BIRZEIT UNIVERSITY

File Carving Tool
ASSIGNMENT 2: USING JAVA AND JAVAFX

Sondos Aabed | 1190652

Digital Forensics Analysis COMP438 | Section 1
Department Of Computer Science
Dr. Mohammad AlKhanafseh

This report was written for the Digital Forensics Analysis coursework, specifically the second assignment.

Contents

Motive and Overview

This project aims to develop a File carving Tool. To allow users to perform file fragmentation, hashing, and reconstructing the file. The project is implemented in java.

This report documents the development process of this project, it contains 4 parts. The first part is concerned with image creation and file choosing. Part two is about searching the file using its signature. Part 3, is about fragmentations and hashing of each of the files. Finally, a suggestion for enhancement is made.

Technologies used

Following, the technologies used to develop this project are explained, those include Java projects and the JavaFX library.

Java Project

This project was created as a Java project configured using JDK 20 and compiler 20.

The following packages were created as shown below. The control package contains controllers. The visualization package contains the scene classes. The model class contains the objects model. Finally, the resources package contains all the images which were retrieved from the flat Icon website. (Flat Icon, 2023)

Figure (1): Project Architecture (packages)
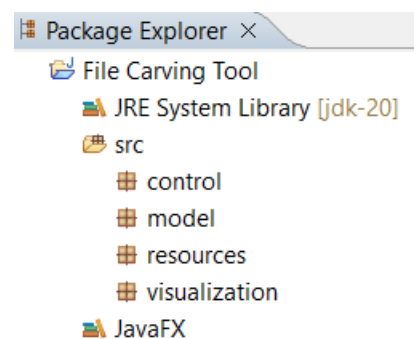
JavaFX Library

The JavaFX was used to develop the graphical user interface (GUI). The latest version is used 21 –ea +23.

Error Handling

Whenever there is an exception caught on the program the Alert box Scene is shown to the user with the message of the cause of the error. For example, the warning shown in the image below shows when the user didn't choose their directory yet.
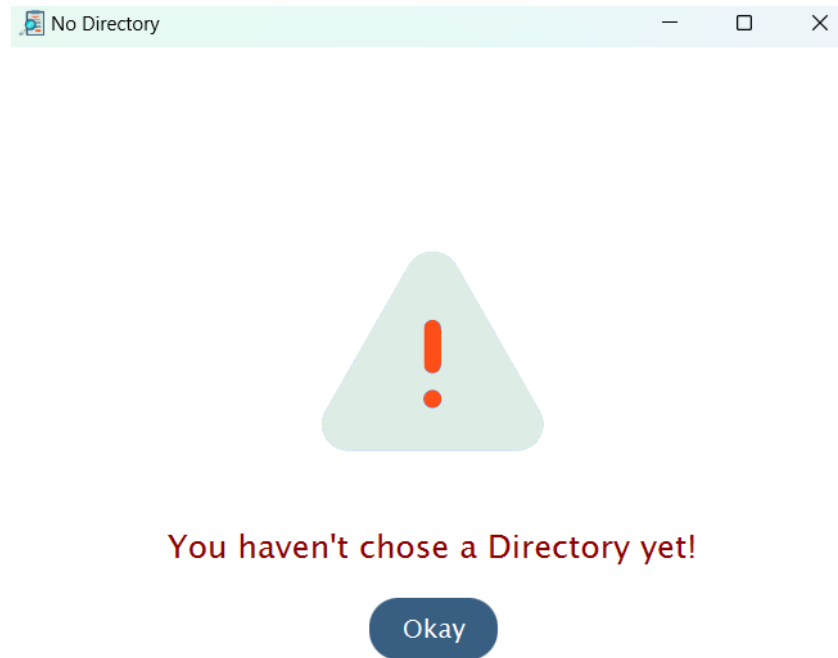

Figure (2): Warning Scene

So let's say the user wants to use this directory to be the forensic image and the target file will be "target file.docx" as preferred. This directory was prepared to test the application since it has different file types and data.

Figure (3): My Directory

Image creation

In the image creation part, the image creation process is presented.

