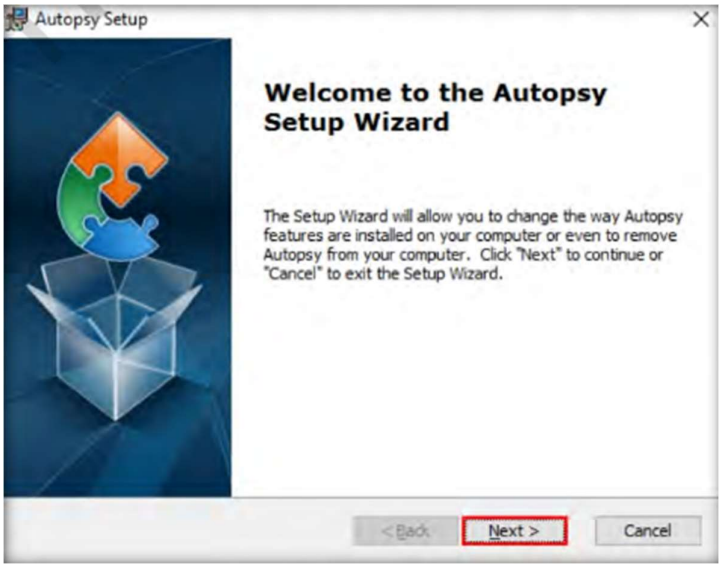
# PRACTICAL NO. 01

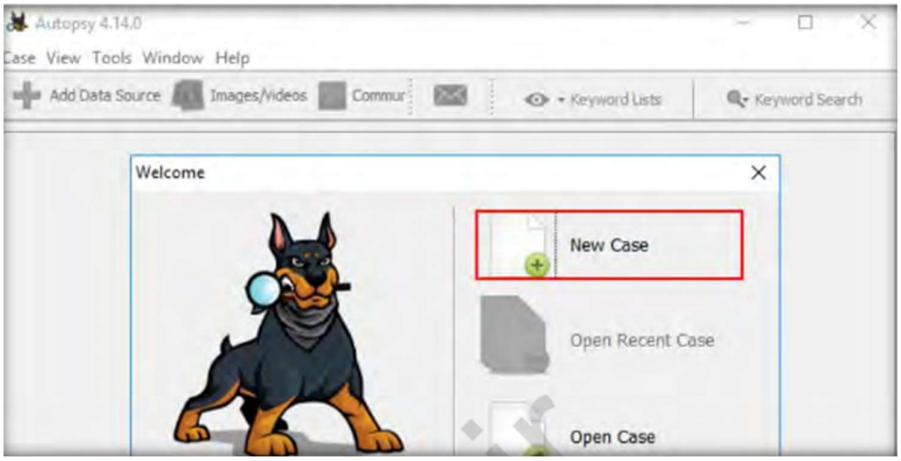
## File System Analysis using The SleuthKit (Autospy, fsstat, istat, fls and img_stat)

**Aim: Exploring Autopsy.**

To install Autopsy, navigate to C:\CHFI-Tools\CHFIv10 Module 03UnderstandingHardDisksandFileSystems\FileSystemAnalysisTools\Autopsy, double-click autopsy-4.14.0-64bit.msi installer and follow the wizard driven installation steps to complete the installation process.

