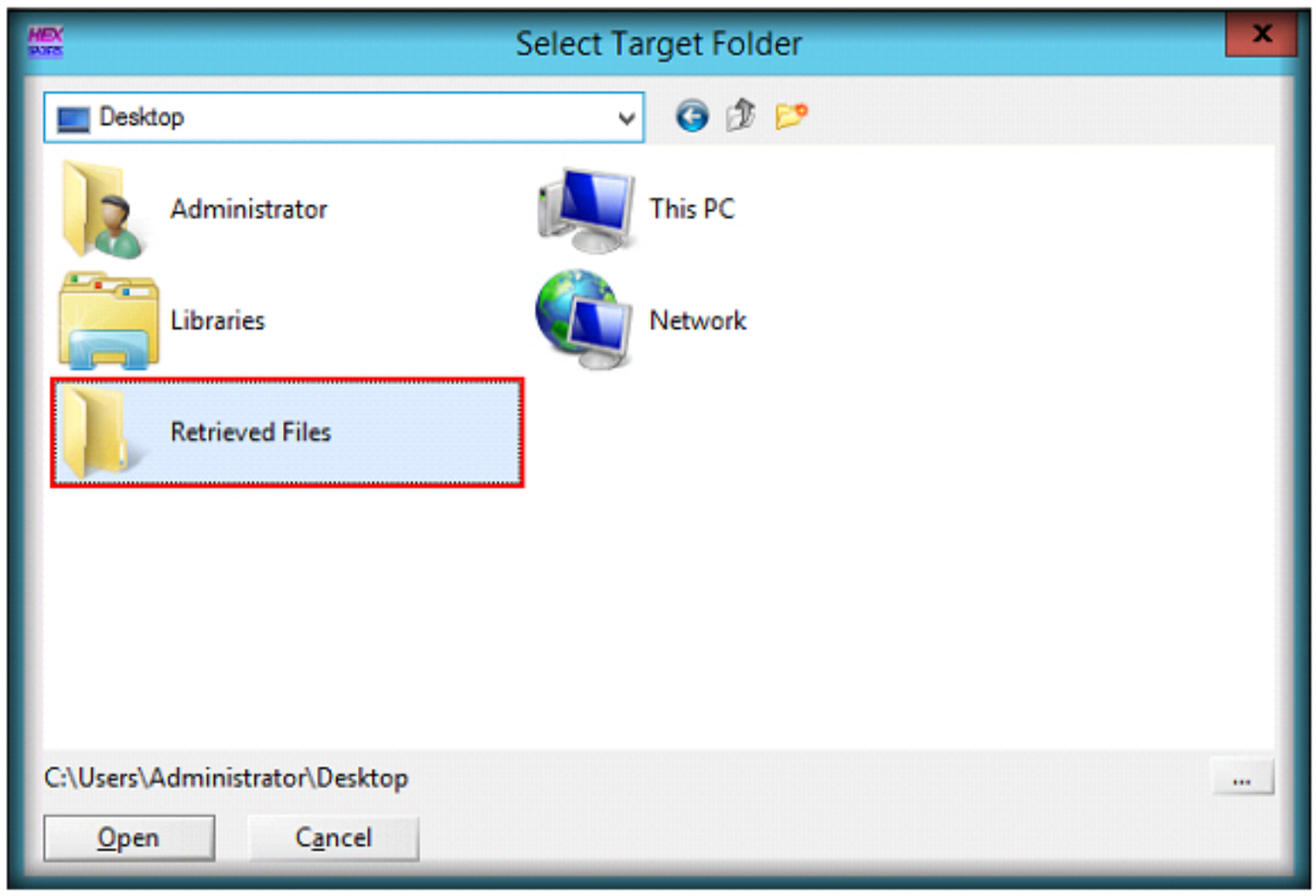
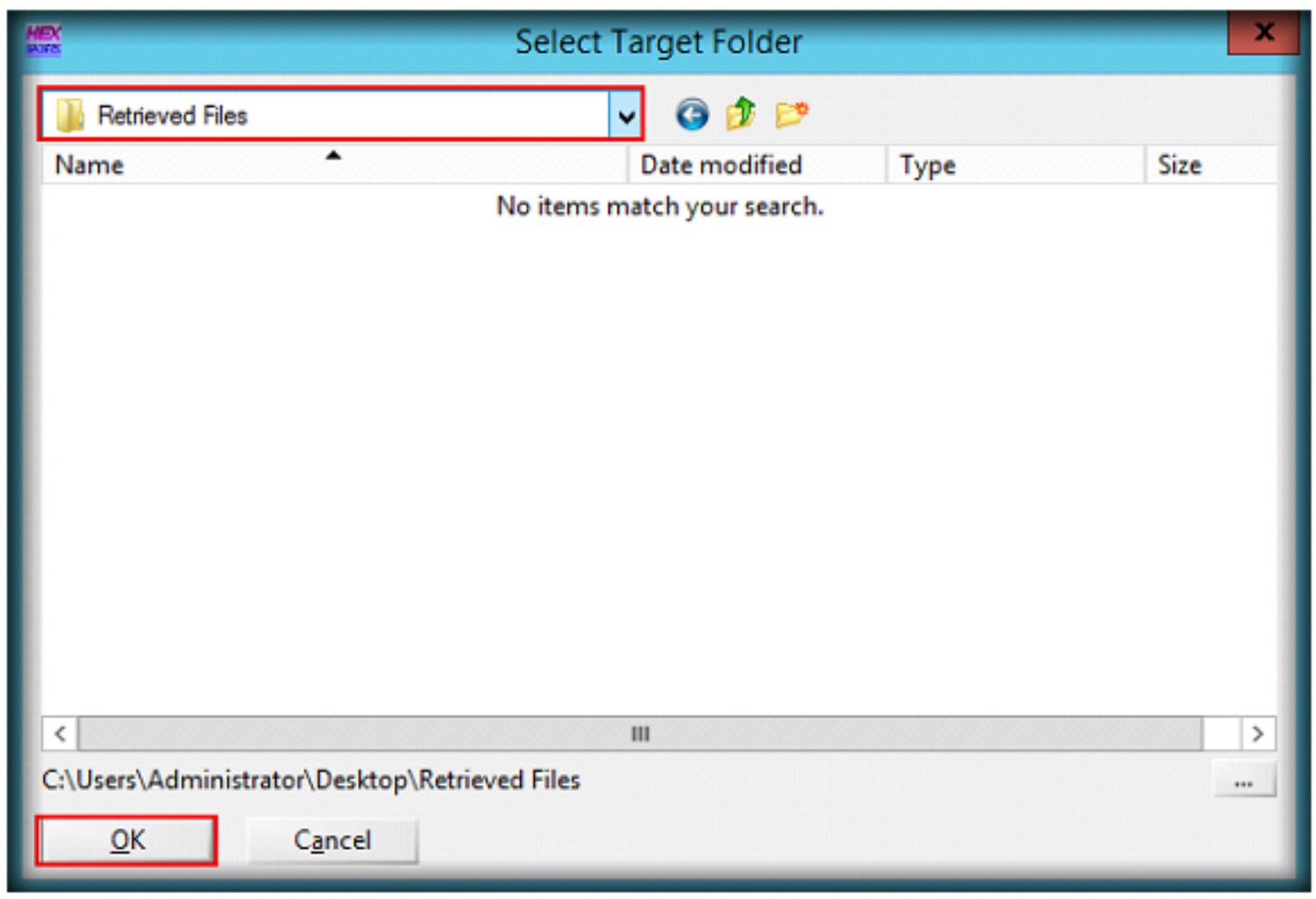


FIGURE 1.10: WinHex Select Target Folder window

WinHex supports files greater than 4GB in size.

15. It will display the following window. Click **OK**.



WinHex features RAM editor, providing access to physical RAM and other processes' virtual memory

FIGURE 1.11: WinHex select target folder

16. To start the recovery process, click **OK** on the **File Header Search** tab. It will close the window and start recovering the deleted hard disk files based on the chosen type.

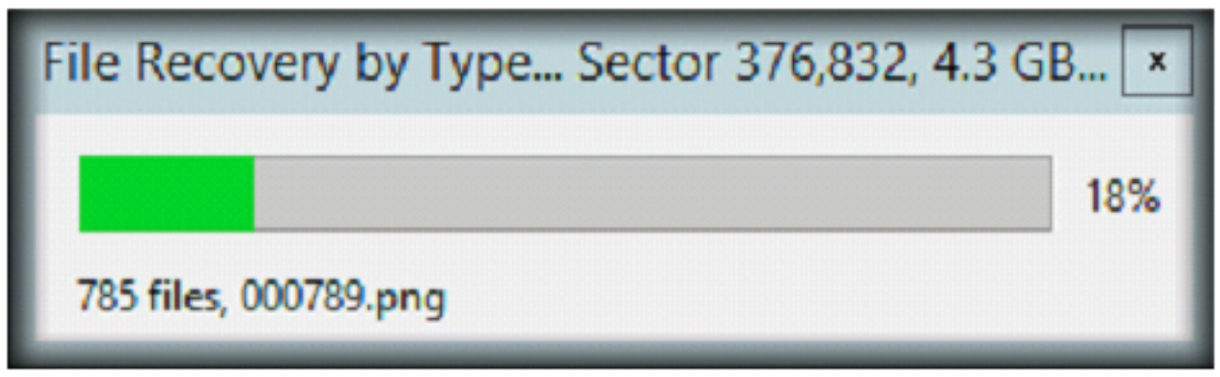


FIGURE 1.12:WinHex recoveryprocessing window

WinHex analyzes and compares files

17. After the recovery process is complete, click **OK** in the **File Recovery by Type** pop-up window to close the processing window.

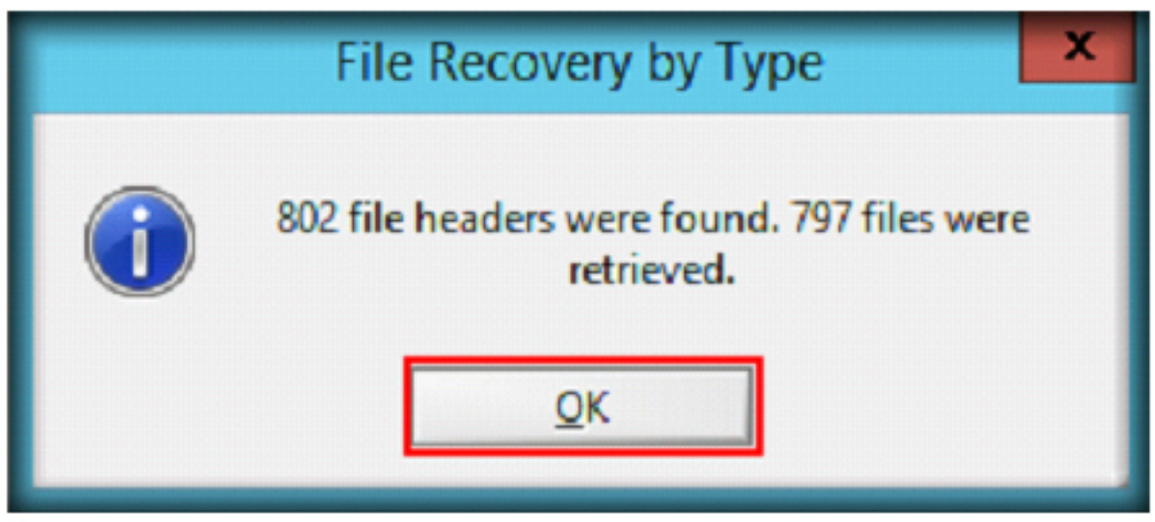


FIGURE 1.13: File Recovery by Type pop-up window

Native support for FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3®, CDFS, UDF

TASK 5

Viewing Retrieved Files

18. To see the recovered files, open the destination folder where you saved the documents.

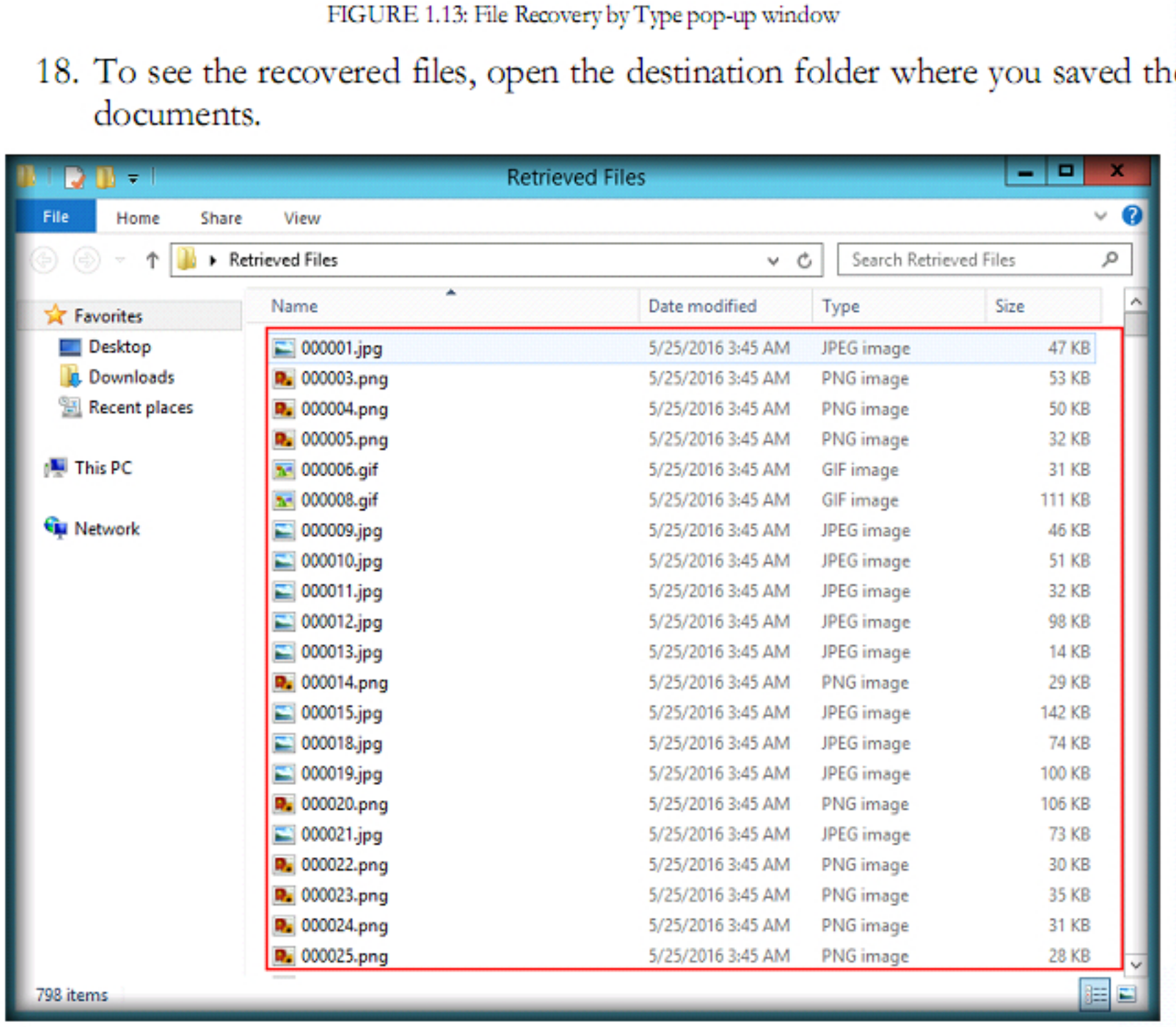


FIGURE 1.14: Retrieved files folder

Edits data structures using templates

Lab Analysis

Check recovered files that have been deleted from the hard disk. Investigate those recovered files and document the results related to the lab exercise.

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

Questions

1. How do you clone a disk using WinHex?
2. How do you make partition backups using WinHex?

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

Lab 2

Analyzing File System Types Using The Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a library and collection of command-line tools that allow you to investigate volume and file system data.

ICON KEY

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

Lab Scenario

Sam had called investigators to catch the criminal, who was leaking the company's secret information. The investigators faced the challenge of scanning large number of systems for identifying the culprit. In order to simplify the search, the investigators used The Sleuth Kit (TSK)to determine the volume and file system data, which reduced their work and helped in finding the culprit in time.

