

Data Acquisition and Duplication

Module 04

Data Acquisition and Duplication

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

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

Lab Objectives

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

- Investigating NTFS streams from hard drives.
- Investigating hidden text strings.
- Extracting the hidden content from hard drives.

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication**

Lab Environment

To carry out the lab, you need:

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

Lab Duration

Time: 30 Minutes

Overview of Data Acquisition and Duplication

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

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

**T A S K 1**

Lab Tasks

Overview

Recommended labs to assist you in data acquisition and duplication:

- Investigating NTFS Drive Using **DiskExplorer for NTFS**.
- Viewing Content of Forensic Image Using **AccessData FTK Imager Tool**.

Lab Analysis

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

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

Lab

1

Investigating NTFS Drive Using DiskExplorer for NTFS

DiskExplorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

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

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

Lab Objectives

The objective of this lab is to help students learn how to investigate the NTFS file system.

In this lab you will learn how to:

- Use **DiskExplorer for NTFS**

Lab Environment

To carry out the lab, you need:

- DiskExplorer for NTFS, located at **C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\DiskExplorer for NTFS**.
- You can also download the latest version of **DiskExplorer for NTFS** from the link <https://www.runtime.org/diskexplorer.htm>.
- Kindly note that if you decide to download the latest version, screenshots shown in the lab might differ.

 **Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication**

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

Lab Duration

Time: 15 Minutes

Overview of DiskExplorer for NTFS

DiskExplorer for NTFS disk editor enables you to investigate your NTFS drive and conduct your own data recovery. It navigates your NTFS drive by jumping to the partition table, boot record, Master file table, or the root directory. It also inspects the file entry details, NT attributes, etc.

Lab Tasks



TASK 1

Launching DiskExplorer Tool

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\DiskExplorer for NTFS**.
2. Double-click **Setup.exe** to launch the setup, and follow the wizard-driven installation steps.

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

3. To launch **DiskExplorer for NTFS**, double-click the shortcut icon (related to DiskExplorer) located on the Desktop.
4. The main window of **DiskExplorer for NTFS** will appear.

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

Drive specifies the loaded drive, floppy, or file with its total number of sectors in decimal and hexadecimal formats.

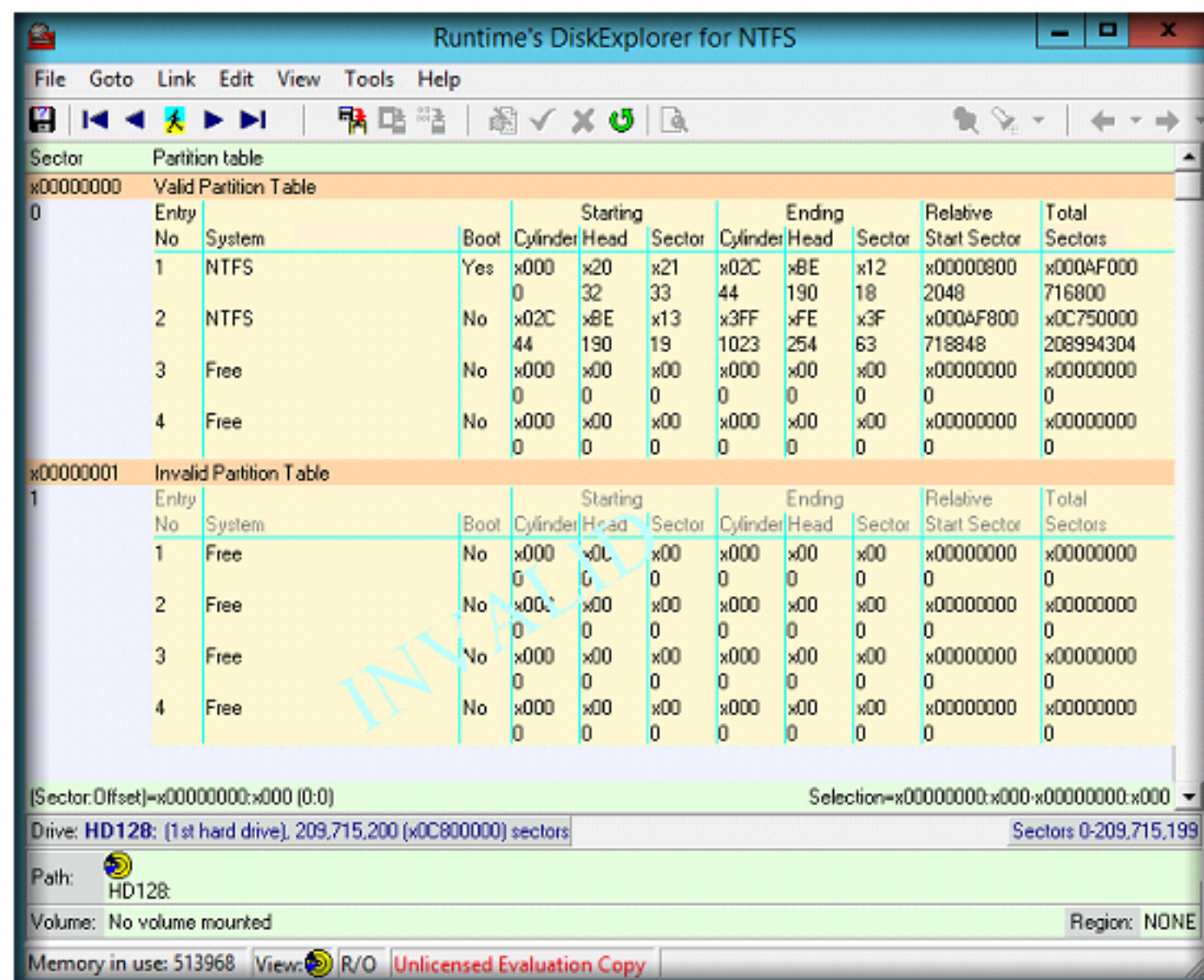


FIGURE 1.1: DiskExplorer for NTFS main window

5. Navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd** for the evidence file for this lab.

Path shows what area of the drive you are currently in and also the steps you can go back or forth by clicking the arrows on the navigation bar.

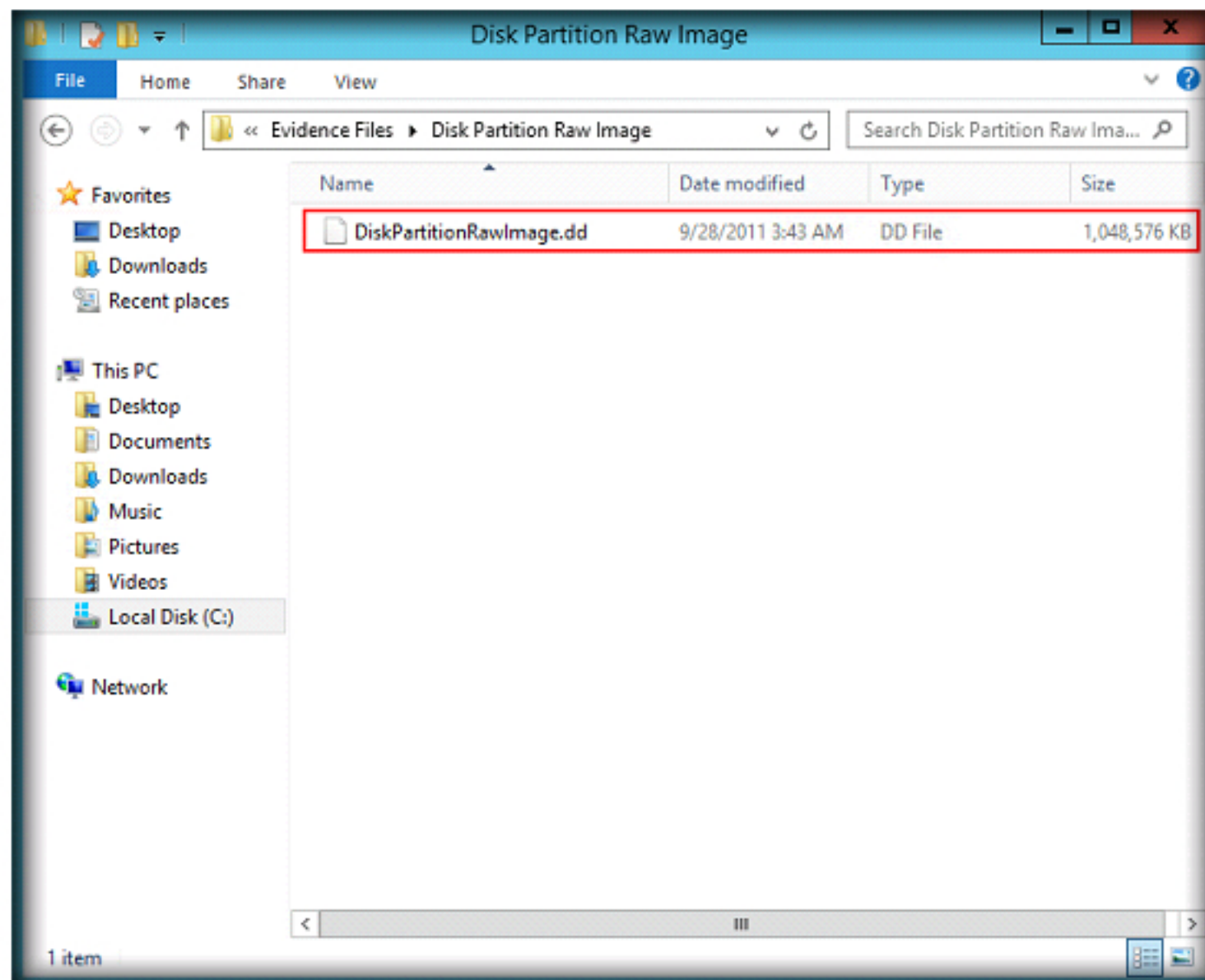


FIGURE 1.2: Evidence file



TASK 2

Selecting an Evidence Image

6. Select **Image** from the **File** menu, and then navigate to **C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd**.

