

PRACTICAL NO. 01

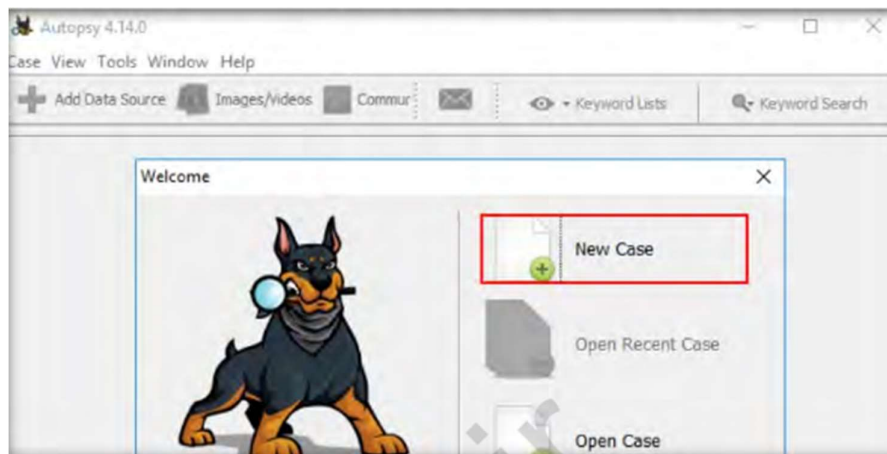
File System Analysis using The SleuthKit (Autopsy, fsstat, istat, fls and img_stat)

Aim: Exploring Autopsy.

To install Autopsy, navigate to C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\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.

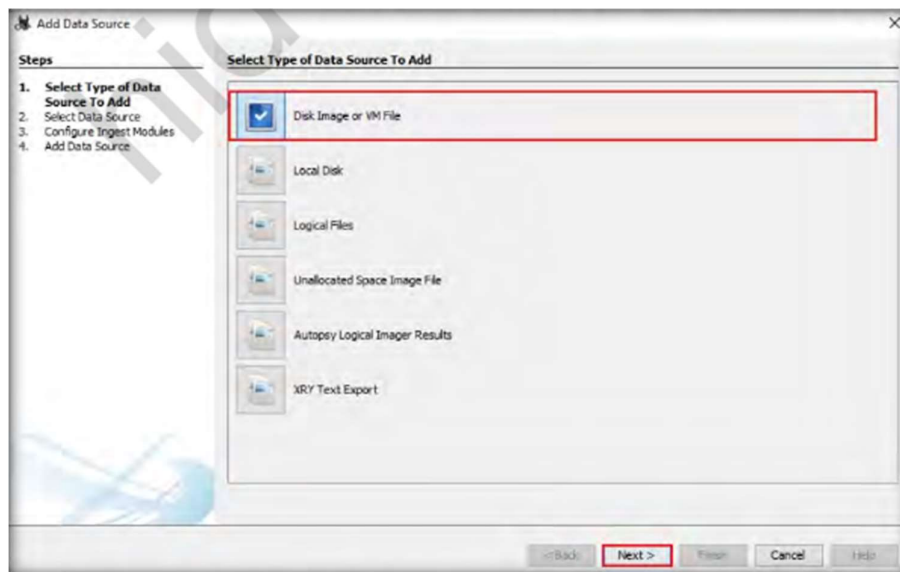
Before specifying the base directory, we will be creating a folder on the Desktop with the name Image File Analysis and setting the path of the Base directory to this folder. Upon setting the base directory, click Next

The screenshot shows the 'New Case Information' window with the 'Case Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Name' field is filled with 'Linux_Analysis'. The 'Base Directory' field is filled with 'C:\Users\Administrator\Desktop\Image File Analysis\'. The 'Case Type' is set to 'Single-user'. The 'Case data will be stored in the following directory:' field is filled with 'C:\Users\Administrator\Desktop\Image File Analysis\Linux_Analysis'. The 'Next >' button is highlighted with a red box.