The project allows the user to choose a file and makes an image of its directory. The below image shows the first scene of the project where the user is asked to browse for the file to make an image of its directory:
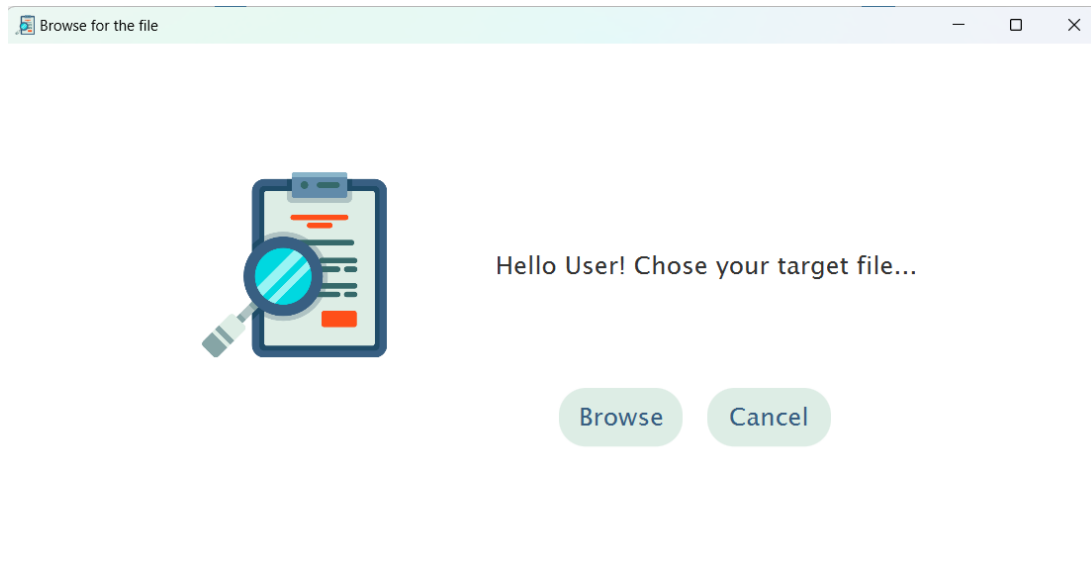
Figure (4): browse scene

After the user selects their file, they are asked to choose the directory that they want to save the image in using the browse file as shown n figure 5:
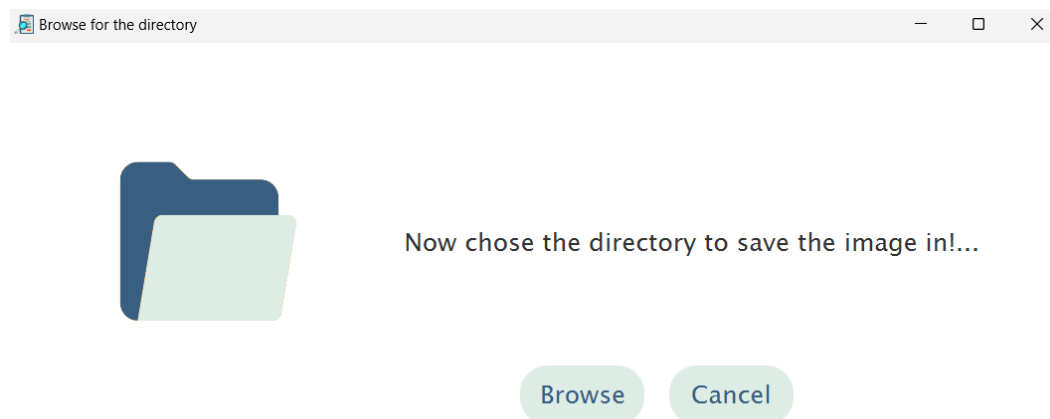
Figure (5): browse scene