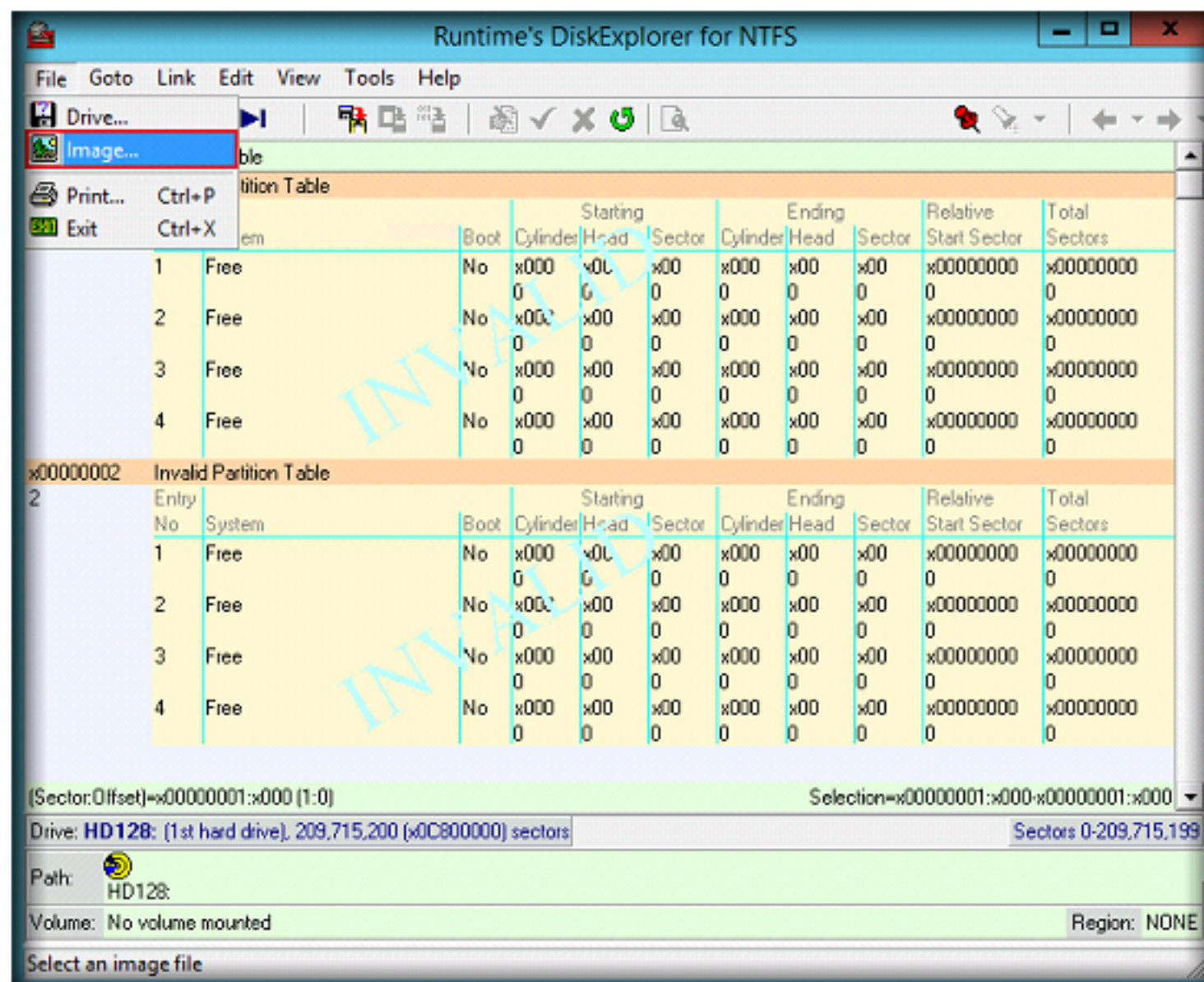


FIGURE 1.3: Select Image from the File menu

7. In the **Files of type** drop-down list, select **All files (*.*)**, and then click **Open**.

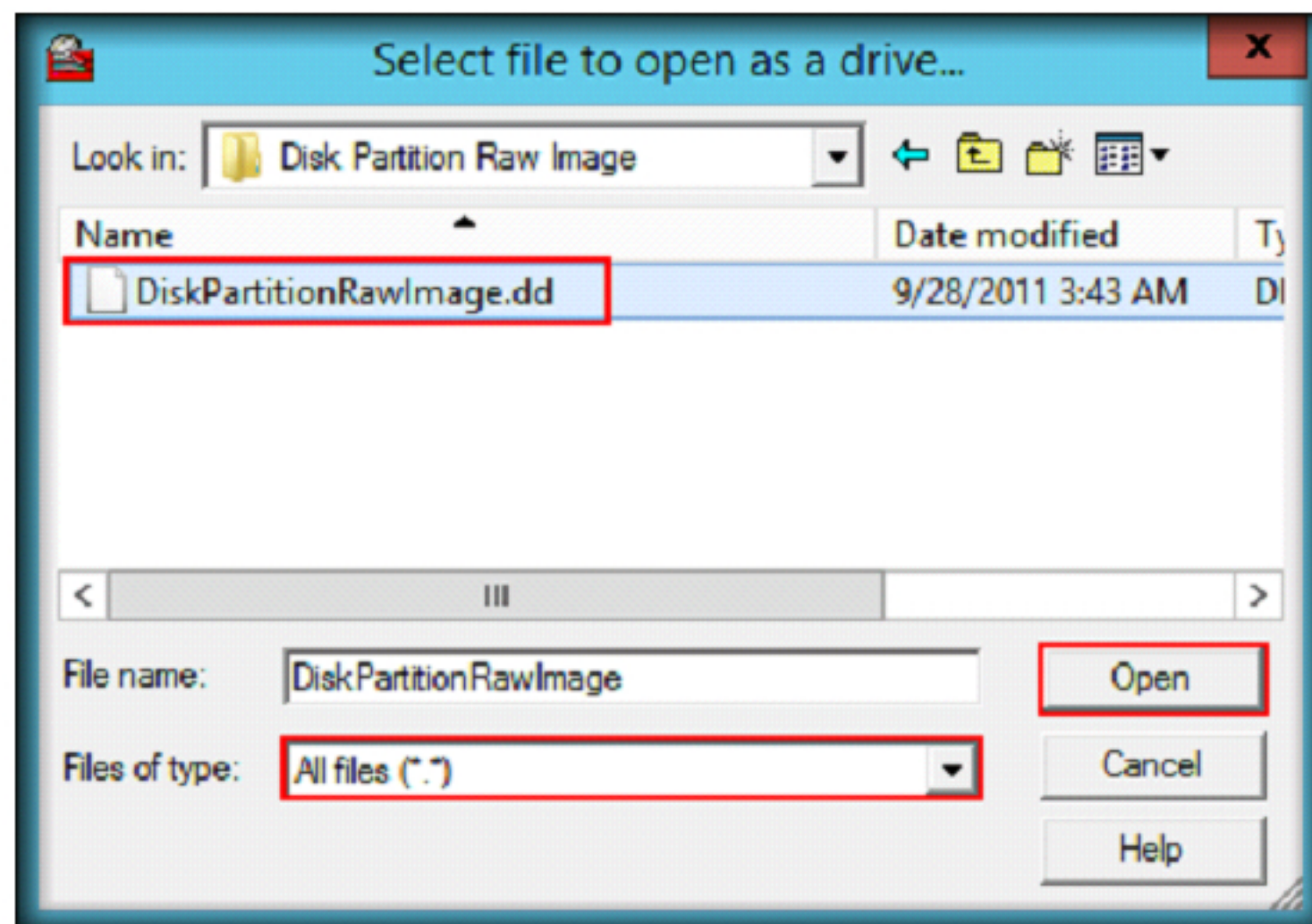


FIGURE 1.4: DiskExplorer for NTFS evidence image selection

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

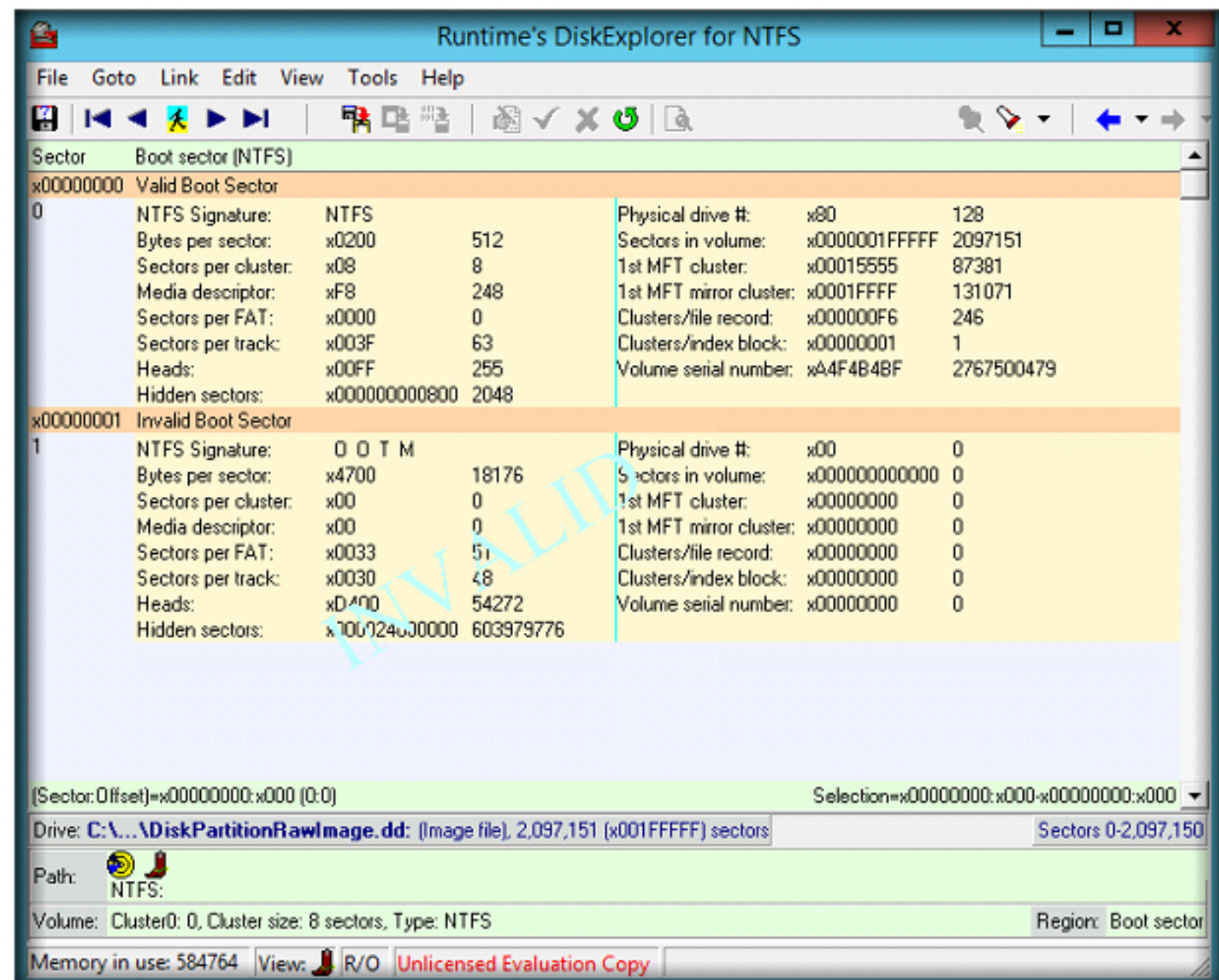


FIGURE 1.5: DiskExplorer for NTFS boot sector

Region lets you switch between boot sector, partition table, MFT, MFT No., and cluster region: simply right-click while the mouse is over the text to the right of "Region."

Volume gives information such as the position of cluster 0, the cluster size, and the type of the drive. To obtain more information on the volume, just click the underlined information line.

TASK 3

Selecting the Sector

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

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

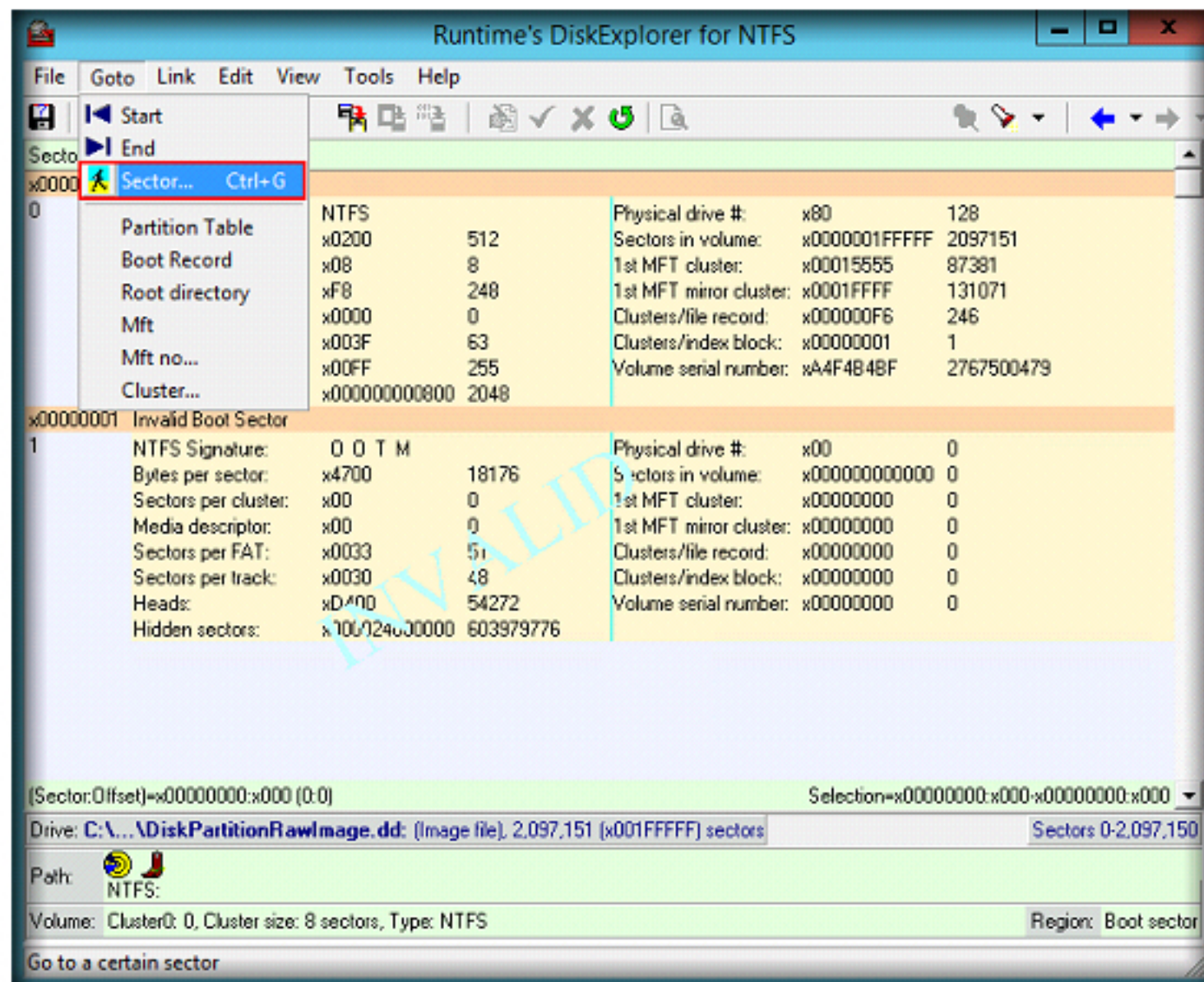


FIGURE 1.6: DiskExplorer for NTFS Sector option

10. In the **Gotosector...** wizard, enter the **hex** value in the **Sector** or **Byte** section to jump to a new position, and then click **OK**.