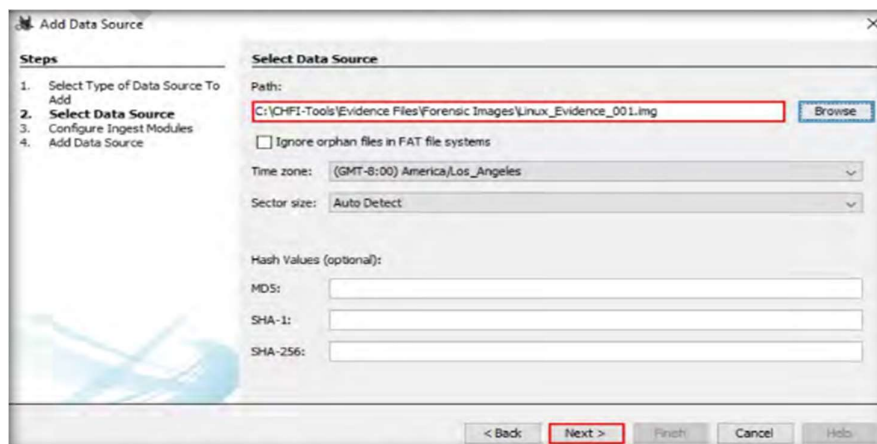
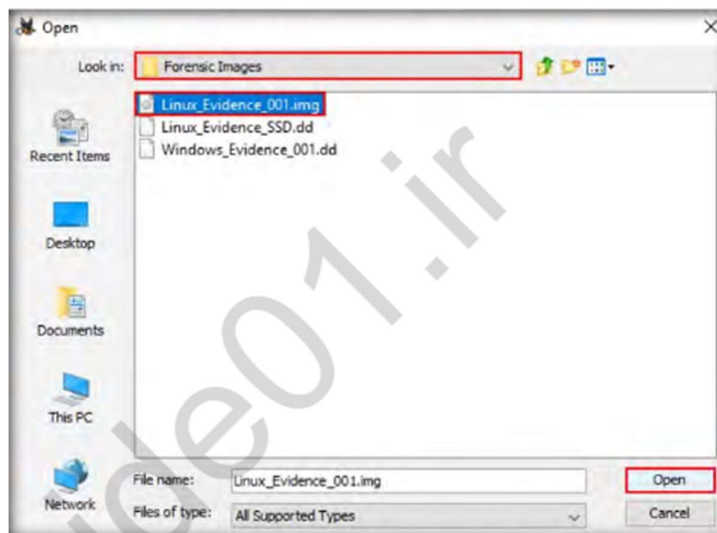
The New Case Information window now shows the Optional Information section where you can specify details such as name of the examiner and case number. For this lab, let us enter the name of the examiner as Jonathan and the case number as 1001-125. You may also fill out the other optional fields. Click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

The screenshot shows the 'New Case Information' window with the 'Optional Information' tab selected. The 'Steps' list on the left shows '1. Case Information' and '2. Optional Information'. The 'Case Number' field is filled with '1001-125'. The 'Examiner Name' field is filled with 'Jonathan'. The 'Phone', 'Email', and 'Notes' fields are empty. The 'Organization' section has a dropdown menu and a 'Manage Organizations' button. The 'Finish' button is highlighted with a red box.