In order to investigate a hard disk, as a forensic investigator you must know the types of file systems and how to analyze them using various tools.

Lab Objectives

The objective of this lab is to help investigators learn and perform file system analysis. The Sleuth Kit (TSK) is used to obtain:

- File system type.
- Metadata information.
- Content information.

Lab Environment

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems

This lab requires:

- The Sleuth Kit (TSK), which is located at **C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK).**
- You can also download the latest version of **The Sleuth Kit** from this link **http://www.sleuthkit.org/sleuthkit/download.php.**
- If you decide to download the latest version, then the screenshots shown in this lab might differ slightly.

- A computer running **Windows Server 2012**.
- Administrative privileges to execute the commands.
- A web browser with an Internet connection.

Lab Duration

Time: 15 Minutes

Overview of The Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a library and collection of command-line tools that allow you to investigate volume and file system data. The library can be incorporated into larger digital forensics tools, and the command-line tools can be used directly to find evidence.

Lab Tasks

TASK 1

Open command window here

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK).**
2. Select **bin** folder, press **Shift + Rightclick** on keyboard and select **Open command window here** from the context menu to open command prompt window.

The filesystem tools allow you to examine filesystems of a suspect computer in a non-intrusive fashion.

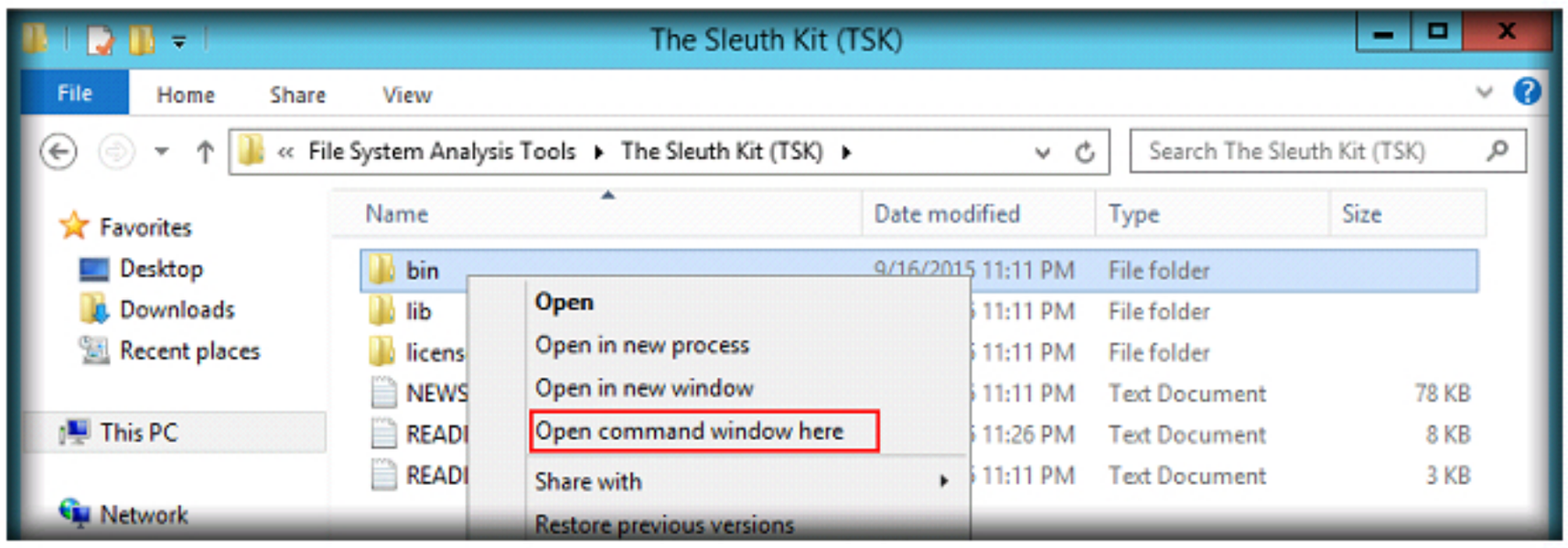


FIGURE 2.1: Windows Server 2012Command Window Here

TASK 2

Viewing the Filesystem Details

3. Now type **fsstat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd"**and then press **Enter** to see the file system details.

It runs on Windows and UNIX platforms.

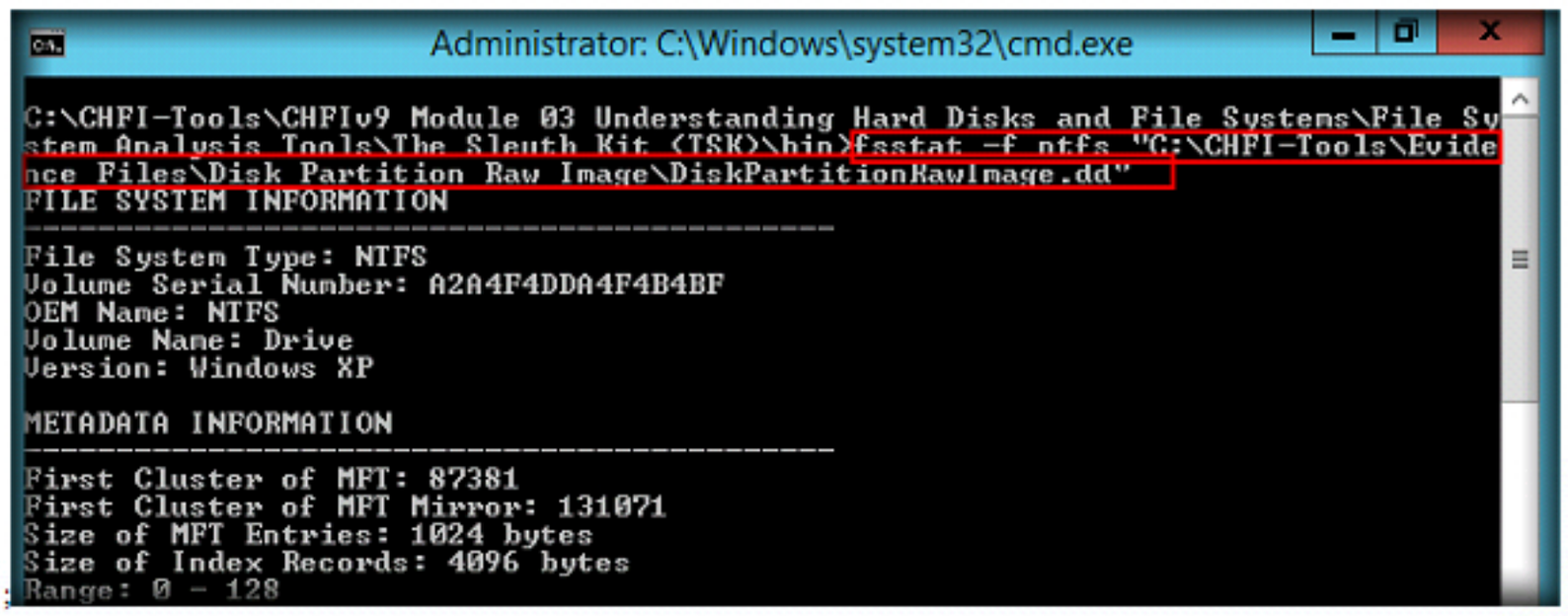


FIGURE 2.2: fsstat showing filesystem details

TASK 3

Viewing the Meta-Data Structure Details

4. Use the **istat** tool of the sleuth kit to view the details of metadata structure.
5. To view the MFT File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 0**

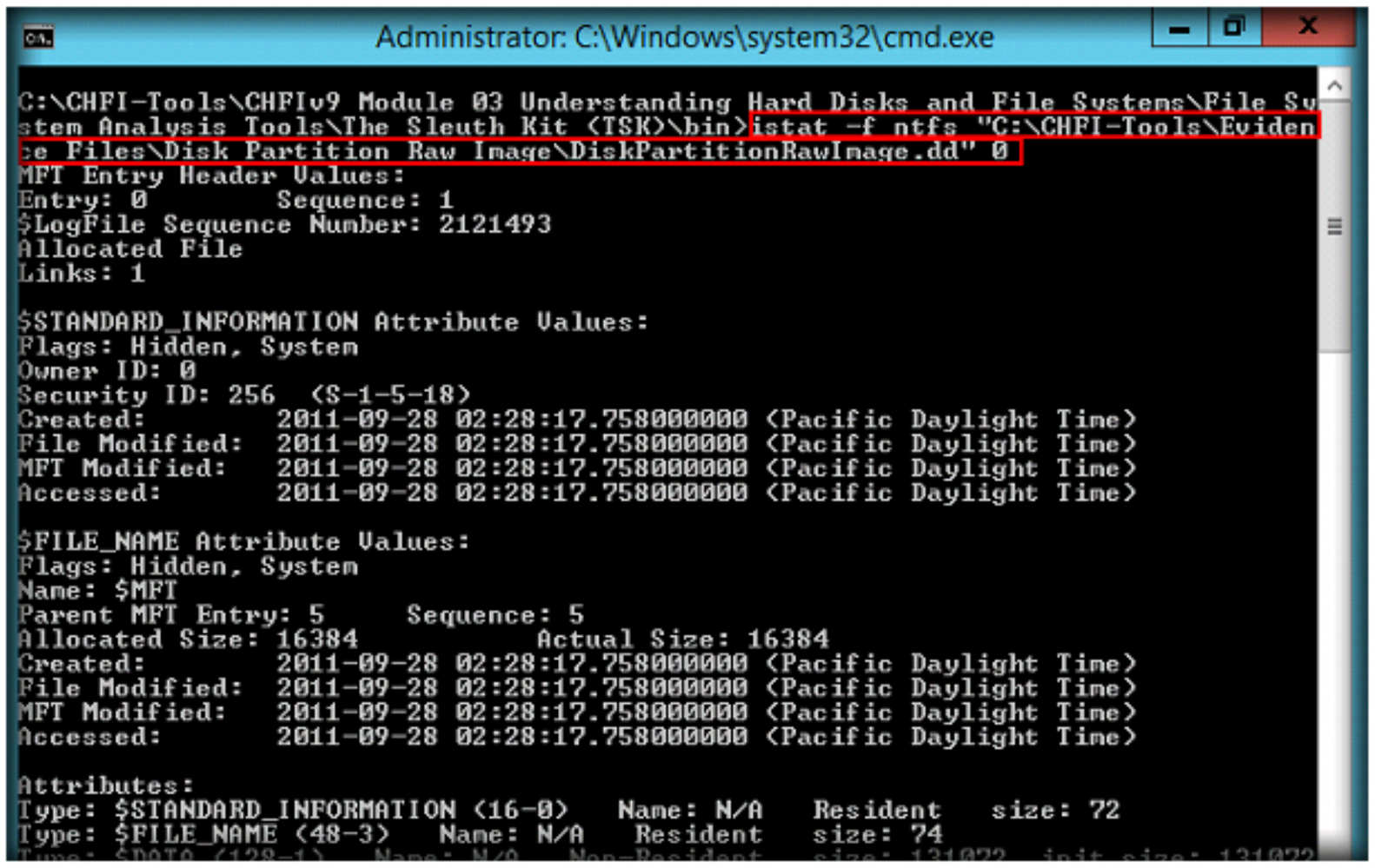


FIGURE 2.3: MFT File overview

It supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks.

Analyzes raw (i.e. dd), Expert Witness (i.e. EnCase), and AFF filesystem and disk images.

Note: Master File Table (MFT) has an entry for every file and directory; hence it is required to find all other files. The layout of the MFT is determined by processing entry 0 in the MFT.

6. To view MFTMirr File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 1**

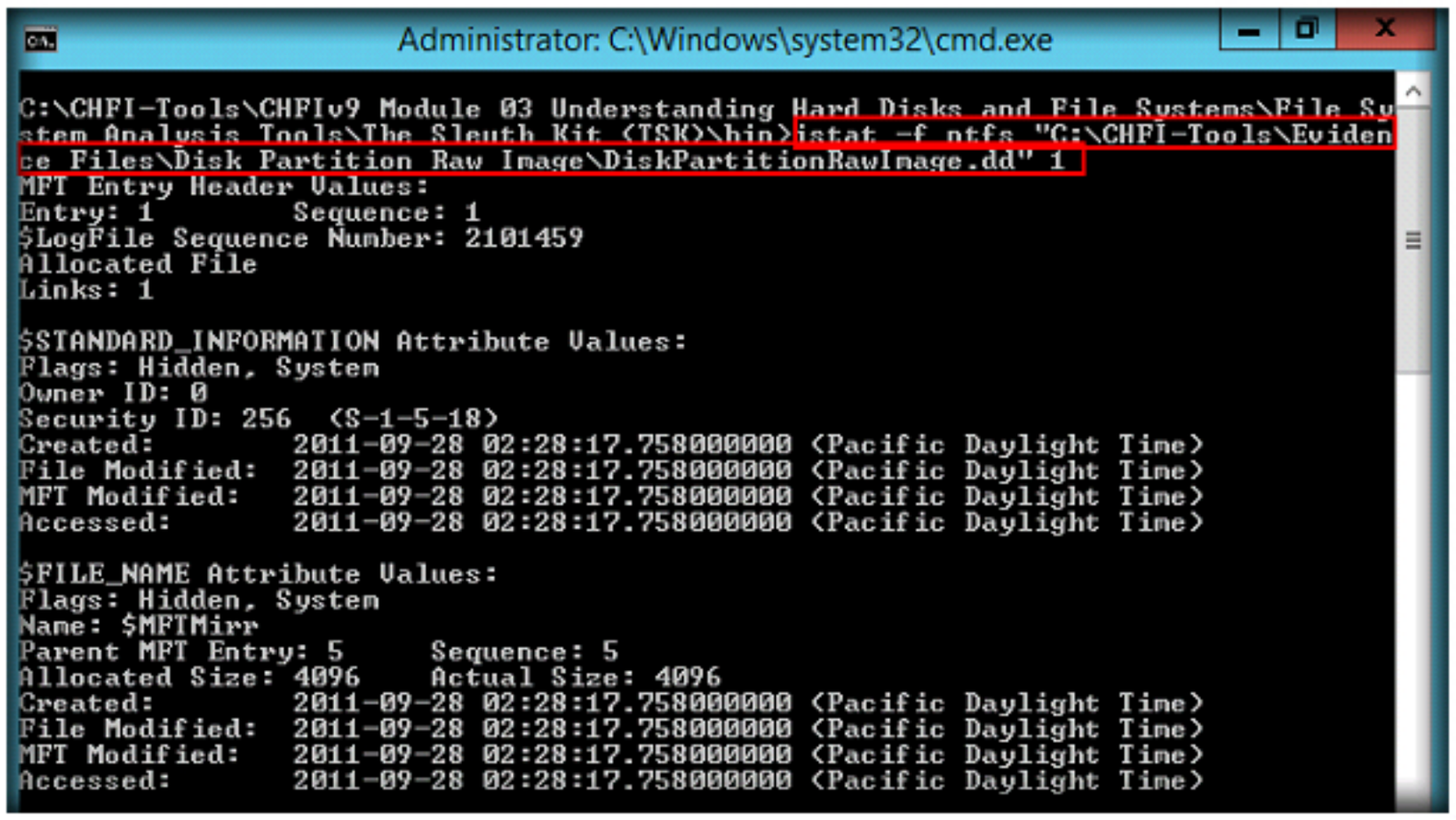


FIGURE 2.4: MFTMirr File Overview

The Sleuth Kitsupports the NTFS, FAT, UFS 1, UFS 2, EXT2FS, EXT3FS, and ISO 9660 filesystems.

The Sleuth Kit tools will show files that have been "hidden" by rootkits and will not modify the A-Time of files that are viewed.

Note: MFT entry 1 is for the MFTMirr file, which has a non-resident attribute that contains a backup copy of the first MFT entries.