Let's create a new folder call it "case1" to be used all along this report.
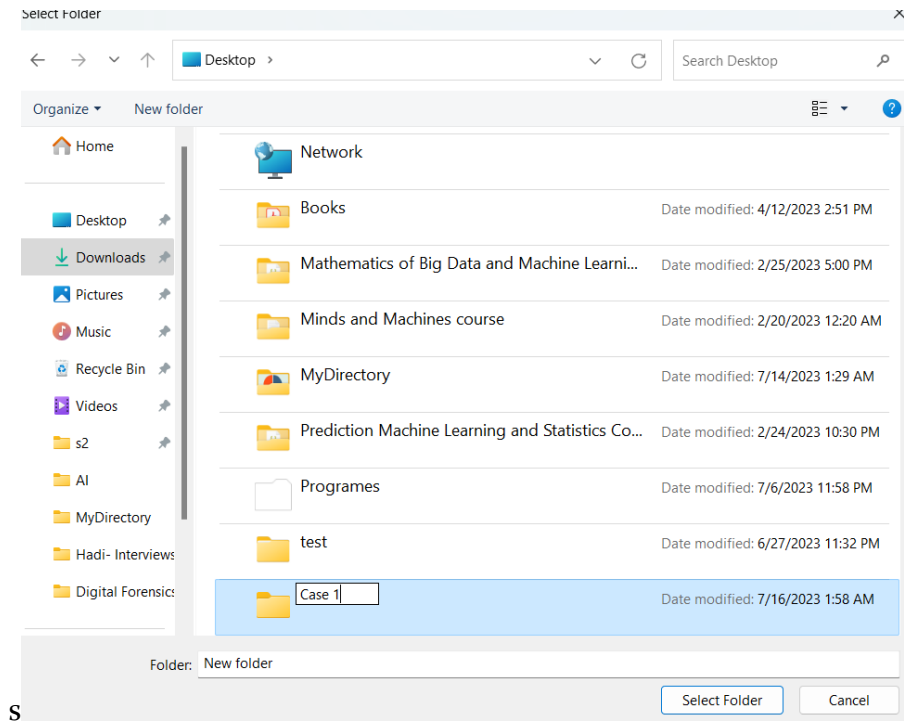
Figure (6): Create a new folder for the case

In the case file, create an image directory to be used for the digital forensics imahe
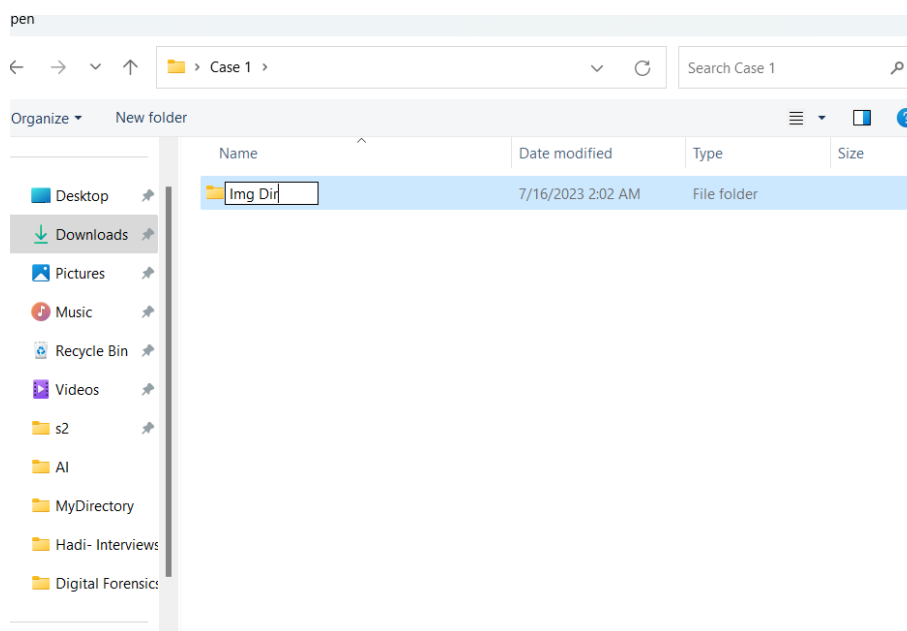
Figure (7): Create an new folder for the image directory