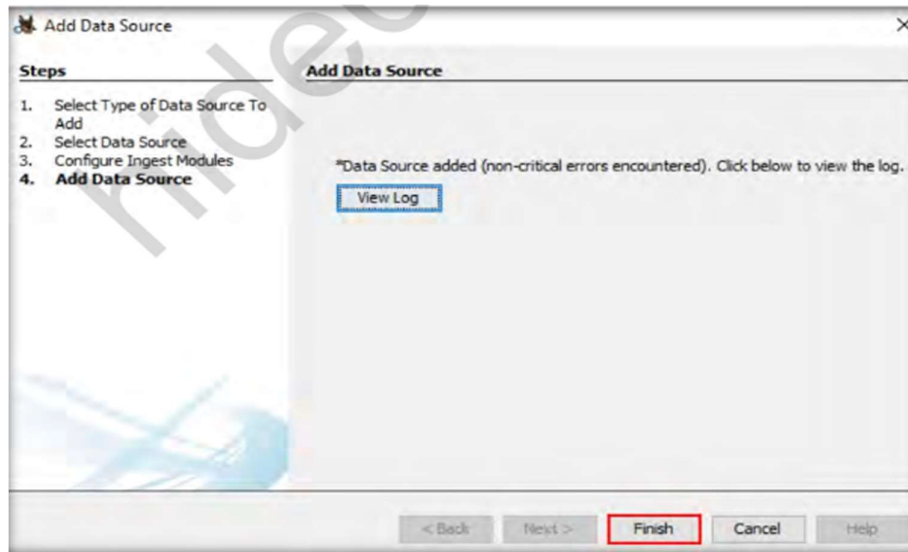
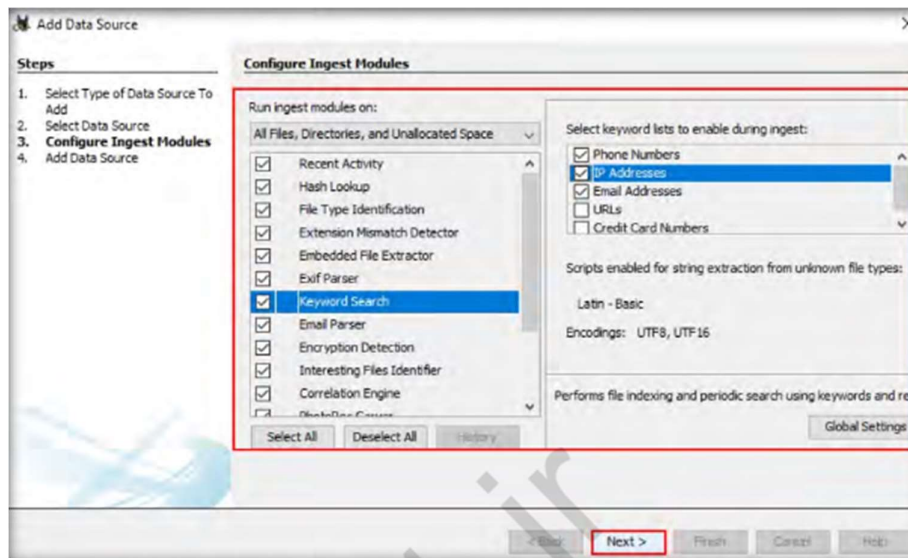
The Add Data Source window now appears displaying the section Select Type of Data Source to Add. Here, you need to select the type of data source to be provided as an input. In this lab, we will be analyzing a disk image; therefore, select the option Disk Image or VM File and click Next.