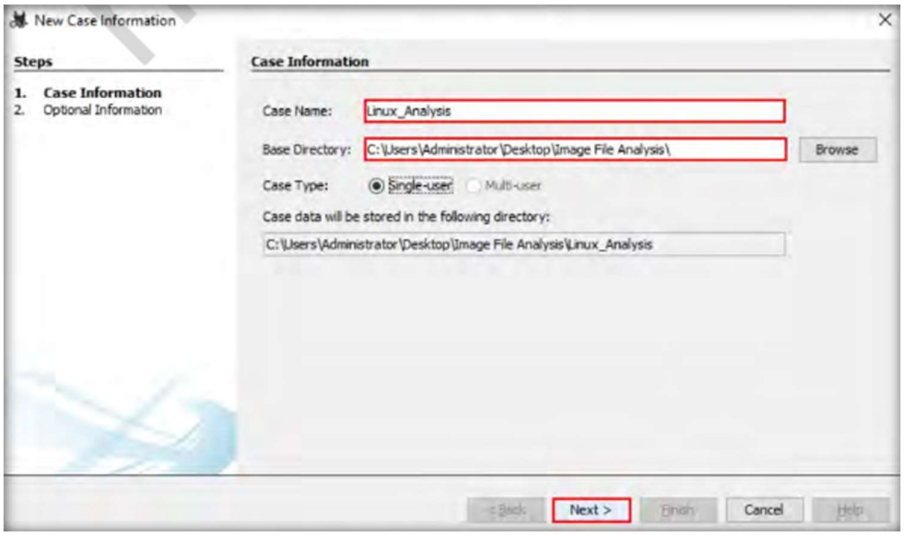



Autopsy Welcome window will appear along with Autopsy main window in the background. In the Welcome window, click New Case.

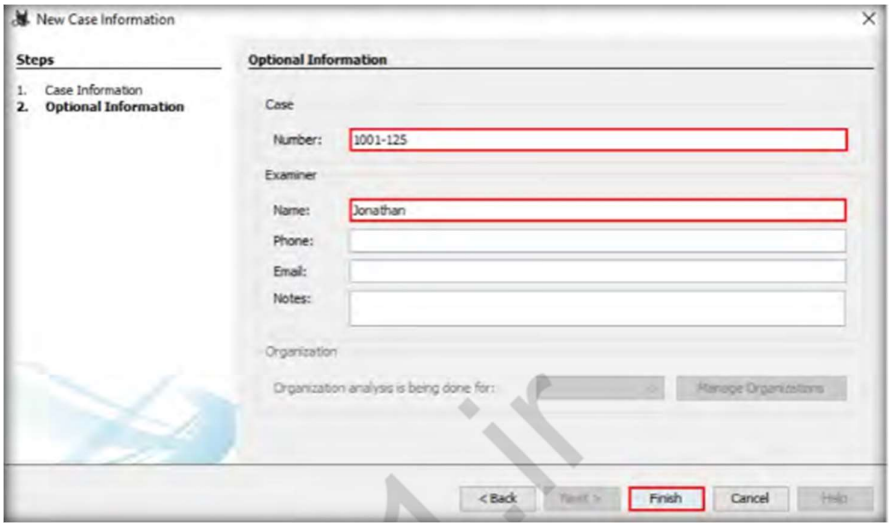



A New Case Information window opens asking you to input the Case Name and the Base Directory. The base directory is the location where the case data will get stored. The case name may be entered according to your identification purpose. In this lab, we are assigning the case name as Linux_Analysis.7.

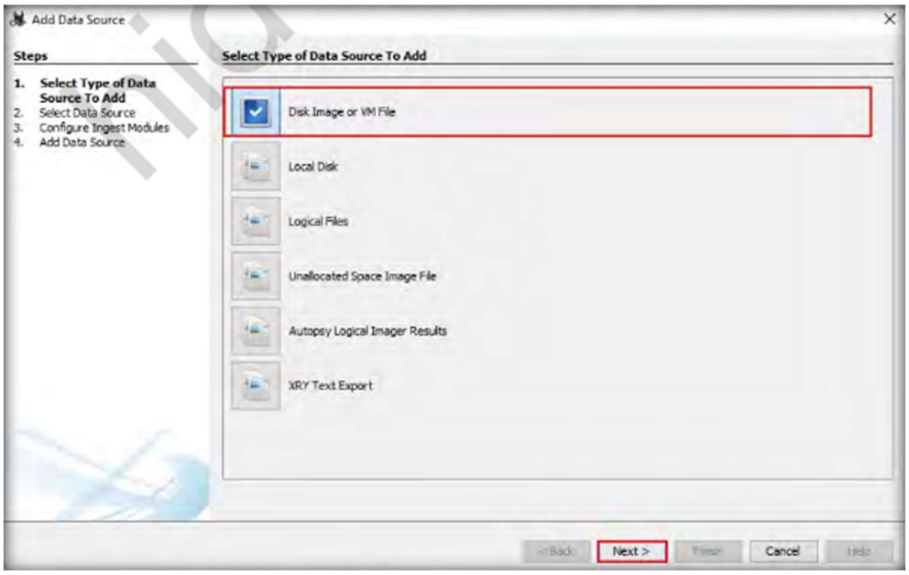
Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder. Upon setting the base directory, click Next



