Assignment 3: CHFIv9 Labs Module 04 Data Acquisition and Duplication

Karthikeyan G
Roll Number: CB.SC.P2CYS24008

January 5, 2025

Lab 1: Investigating NTFS Drive Using DiskExplorer for NTFS

DiskExplorer for NTFS is a powerful disk editor that enables you to investigate NTFS drives and conduct data recovery effectively.

Lab Scenario

NTFS has become the default storage format for various devices due to its robust features such as compression and encryption. These features can also be exploited to hide data, making NTFS a critical focus for forensic investigations.

To excel as a forensic investigator, it is essential to master the process of acquiring files from storage devices, analyzing file systems, and extracting relevant data for evidence collection.

Screenshots and Procedure

Below are the steps and corresponding screenshots that document the process of investigating an NTFS drive using DiskExplorer for NTFS.

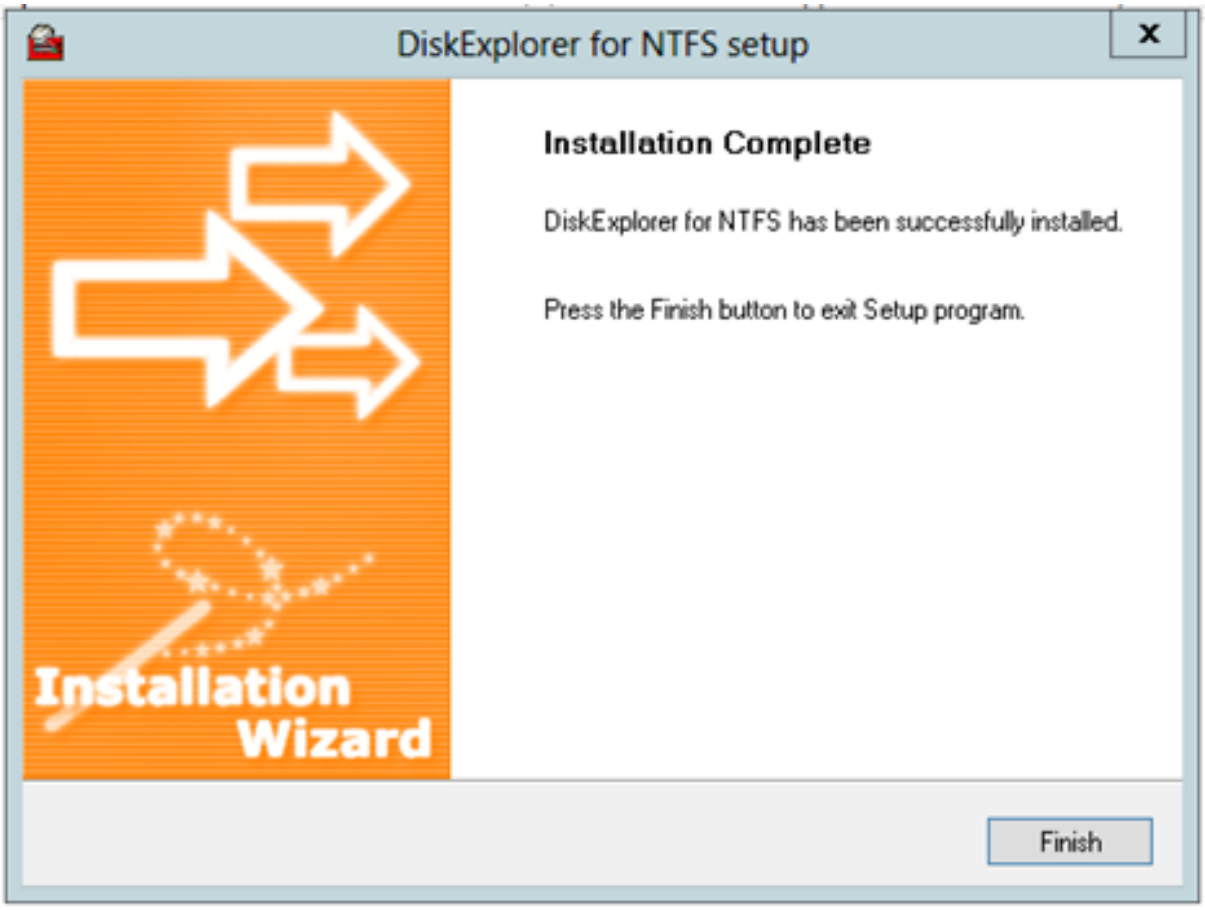

Figure 1: Installation of DiskExplorer for NTFS completed successfully. This tool is essential for analyzing NTFS drives and retrieving critical data.