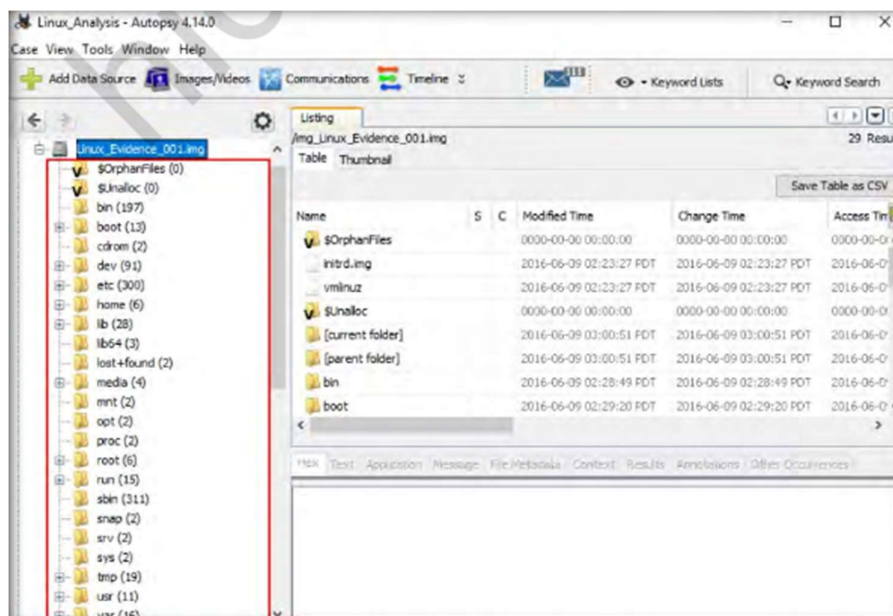
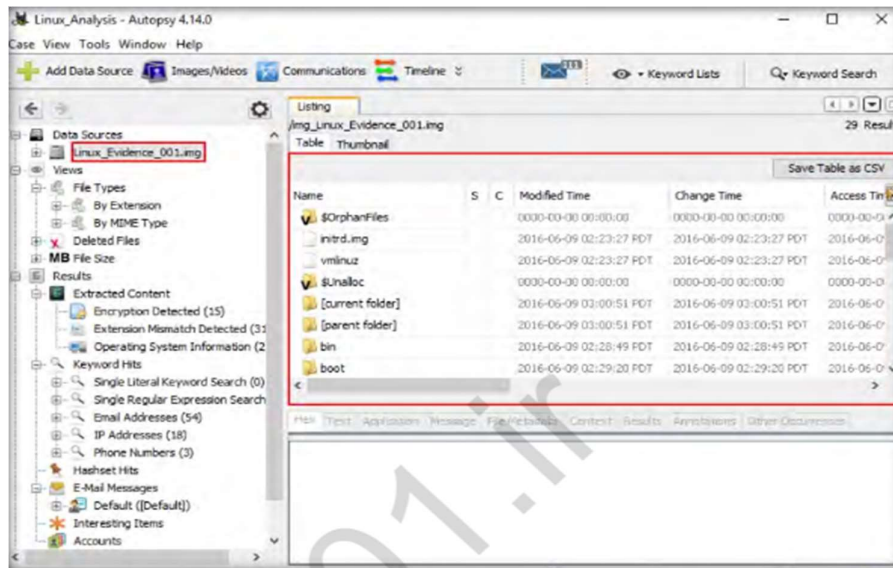
A window (named Open) will appear where you need to specify the forensic image. Navigate to C:\CHFI-Tools\Evidence Files\Forensic Images, select Linux_Evidence_001.img and click Open.



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:



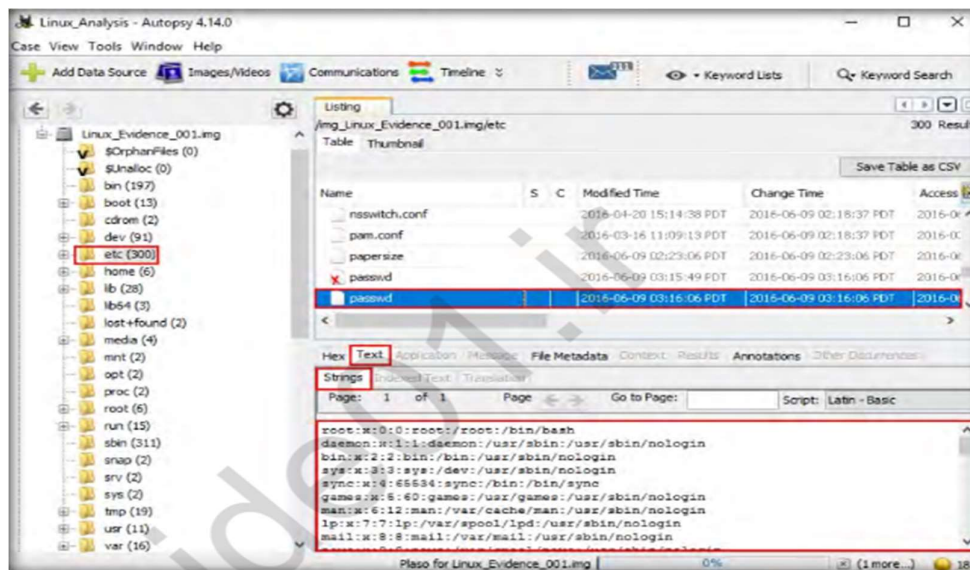
You may examine all the required files stored in the image as a part of filesystem analysis. In this lab, we are going to view the passwd file that is stored in /etc location. Therefore, select the etc folder from the left pane.

