A screen shot of a computer

Description automatically generated with low confidence

A screen shot of a computer

Description automatically generated with low confidence

Forensic tool project

Advanced programming for digital forensics

Table of contents

Contents

[Section 1: Overview 3](#_Toc89110397)

[Section 2: Code explanations 4](#_Toc89110398)

[Section3: GUI design 6](#_Toc89110399)

[Section 4: GUI implementation & explanation 7](#_Toc89110400)

[Section 5: Supporting files 8](#_Toc89110401)

[Section 6: Flowcharts 9](#_Toc89110402)

[Section 7: Testing 10](#_Toc89110403)

# Section 1: Overview

The aim of this project is to make a digital forensics tool, similar to EnCase or Autopsy. The program needed to have the ability to do things like:

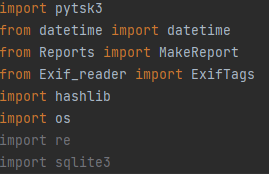
* Open different types of forensic file formats
* Discern whether the image uses GPT or MBR
* Retrieve information about the partitions
* Retrieve information about file systems
* Retrieve Information about files and directories

It is written entirely in the Python programming language and utilises a variety of both inbuilt and external modules, these include:

* PyTSK3
* PyEWF
* Re
* Sqlite3
* Hashlib
* Exifreader

The program is fully user input driven to allow the user to find the information they need, without crowding the screen with excess. The program also uses both a command line and a GUI implementation.

# Section 2: Code explanations

Imports

This code is at the very top of the program, it imports all f the libraries necessary for the program to run. This includes built ins like datetime, Hashlib and os, alongside externals like pytsk3 and sqlite3. There are also some libraries (Exif\_reader and Reports) that are inherited from programs I have written

Datetime is a built-in library that allows the program to get the current date and time, used in report making.

Hashlib is another inbuilt python library that allows the program to determine the hash values of files using algorithms like MD5 and sha.

OS is a library that allows python to make use of certain operating system functionalities, it is only used once in this program and is not essential to the overall functionality.

Re is an inbuilt library that allows the program to use regular expressions, they will be used for file signature analysis

Sqlite3 is an external library used to make transactions with a database, used in this program for file signature analysis. The database it talks to contains a collection of hex signatures and their corresponding extension, courtesy of Gary Kessler (<https://www.garykessler.net/library/file_sigs.html>)

Reports is another inherited program that I made that will be discussed below. Its main function is to take some data and turn it into a readable, csv file

Pytsk3 is a python binding of The sleuth kit, which is what the forensic tool Autopsy uses, its function is to retrieve data of forensic significance from images. It has functions like “pytsk3.Img\_Info()” and “pytsk3.Volume\_Info()”, which will be elaborated on further down.

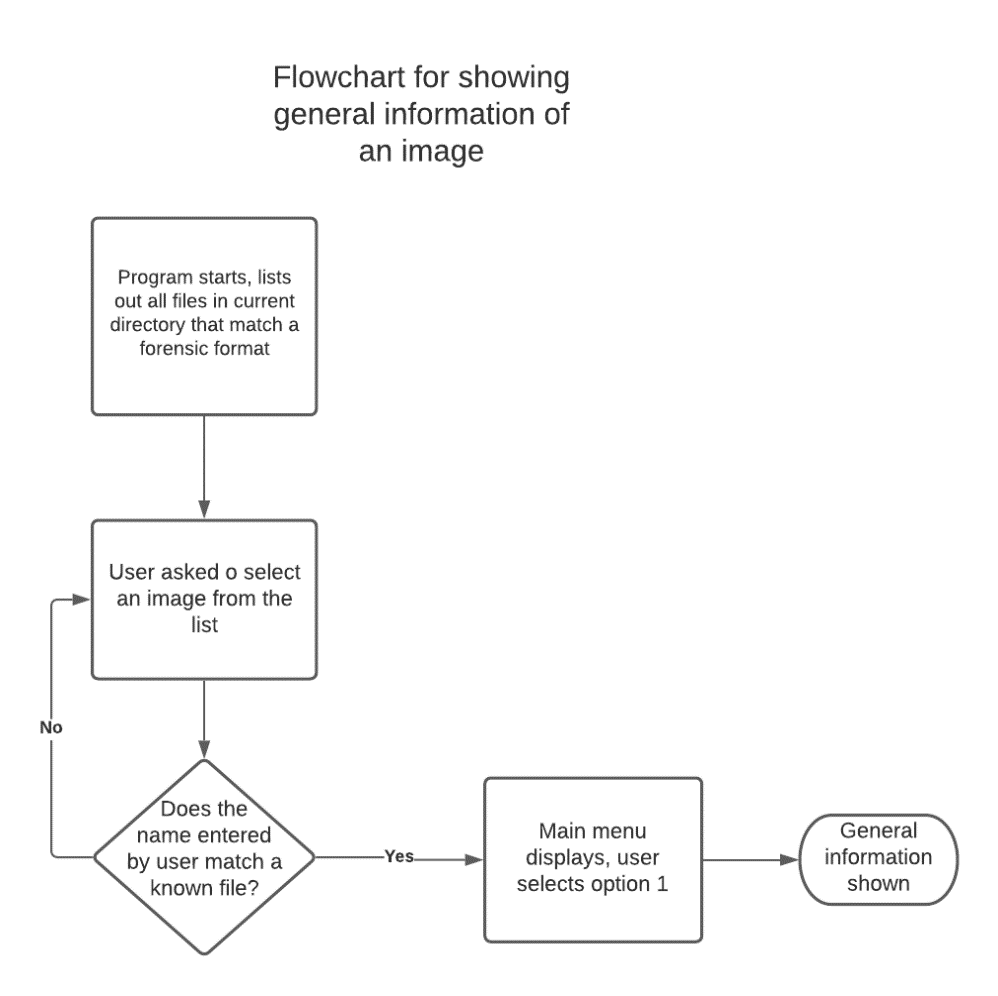
Exif\_reader is an inherited program I made that will be discussed in greater detail below. Its primary function is to accept the name of a file and return EXIF tags that I deemed forensically significant.

# Section3: GUI design

# Section 4: GUI implementation & explanation

# Section 5: Supporting files

# Section 6: Flowcharts



This flowchart shows the process of showing general information about the image like its name, size, cluster count and unallocated space. It comprises of 5 steps.

This is a larger flowchart; it shows the process of going from the main menu to viewing file metadata from a user selected file.

Diagram

Description automatically generated

# Section 7: Testing