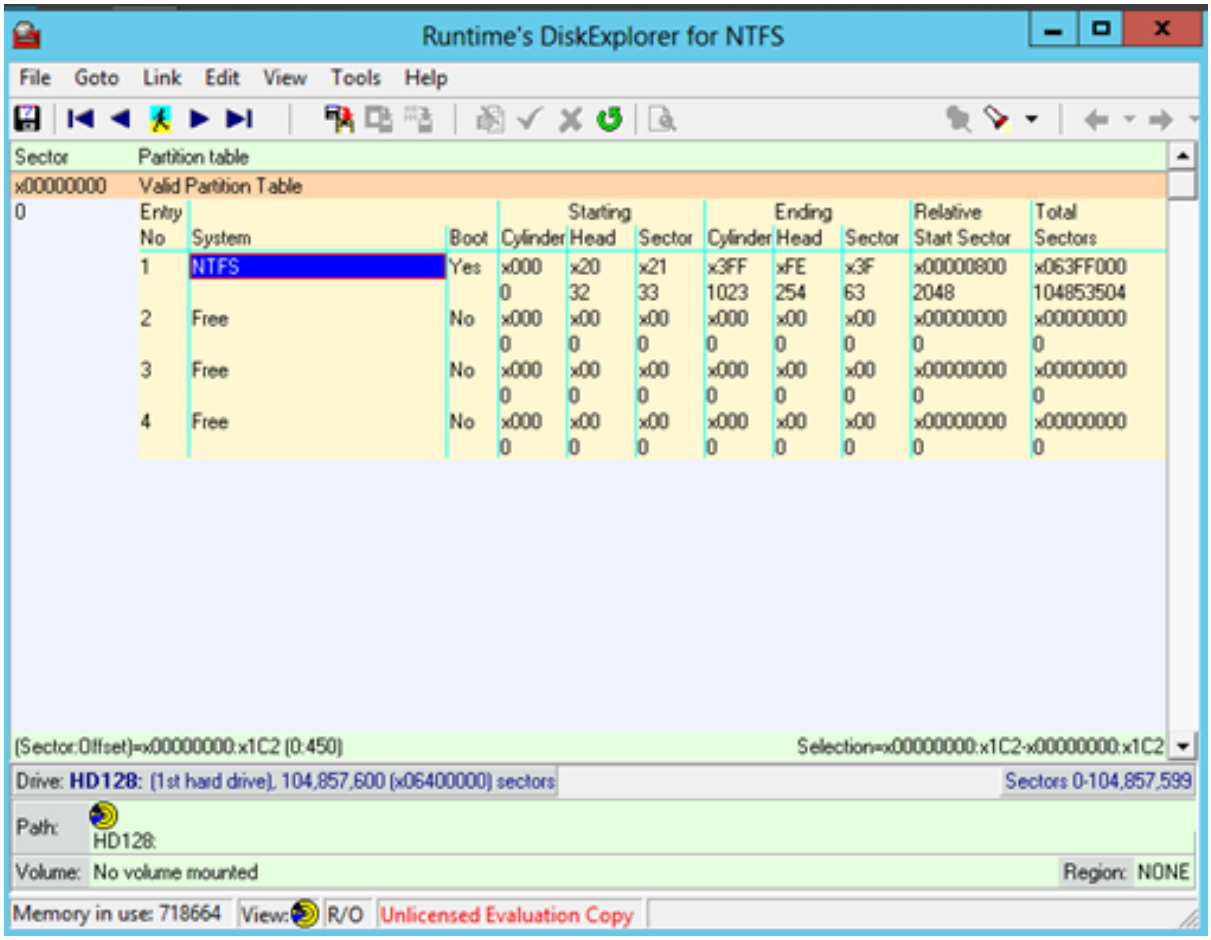

Figure 2: Launching the DiskExplorer for NTFS tool. The user interface provides options for accessing and analyzing NTFS drives.

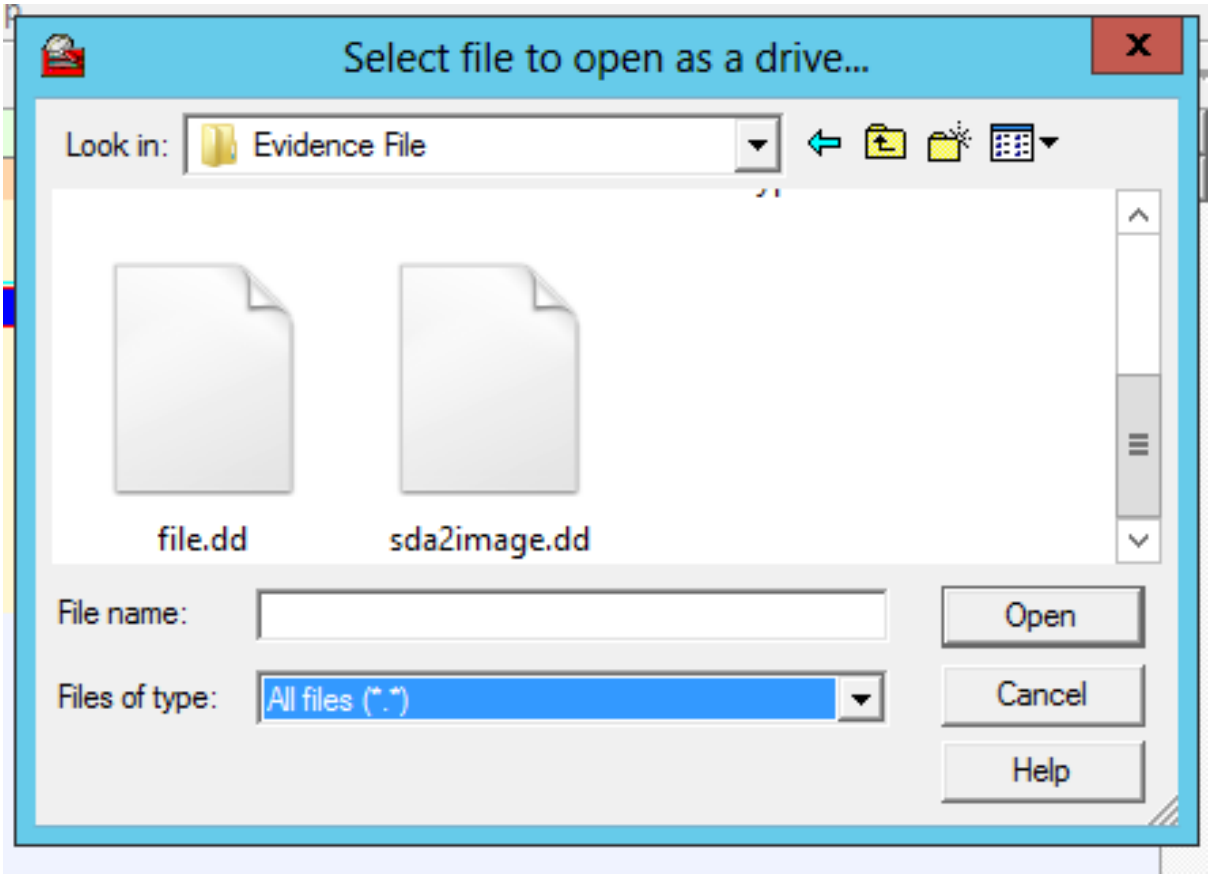

Figure 3: The evidence file folder containing the target NTFS image files for investigation.