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

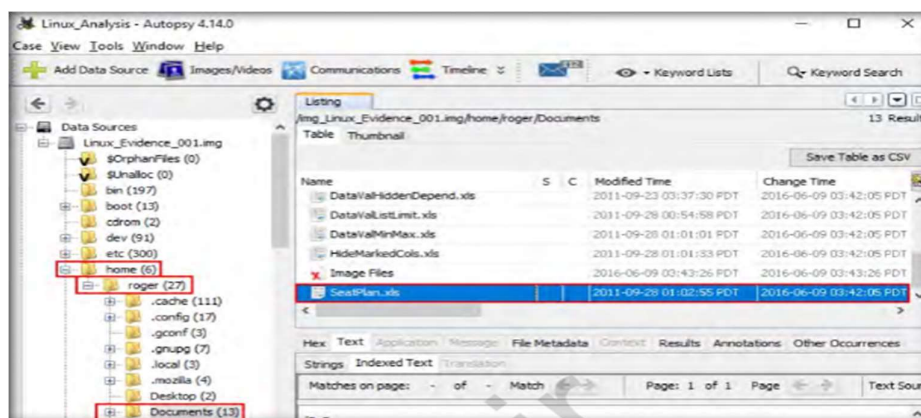
Scroll down the window, select the passwd file and click the Text tab.

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

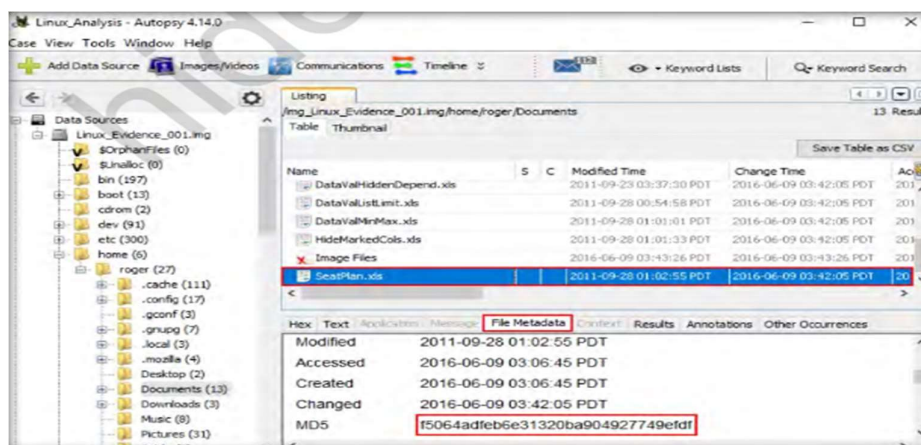
as shown in the following screenshot:



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

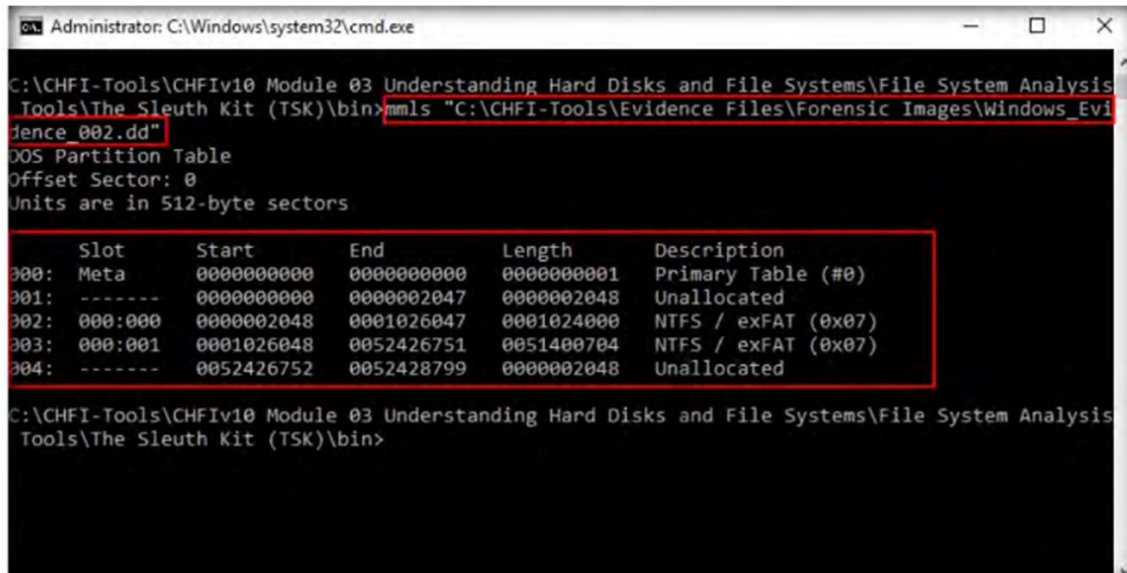


Click on File Metadata and scroll down the section to find the MD5 value for the SeatPlan.xls file.



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:

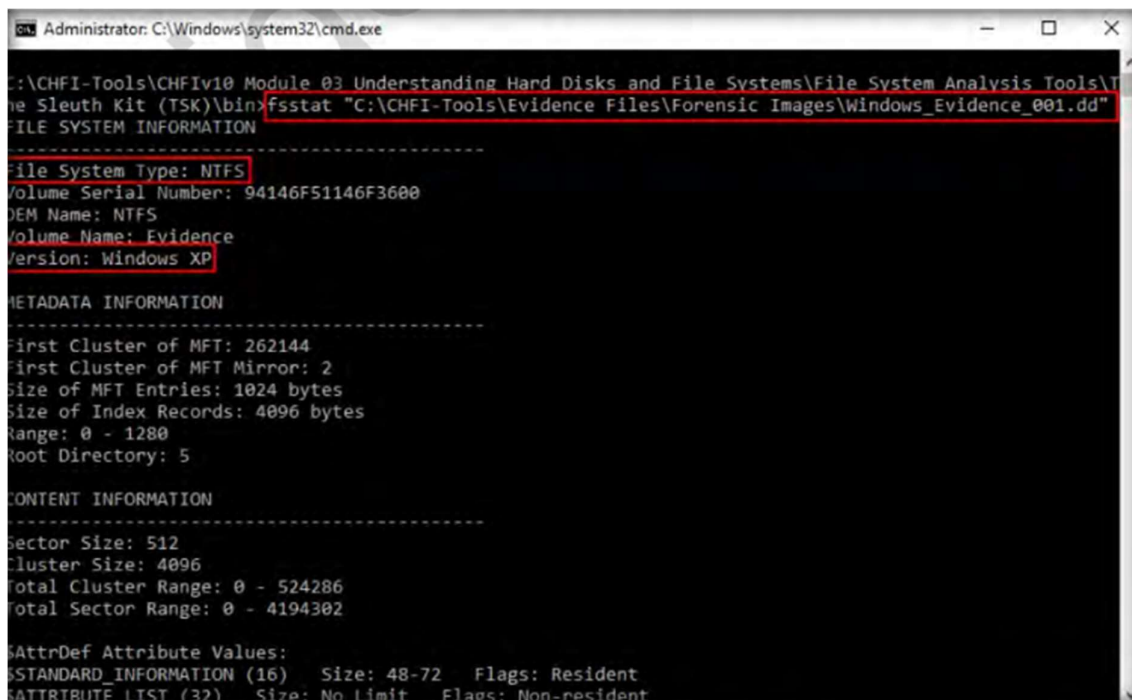


```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>mmls "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_002.dd"
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start      End      Length  Description
  -----
000: Meta      0000000000  0000000000  0000000001 Primary Table (#0)
001: -----      0000000000  0000002047  0000002048 Unallocated
002: 000:000      0000002048  0001024000  0001024000 NTFS / exFAT (0x07)
003: 000:001      0001026048  0052426751  0051400704 NTFS / exFAT (0x07)
004: -----      0052426752  0052428799  0000002048 Unallocated

C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>
```