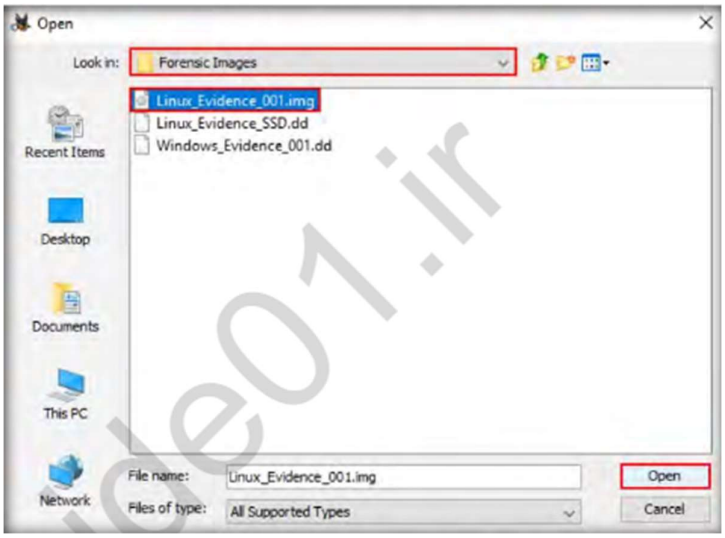

The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click Finish after entering the details for optional fields.

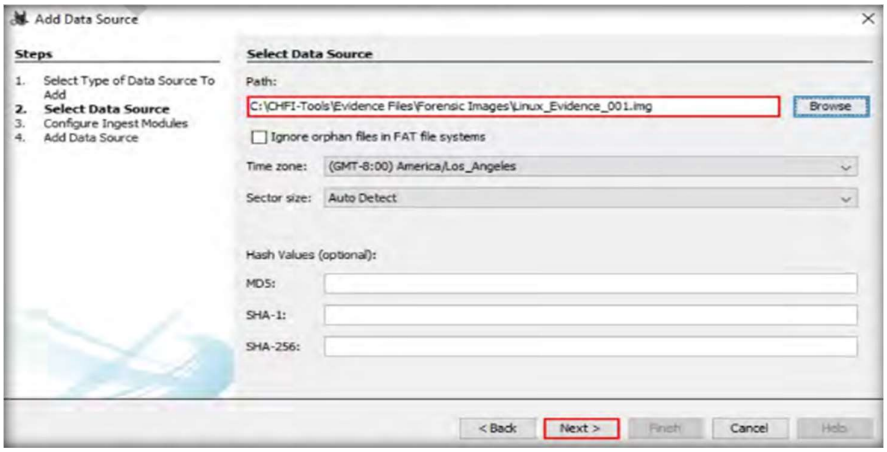



The Add Data Source window now appears displaying the section Select Type of Data Source to Add. Here,you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.