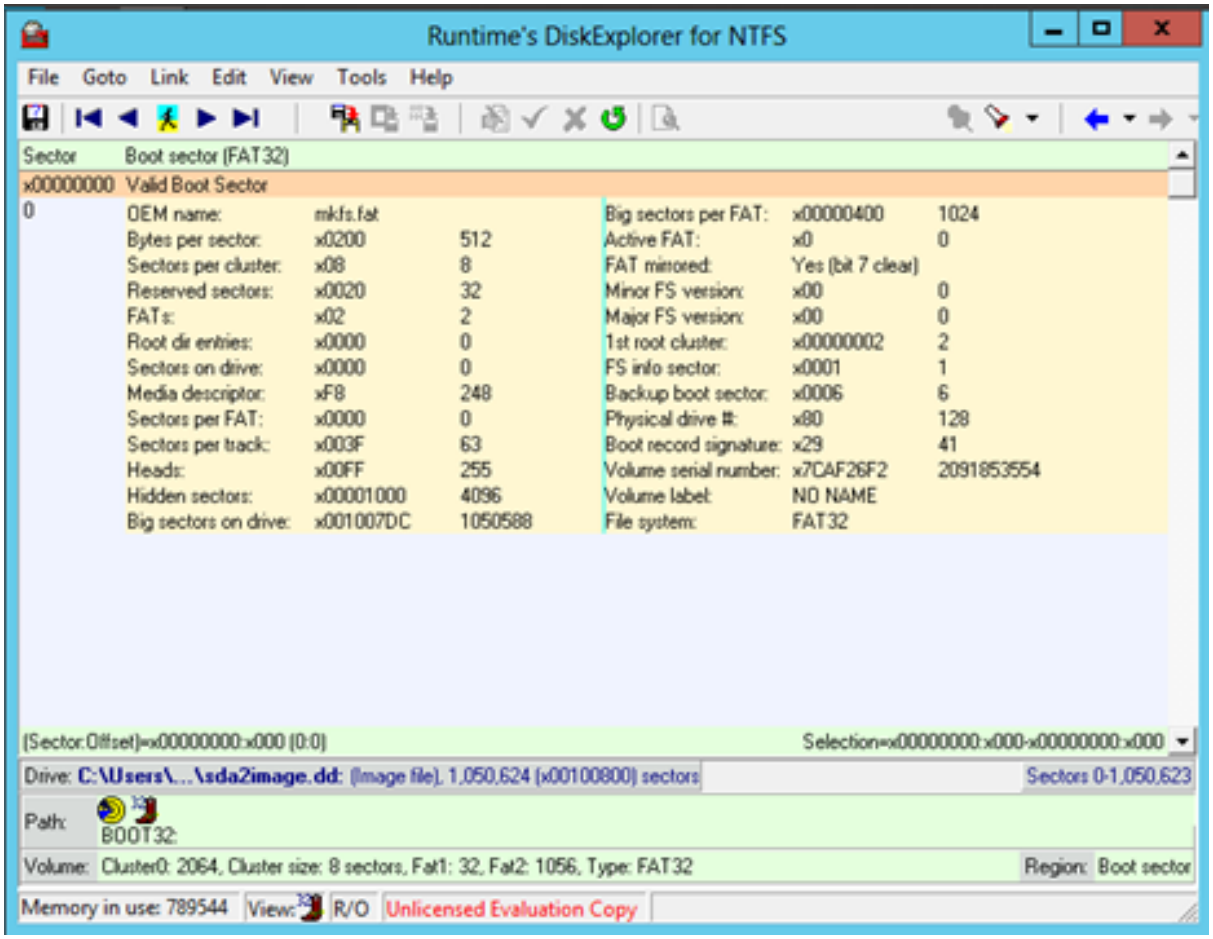

Figure 4: Selection of the file `SDA2image.dd`. This file represents a disk image created for forensic analysis.

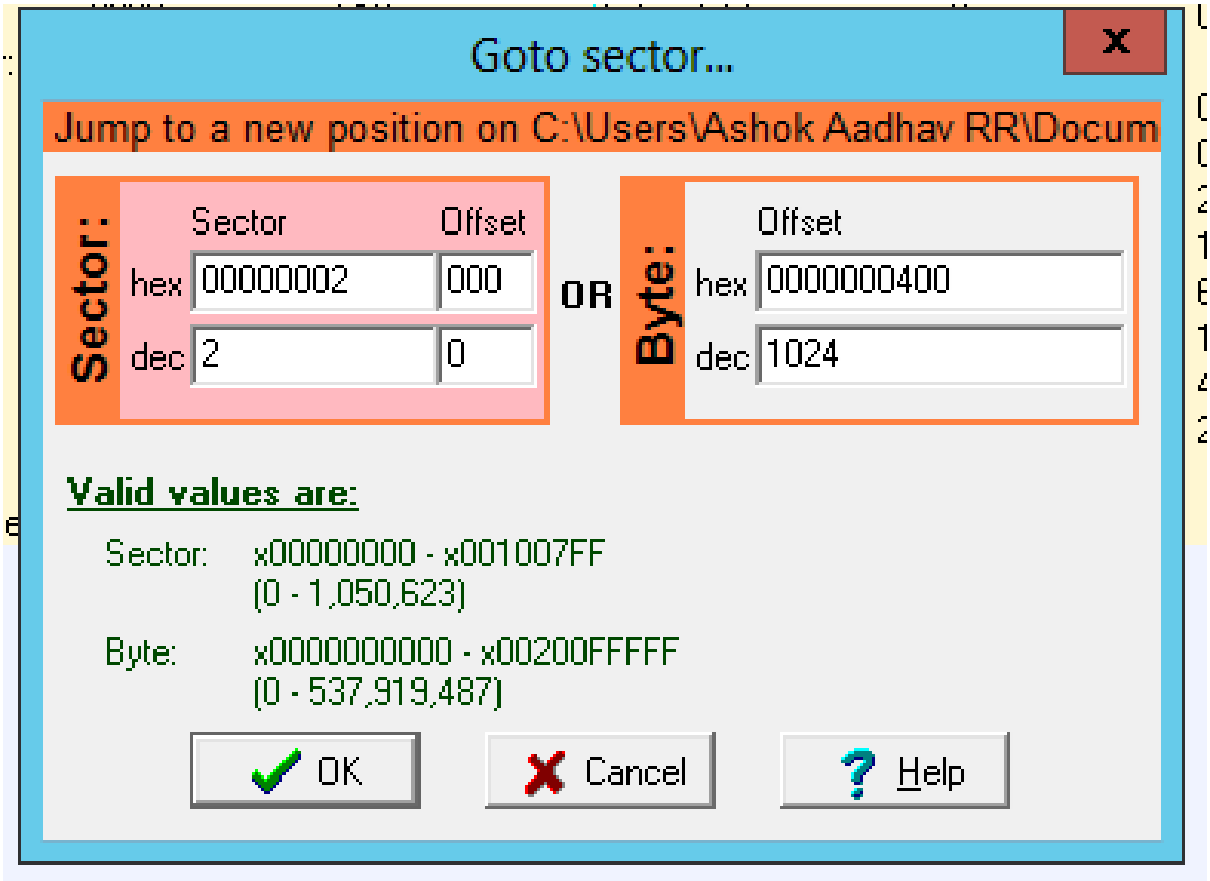

Figure 5: Details of the selected image file displayed. The tool identifies and validates the boot sector information of the disk image.