Similarly, to view the type of file system and the OS related to the image, type `fsstat "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_001.dd"` and then press Enter.



```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>fsstat "C:\CHFI-Tools\EvidenceFiles\ForensicImages\Windows_Evidence_001.dd"
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: 94146F51146F3600
Volume Name: Evidence
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 262144
First Cluster of MFT Mirror: 2
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 1280
Root Directory: 5

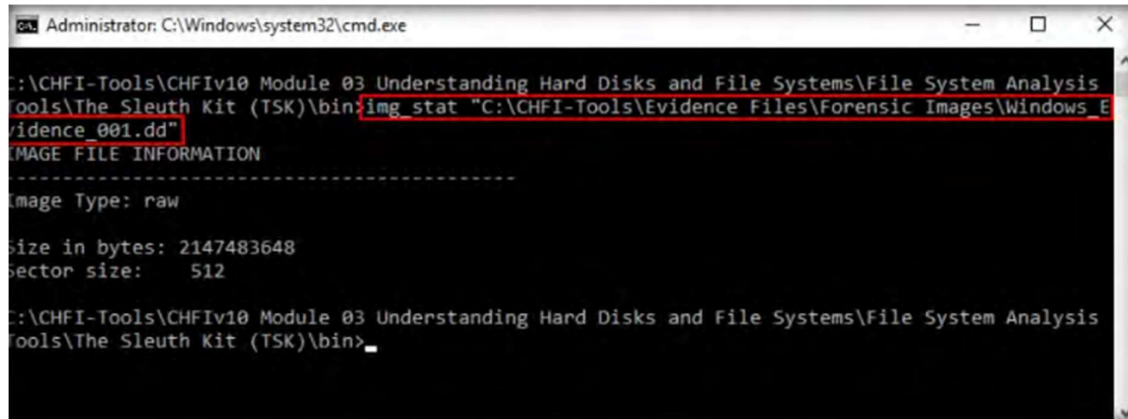
CONTENT INFORMATION
-----
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 524286
Total Sector Range: 0 - 4194302

AttrDef Attribute Values:
STANDARD_INFORMATION (16) Size: 48-72 Flags: Resident
ATTRIBUTE_LIST (32) Size: No Limit Flags: Non-resident
```