Now that the user has created their image successfully, they are notified to either to make editing on their file or just keep it as it is. As the following scene shows in figure 8:
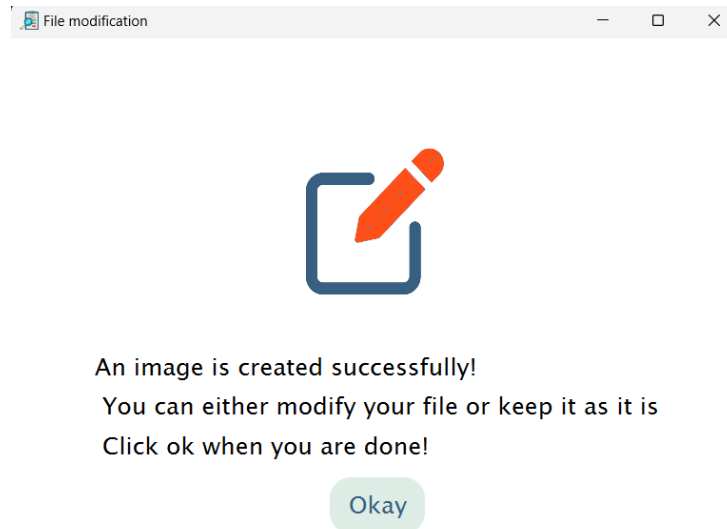
Figure (8): Edit your file or not

Let's check the image directory folder to see the image created:

Figure (9): Image copied

Afterward, the home scene is shown for them to choose what they want to do with their file and directory:
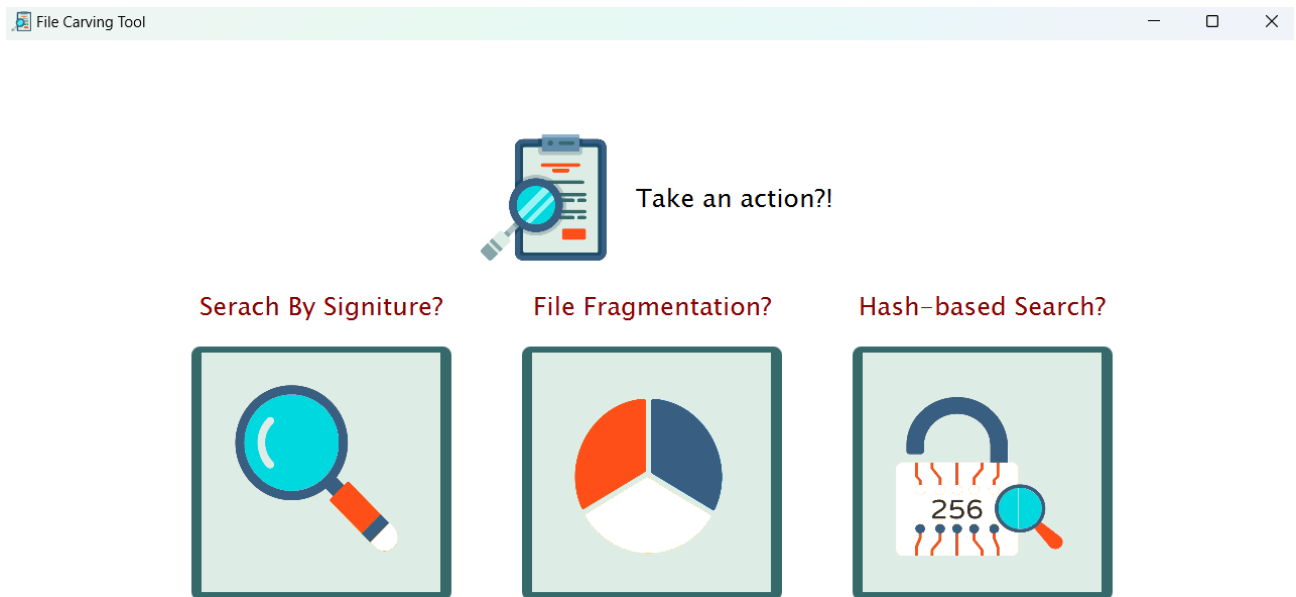
Figure (10): Home Scene

Each of these buttons performs different functionalities as required:

- **Search by signature?**
- **File fragmentation?**
- **Hash-based Search?**

Part one

In this part, the search by header functionality is presented.