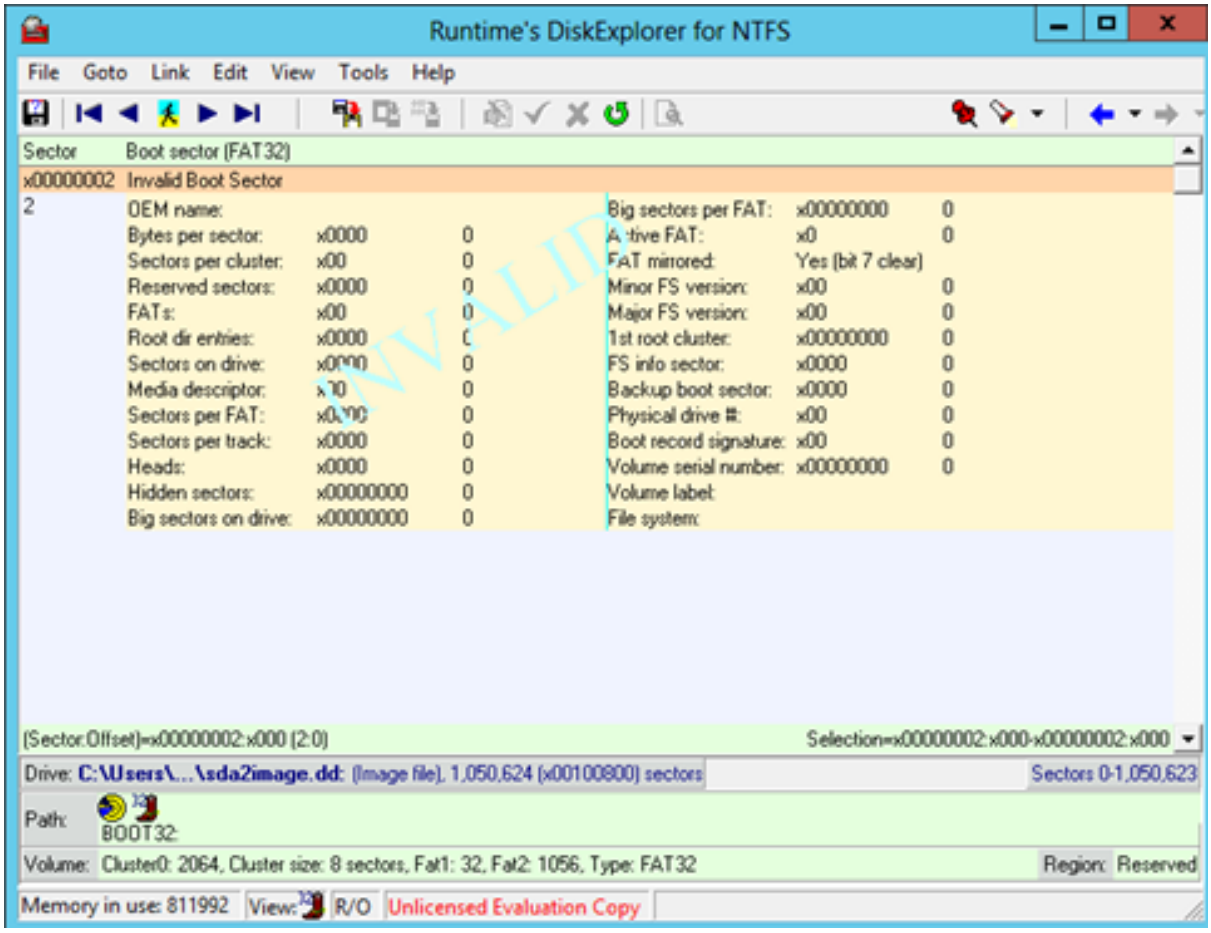

Figure 6: The entered sector displays detailed information, allowing a forensic investigator to analyze specific areas of the disk.

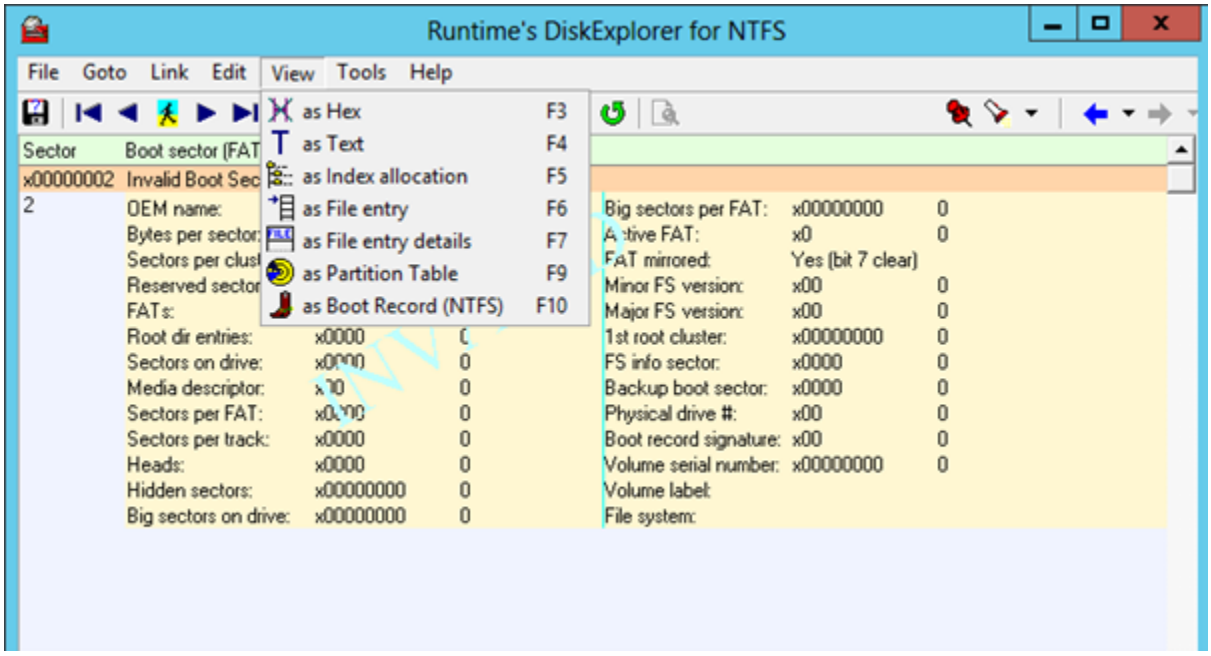

Figure 7: Switching to HEX view using `VIEW -> HEX` to examine raw data. Hexadecimal representation provides a deeper understanding of the file structure.