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

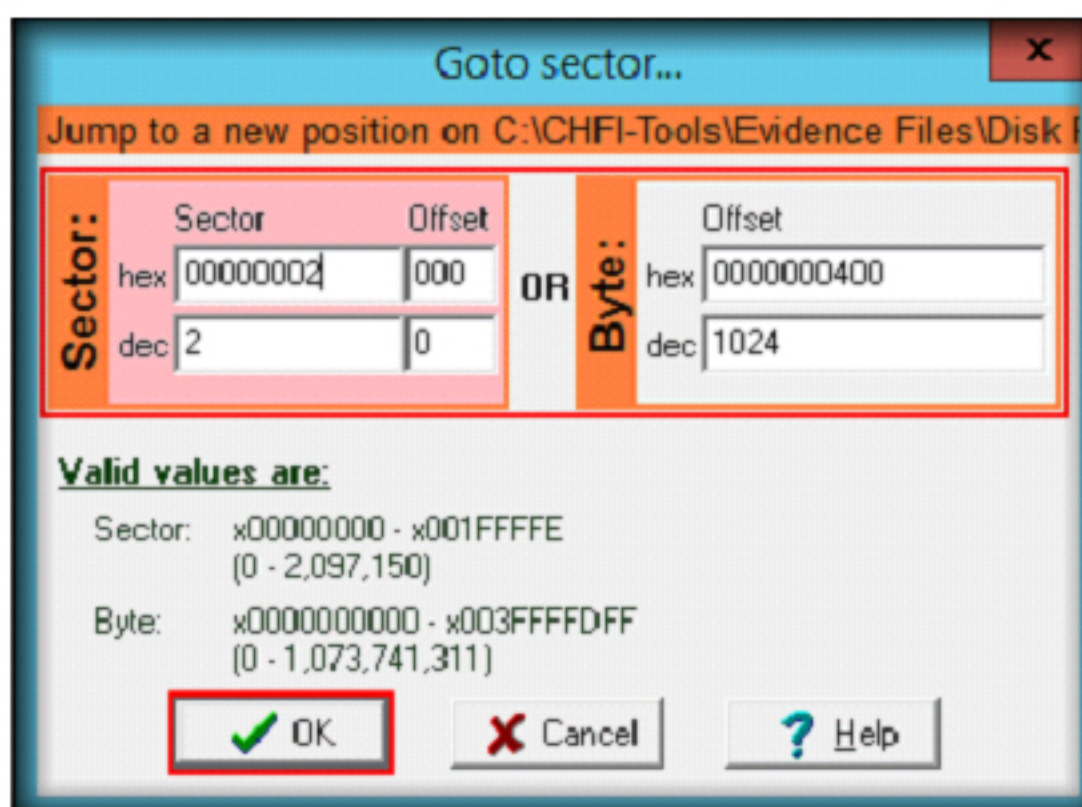


FIGURE 1.7: DiskExplorer for NTFS Gotosector wizard

11. It will display the entered sector information; the screen will look as shown below:

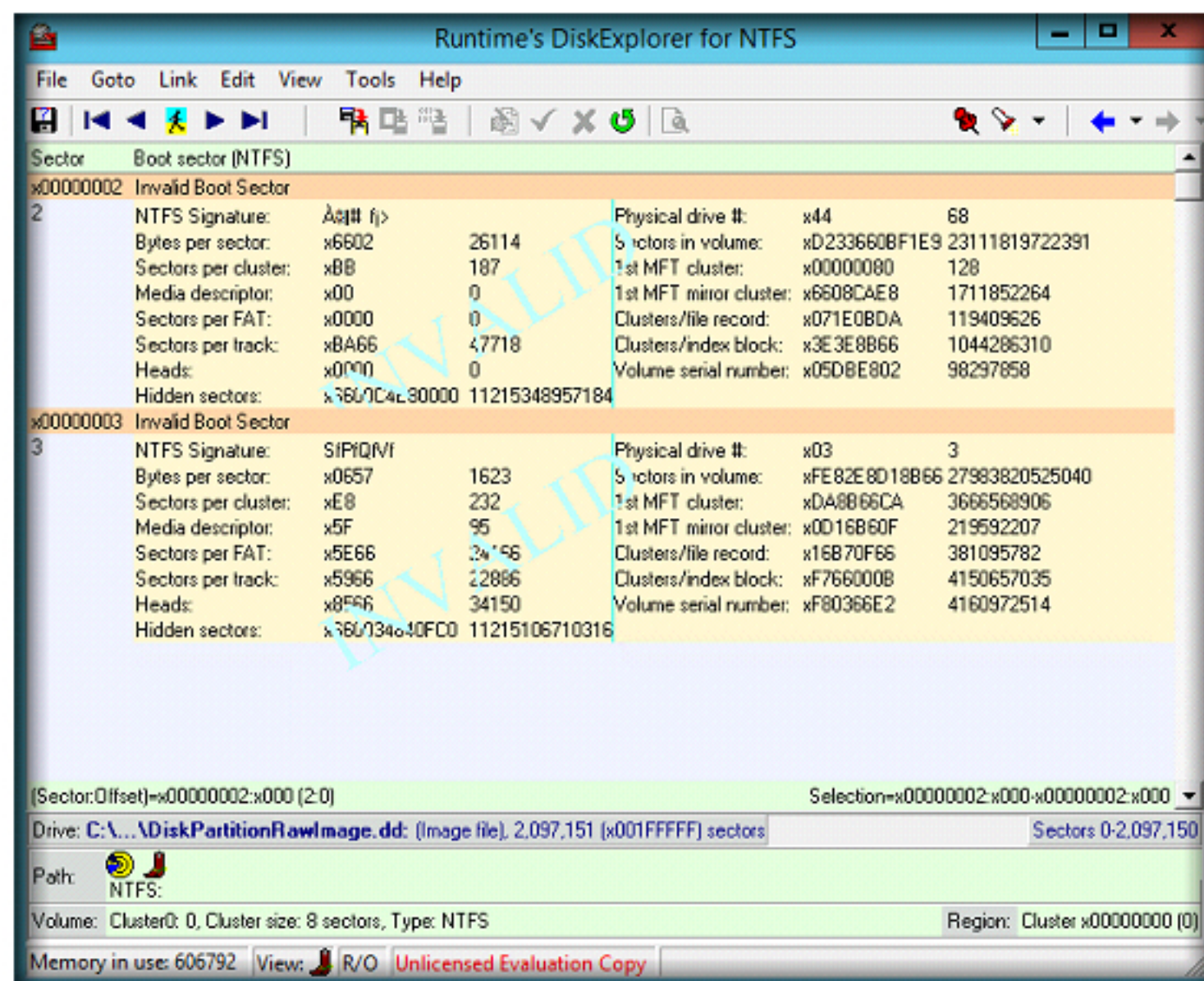


FIGURE 1.8: DiskExplorer for NTFS window

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

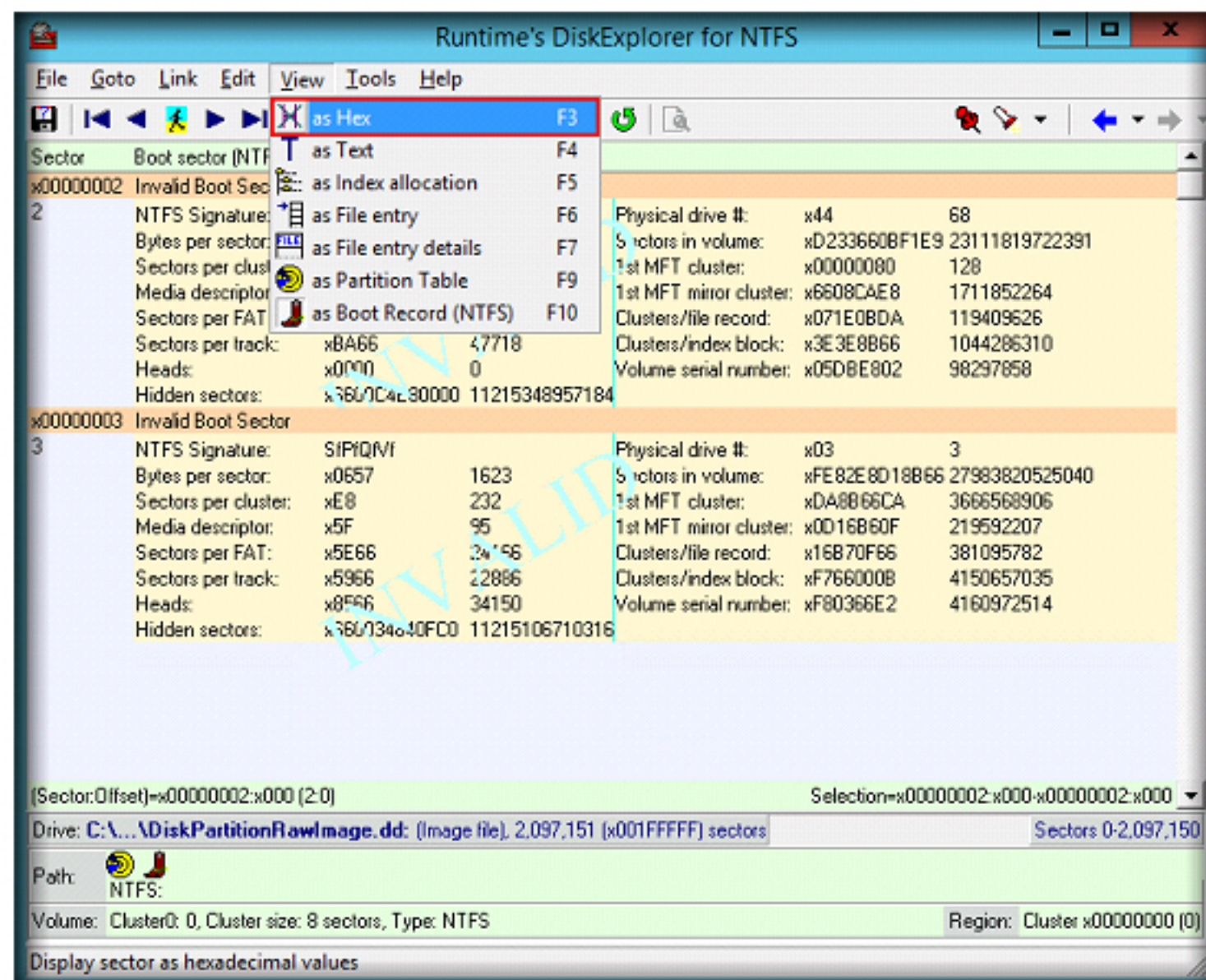


FIGURE 1.9: DiskExplorer for NTFS hex option



TASK 4

Viewing the Hex Values of Selected Sector

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

📖 Navigating with links is the most efficient way of moving through the drive. Depending on the current context, links provide a list of areas where you can jump next.