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

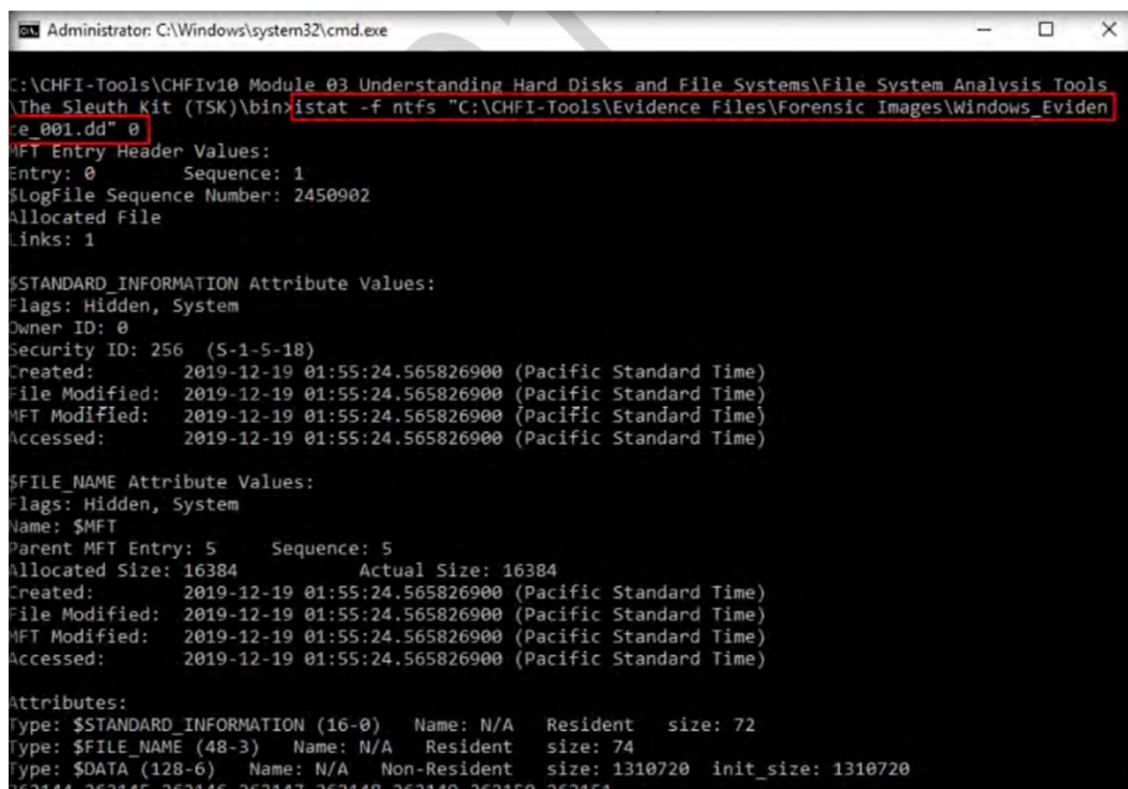
Use the img_stat command to view the details of the selected image. Type `img_stat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"` and press Enter to view the details.



```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>img_stat "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd"
IMAGE FILE INFORMATION
-----
Image Type: raw
Size in bytes: 2147483648
Sector size: 512
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>
```

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.



```
Administrator: C:\Windows\system32\cmd.exe
C:\CHFI-Tools\CHFIv10 Module 03 Understanding Hard Disks and File Systems\File System Analysis Tools\The Sleuth Kit (TSK)\bin>istat -f ntfs "C:\CHFI-Tools\Evidence Files\Forensic Images\Windows_Evidence_001.dd" 0
MFT Entry Header Values:
Entry: 0          Sequence: 1
LogFile Sequence Number: 2450902
Allocated File
Links: 1

$STANDARD_INFORMATION Attribute Values:
Flags: Hidden, System
Owner ID: 0
Security ID: 256 (S-1-5-18)
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

$FILE_NAME Attribute Values:
Flags: Hidden, System
Name: $MFT
Parent MFT Entry: 5 Sequence: 5
Allocated Size: 16384 Actual Size: 16384
Created: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
File Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
MFT Modified: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)
Accessed: 2019-12-19 01:55:24.565826900 (Pacific Standard Time)

Attributes:
Type: $STANDARD_INFORMATION (16-0) Name: N/A Resident size: 72
Type: $FILE_NAME (48-3) Name: N/A Resident size: 74
Type: $DATA (128-6) Name: N/A Non-Resident size: 1310720 init_size: 1310720
262144 262145 262146 262147 262148 262149 262150 262151
```

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.