7. To view the Boot File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 7**

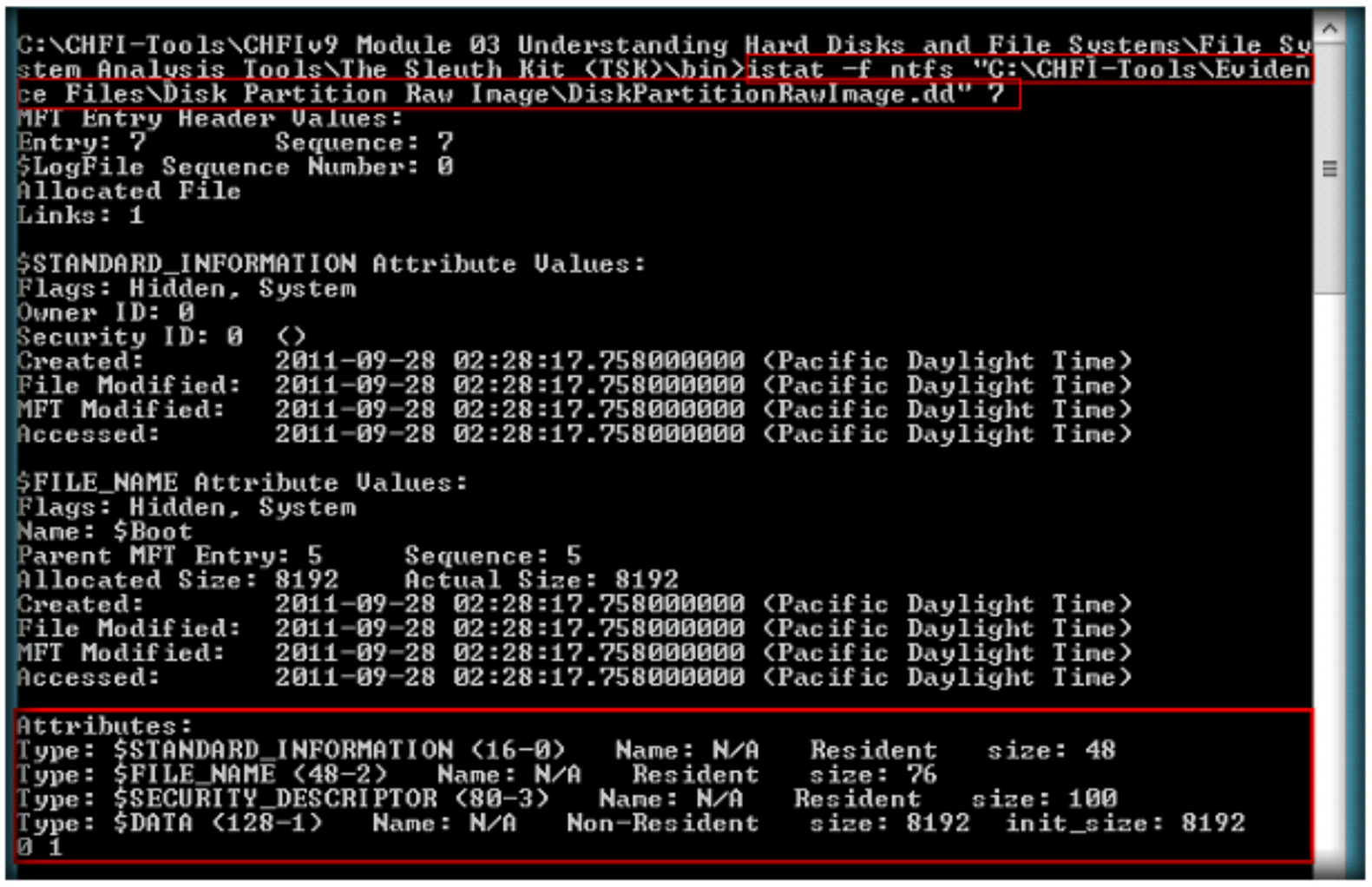


FIGURE 2.5: Boot file overview

Lookup file hashes in a hash database, such as the NIST NSRL, Hash Keeper, and custom databases that have been created with the md5sum tool.

Note: The Boot file system metadata file is located in MFT entry 7 and contains the boot sector of the file system.

TSK displays the details and contents of all NTFS attributes.

8. To view the File Volume Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 3**

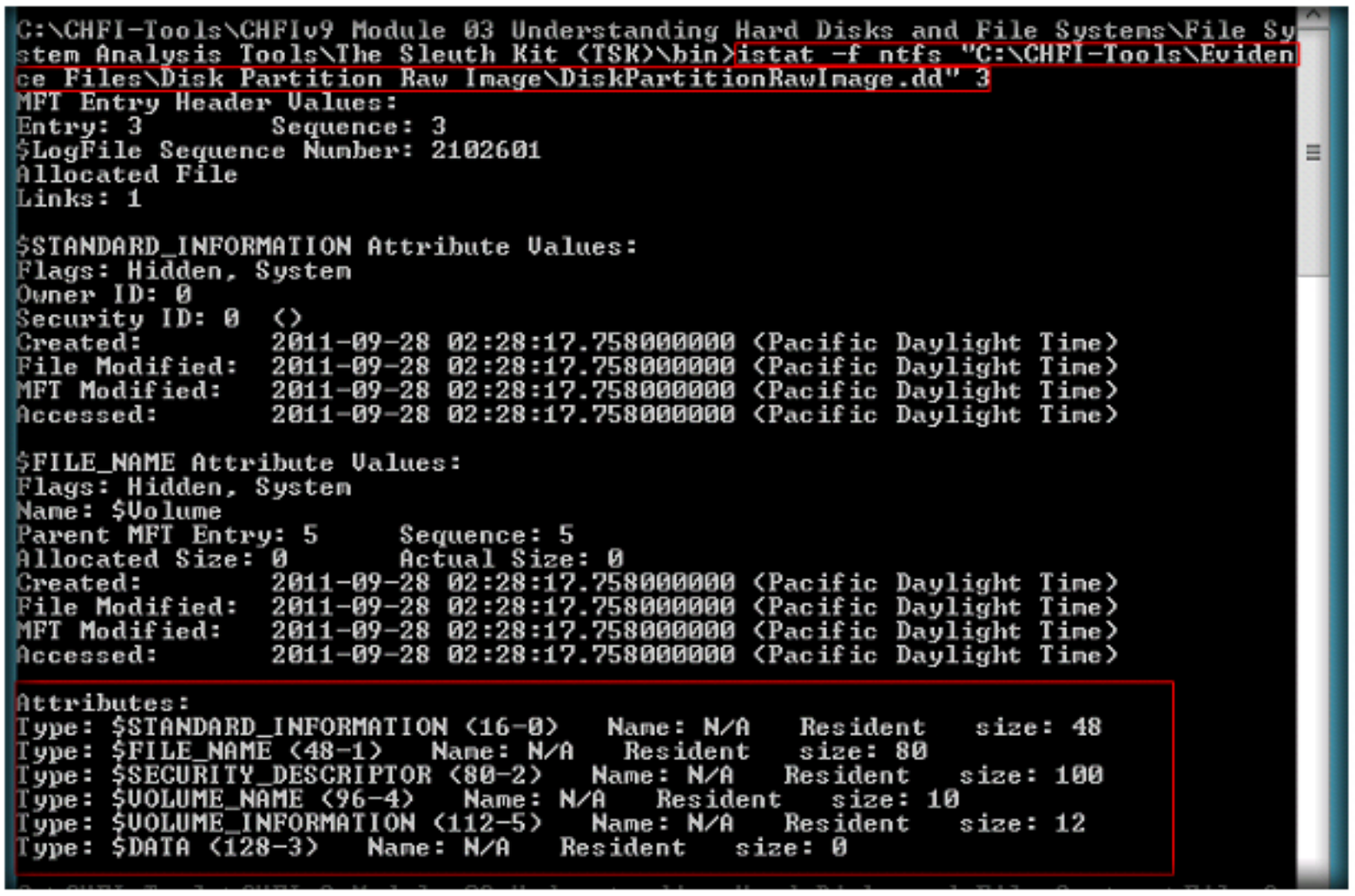


FIGURE 2.6: File volume overview

With TSK you can lookup file hashes in a hash database, such as the NIST NSRL, Hash Keeper, and custom databases that have been created with the md5sum tool.

Note: The Volume file system metadata file is located in MFT entry 3 and contains the volume label and other version information.

9. To view AttrDef File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 4**

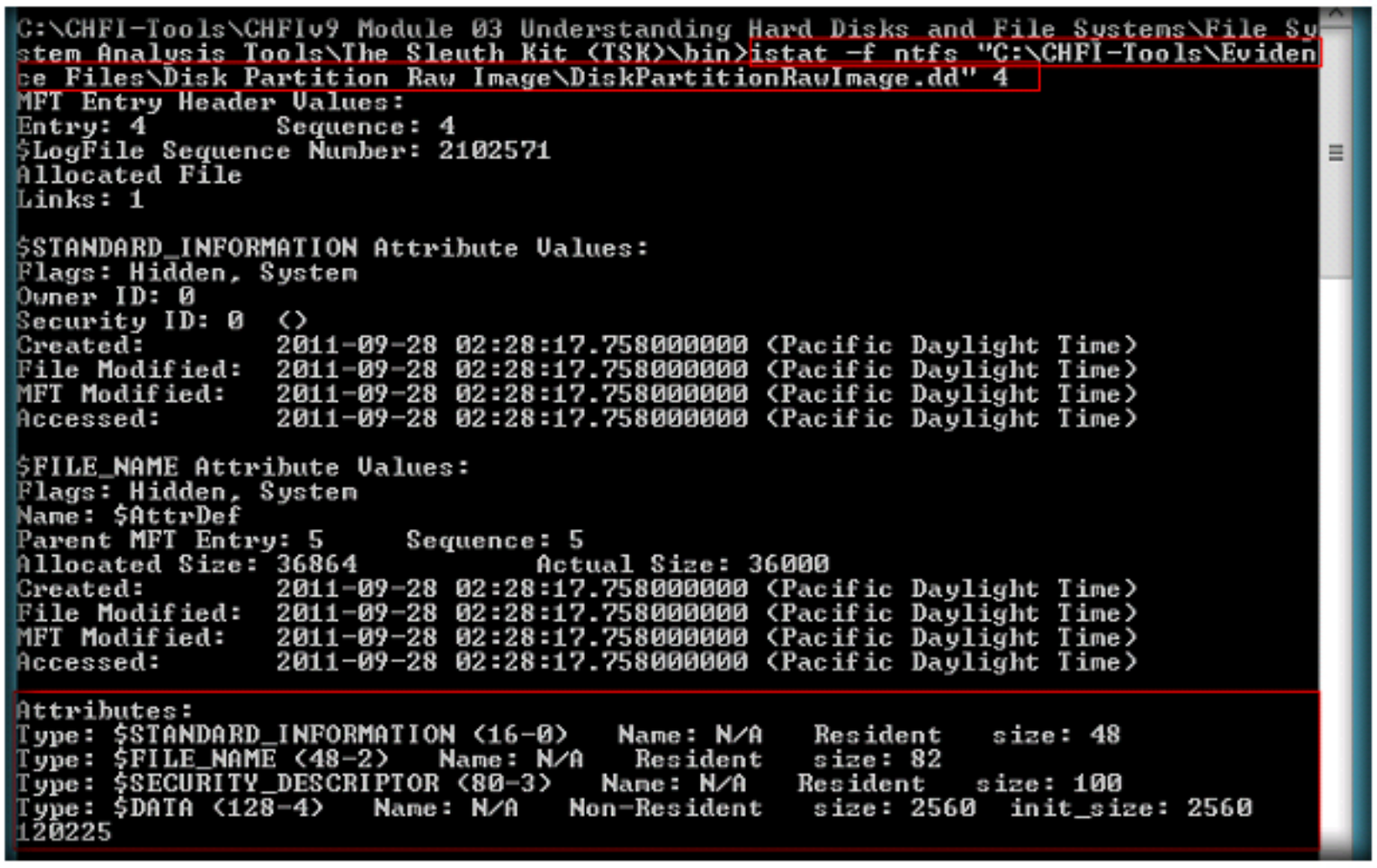


FIGURE 2.7: AttrDef file overview

TSK is written in C and Perl and uses some code and design from The Coroner's Toolkit (TCT).

Note: The MFT entry for AttrDef filesystem metadata file is 4. It defines the names and type identifiers for each type of attribute.

10. To view Bitmap File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 6**

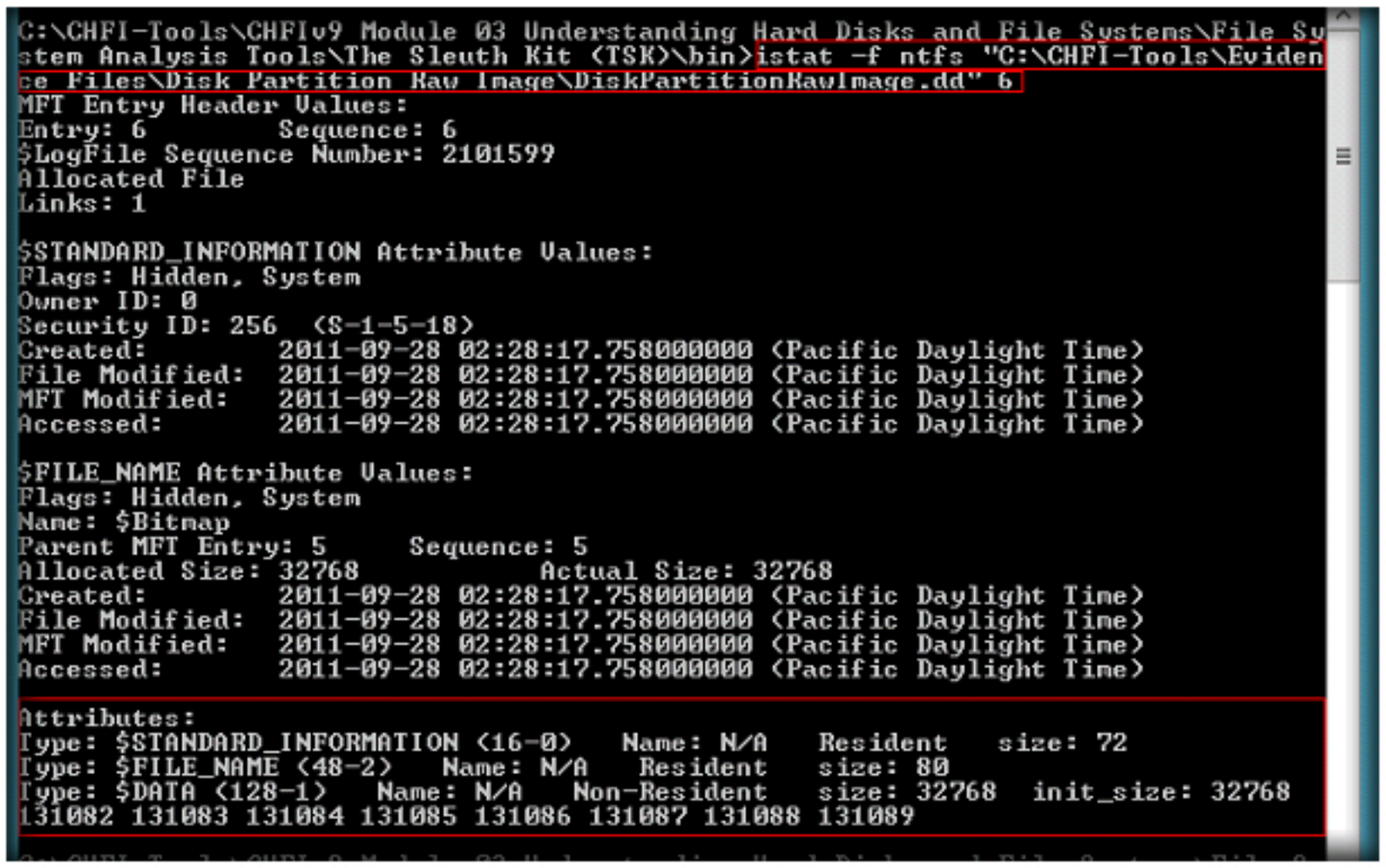


FIGURE 2.8: Bitmap file overview

TSK has been tested on:

- Linux
- Mac OS X
- Windows (Visual Studio and mingw)
- CYGWIN
- Open & FreeBSD
- Solaris

Note: The MFT entry of the Bitmap file system metadata file that determines the status of the cluster is 6

11. To view the BadClus File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 8**

The Autopsy Forensic Browser is a graphical interface to the tools in TSK.