File Search

The user enters the file signature manually.
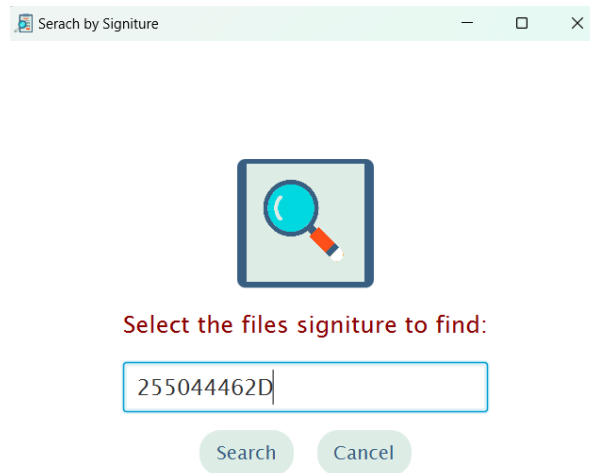
Figure (11): Search Scene

Now that the user have entered their signature and clicked search, a table view of the results is shown to them as shown in figure 8:
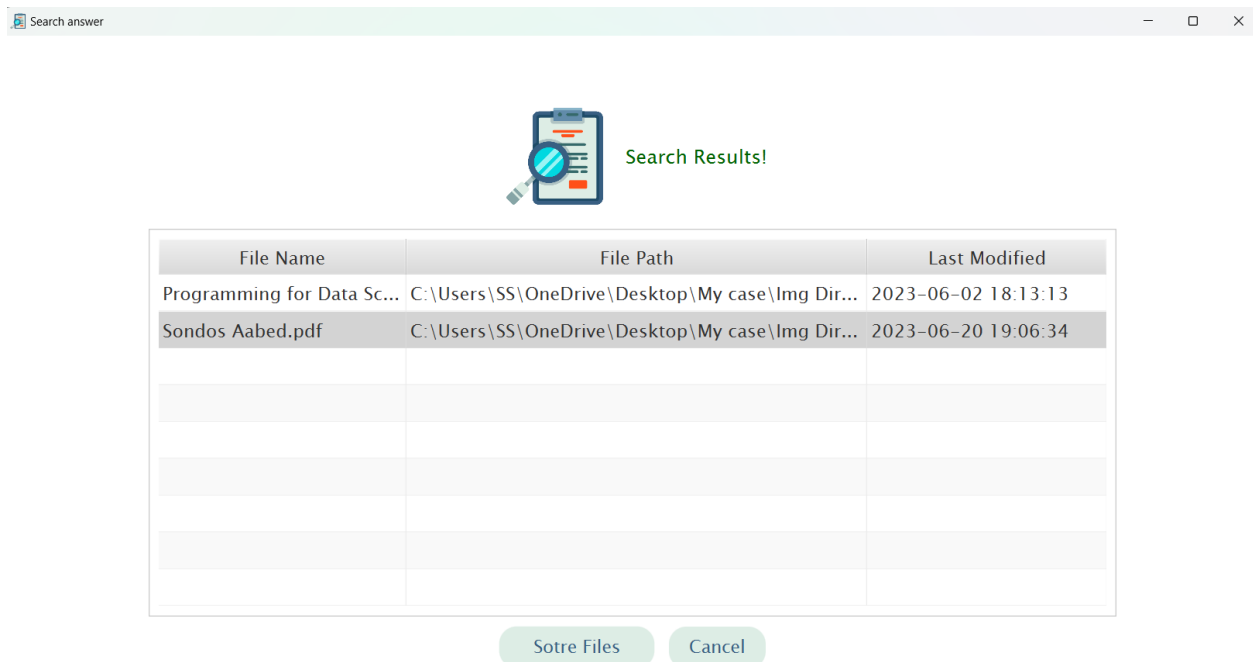
Figure (12): List of retrieved files