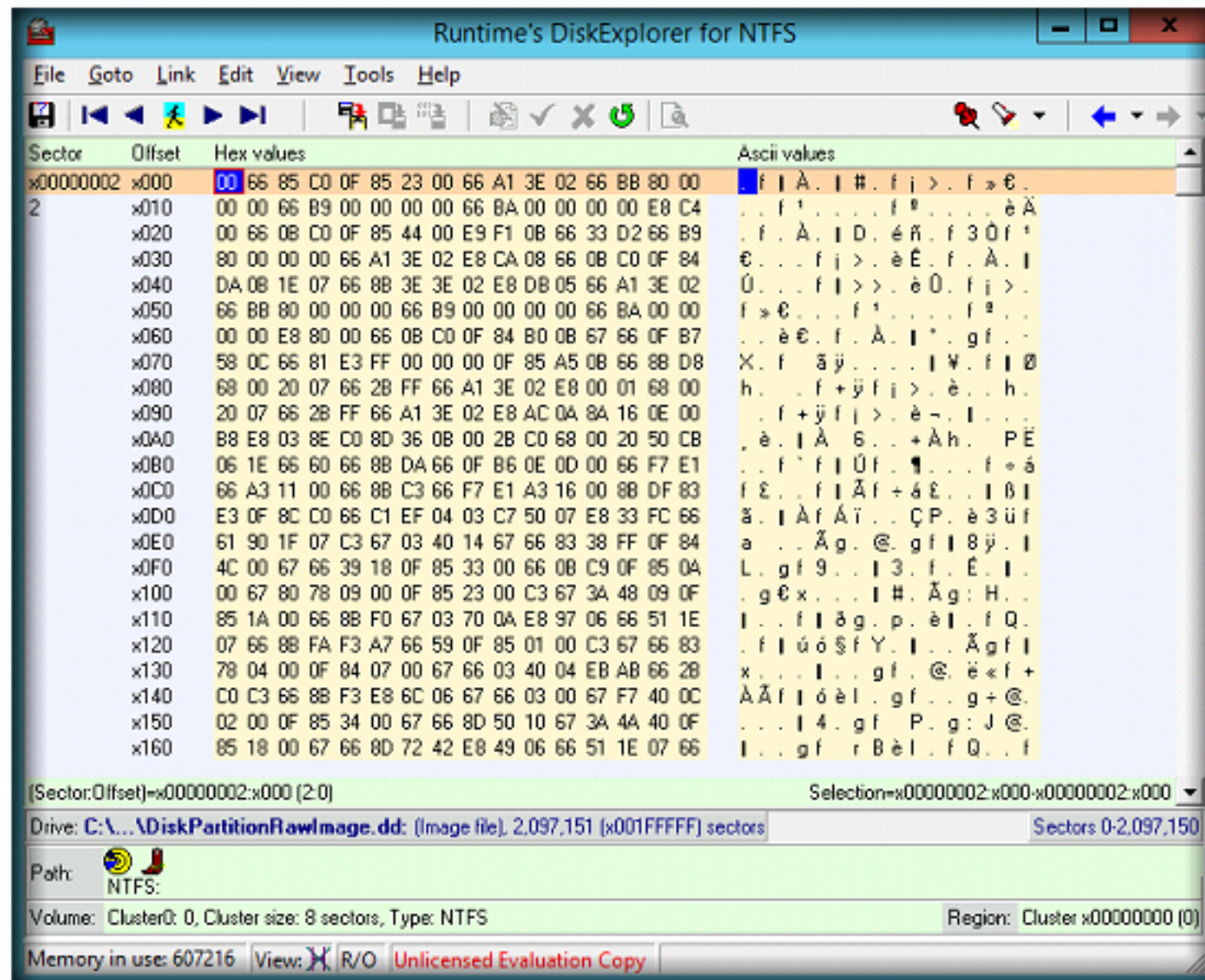


FIGURE 1.10: DiskExplorer for NTFS Hex View of image drive

14. On the menu bar, click **Edit → Select All**.

📁 You can also load an image file or a remote drive by pressing the corresponding buttons at the bottom of the window.

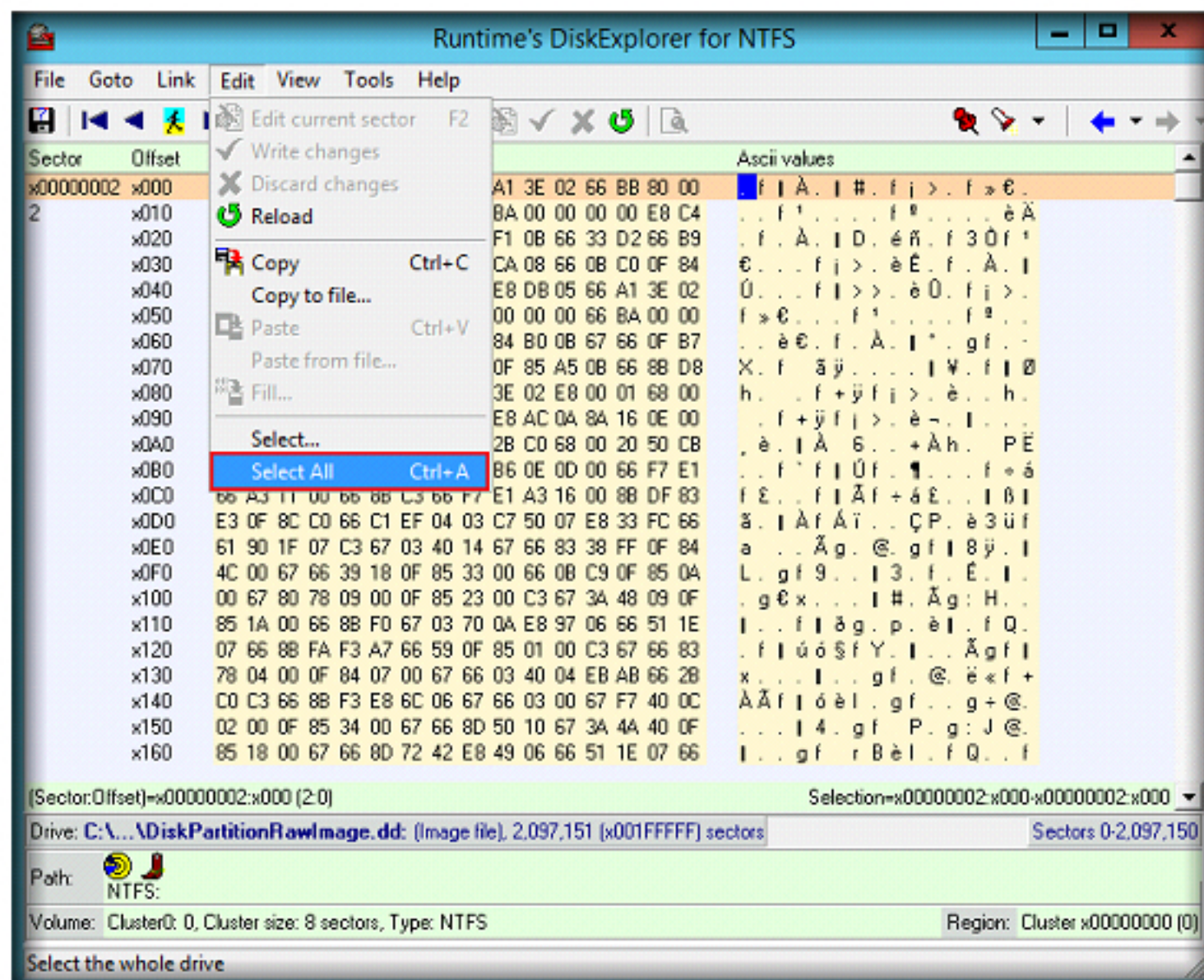


FIGURE 1.11: DiskExplorer for NTFS window. Select All option

15. The entire drive in **Hex** should be highlighted, as shown in the figure:

☞ All available physical drives (HDs and their partitions, floppy drives) and logical drives are listed on the left side of the window.