The C library of TSKcan be incorporated into larger digital forensic tools.

```
C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File Sy
stem Analysis Tools\The Sleuth Kit (TSK)\bin>istat -f ntfs "C:\CHFI-Tools\Eviden
ce Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 8
MFT Entry Header Values:
Entry: 8        Sequence: 8
$LogFile Sequence Number: 2101669
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256  (S-1-5-18)
Created:        2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
File Modified:  2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
MFT Modified:   2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
Accessed:       2011-09-28 02:28:17.758000000 (Pacific Daylight Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $BadClus
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
File Modified:  2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
MFT Modified:   2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
Accessed:       2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
```

FIGURE 2.9: BadClus file overview

TSK can be run on a live Windows or UNIX system during incident response.

Note: NTFS keeps track of the damaged clusters by allocating them to a $DATA attribute of the Bad Clus file system metadata file. The MFT entry is 8

12. To view the Secure File Overview, type **istat -f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 9**

The C library of TSK can be incorporated into larger digital forensic tools.

TSK's command-line tools can be used directly by a user.

```
C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems\File Sy
stem Analysis Tools\The Sleuth Kit (TSK)\bin>istat -f ntfs "C:\CHFI-Tools\Eviden
ce Files\Disk Partition Raw Image\DiskPartitionRawImage.dd" 9
MFT Entry Header Values:
Entry: 9        Sequence: 9
$LogFile Sequence Number: 2109402
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 257  (S-1-5-18)
Created:        2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
File Modified:  2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
MFT Modified:   2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
Accessed:       2011-09-28 02:28:17.758000000 (Pacific Daylight Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System, Index View
Name: $Secure
Parent MFT Entry: 5     Sequence: 5
Allocated Size: 0       Actual Size: 0
Created:        2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
File Modified:  2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
MFT Modified:   2011-09-28 02:28:17.758000000 (Pacific Daylight Time)
Accessed:       2011-09-28 02:28:17.758000000 (Pacific Daylight Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0)   Name: N/A   Resident   size: 72
Type: $FILE_NAME (48-7)   Name: N/A   Resident   size: 80
Type: $DATA (128-8)   Name: $SDS   Non-Resident   size: 263832  init_size: 26383
2
120160 120161 120162 120163 120164 120165 120166 120167
120168 120169 120170 120171 120172 120173 120174 120175
120176 120177 120178 120179 120180 120181 120182 120183
120184 120185 120186 120187 120188 120189 120190 120191
120192 120193 120194 120195 120196 120197 120198 120199
120200 120201 120202 120203 120204 120205 120206 120207
120208 120209 120210 120211 120212 120213 120214 120215
120216 120217 120218 120219 120220 120221 120222 120223
120224
```

FIGURE 2.10: Secure file overview

Note: Secure file metadata file system stores the security descriptors that define the access control policy for a file or directory. The MFT entry for this is 9.

TASK 4

Listing the Files and Directory Names

13. Use the **fls** command-line tool of TSK to list the files and directory names. Type **fls-f ntfs "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd"** and then press **Enter.**

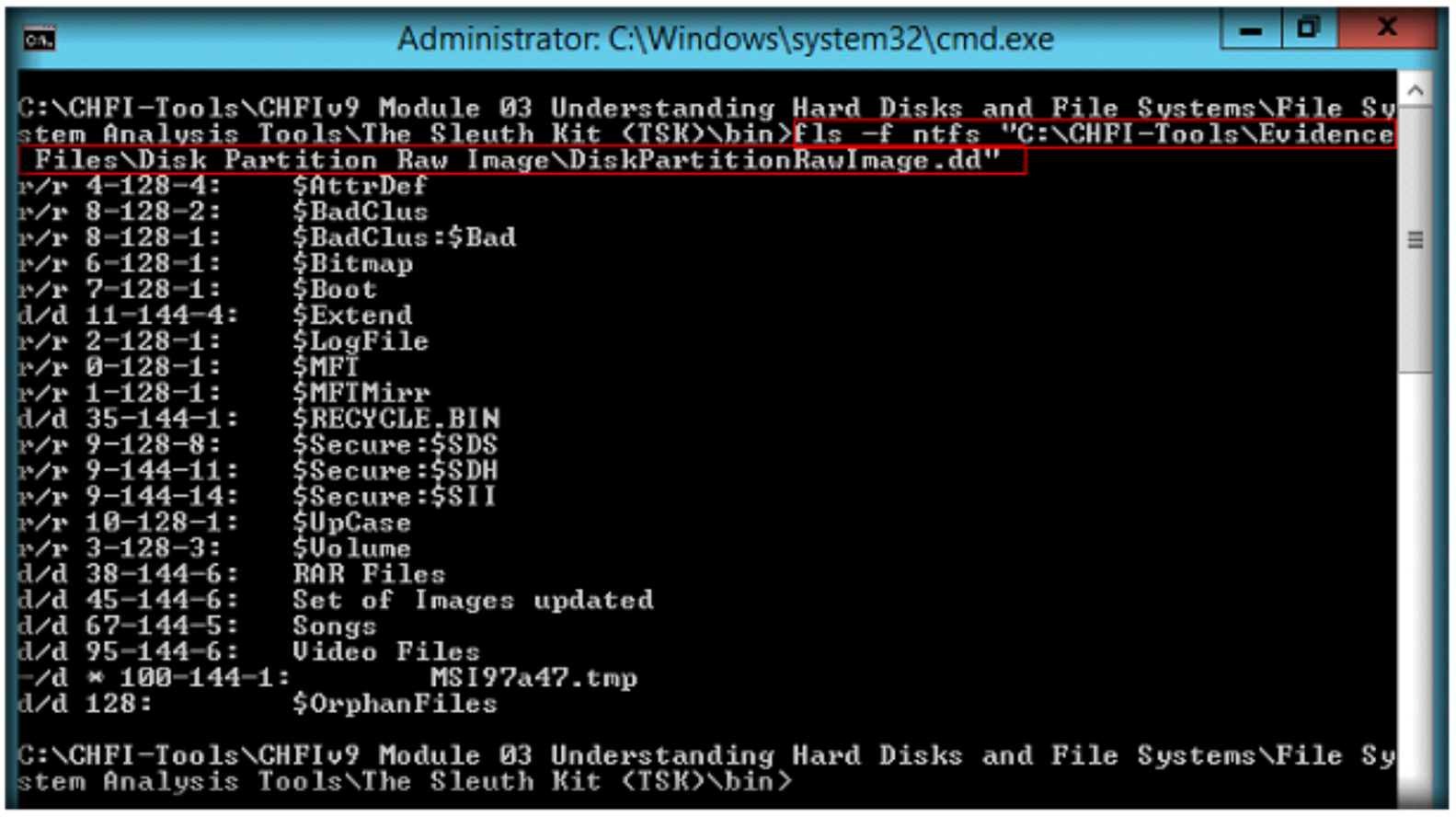


FIGURE 2.11: Listing files and directory names

14. To see only the deleted entries, type **fls -d "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd"**

The -V command of any tool in TSK displays the version of TSK.

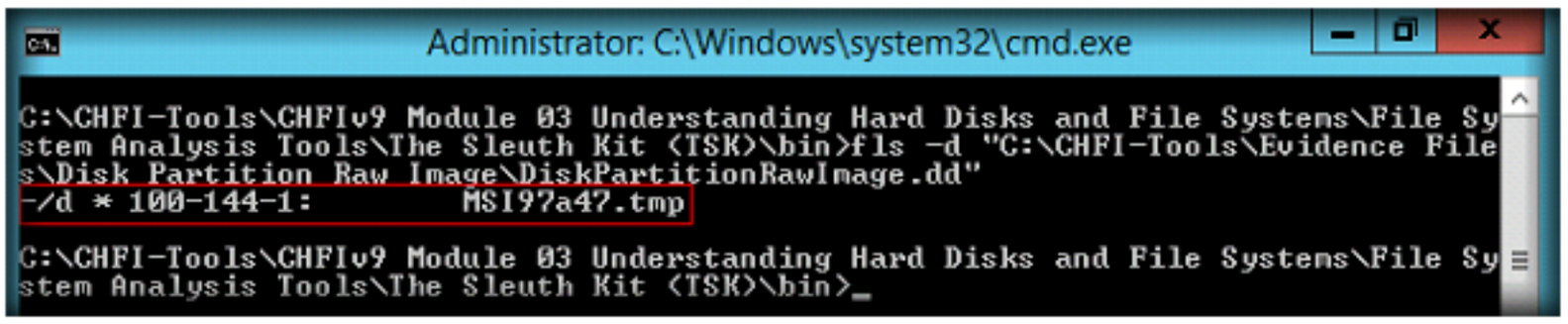


FIGURE 2.12: Viewing deleted entries

TASK 5

Viewing the Image File Details

15. Use the **img_stat** command to see the details of an image. Type **img_stat "C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd"** and press **Enter** to see the details of an image file.

The volume system (media management) tools of the sleuth kit allow you to examine the layout of disks and other media.

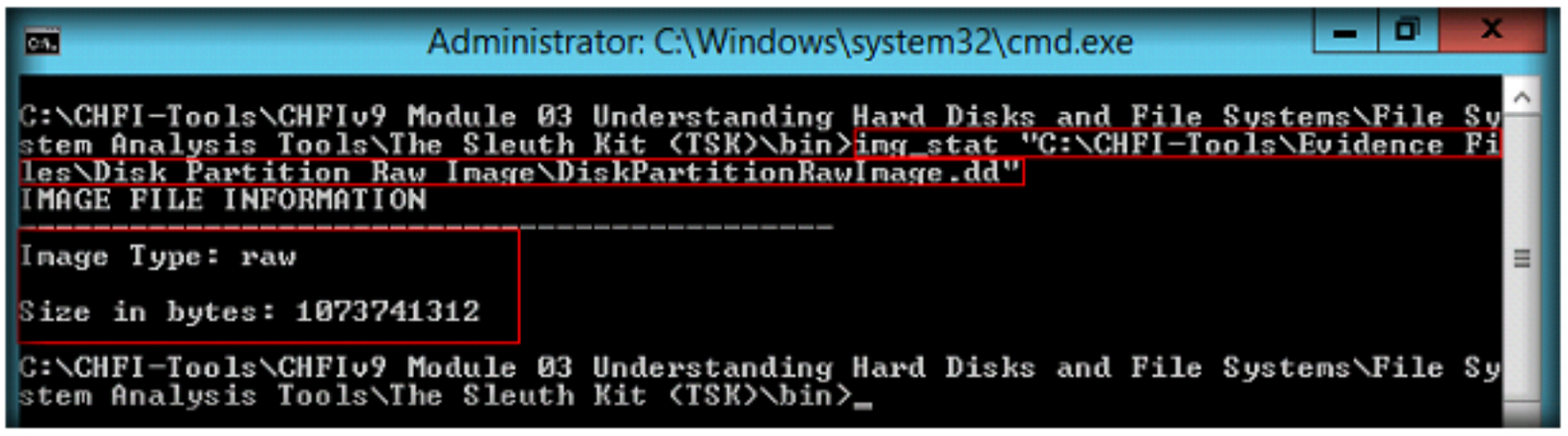


FIGURE 2.13: Viewing image file details

Lab Analysis

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

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

Questions

1. Determine the other options of **istat** command-line tool.
2. Determine the other options of **fls** command-line tool.

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

Lab 3

Analyzing Raw image using Autopsy

Autopsy is a digital forensics platform used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

ICON KEY

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

Lab Scenario

An inspector, who is probing a murder incident, has found a dead system as a part of investigation in a crime scene and suspects that the system is related to the incident and could provide clues about it. When he brings the system to cyber forensics department, the forensic investigator uses Autopsy to replicate the hard disk. On further analysis of the file systems they found some obscene videos and pictures that could have been the cause of the murder.

In order to investigate a hard disk, as a forensic investigator you must know the types of file systems and how to analyze them using various tools.

Lab Objectives

The objective of this lab is to help investigators learn and perform file system analysis using Autopsy:

- File system type.
- Metadata information.
- Content information.

Lab Environment

This lab requires:

- Autopsy, is an inbuilt tool in Kali Linux.
- You can also download the Windows based version of **Autopsy** from the link **http://www.sleuthkit.org/autopsy/.**
- Kindly note that if you decide to download the latest version, then the screenshots shown in this lab might differ slightly.
- A computer running **Kali Linux**.
- A Computer running **WindowsServer2012** machine to access CHFI-Tools directory.
- Administrative privileges to execute the commands.
- A web browser with an Internet connection.

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 03 Understanding Hard Disks and File Systems

Lab Duration

Time: 25 Minutes

Overview of Autopsy

Autopsy was designed to be intuitive out of the box. All results are found in a single tree. Autopsy was designed to be an end-to-end platform with modules that come with it out of the box and others that are available from third-parties.