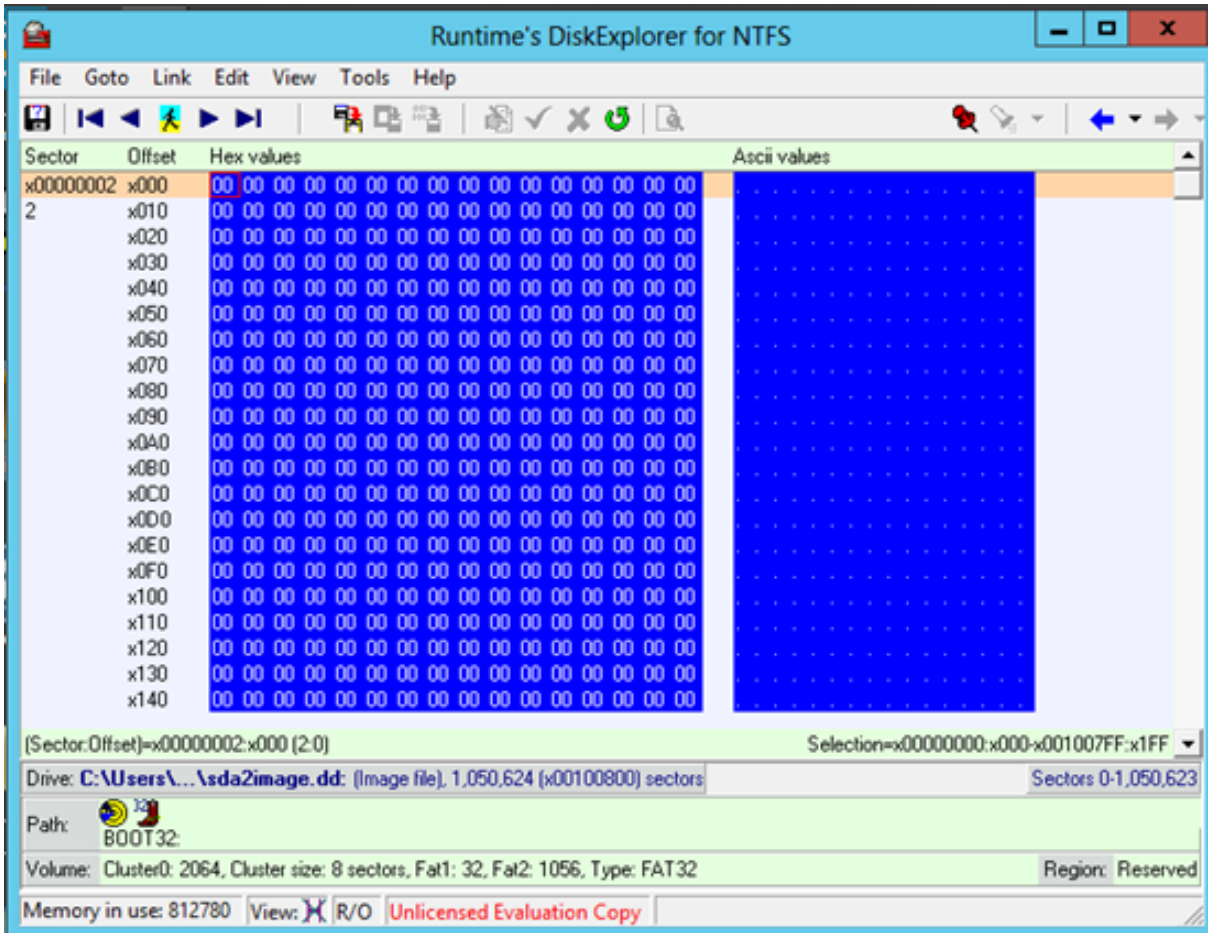

Figure 8: Using `EDIT -> SELECT ALL`, the entire drive's contents are highlighted in HEX format. This data can be copied for further processing and analysis.

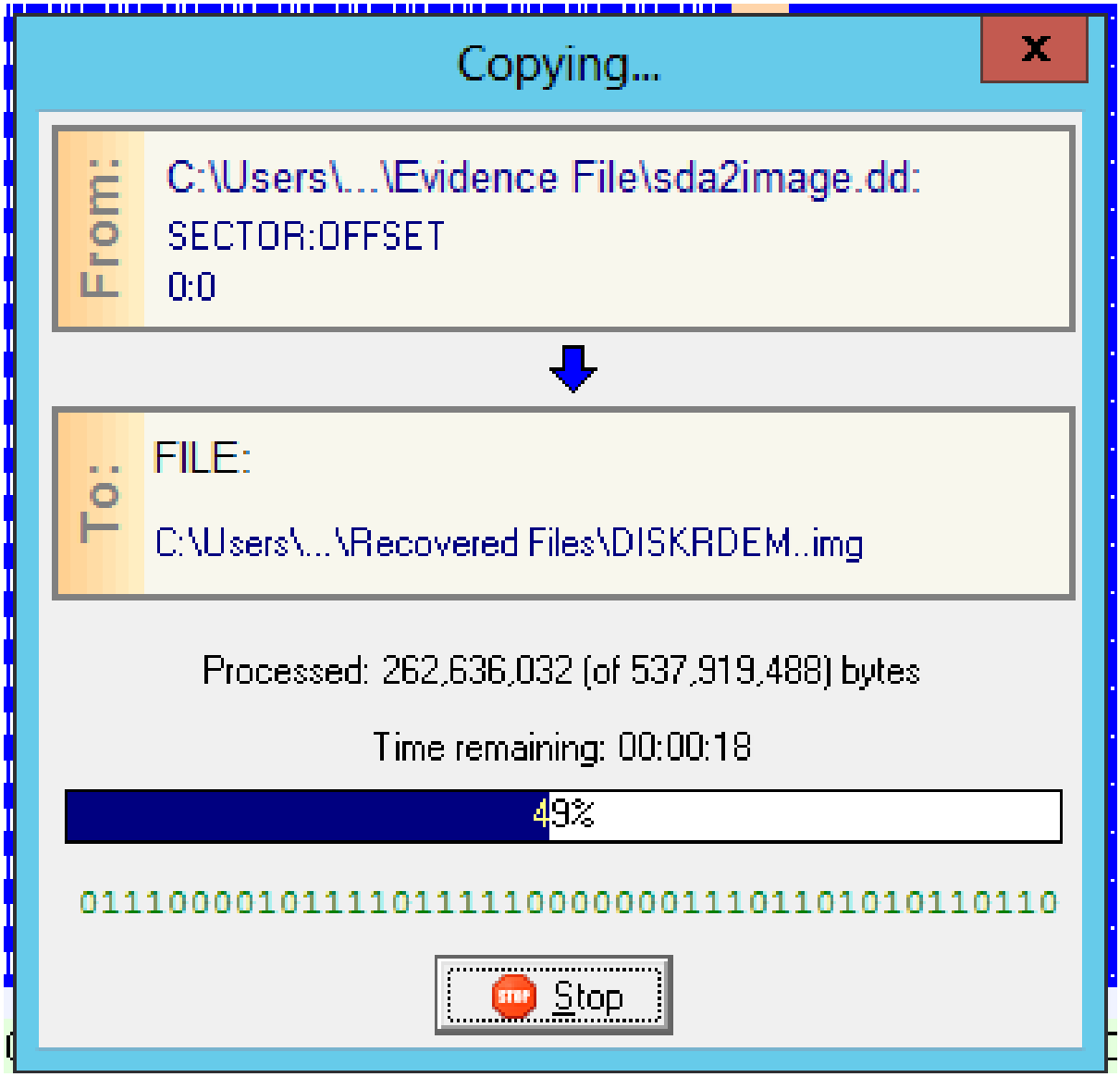

Figure 9: The process of copying the image file begins. The extracted data will be utilized for recovery and evidence collection.

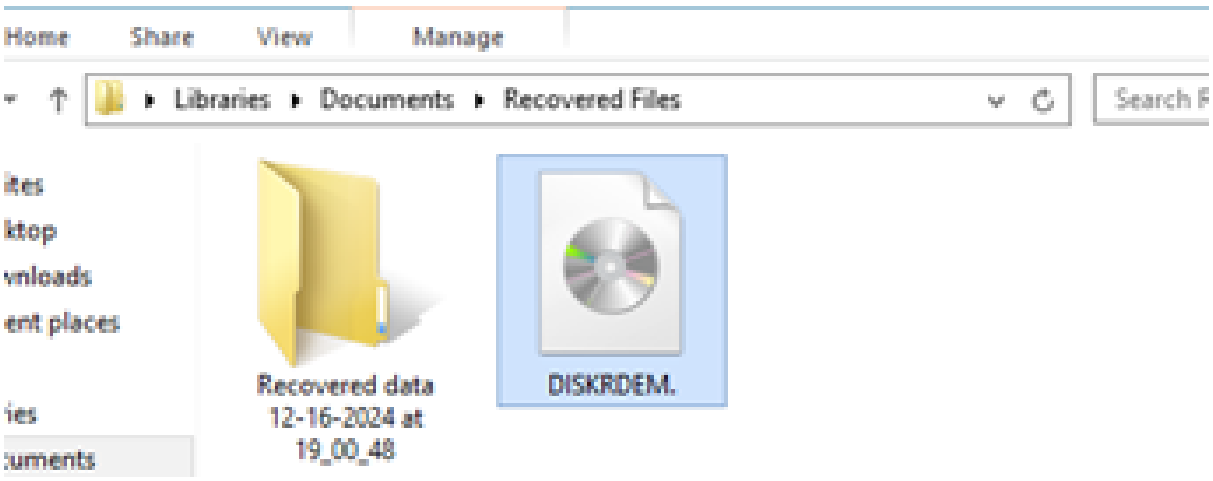

Figure 10: Recovered files are stored in the designated folder. This demonstrates the successful retrieval of data from the NTFS disk image.