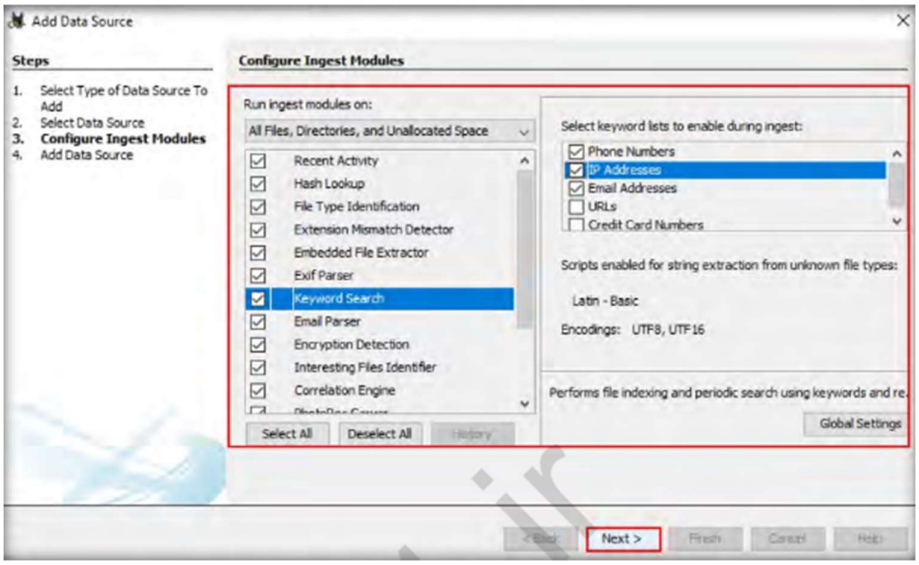


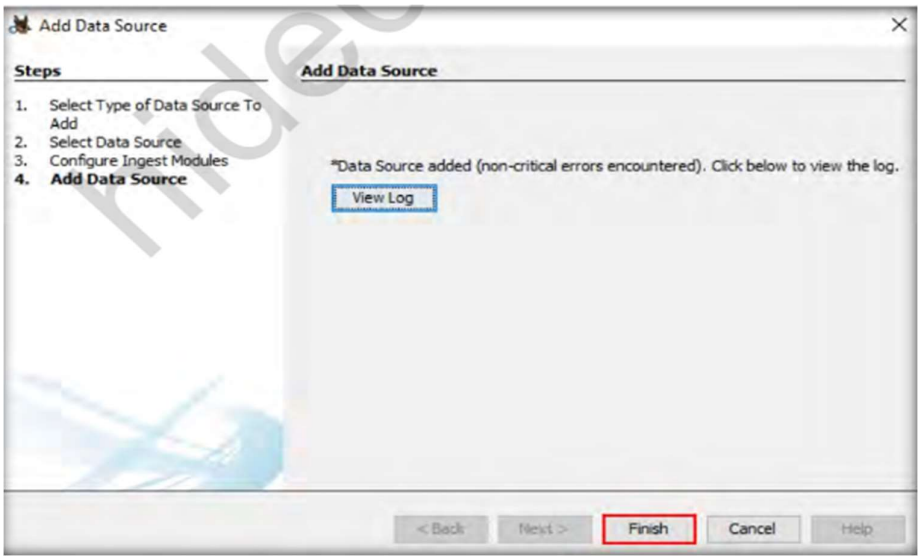

A window (named Open) will appear where you need to specify the forensic image. Navigate to C:\CHFI-Tools\Evidence Files\Forensic Images, select Linux_Evidence_001.img and click Open.