Lab Tasks

TASK 1

Launch Autopsy

1. To launch Autopsy, navigate to **Applications → 11 – Forensics → autopsy.**

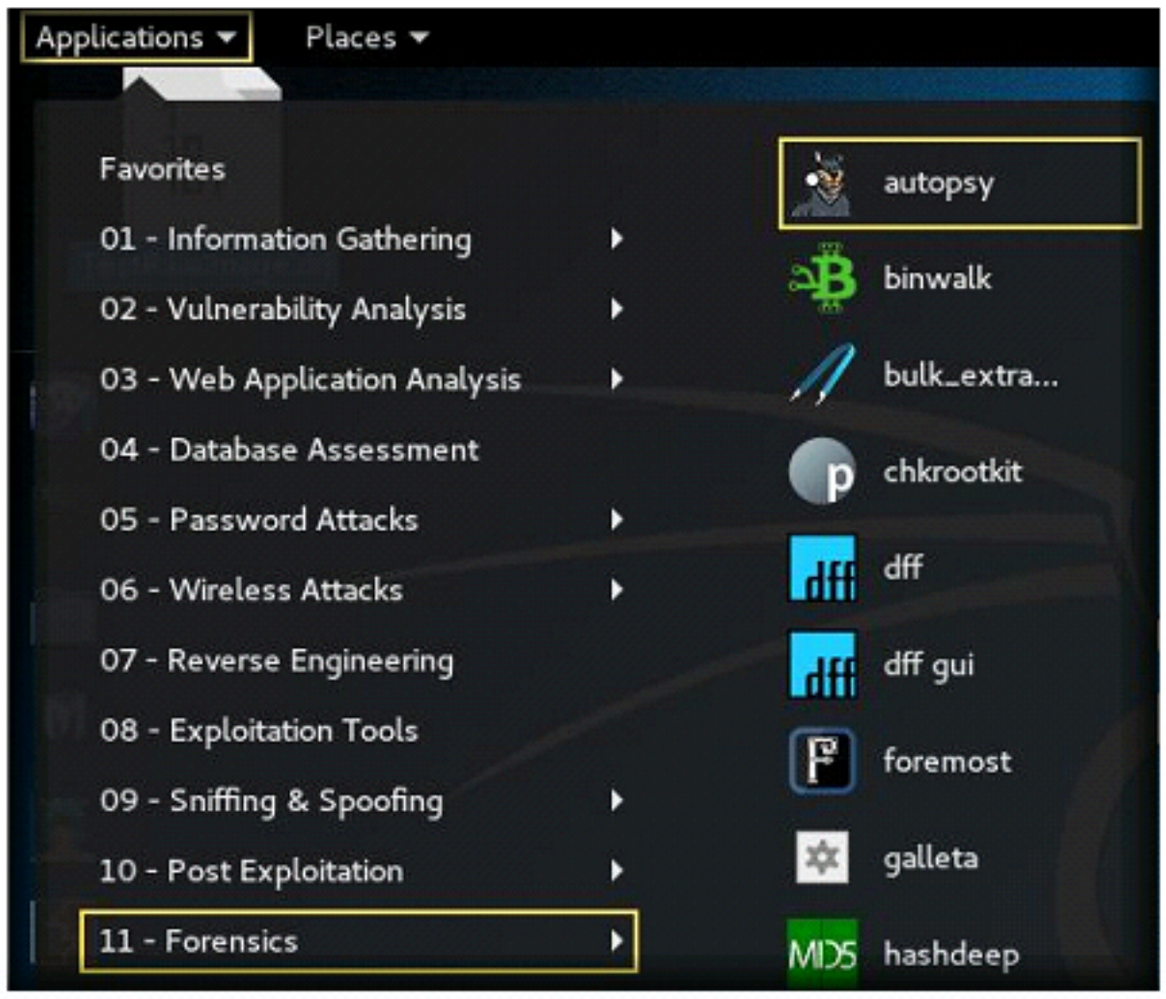
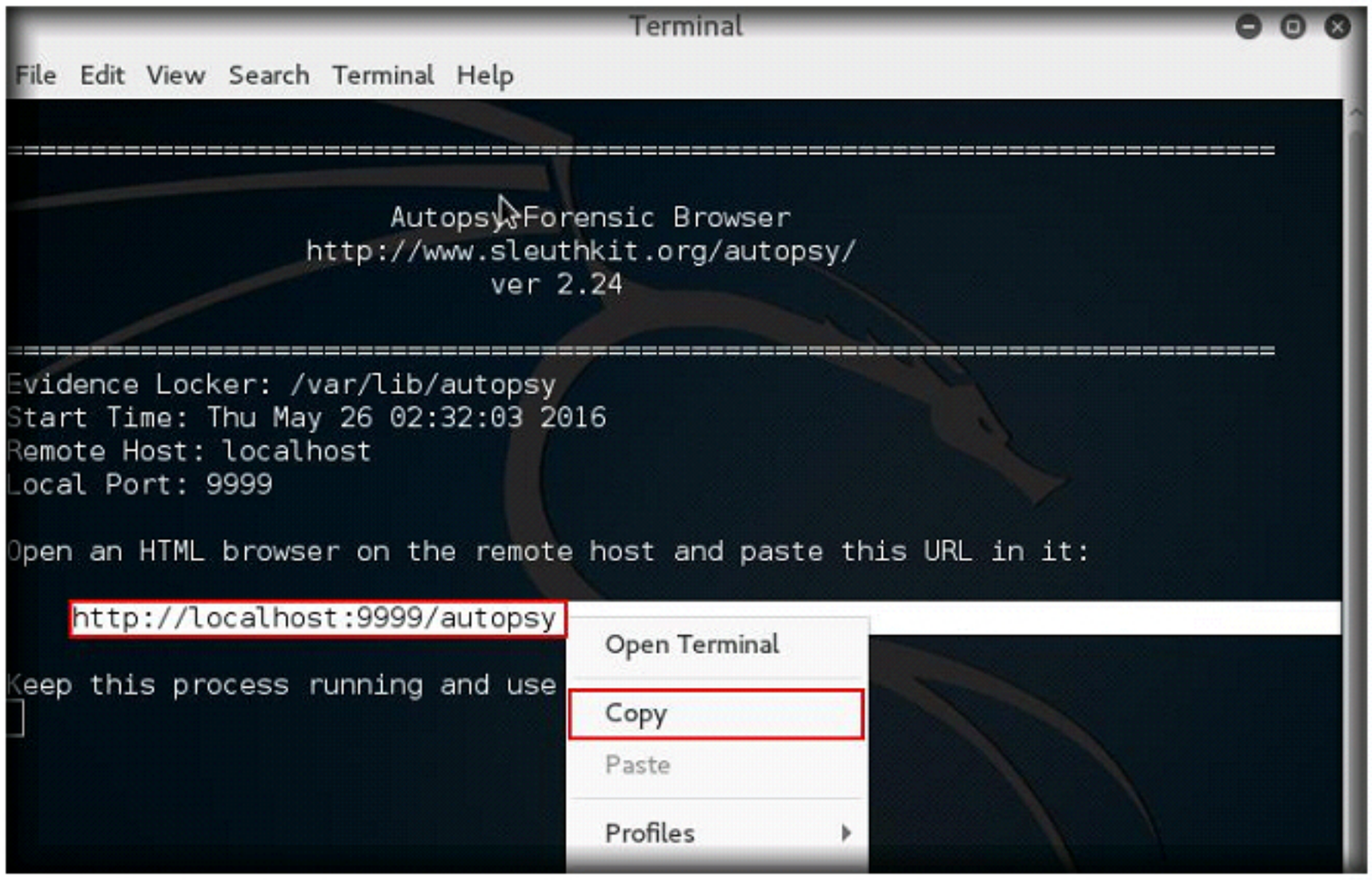


Figure 3.1: Launching Autopsy in Kali Linux

Autopsy analyzes disk images, local drives, or a folder of local files. Disk images can be in either raw/dd or E01 format. E01 support is provided by libewf.

2. Terminal window opens once you click on **Autopsy** icon from the Applications menu.
3. In the **terminal** window it will instruct to open a **browser** and browse the URL http://localhost:9999/autopsy, copy the given URL as shown in the screenshot.

   Note: Do not close the terminal window until the process is completed.



Autopsy has an extensible reporting infrastructure that allows additional types of reports for investigations to be created. By default, an HTML, XLS, and Body file report are available.

Figure 3.2: Autopsy Terminal window

4. Once the link is copied, now click **Iceweasel** icon from the task bar to open a web browser.
5. **Paste** the copied link in the Iceweasel browser's address bar and press **Enter**.

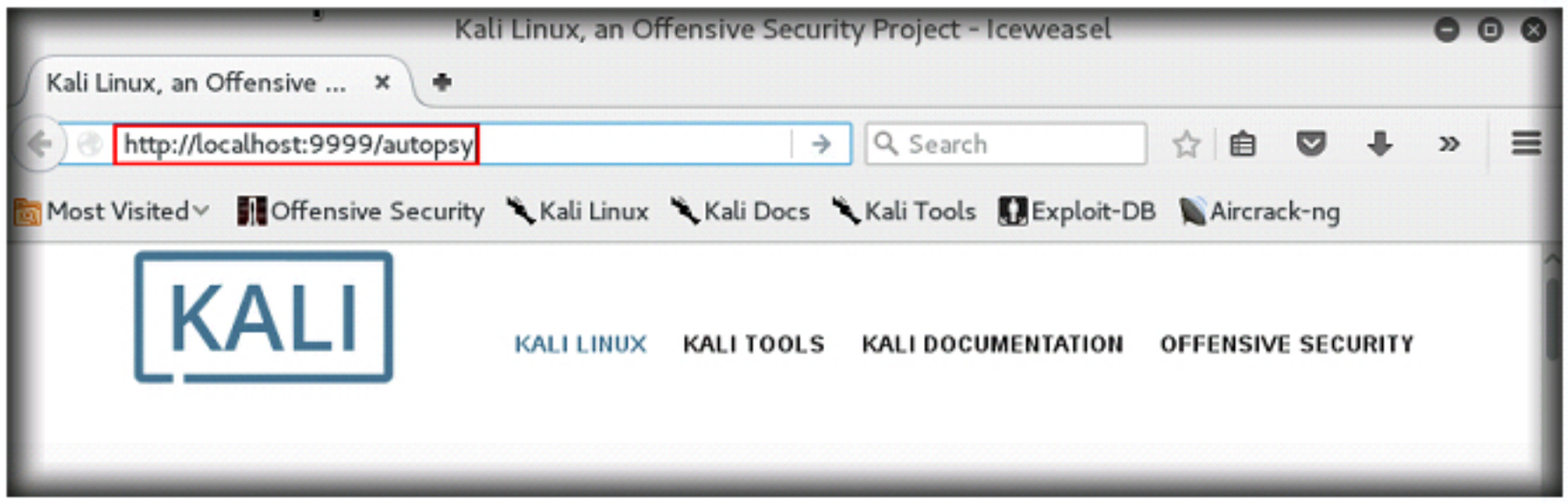


Figure 3.3: Accessing Autopsy link in Browser

TASK 2

Creating New Case

6. Autopsy main window appears as shown in the screenshot, click **NEW CASE** button to start the investigating process.

   Note: Ignore the Warning message in autopsy main window.

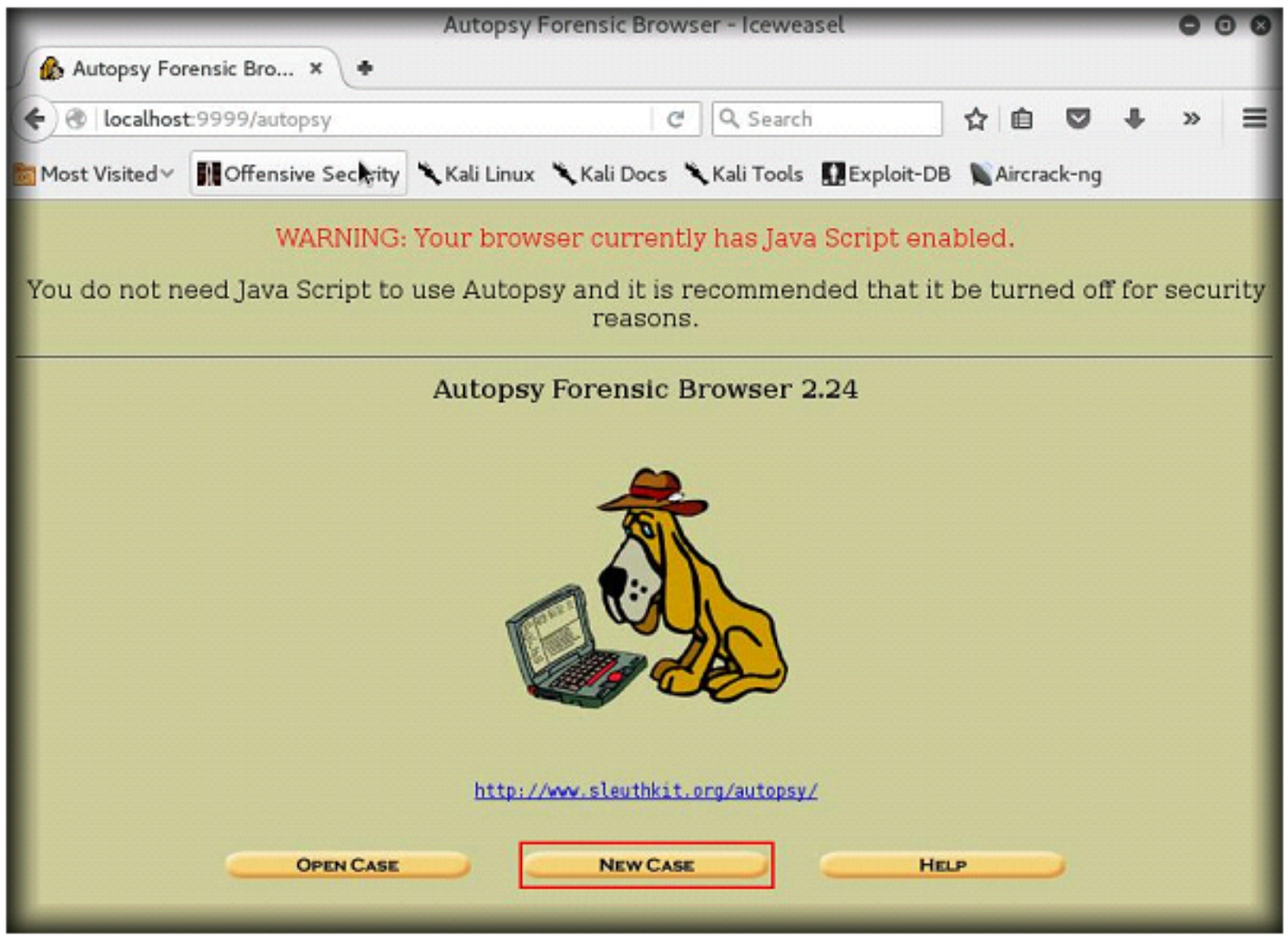


Figure 3.4: Autopsy main window

Directory List

The left-hand side window has four main options:

Directory Seek

File Name Search

Hide / Expand Directories

Show All Deleted Files

7. **CREATE A NEW CASE** page subsequently appears, fill the required details.

8. In this lab we have given this case a numerical case name as **100**, and description as **Test**, and Investigator name as **Johnathan**, and click **NewCase**.

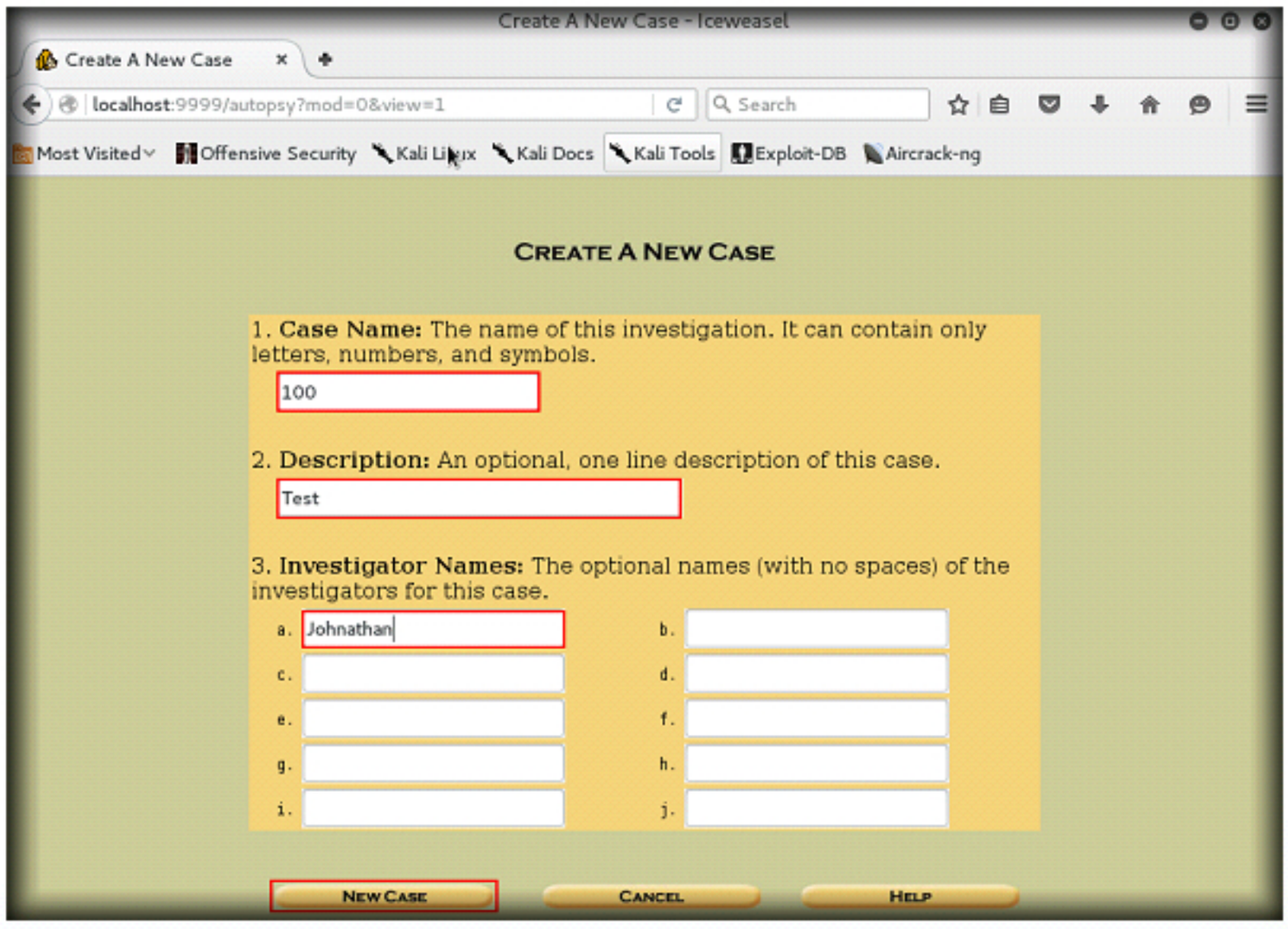


Figure 3.5: Creating a New Case

TASK 3

Adding Host

9. Once you click on "**NewCase**" button in the previous screen, it will redirect you to the **Creating Case** webpage.
10. Now, click **ADDHOST** button.