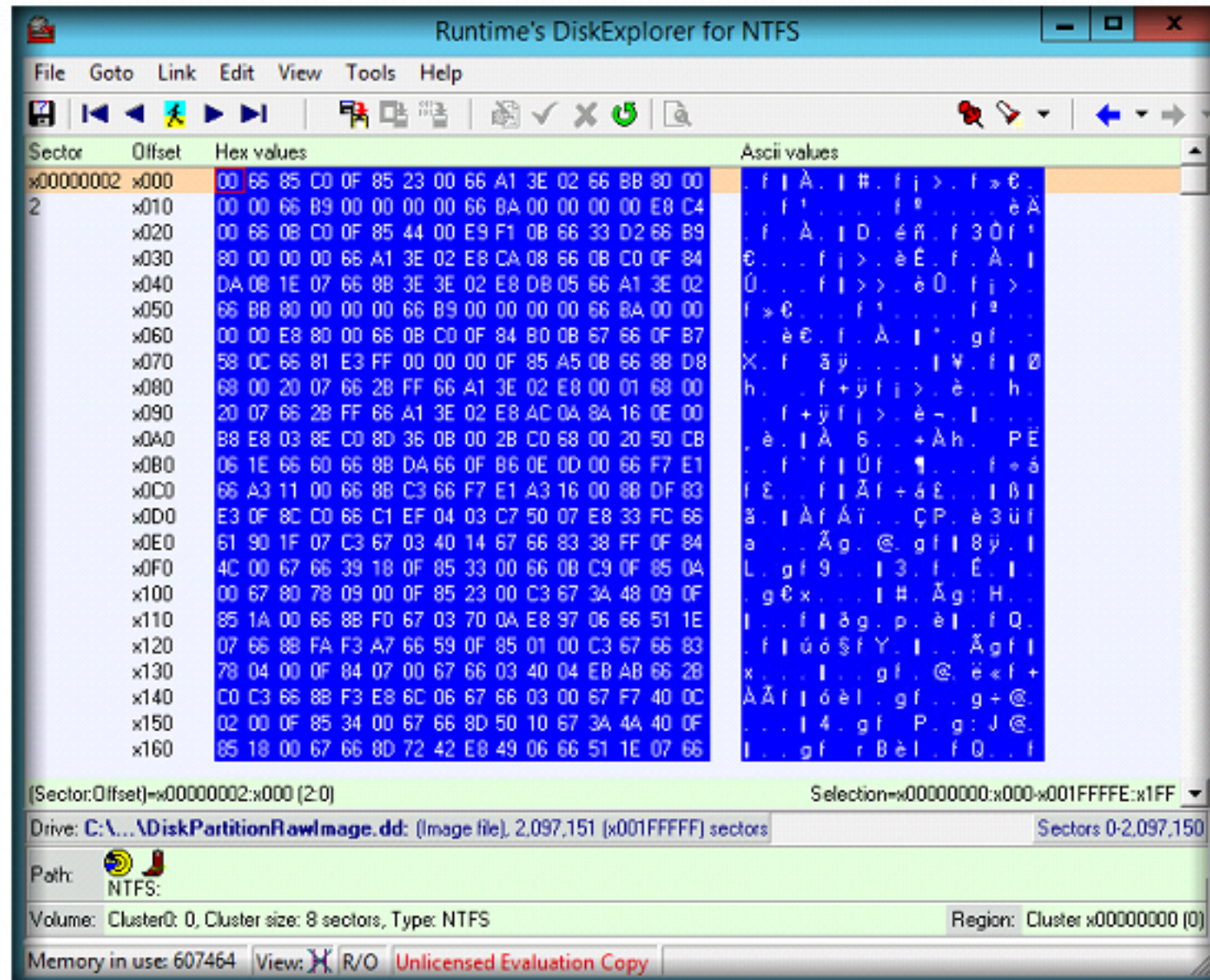


FIGURE 1.12: DiskExplorer for NTFS window



TASK 5

Copying the Files

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

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

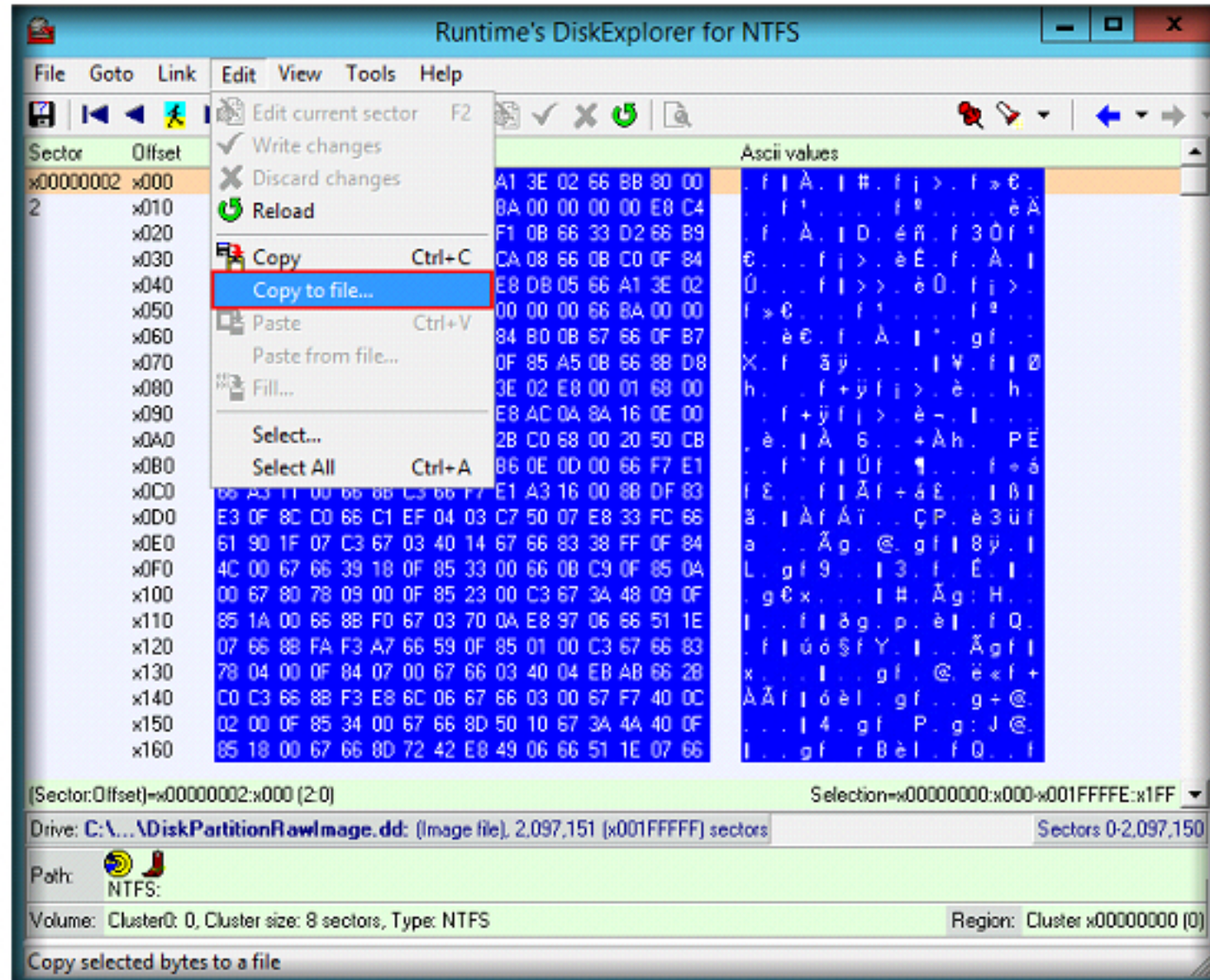


FIGURE 1.13: DiskExplorer for NTFS Copy to file option

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

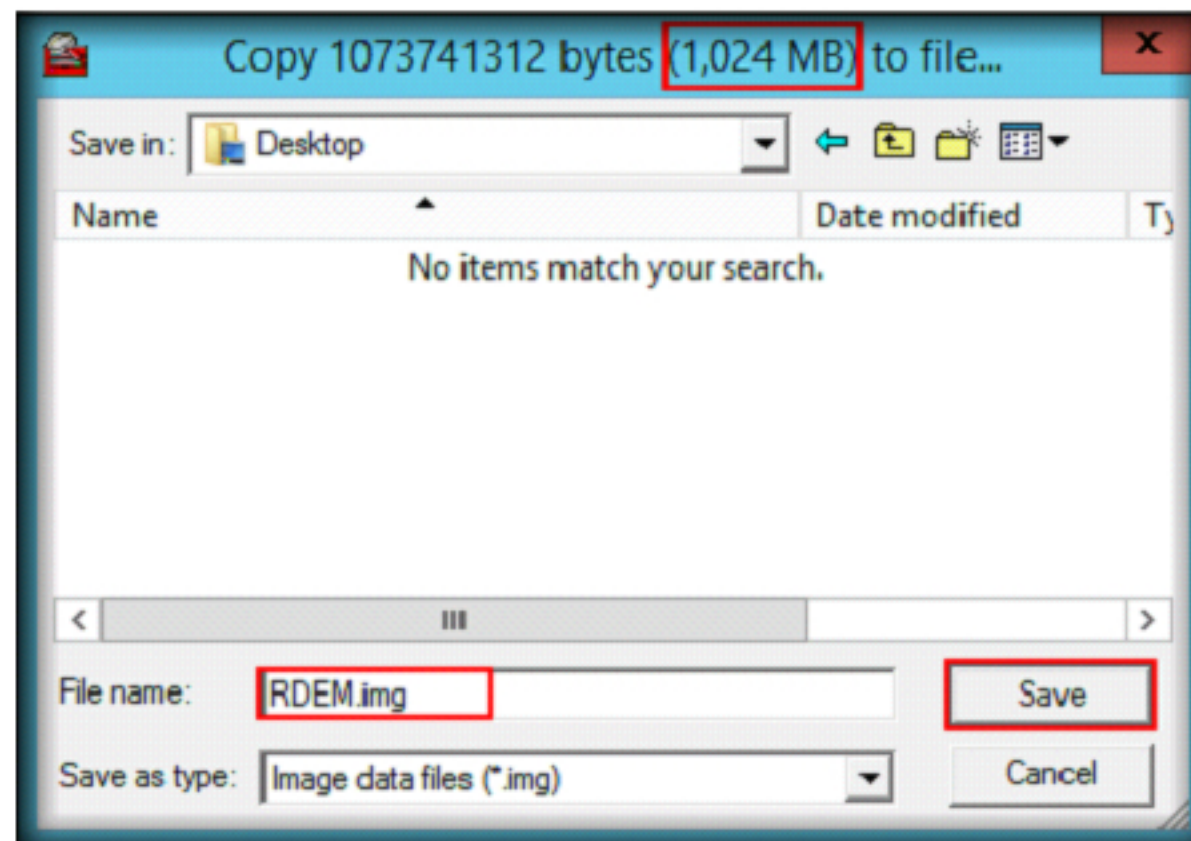


FIGURE 1.14: DiskExplorer for NTFS save option

18. In the **Confirm** pop-up window, click **Yes** to split an image file into several files, as the destination drive might not accept very large files.

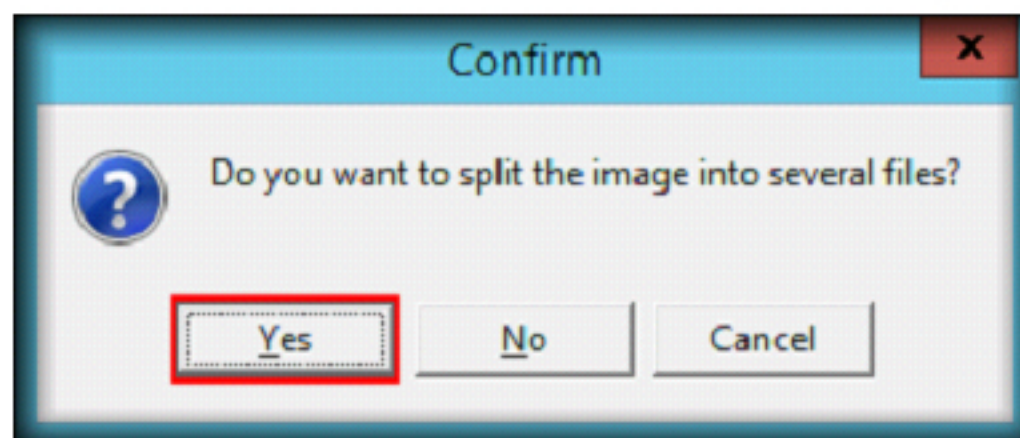


FIGURE 1.15: DiskExplorer for NTFS Confirm

19. This process will start copying the image files.

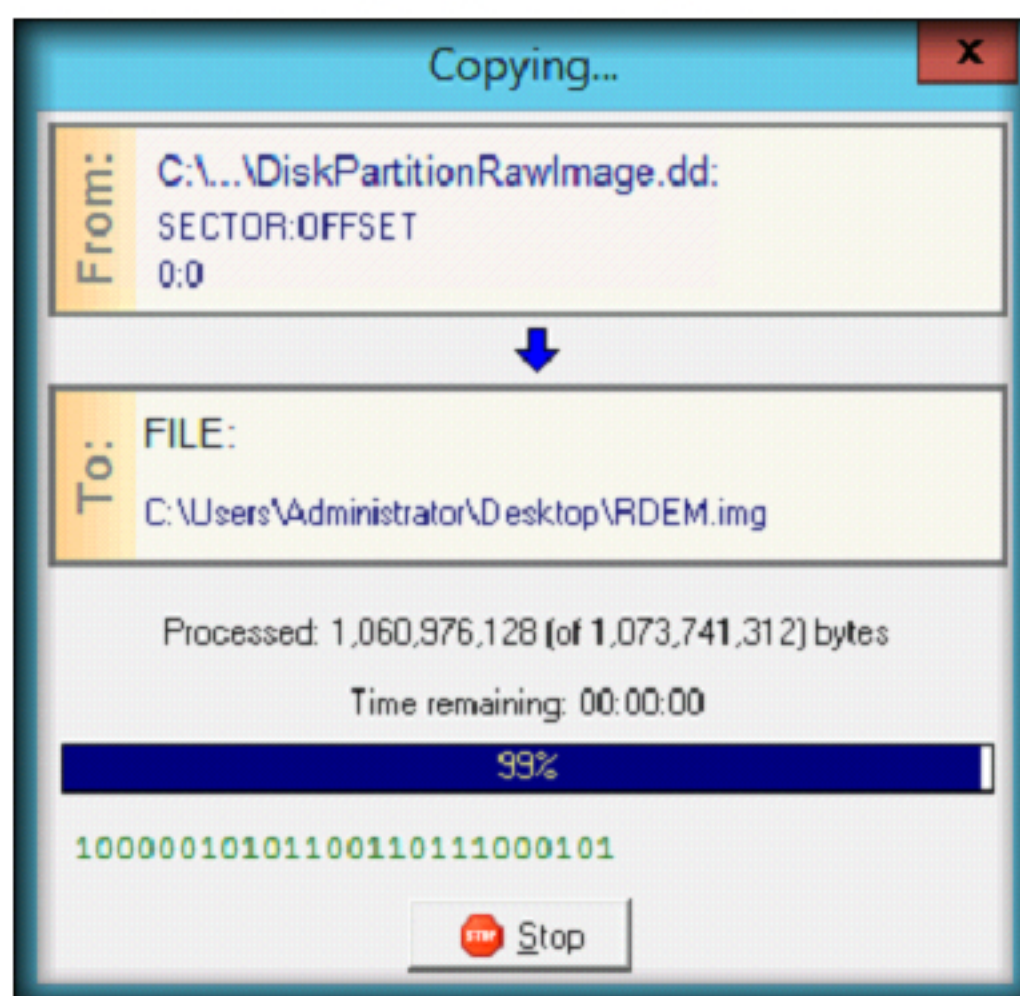


FIGURE 1.16: DiskExplorer for NTFS Copying window

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

Lab Analysis

Analyze and document the results related to the lab exercise.

