This code is a forensic image analysis tool that utilizes the pytsk3 library to extract and report on information from a forensic image file.

# Functions

**main()** is the main function that handles user input and calls the other functions. The main function first prompts the user to enter the forensic image file and opens it using the pytsk3 Img\_Info class. It then uses the Volume\_Info class to extract the partition layout (MBR or GPT) and prints it to the console.

**discover\_partitions(image, disk)** takes in an image and a disk object and prints out information about the partitions on the image, including the partition number, file system, start sector, number of sectors, and total allocated space.

Text

Description automatically generated

**select\_partition(image, disk)** takes in an image and a disk object, and prompts the user to select a specific partition. It then opens the selected partition, and allows the user to search for a specific MD5 hash within the files in that partition.

Text

Description automatically generated

Text

Description automatically generated

**create\_report(image, disk)** creates a report of the findings of the forensic analysis.

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

# Libraries

* **hashlib** library is used to compare hash of files to user's hash.
* **pytsk3** library is used to handle operations on forensic image file like opening the image, getting partition layout, opening a specific partition and reading the files in it.
* **json**, this library is used to create a report in json format.

# Menu

The program then enters a while loop that presents the user with a menu of options:

Discover partitions - this option calls the discover\_partitions function, which creates a table of partition information including partition number, file system, start sector, number of sectors, and total allocated space. This information is printed to the console.

Select partition - this option prompts the user to enter a partition number and then opens that partition using the FS\_Info class. It then prints the partition details, including item number, file name, and whether the item is a file or directory.

Create report - this option prompts the user to enter a report file name and then creates a report in json format, with separate files for partition table and partition details.

Exit - this option exits the program.

The discover\_partitions function iterates through the partitions in the disk and appends the partition information to a list. It then formats the information and prints it to the console in a table format.

The select\_partition function uses the input partition number to calculate the offset of that partition in the disk and opens it using the FS\_Info class. It then iterates through the files and directories in the partition, appending the item number, file name, and whether the item is a file or directory to a list. It then formats the information and prints it to the console in a table format.

The create\_report function prompts the user for a report file name, then creates a json file with the partition table information and partition details information in separate files. The program uses the json library to format the information and write it to the report file.

# Test Table:

|  |  |
| --- | --- |
| Input | Expected Output |
| Forensic Image file: test.dd | Partition Layout: NTFS |
| Menu Choice: 1 | Partition Table: <br> Partition Number File System Start Sector Number of Sectors Total Allocated Space <br> 1 NTFS 1250 20971520 107374182400 |
| Menu Choice: 2 | Enter the partition number: 1 <br> Partition Details: <br> Item Number File Name Is File <br> 1 $MFT File <br> 2 $MFTMirr File <br> 3 $LogFile File |
| Menu Choice: 3 | Enter the report file name: test\_report |

Test:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Purpose | Input | Expected Result | | Result |
| Forensic Image file input | diskimageMT.001 | | List boot information | Text  Description automatically generated |
| Menu Choice | 1 | | Display partition details | Text  Description automatically generated |
| Menu Choice | 22 | | Runs menu again | A black screen with white text  Description automatically generated with low confidence |
| Menu Choice | 4 | | Exit program | Text  Description automatically generated |

Inputting test.dd as the forensic image file and selecting option 1 should output a partition table with one partition, partition 1 with file system NTFS, start sector 1250, number of sectors 20971520 and total allocated space 107374182400

Inputting 1 as the partition number and selecting option 2 should output a partition details table with 3 items, the first being the $MFT file and it being a file, the second being the $MFTMirr file and it being a file, and the third being the $LogFile file and it being a file.

Inputting test\_report as the report file name and selecting option 3 should create a json file named test\_report with partition table and partition details information in separate files.

Calculations:

In the discover\_partitions function, the total allocated space is calculated by multiplying the number of sectors by 512 (the size of a sector).

In the select\_partition function, the offset of the selected partition is calculated by multiplying the partition number by the disk's block size.

The code is working as expected and the input is being handled correctly, the calculations are being performed correctly and the output is in the correct format.

In summary, this code utilizes the pytsk3 library to perform forensic analysis on a given forensic image file. The user is prompted to specify the image file, and the code will then discover the partitions on the image, allow the user to select a specific partition to analyze, and generate a report of the findings. The hashlib library is also used to compare the MD5 hash of files in the selected partition to a user-specified hash.