As shown in the previous image, the users have the option to store the retrieved files of the search process. When the user clicks Store files they are asked to choose the directory to save their works.
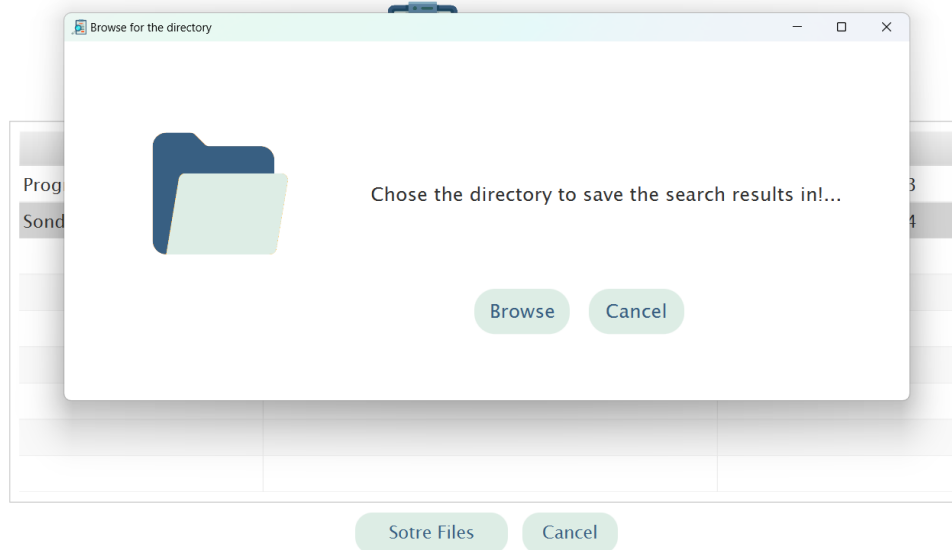
Figure (13): Directory chooser

If the storing went successfully they are shown this scene:
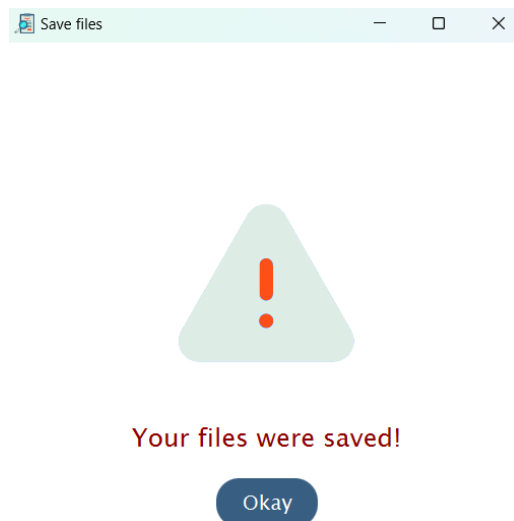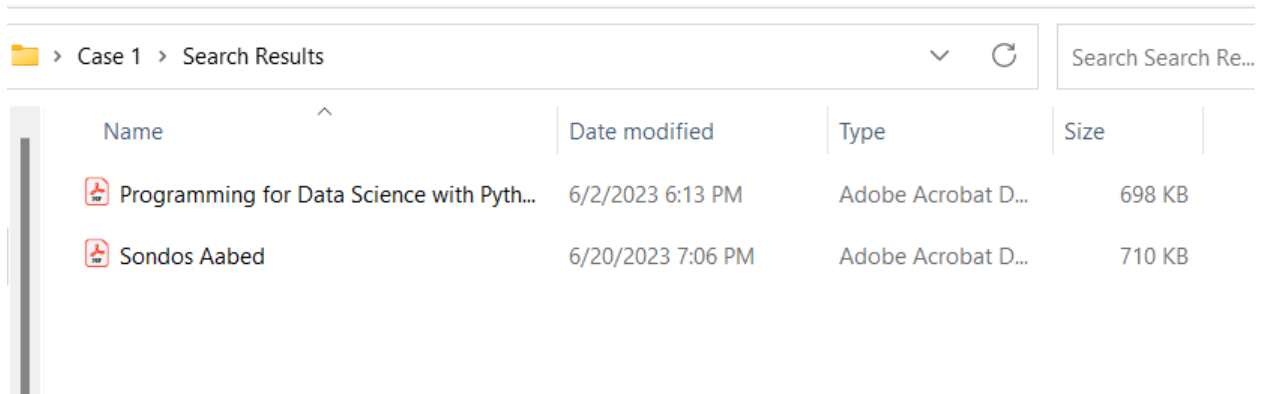
Figure (14): Search results