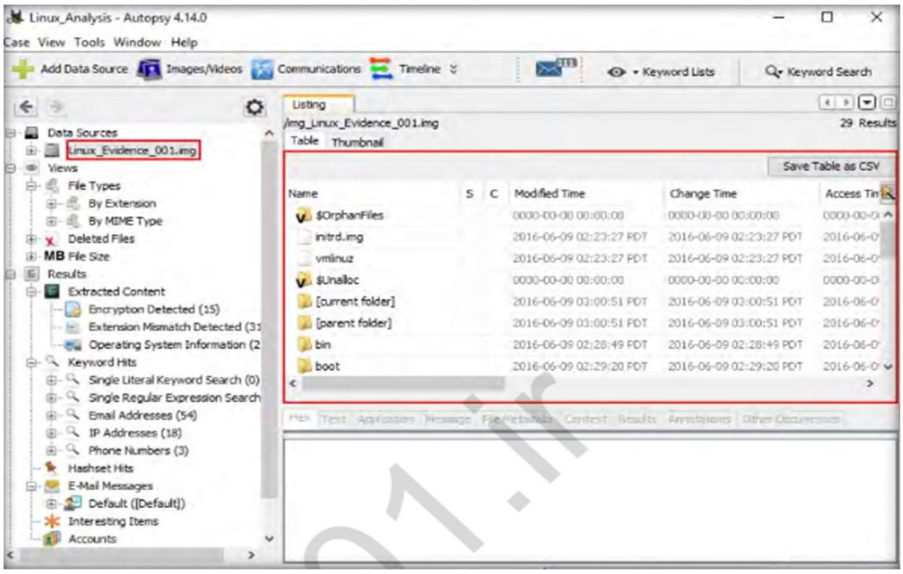



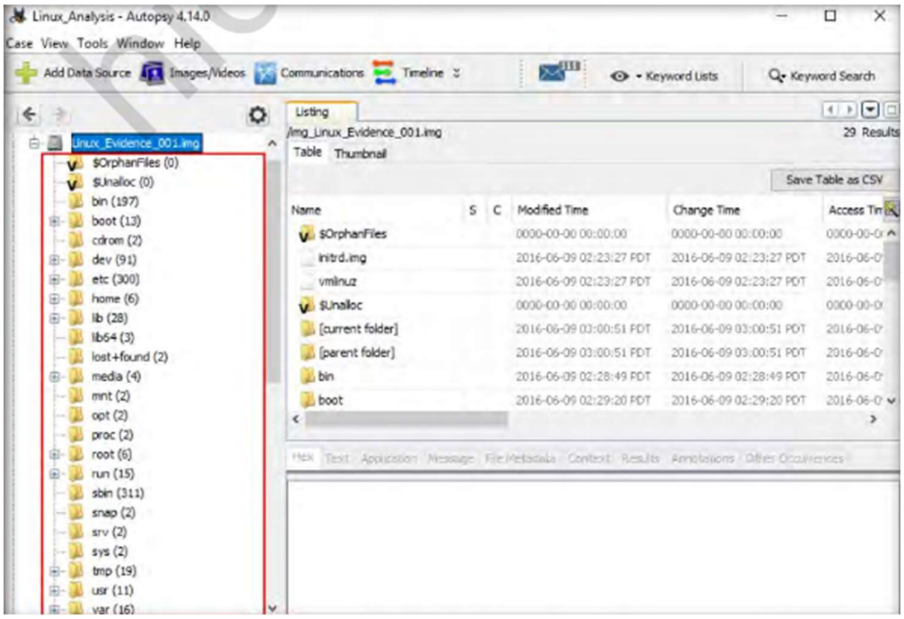
The Add Data Source window now displays the Configure Ingest Modules section, which contains lists of options that are checked. Select the options according to your requirement and click Next.




The application now displays the result in the Autopsy main window. Expand the Data Sources node in the left pane and click on the image file i.e.,Linux_Evidence_001.img. This will show the contents of the image file, as shown in the following screenshot:



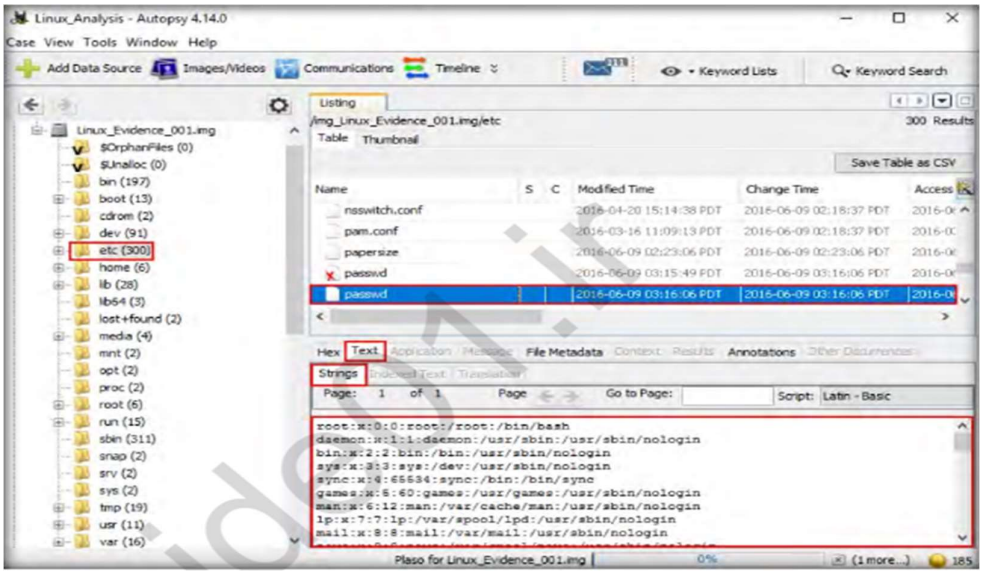

You may examine all the required files stored in the image as a part of filesystem analysis. In this lab, we are going to view the passwd file that is stored in \etc location. Therefore, select the etc folder from the left pane.

Upon selecting the folder, all the files and folders present in etc are displayed in the right pane of the window.