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

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

Viewing Content of Forensic Image Using Access Data FTK Imager Tool

FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as AccessData®Forensic Toolkit® (FTK) is warranted.

Lab Scenario

As part of investigation in an information theft case, the senior investigator Alex has come to a conclusion of scanning all the systems using the AccessData FTK Imager tool to know if the deleted files on the systems contain any desired information. The tool has not only saved the investigator's time but also saved the hectic process of recovering every deleted file from the system.

To be an expert **forensic investigator**, you must understand how to analyze file systems and collect the data from those file systems.

Lab Objectives

All the system related data remains saved in the system hard disk. When an incident occurs, there is a probability that the system is shutdown and switching it on would make changes in the evidence present on it. Even if the system is on, the investigators should not use forensics techniques on it directly, as it may tamper the evidence and render it useless during the trial. Therefore, an investigator should always create a duplicate of the storage and this lab will help you to create an image of the file you need to investigate.

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Environment

 **Tools** demonstrated in this lab are available in **C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication**

To carry out the lab, you need:

- AccessData FTK Imager, located at **C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\AccessData FTK Imager**.
- You can also download the latest version of **AccessData FTK Imager** from the link <http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.4.2>.
- Kindly note that, if you decide to download the latest version, screenshots shown in the lab might differ.
- A computer running **Windows Server 2012**.
- Administrative privileges to run tools.

Lab Duration

Time: 15 Minutes

Overview of AccessData FTK Imager

AccessData FTK Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool is necessary or not. It can also create perfect copies (forensic images) of computer data without making changes to the original evidence.

Lab Tasks



TASK 1

Selecting the Forensics Image

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 04 Data Acquisition and Duplication\Data Acquisition Tools\Accessdata FTK Imager**.
2. Double-click **AccessData_FTK_Imager_3.4.2.exe** to launch the setup, and follow the wizard-driven installation instructions.
3. The system will launch AccessData FTK Imager automatically after installation. The **AccessData FTK Imager** main window appears.

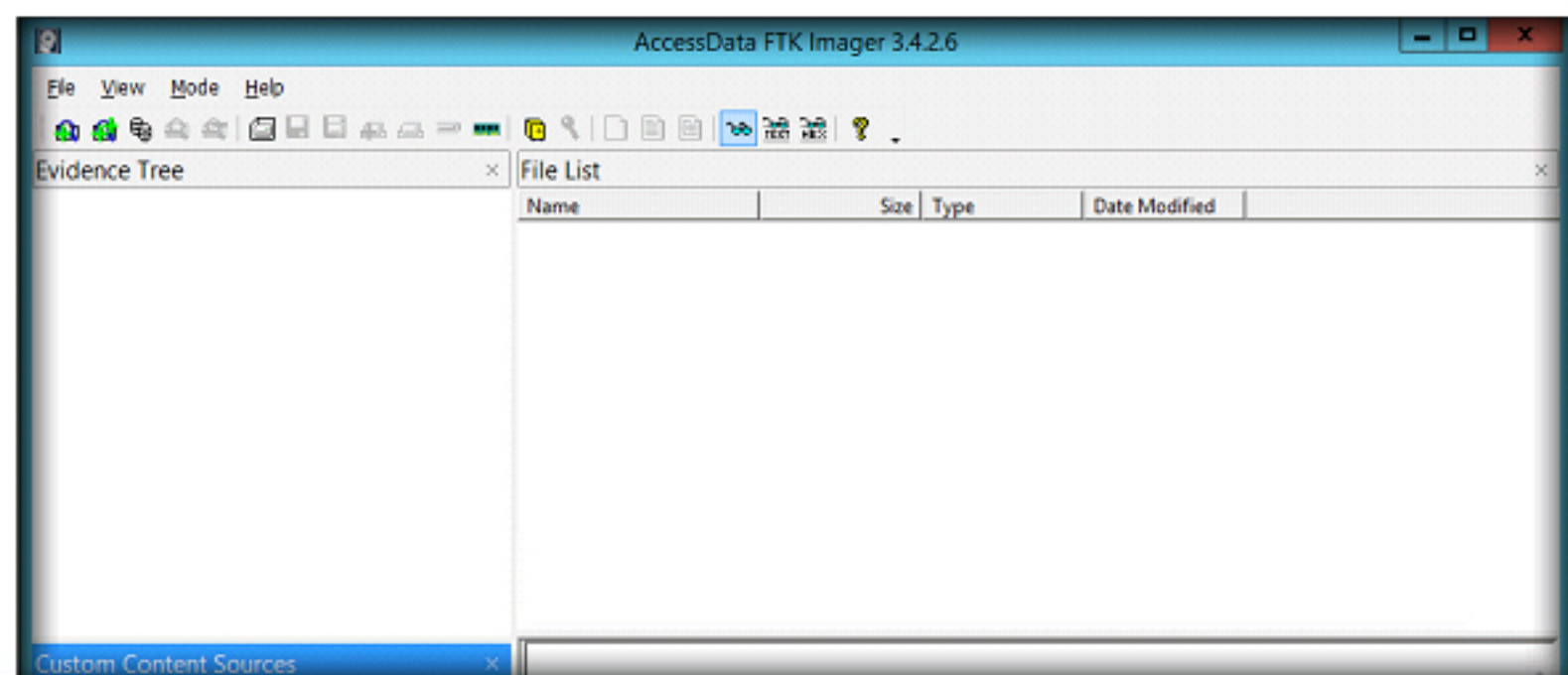


FIGURE 2.1: AccessData FTK Imager

4. Click **File** → **Add Evidence Item** to add evidence, or click the **Add Evidence Item** button on the toolbar.

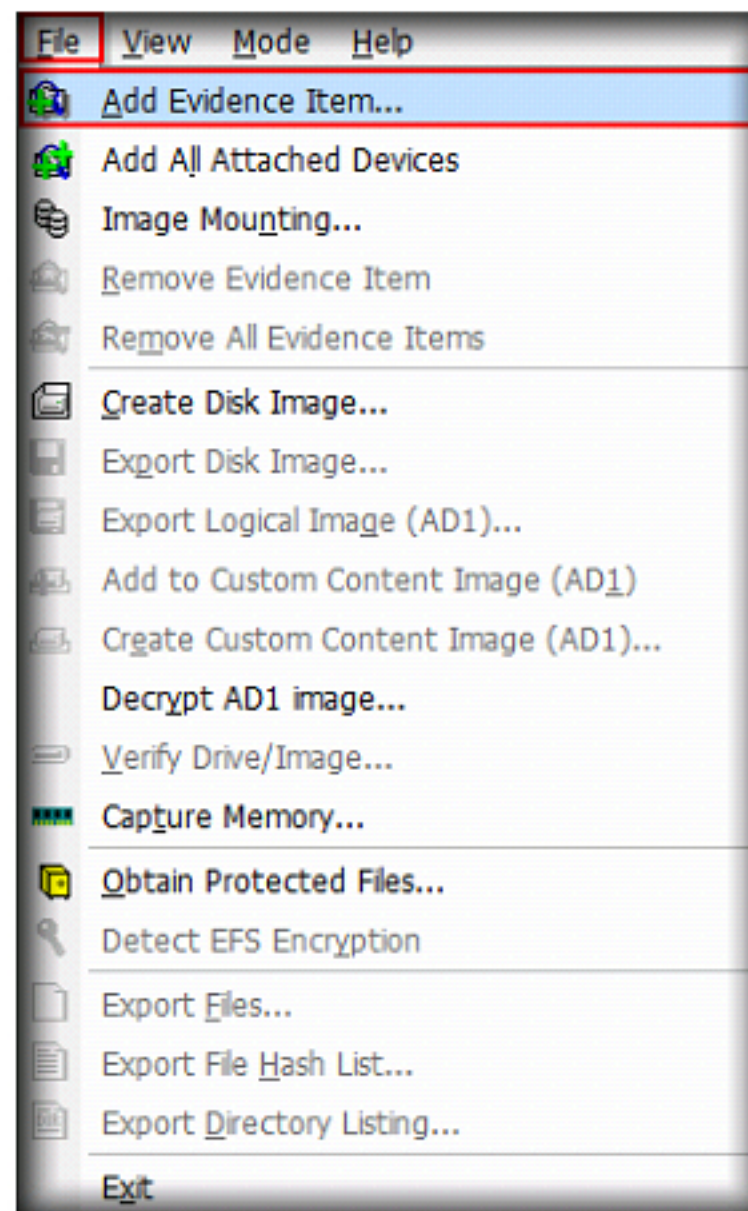


FIGURE 2.2: AccessData FTK Imager file menu

5. Select the **Image File** option from the **Select Source** wizard and then click **Next**.

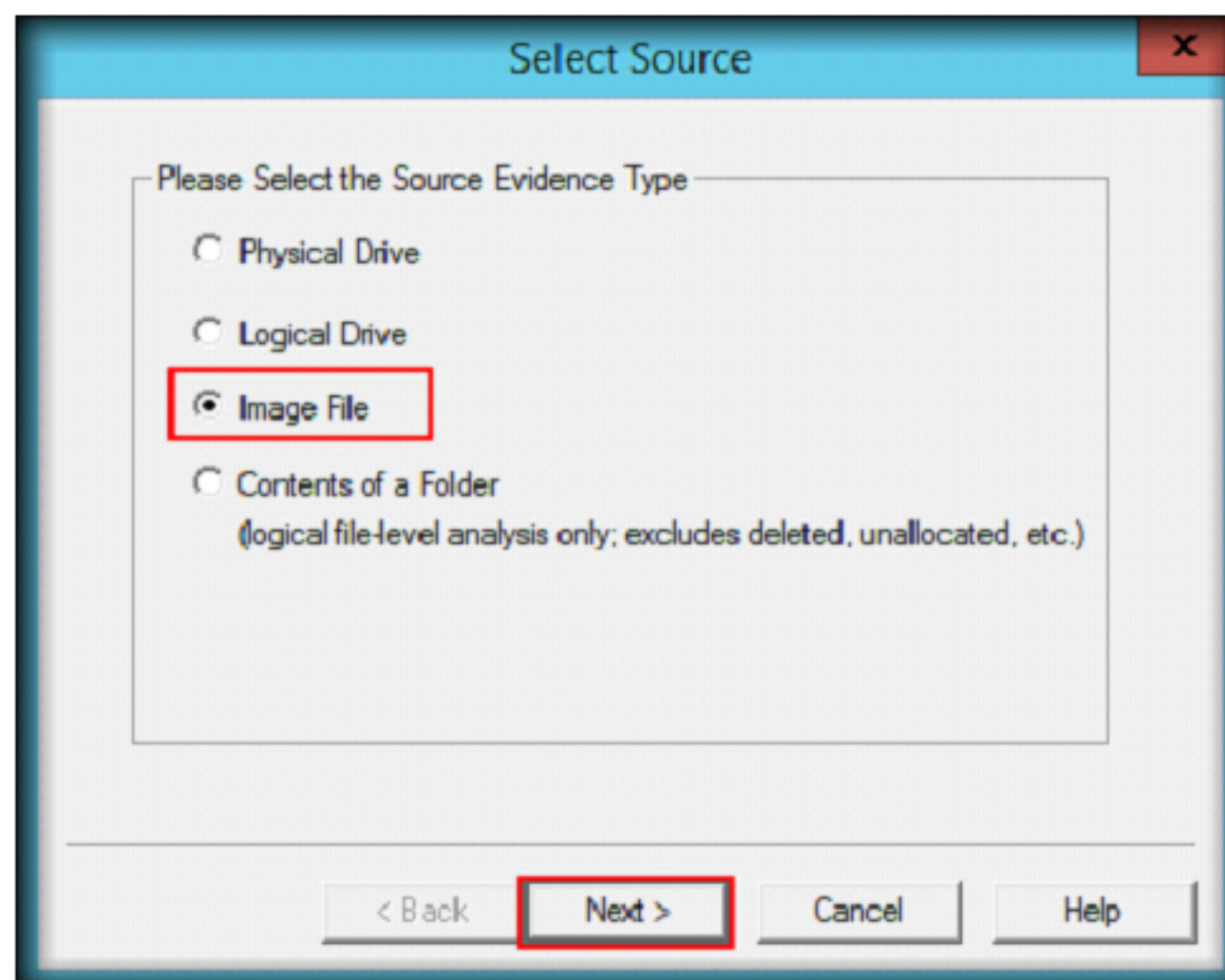


FIGURE 2.3: AccessData FTK Imager selecting source

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

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

6. Click the **Browse** button to specify the image file path (**C:\CHFI-Tools\Evidence Files\Disk Partition Raw Image\DiskPartitionRawImage.dd**) and then click **Finish**.