Now let's check the directory that was chosen to see if the search saving functions or not

Figure (10): Storing the search files

Otherwise, if there were no files found the user will get this message
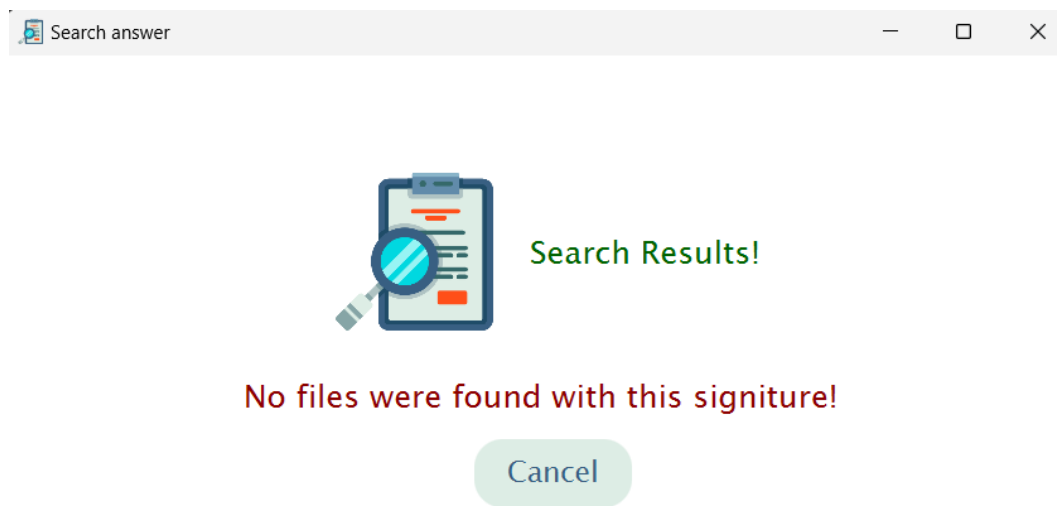
Figure (11): No file was found

Part two

In this chapter. The fragmentation, hashing and hash-based search is presented.

Fragmentation

When the fragmentation action is taken the user is shown this scene where they can chose how many fragments they want to make on their target file.
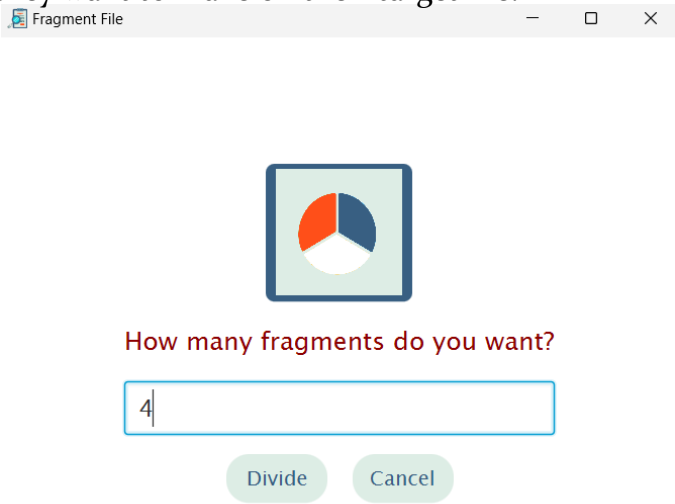
Figure (12): Number of fragments

After they click divide the table view shows them information about the fragments:

Fragment #	Size in Bytes	Hash Value
1	46080	fc2b5b3437a4b883067c7088601b2a59
2	46080	c419f52ce8f909fd06ec346a9eefc100
3	46080	7babb43752fa4e04a0a1cd52b95d6649
4	42933	c638f5f1a1e98bed45f2ec4a3d961f7f
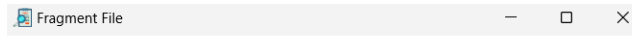
Figure (13): Number of fragments

Hash-Based Search

In this functionality, the user is asked first to define the number of fragments they want:
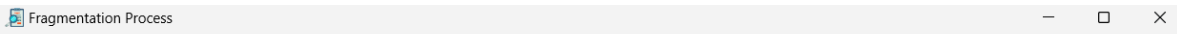
Figure (14): Define the Number of fragments

After they chose 4, a signature-based search is conducted of the target file signature which is DOCX preferably and the search results are fragmented each fragment is then compared with the hash of the original file and matched and shown.