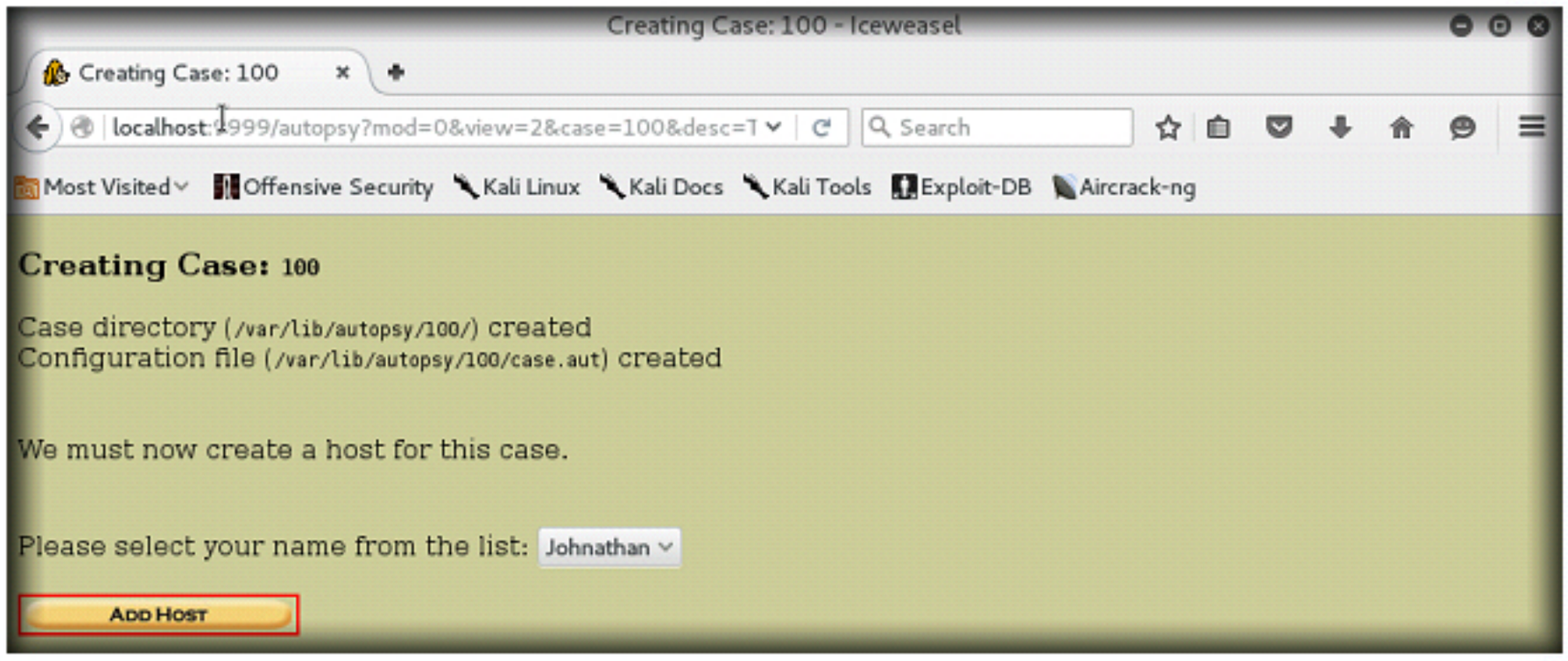
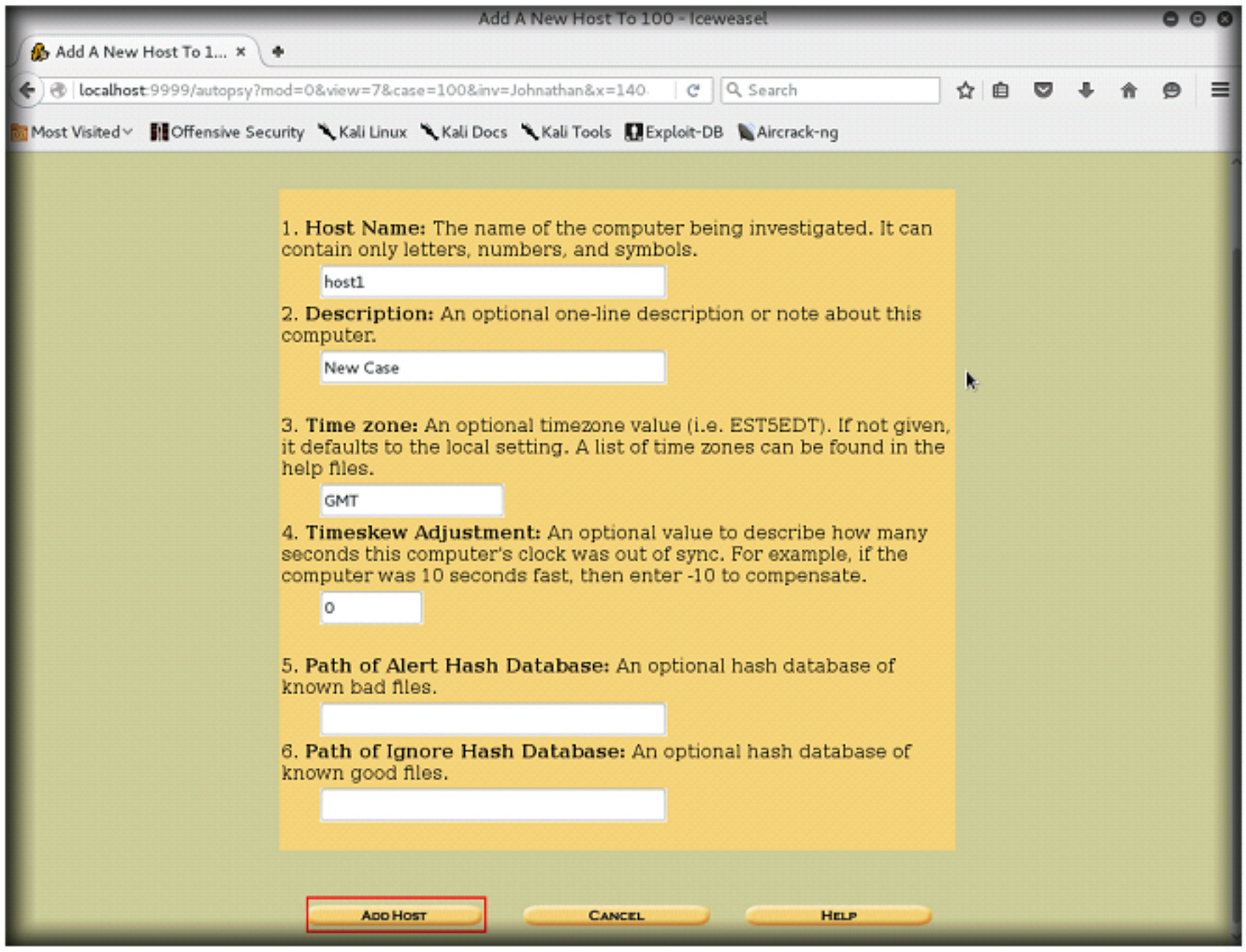


Figure 3.6: Adding a Host

11. **ADDA NEW HOST** webpage next appears where you need to fill the details, and click **ADDHOST** button.



This screen simply gives us the name of the case, where the case will be stored (/var/lib/autopsy/100), and where its configuration file will be stored (/var/lib/autopsy/100/case.aut).

Figure 3.7: Host Details

TASK 4

Adding Image

12. After successfully adding host to autopsy, it will appear as shown in the screenshot.
13. Now, we need to add an image for investigation. Click **ADDIMAGE** button.

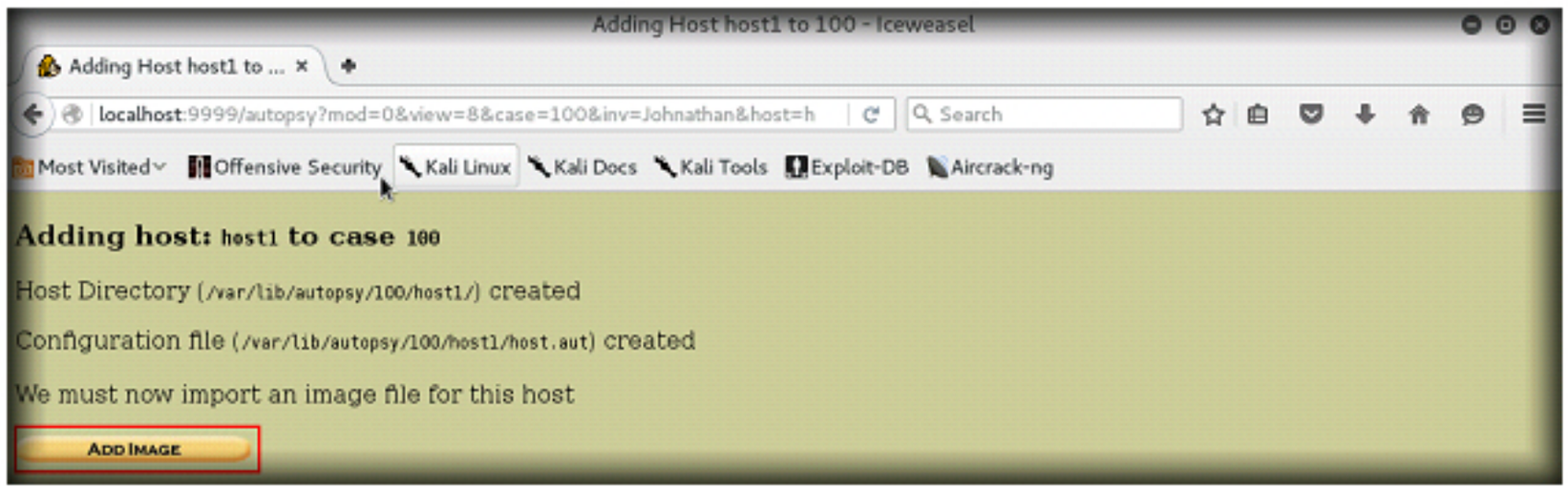


Figure 3.8: Add Image

14. Click **ADD IMAGE FILE** button to add an image for investigation.

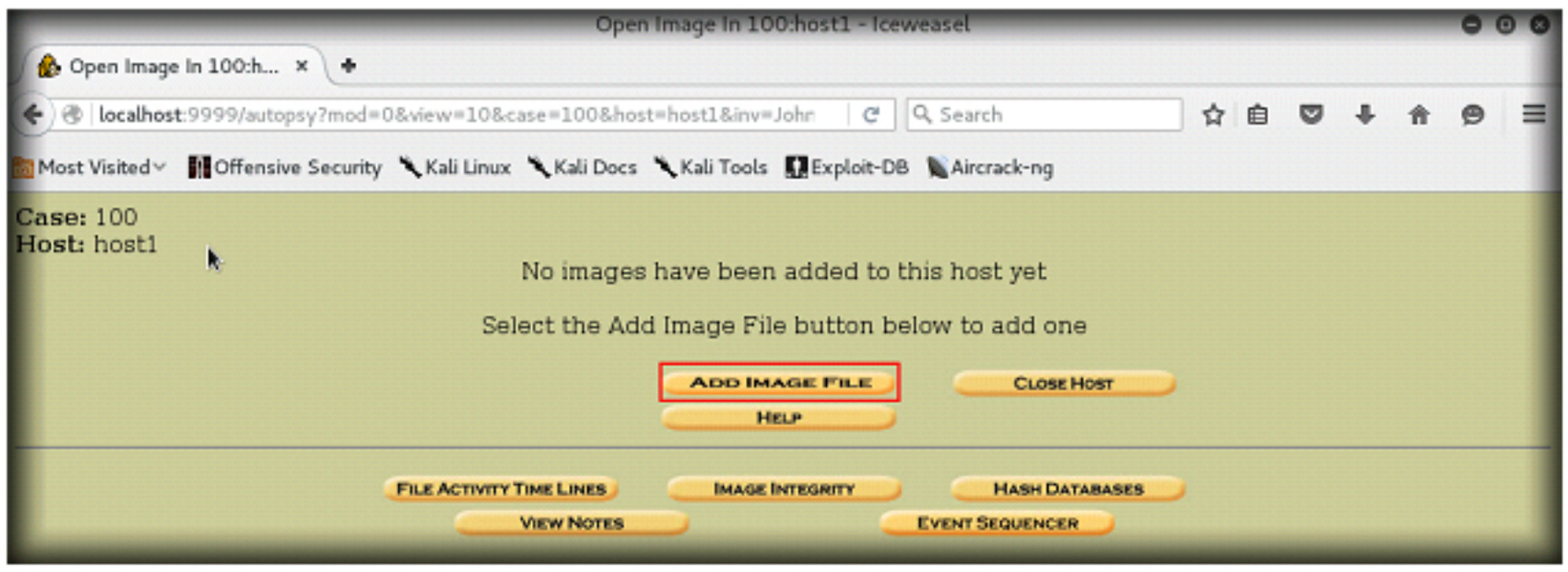


Figure 3.9: Adding and Image

Autopsy will start to analyze these data sources and add them to the case and internal database. While it is doing that, it will prompt you to configure the Ingest Modules.

15. **ADD A NEW IMAGE** page appears; here we need to provide the location of the image in the **Location** field, **Type** of the Image, and **Import Method**.

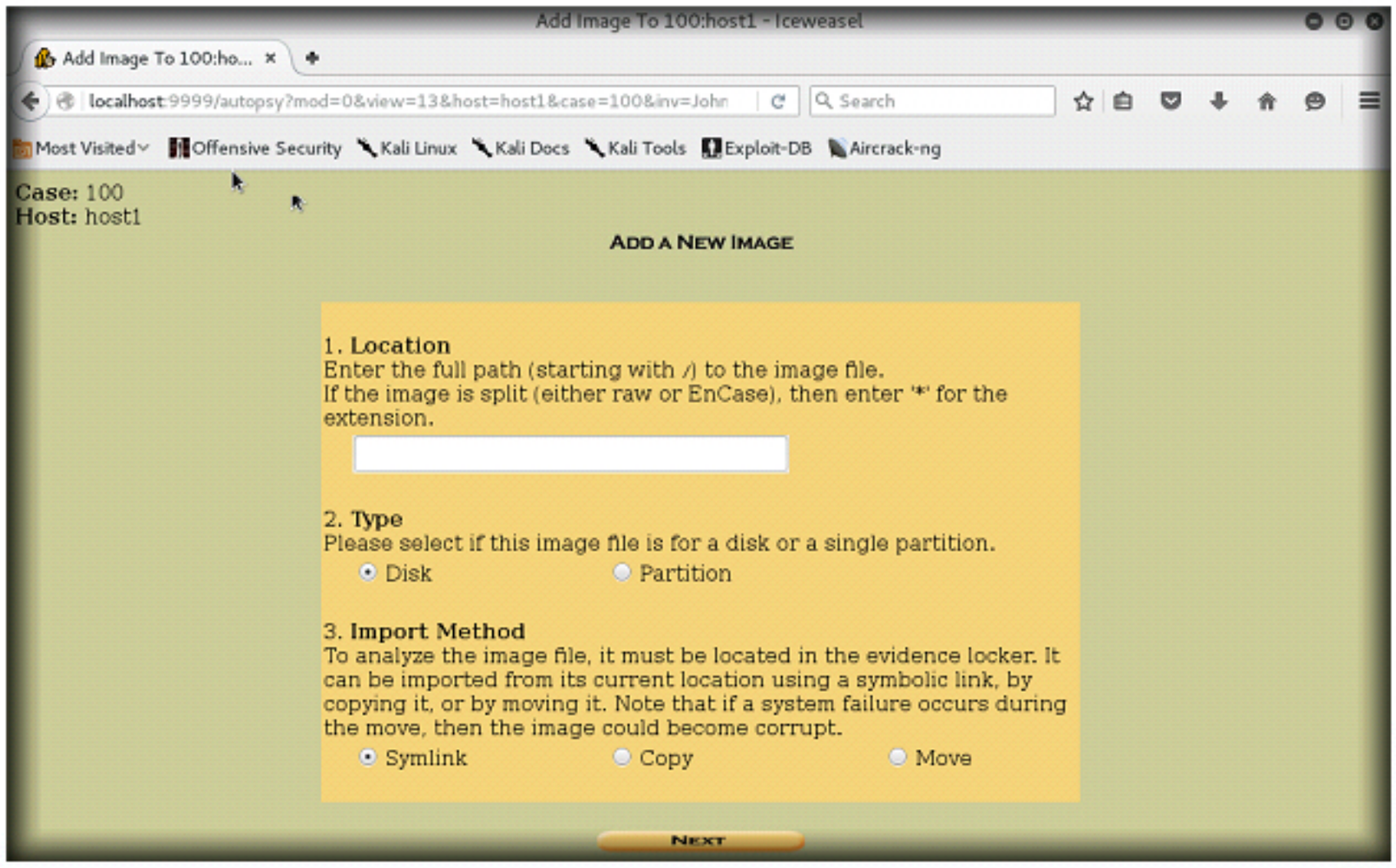


Figure 3.10: Add a New Image

A dead analysis occurs when a dedicated analysis system is used to examine the data from a suspect system. In this case, Autopsy and The Sleuth Kit are run in a trusted environment, typically in a lab. Autopsy and TSK support raw, Expert Witness, and AFF file formats.