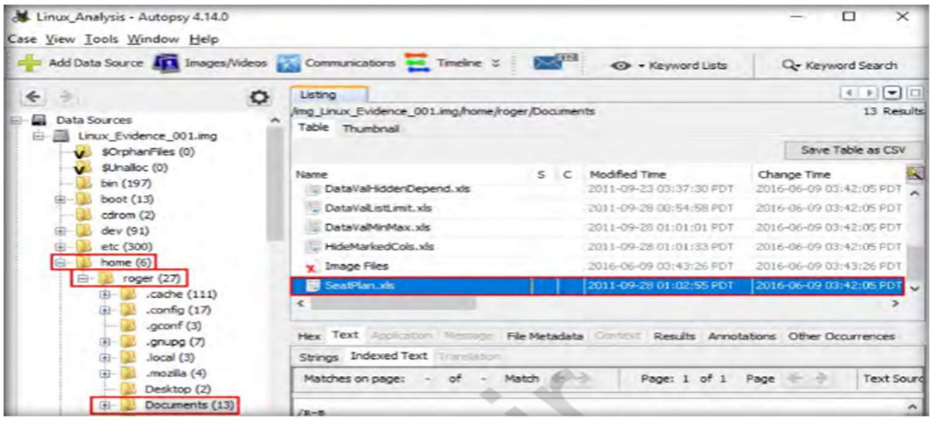
Scroll down the window, select the passwd file and click the Text tab.

Autopsy displays all the text (user account information) present in the passwd file, under the Strings tab,

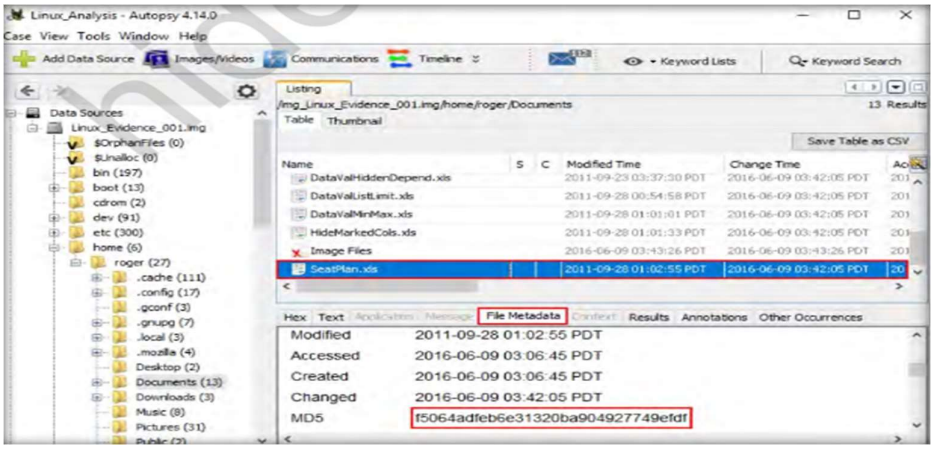
as shown in the following screenshot:




The SeatPlan.xls file appears in the right pane of the Autopsy window. Click the file.

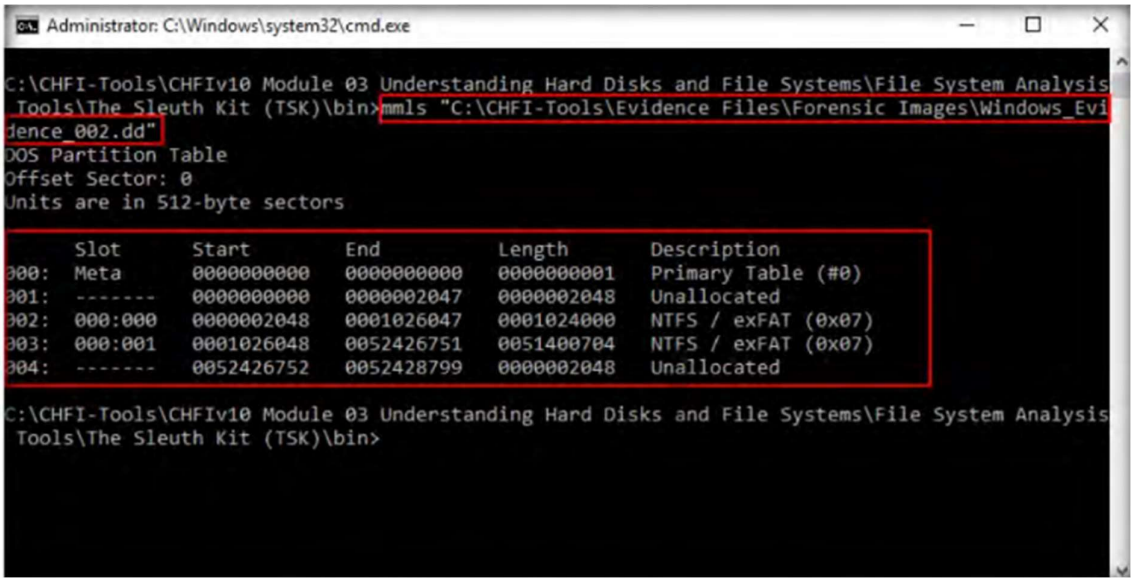



Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.