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.

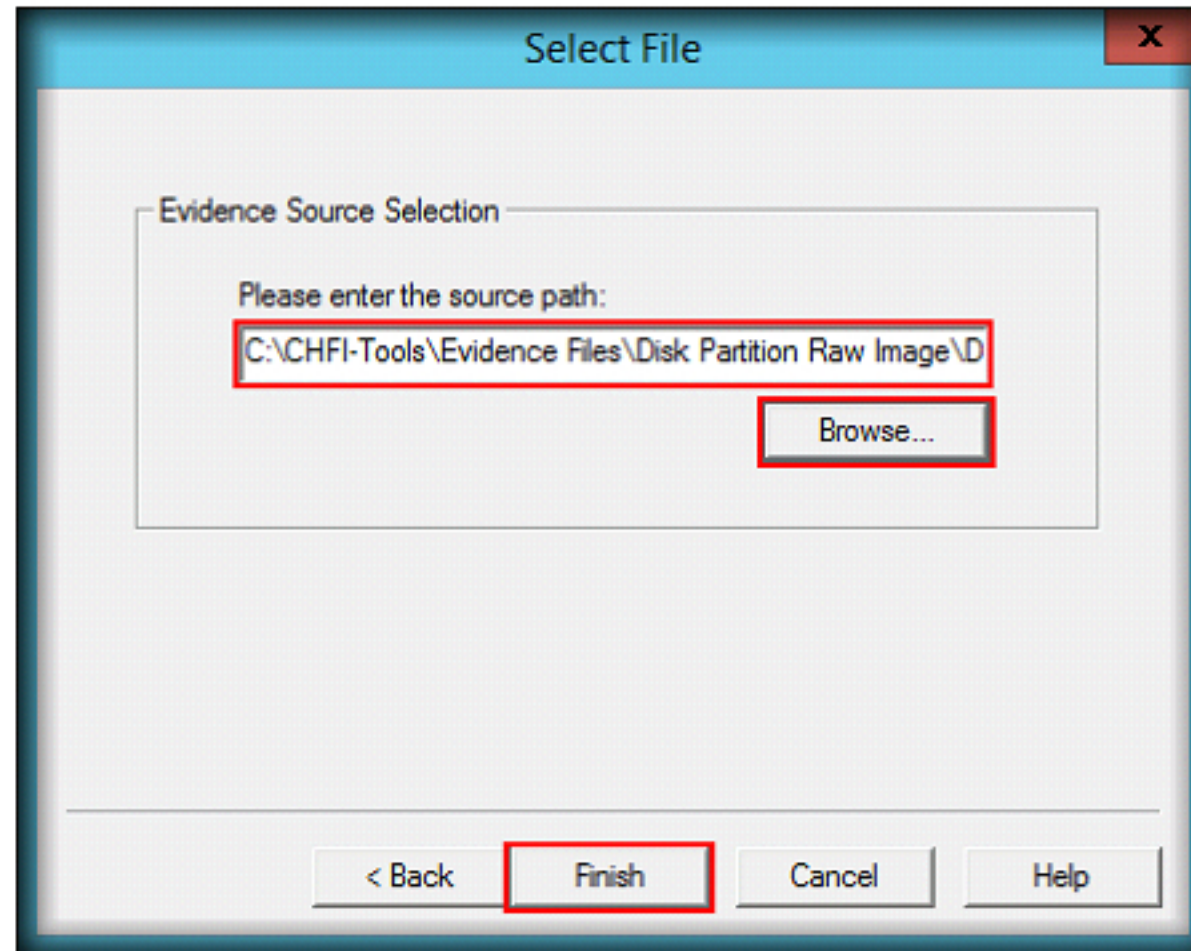


FIGURE 2.4: AccessData FTK Imager giving path of image file

7. The evidence appears in a tree, as shown in the following screenshot:

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

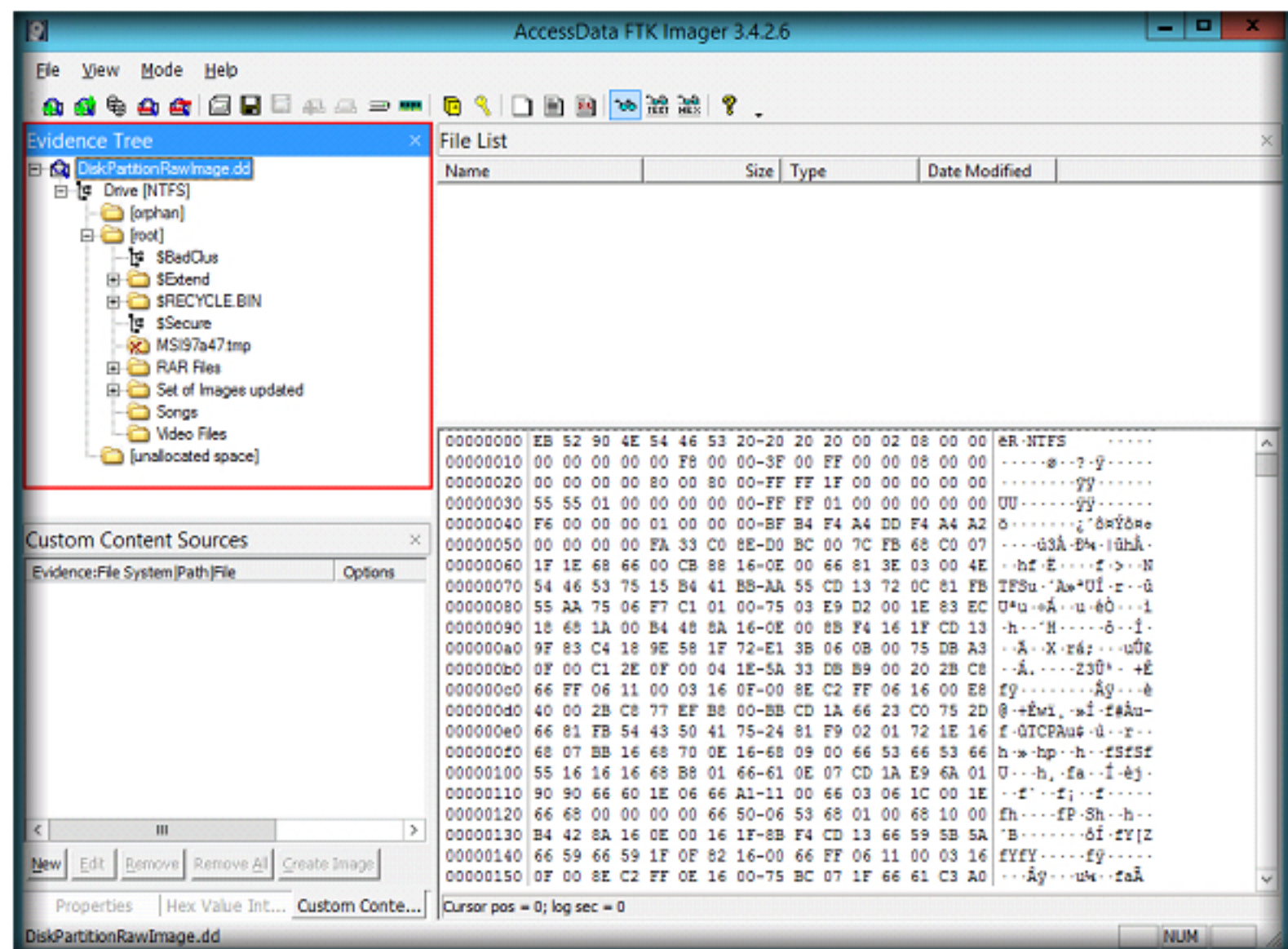


FIGURE 2.5: AccessData FTK Imager giving Evidence Tree

TASK 2

Viewing the Content of a Forensics Image

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).

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

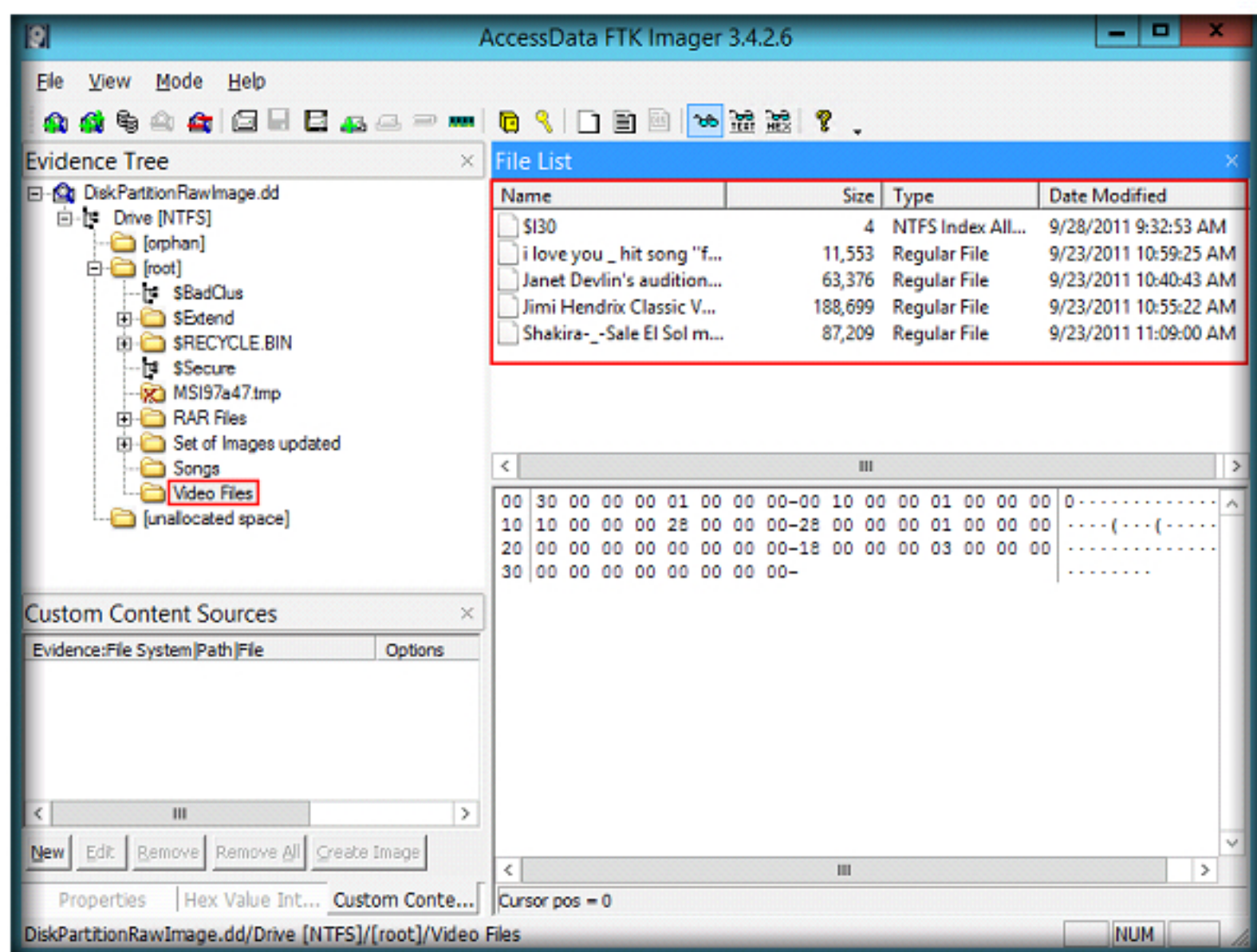


FIGURE 2.6: AccessData FTK Imager File List

9. To view the **Hex** value of that particular file, select the file from the **File List** and click the **Hex** icon on the toolbar.
10. Hex values of the selected file will be displayed in the **bottom-right** pane.