16. Minimize the browser window, double-click **chfi-tools on 10.0.0.12** on desktop and navigate to **EvidenceFiles → Disk Partition Raw Image** and copy **DiskPartionRawImage.dd** file and paste it on desktop.

    Note: **10.0.0.12** is the IP Address of **Windows Server 2012**virtual machine. IP Addresses may differ as per your network infrastructure.

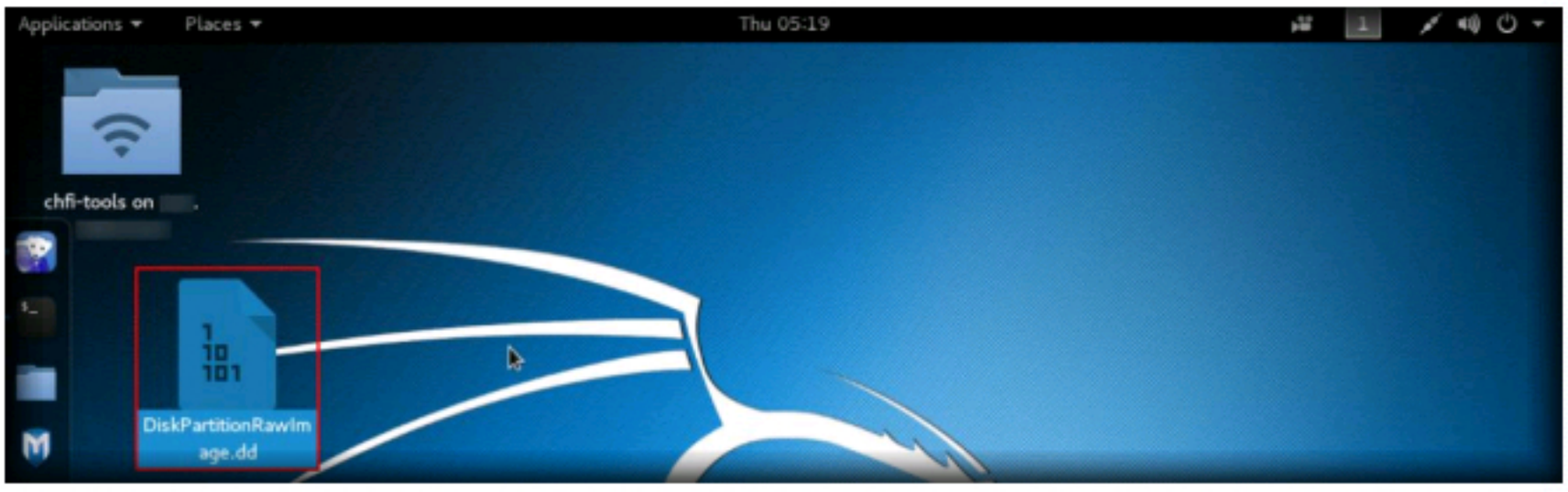


Figure 3.11: Sample Image file on Desktop

17. Maximize the Autopsy browser, and drag **DiskPartionRawImage.dd** file in the **Location** field.

18. In **Type** section choose **Partition** radio button, leave the other settings to default, and click **NEXT**.

    Note: While you are dragging the image file, the path will be shown as **file:///....,** delete **file://**

A live analysis occurs when the suspect system is being analyzed while it is running. In this case, Autopsy and The Sleuth Kit are run from a CD in an untrusted environment. This is frequently used during incident response while the incident is being confirmed. After it is confirmed, the system can be acquired and a dead analysis performed.

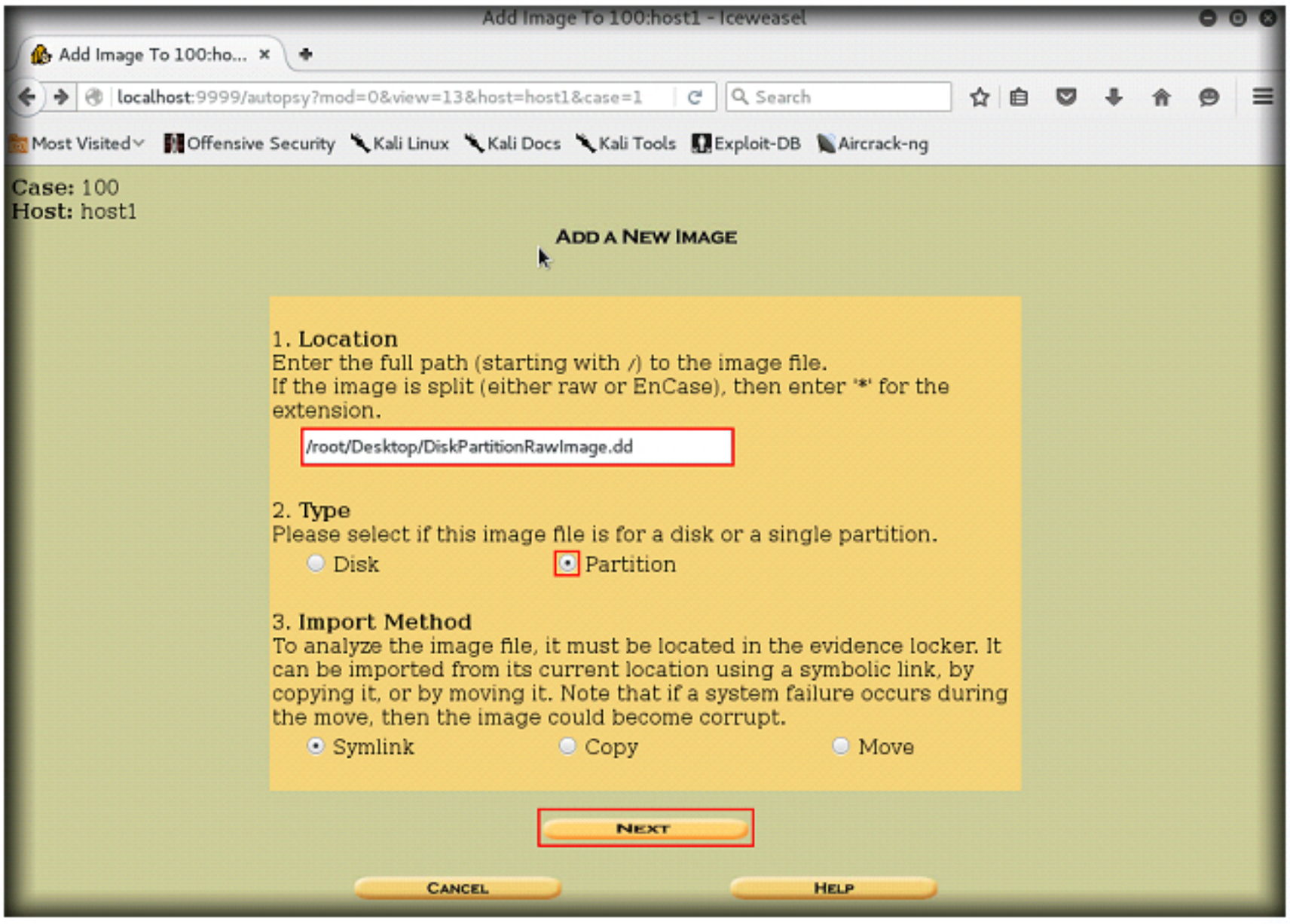


Figure 3.12: Image Added for Investigation

19. **Image File Details** webpage next appears, leave the settings to default and click **ADD**.

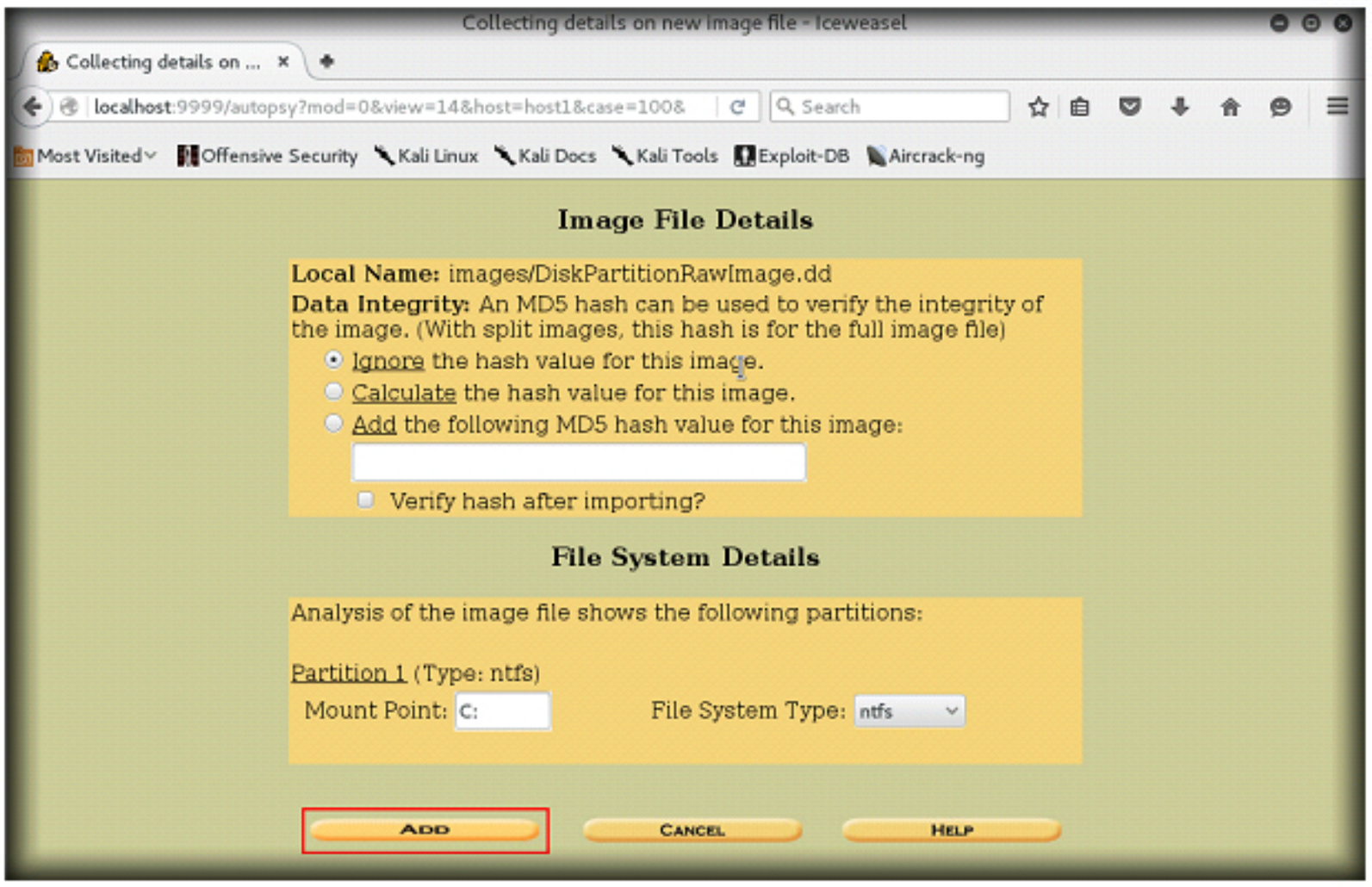


Figure 3.13: Image File Details

20. **Testing partitions** page appears, click **OK**.

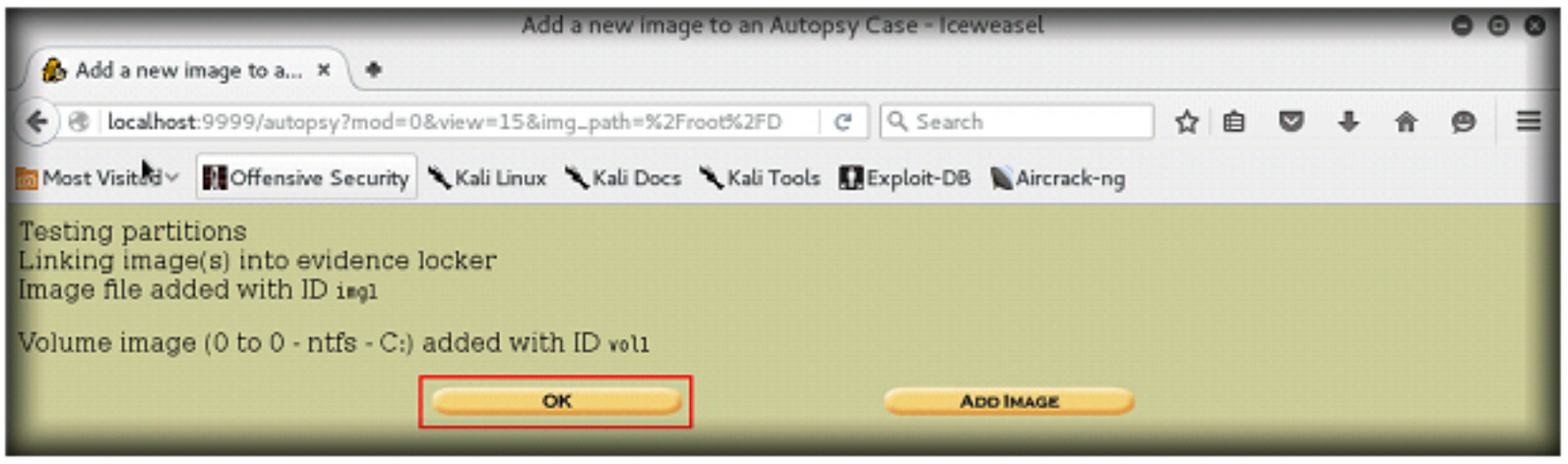


Figure 3.14: Testing partitions page

TASK 5

Analyzing Added Image

21. Once the image is added to Autopsy database, you can analyze the image. To analyze the image click **ANALYZE**.

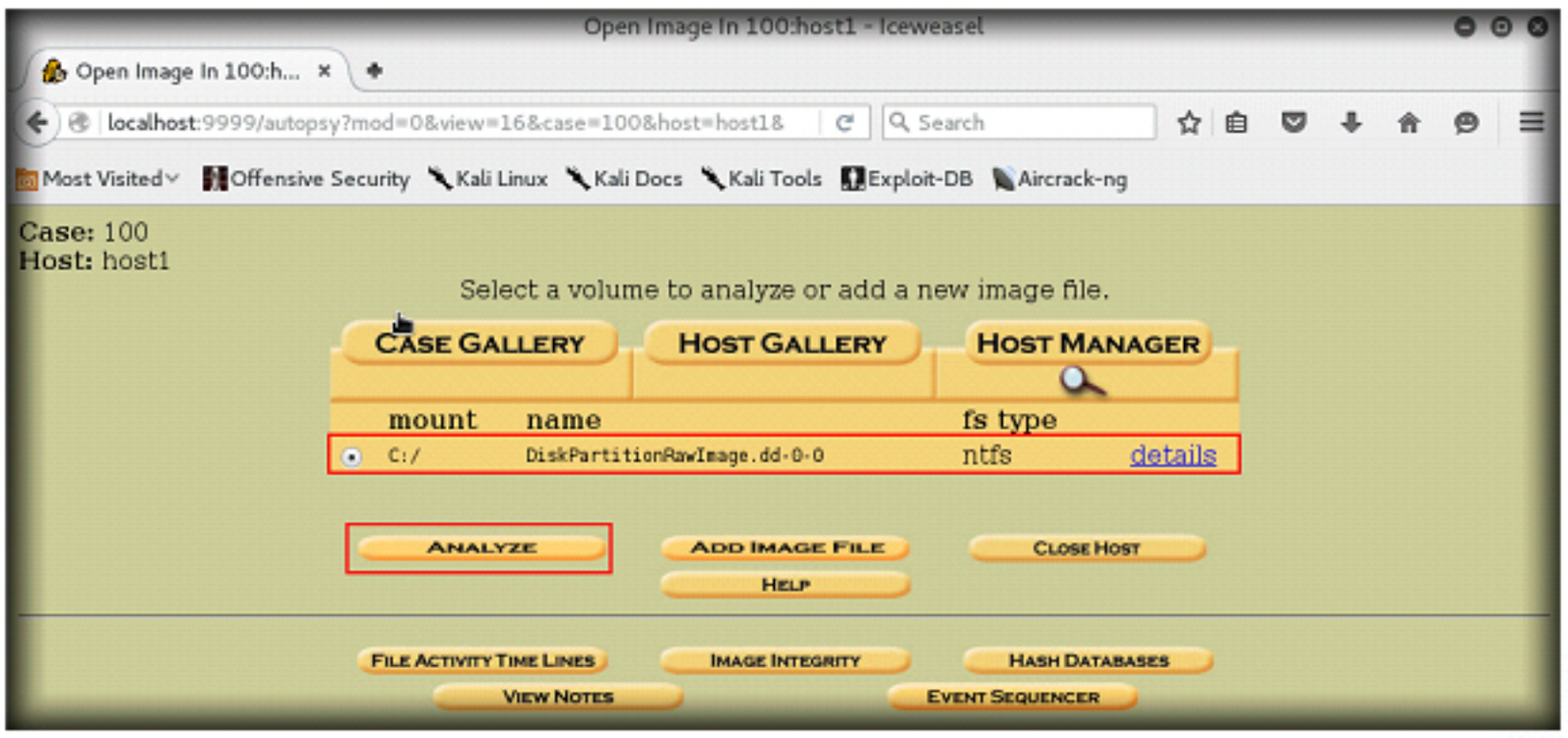


Figure 3.15: Analyzing the Added Image

22. To start analyzing the added disk image, you can choose the analysis mode from the above tabs as shown in the screenshot.