Lab 2: Viewing Content of Forensic Image Using AccessData FTK Imager Tool

FTK® Imager is a powerful data preview and imaging tool designed to allow investigators to quickly assess electronic evidence. The tool helps determine whether a forensic image warrants further analysis using advanced tools such as **AccessData® Forensic Toolkit® (FTK)**.

Lab Scenario

FTK Imager enables investigators to mount and preview forensic image files to extract and validate evidence. By allowing the visualization of disk images and file systems, it streamlines the identification of critical data for forensic analysis.

Screenshots and Procedure

Below are the steps and corresponding screenshots that document the process of using FTK Imager for viewing and extracting evidence from forensic image files.

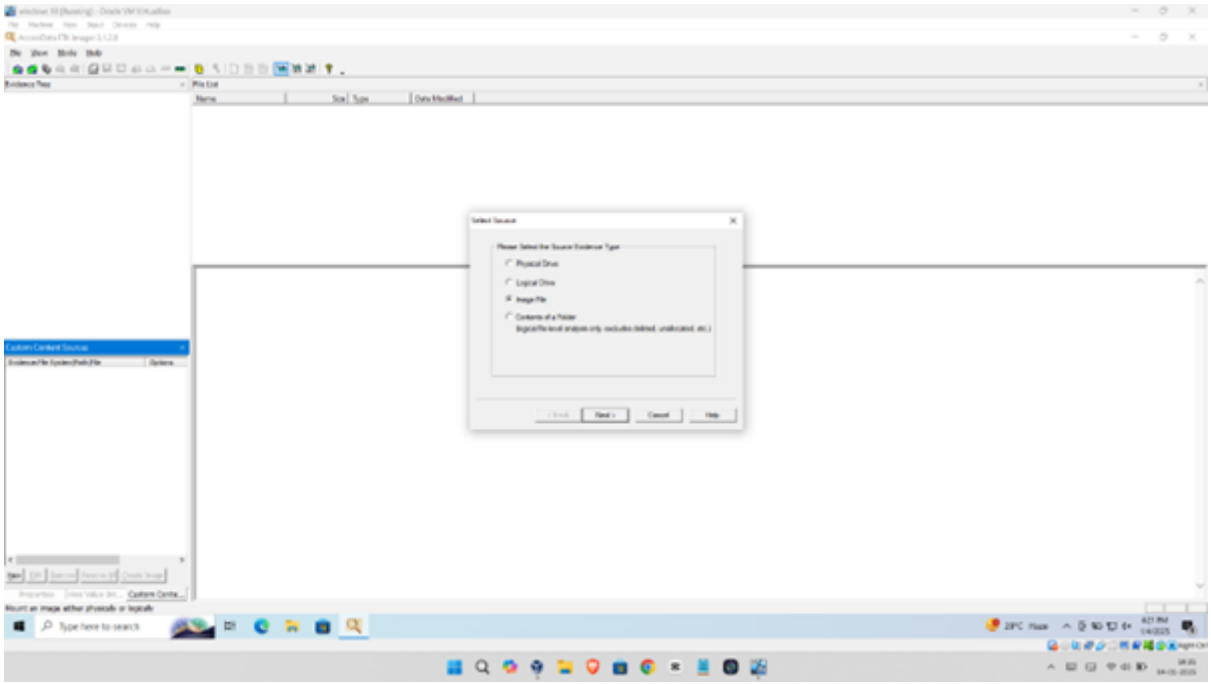

Figure 11: Launching FTK Imager. The tool's user interface allows forensic investigators to add evidence items and analyze forensic image files.

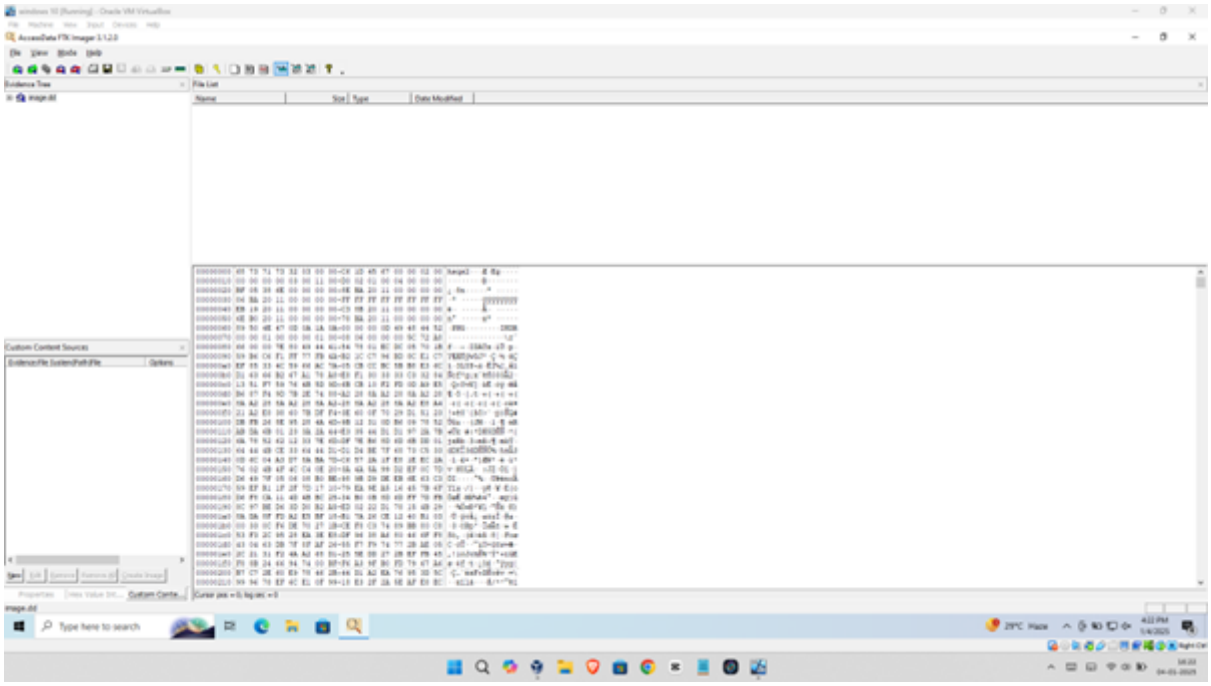

Figure 12: Adding the evidence image file using the `Add Evidence Item` option in the top-left corner. The image file was created earlier in Ubuntu and is 250MB in size.