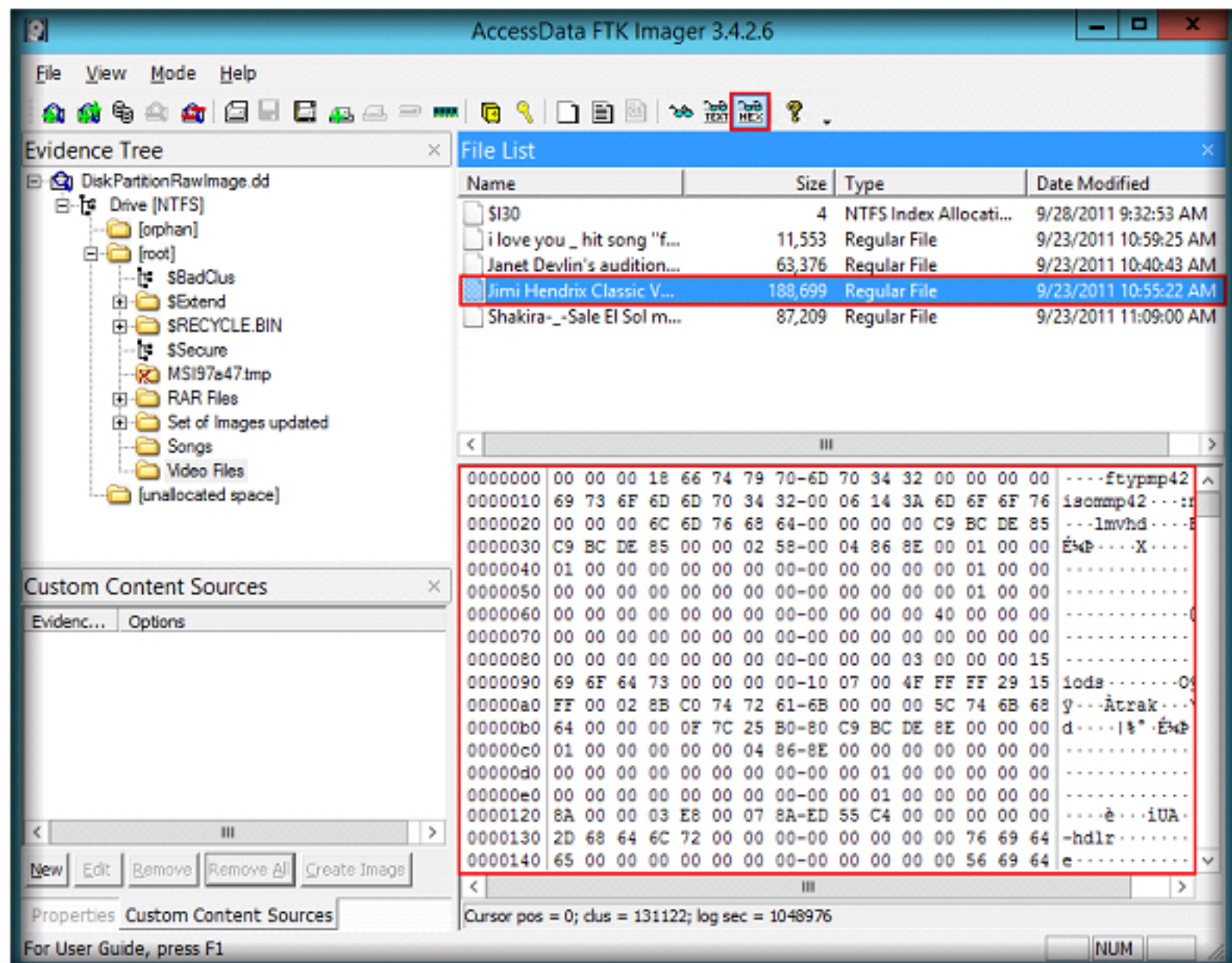


FIGURE 2.7: AccessData FTK Imager Hex view

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

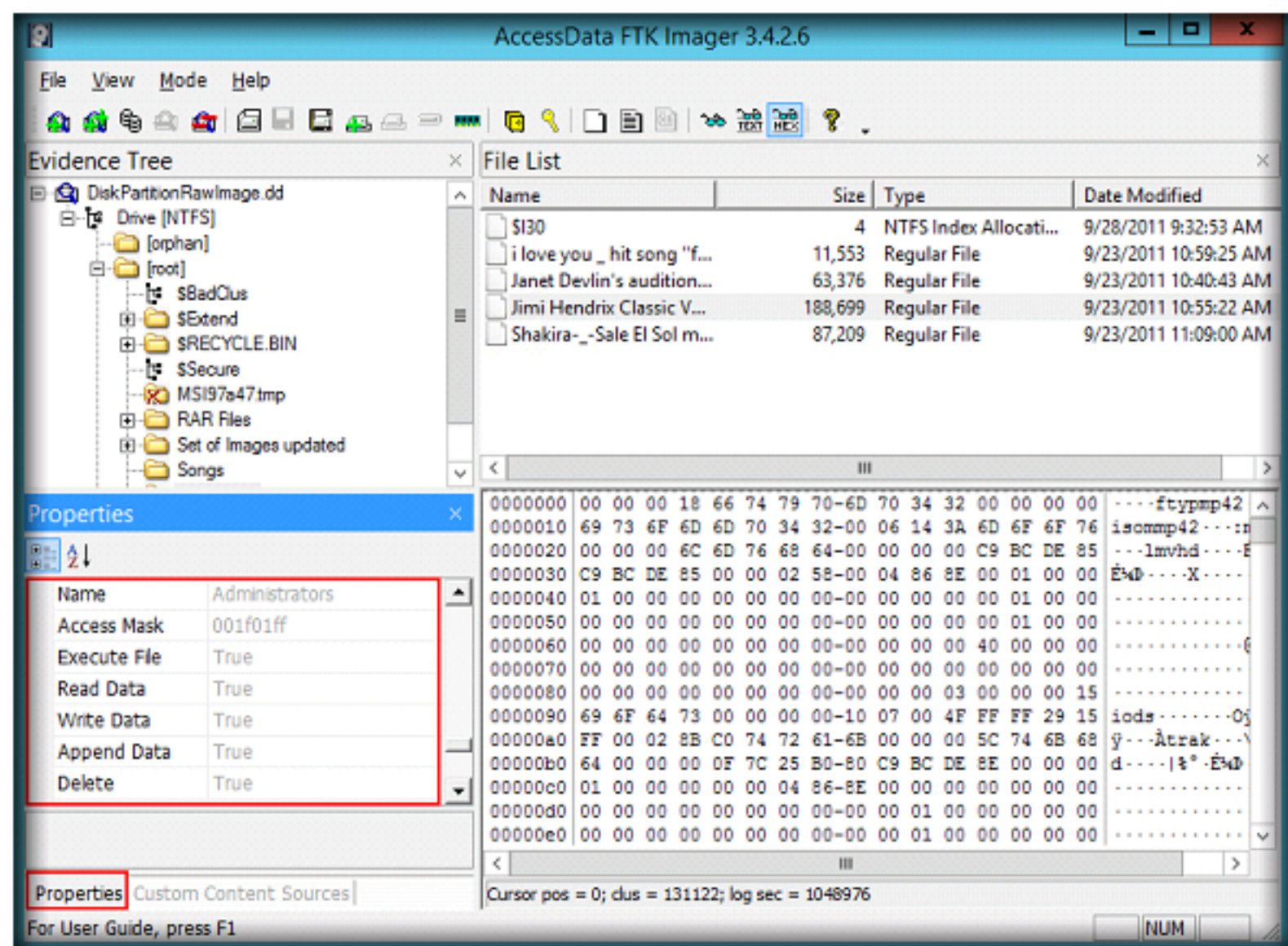


FIGURE 2.8: AccessData FTK Imager Properties window

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

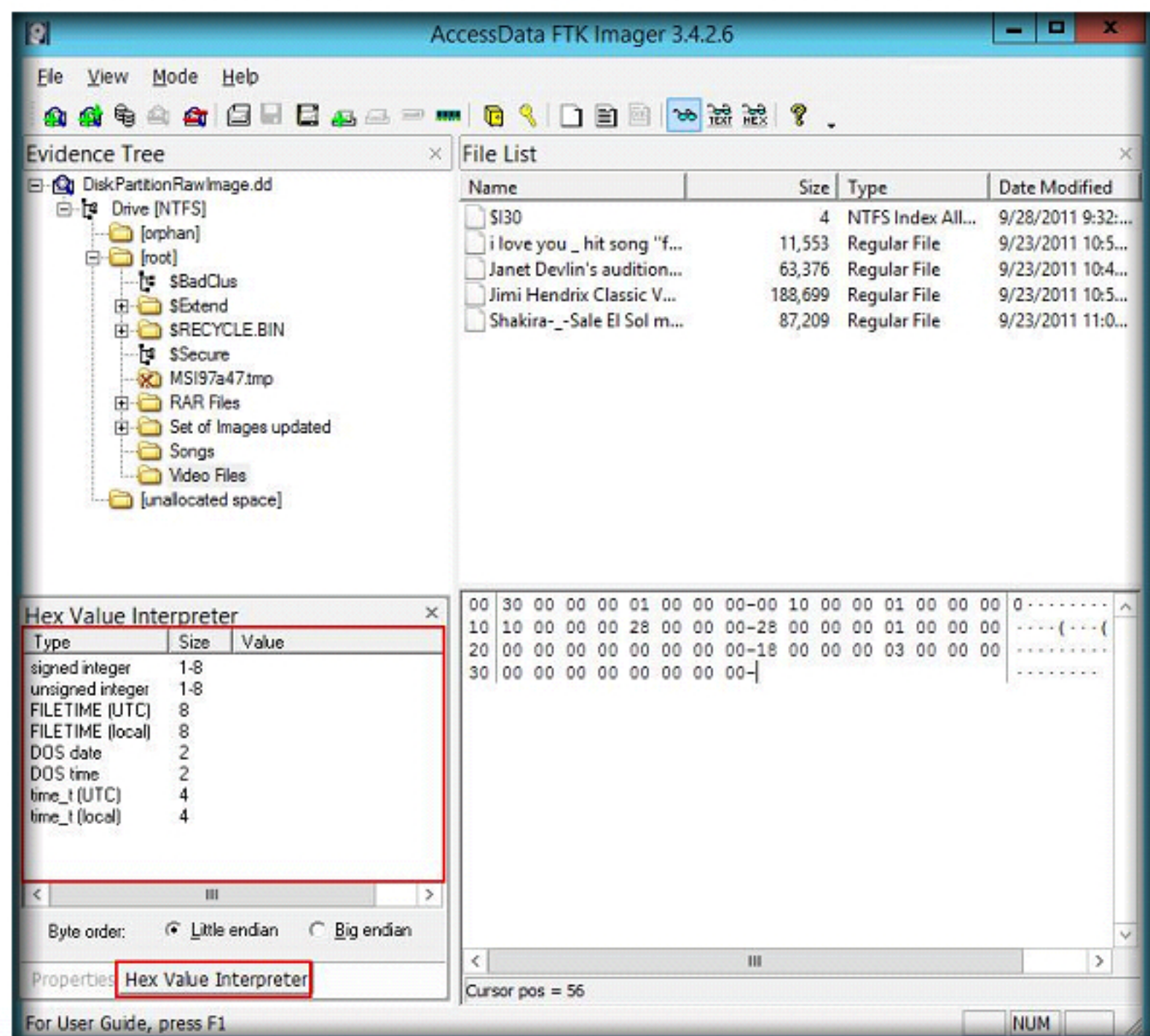


FIGURE 2.9: AccessData FTK Imager Hex Value Interpreter window

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