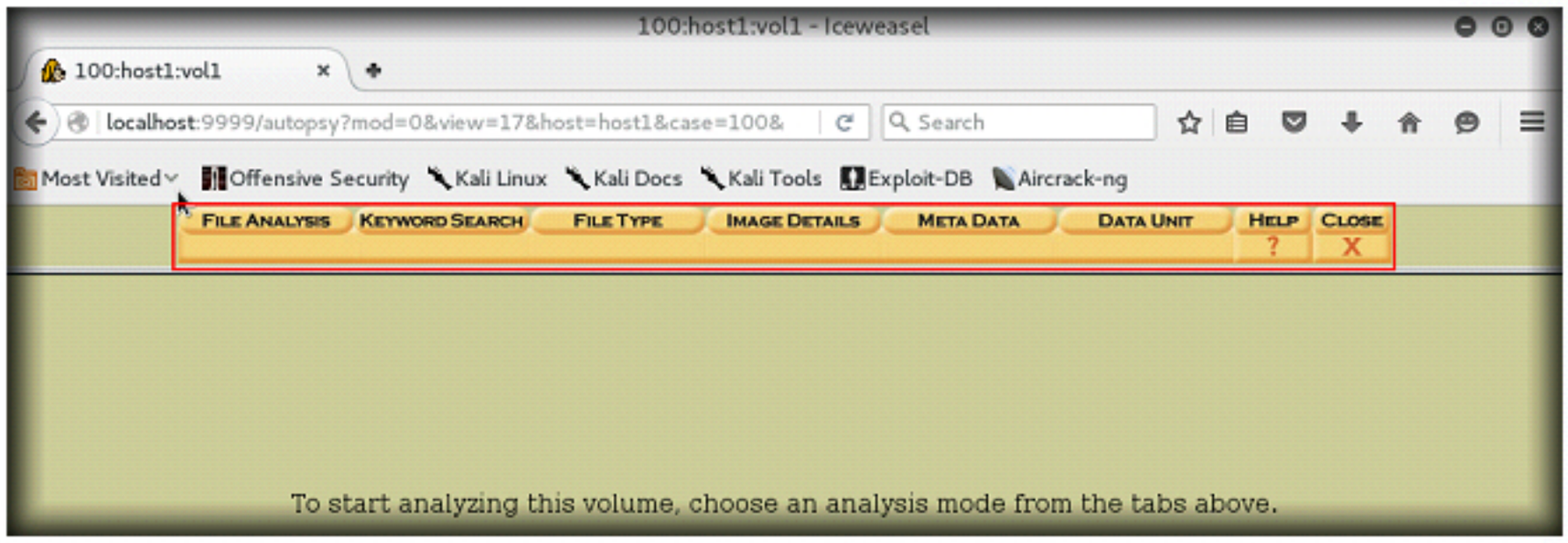
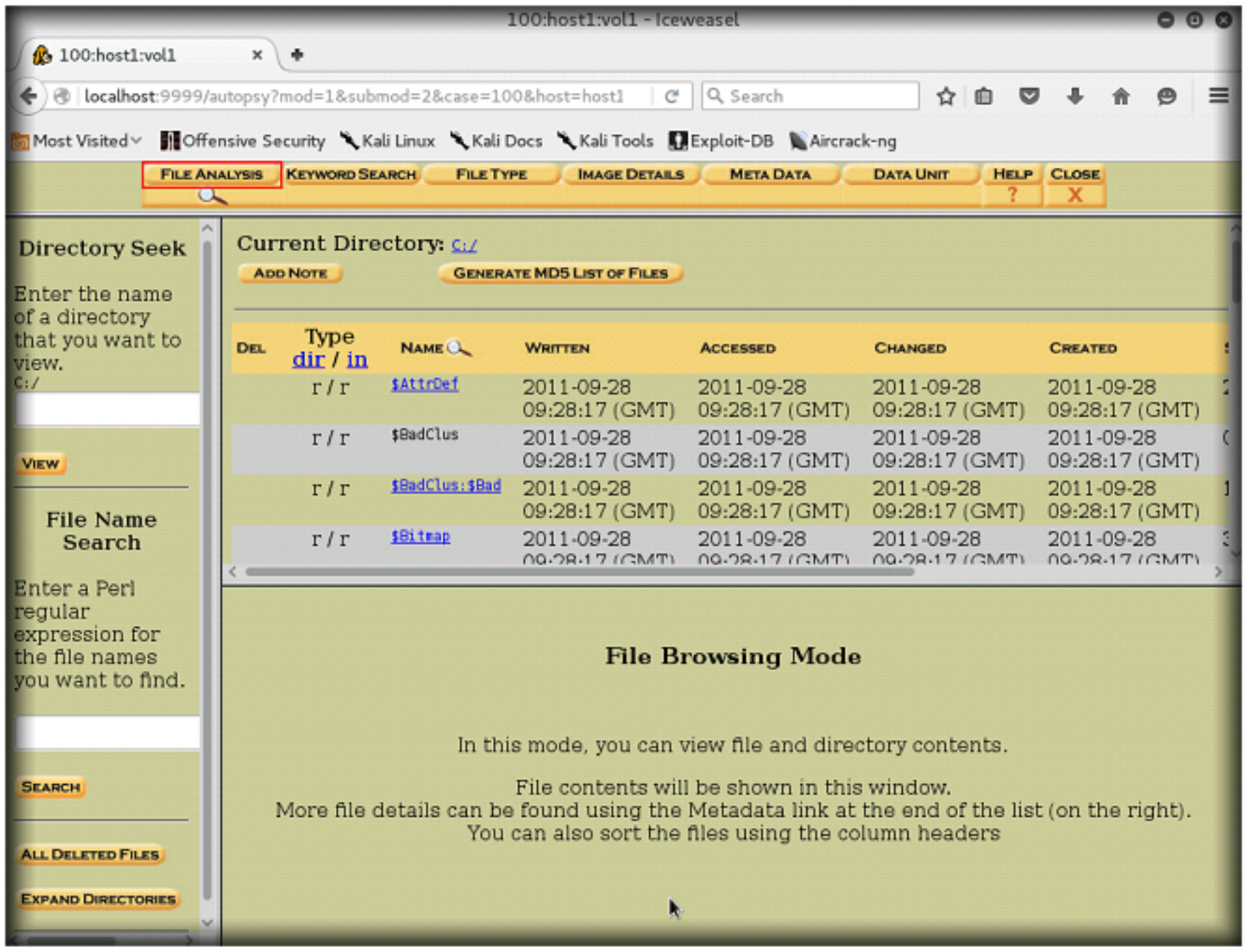


Figure 3.16: Analysis Method

23. To do file analysis, click **FILEANALYSIS** button that allows you to analyze an image from the file and directory perspective.

24. **File Analysis** is used to examine the directories and files for evidence. It also performs basic binary analysis to extract the ASCII strings.



📖File Listing: Analyze the files and directories, including the names of deleted files and files with Unicode-based names.

Figure 3.17: Analysis of the Added Image

25. To generate MD5 hashes of the contained files, click **GENERATE MD5 LIST OF FILES** button, it will open in a new tab of the browser with the list of Hash values of image.

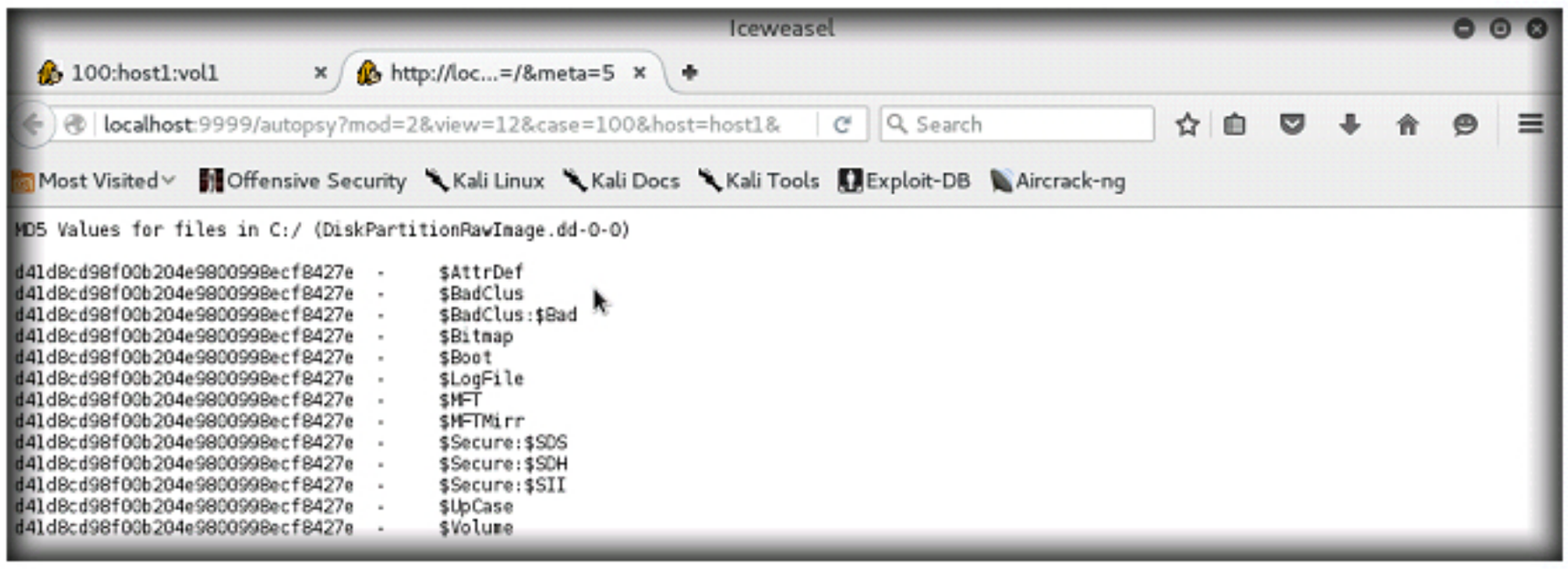


Figure 3.18: MD5 Hash values of the contents

26. Click **IMAGEDETAILS** button to view the complete File system of the added image, where you can view **FILE SYSTEM INFORMATION**, **METADATA INFORMATION**, and **CONTENT INFORMATION**.

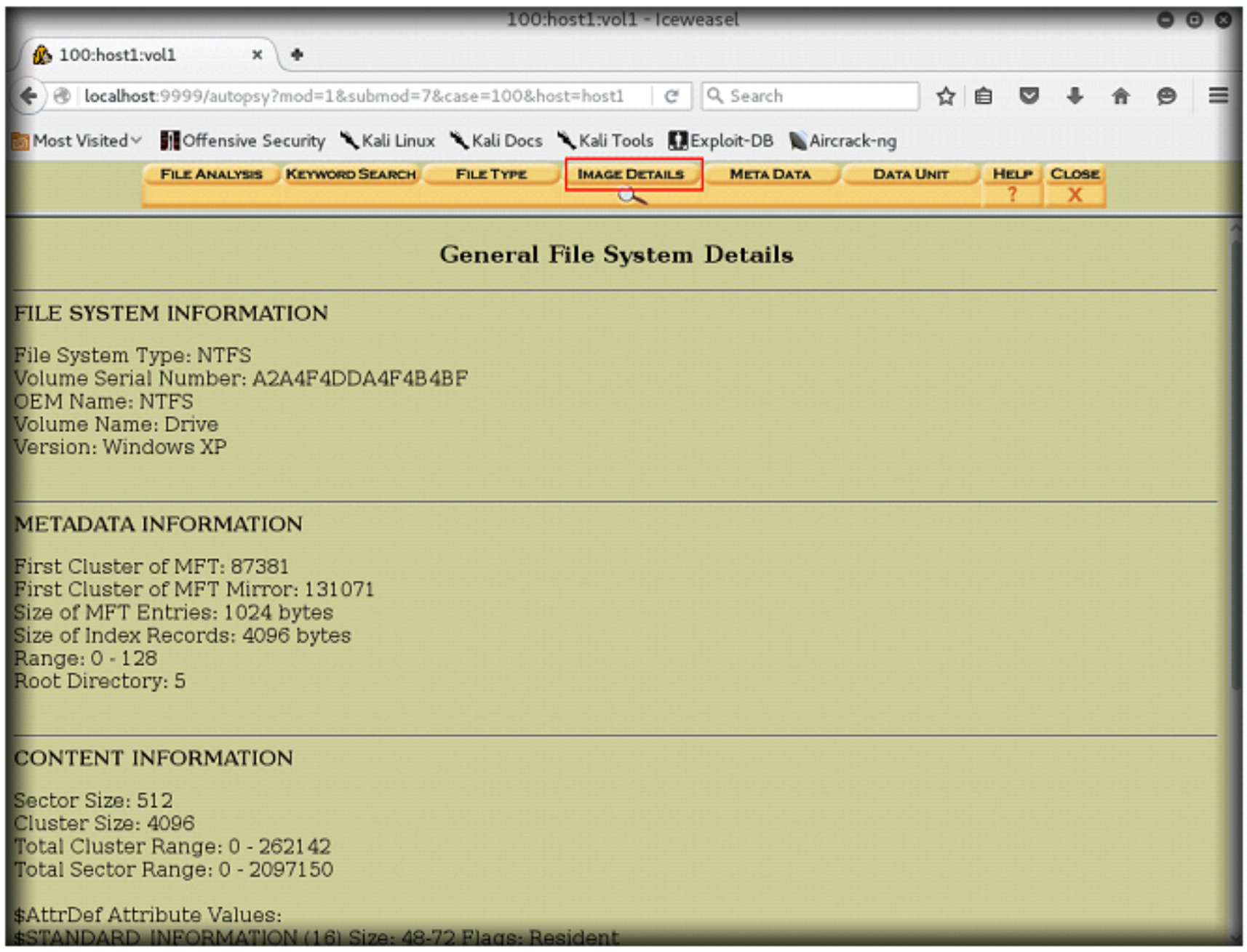


Figure 3.19: Image Details

Thus, you can go through the all the required options of the Autopsy in detail required for your investigation.

Lab Analysis

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

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

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