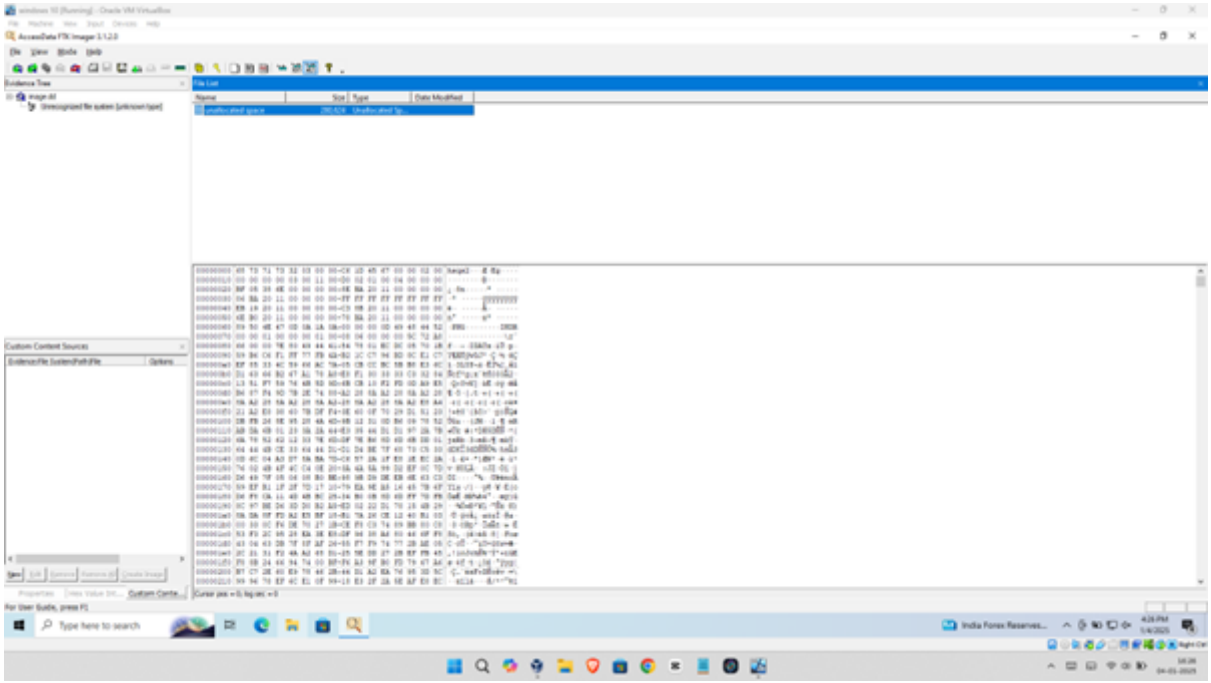

Figure 13: Hexadecimal view of the data is enabled by clicking the `HEX` button on the top panel. This view provides a low-level representation of the file contents.

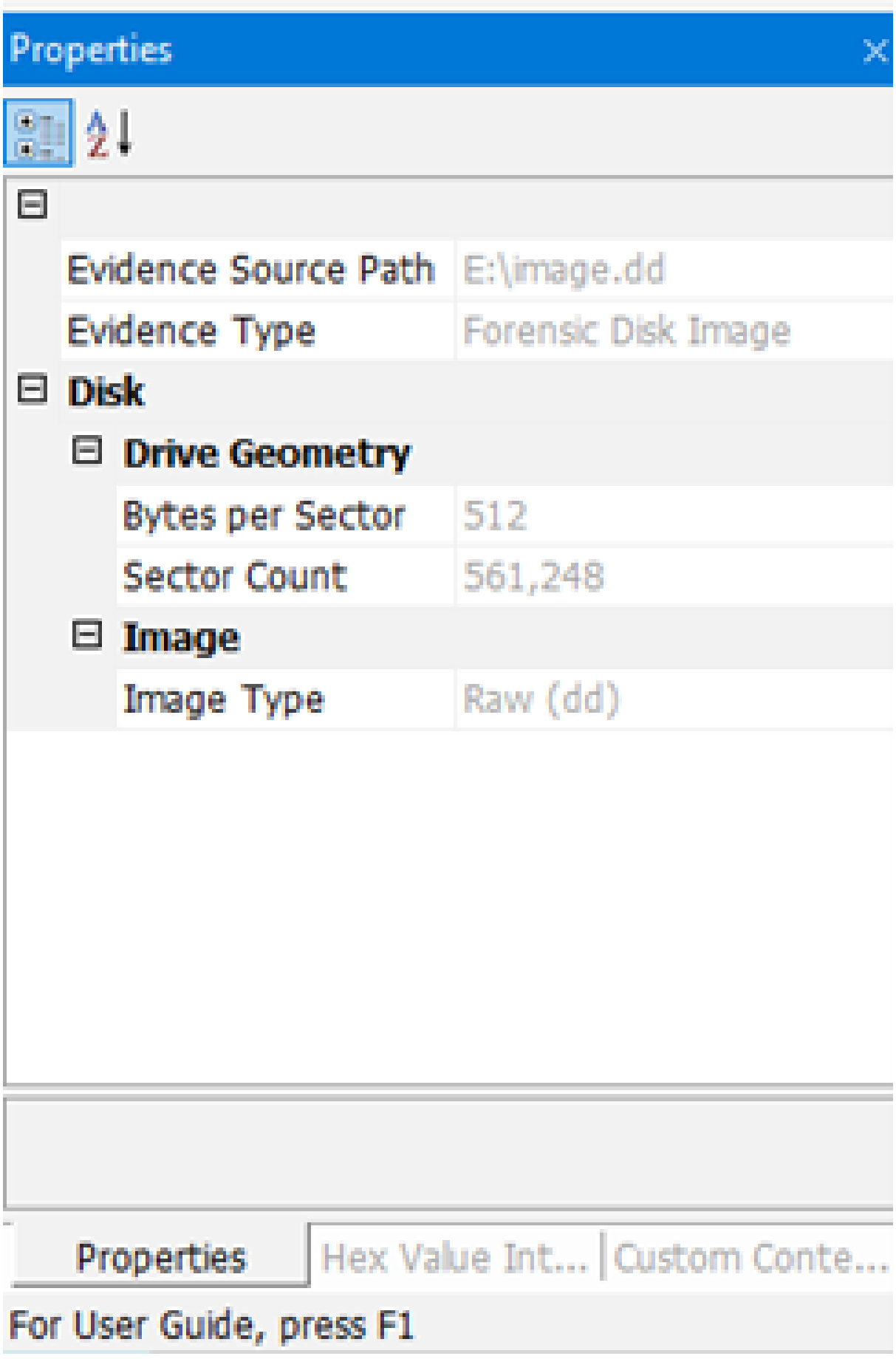

Figure 14: Recovered files are displayed in the designated folder after successful data extraction from the forensic image. This ensures the integrity and usability of the retrieved data for further analysis.