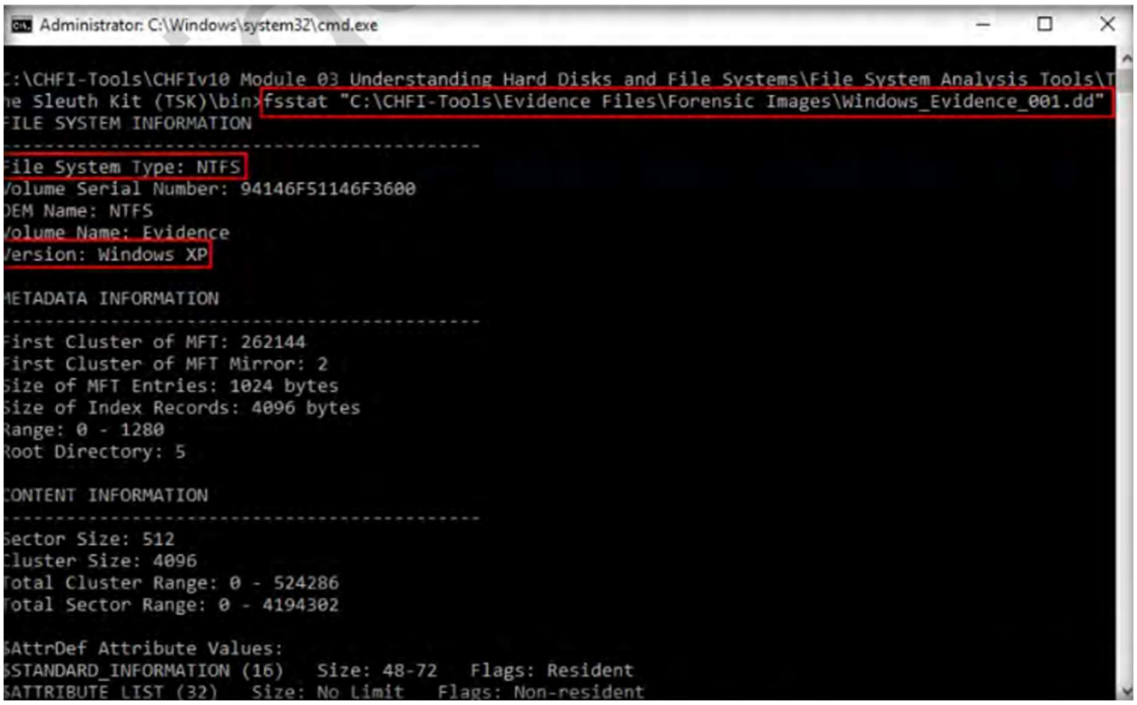


**To study fsstat**

To view partition tables associated with Windows_Evidence_002.dd, type mmls "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_002.dd"and press Enter. This displays the partition layout of a volume system (partition tables) associated with the image file, as shown in the following screenshot:



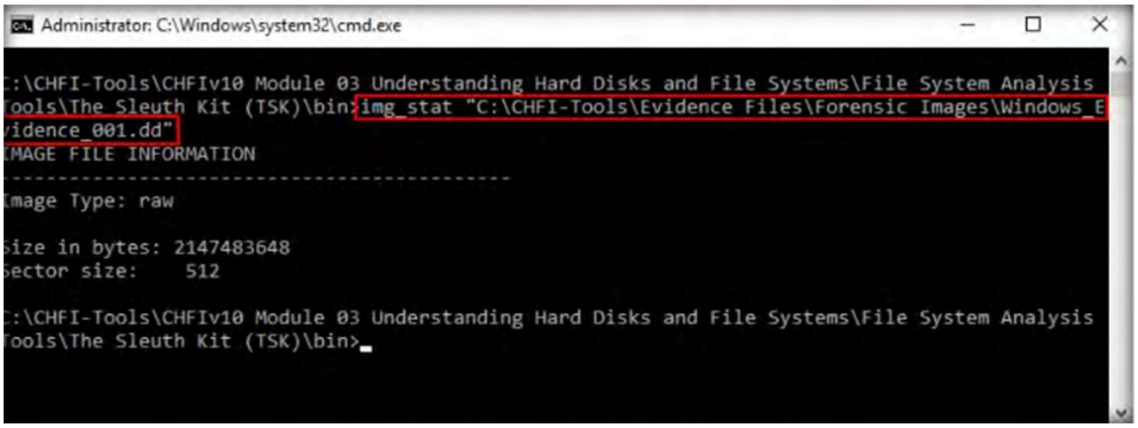

Similarly, to view the type of file system and the OS related to the image, type fsstat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"and then press Enter.




From the above screenshot, it can be observed that the file system is NTFS and the source OS is Windows XP

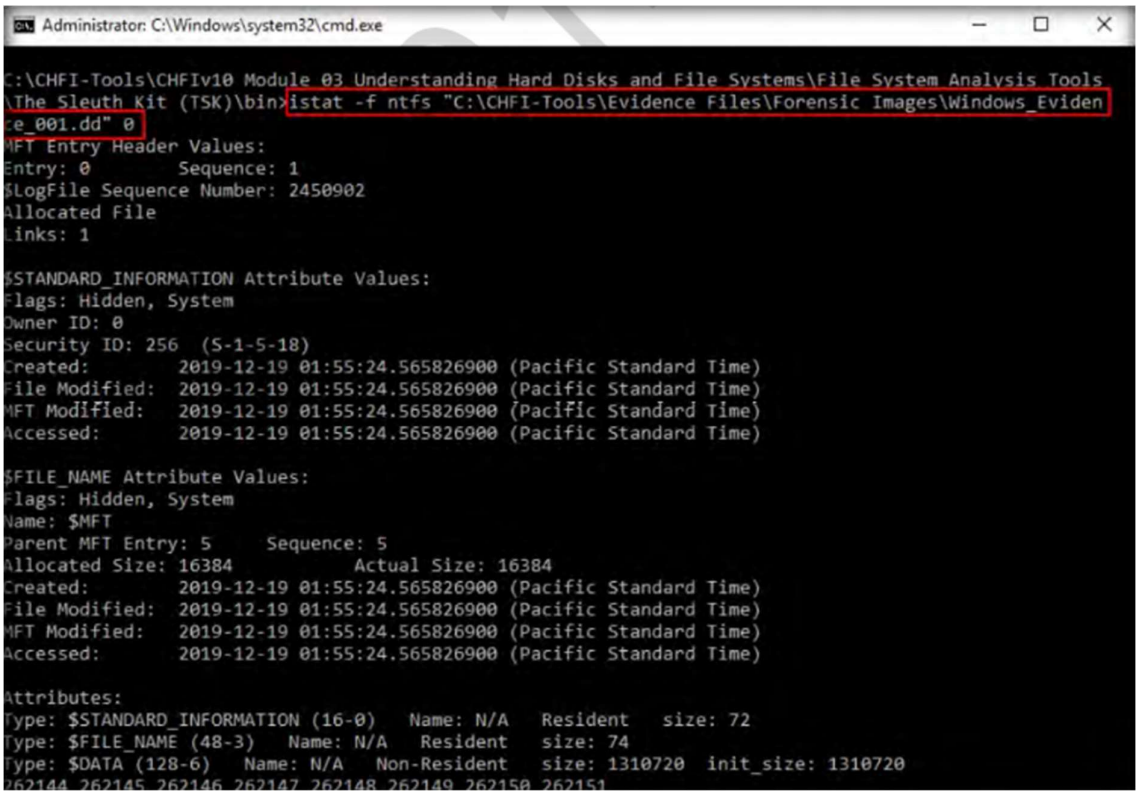
**To Study img_stat**

Use the img_stat command to view the details of the selected image. Type img_stat"C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"and press Enter to view the details.




**To Study istat**

Use the istat tool in The Sleuth Kit to view the details of metadata structure. To display an overview of the MFT file, type istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 0 and press Enter to view the details.




To display the MFTMirr File Overview, type istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 1 and press Enter.