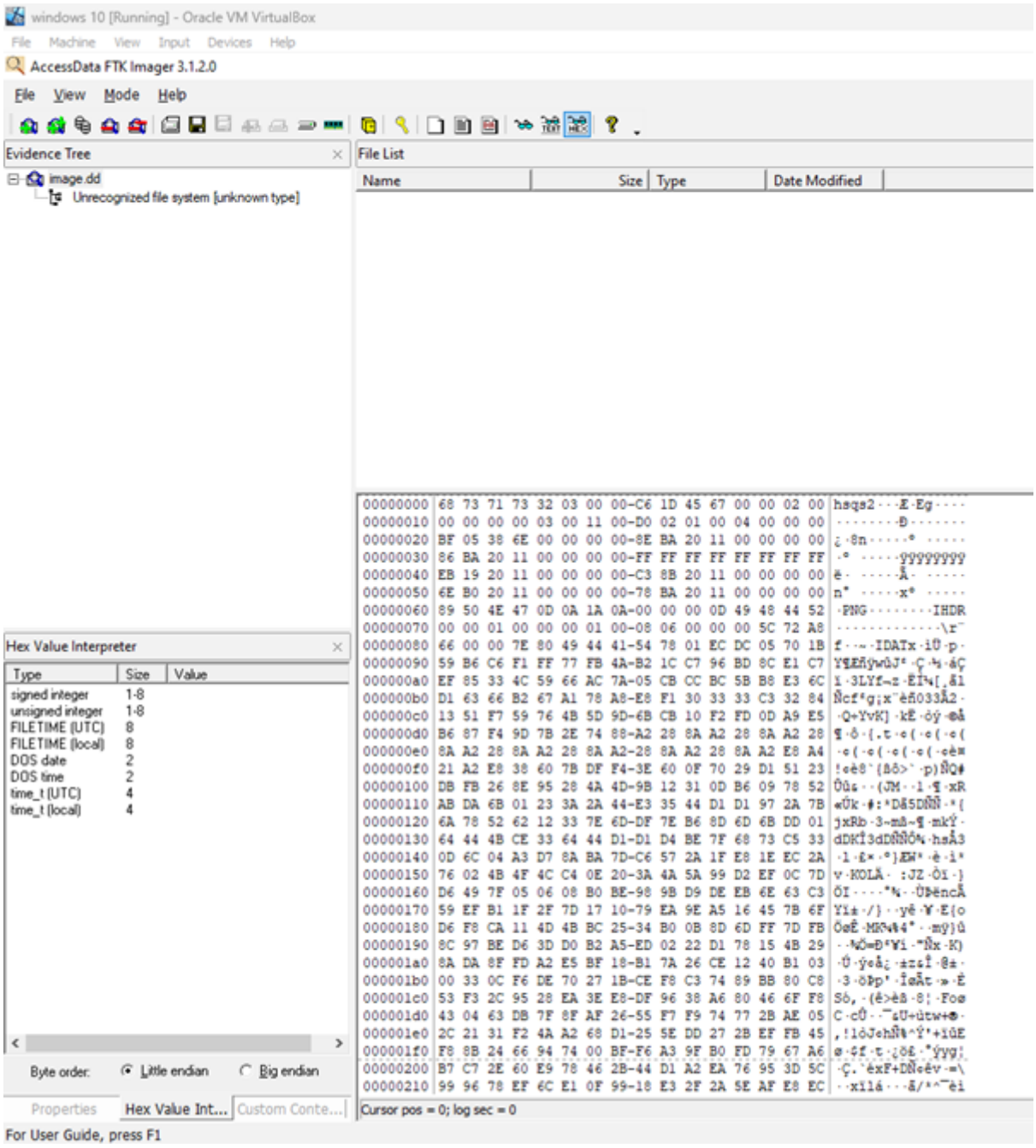

Figure 15: File properties and details are shown at the bottom-left corner of the interface. This feature allows investigators to examine metadata, permissions, and other attributes of the files.

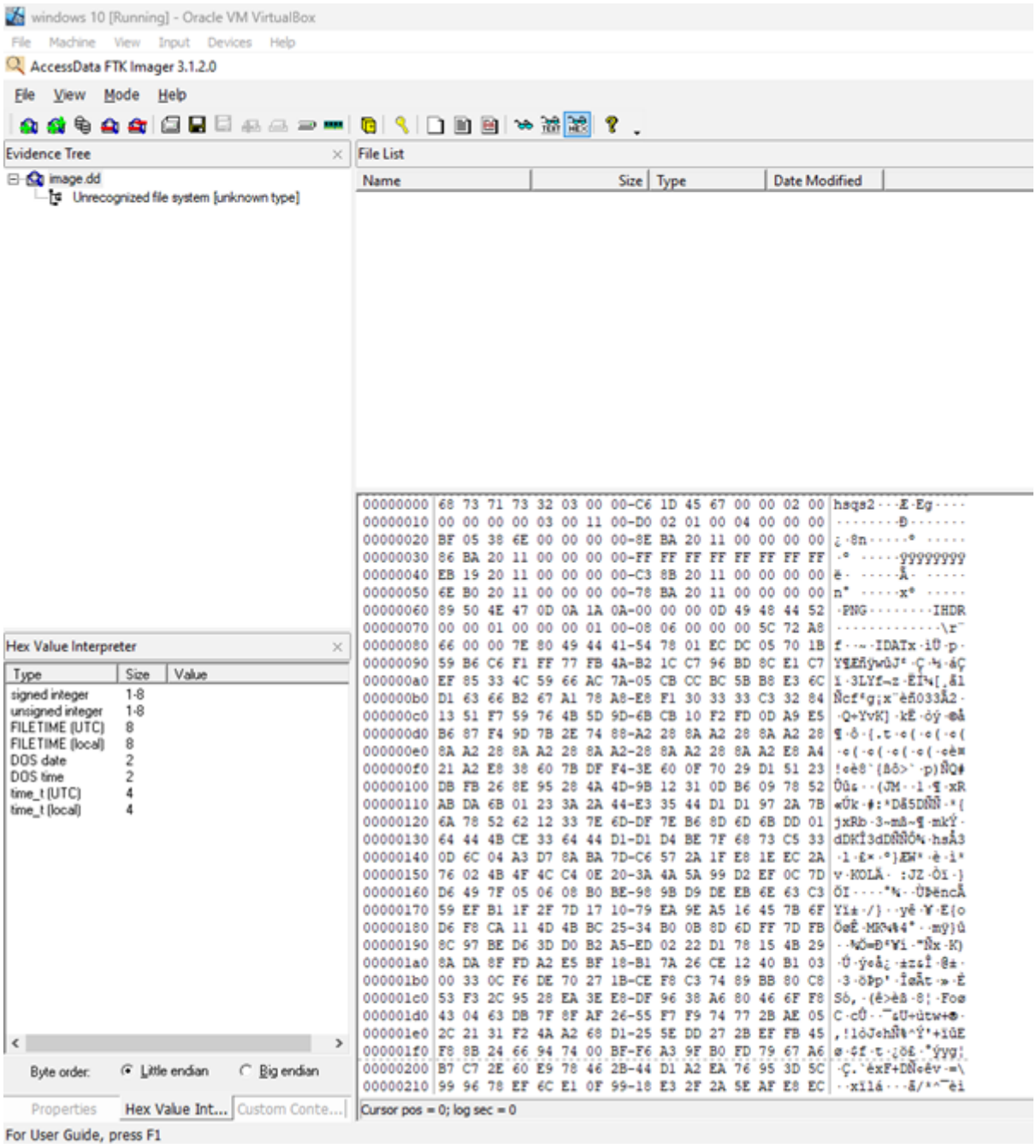

Figure 16: The Hexadecimal Interpreter tool is used to decode and interpret HEX values for better understanding of file structure and content.