Hash–Based Search Results!

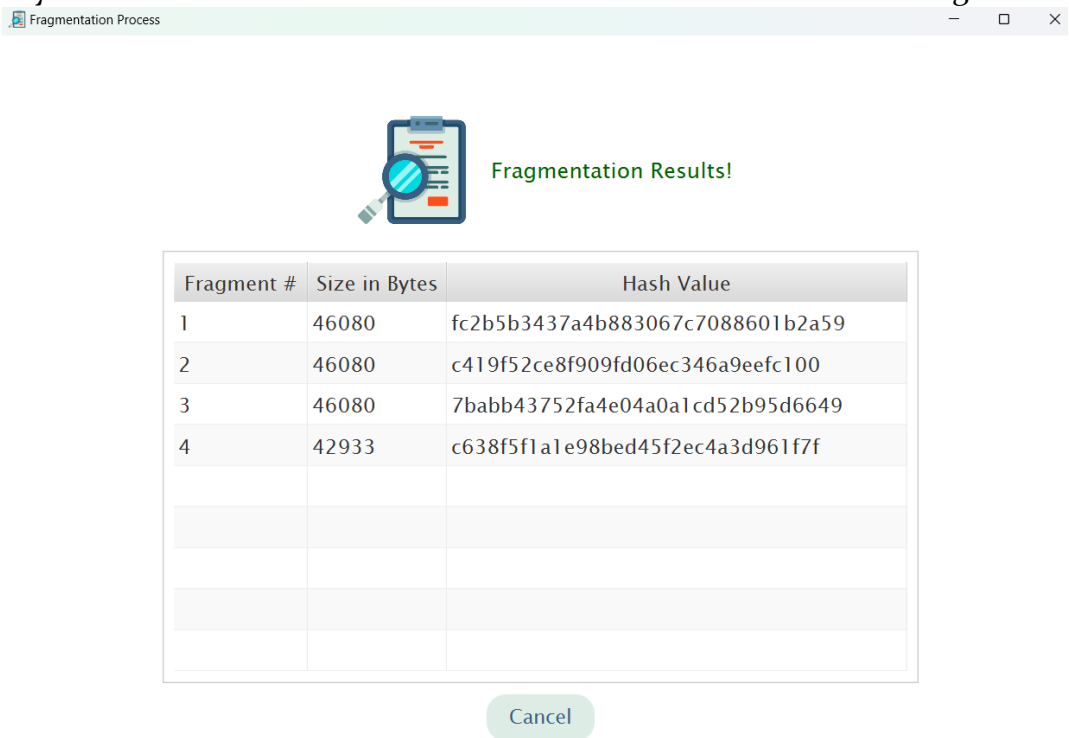| Fragme...	Original File Hash	Search Result File H...	Match
1	fc2b5b3437a4b88306	20baddcb8e0cdf1bbd	Not Matched
1	fc2b5b3437a4b88306	c006dc535ed7e74b9a	Not Matched
1	fc2b5b3437a4b88306	b592918847642cb...	Not Matched
2	c419f52ce8f909fd06	fc2b5b3437a4b88306	Not Matched
2	c419f52ce8f909fd06	c419f52ce8f909fd06	Match
2	c419f52ce8f909fd06	7babb43752fa4e04a0	Not Matched
2	c419f52ce8f909fd06	c638f5f1a1e98bed45	Not Matched
2	c419f52ce8f909fd06	fc2b5b3437a4b88306	Not Matched
2	c419f52ce8f909fd06	c419f52ce8f909fd06	Match

Figure (15): Hash-Based Search

The users are also able to click on File Reconstruction to reconstruct the file if each of the fragments of the target file has found a match on the hash based search. They are able to choose the directory that they want to their file to be reconstructed in.
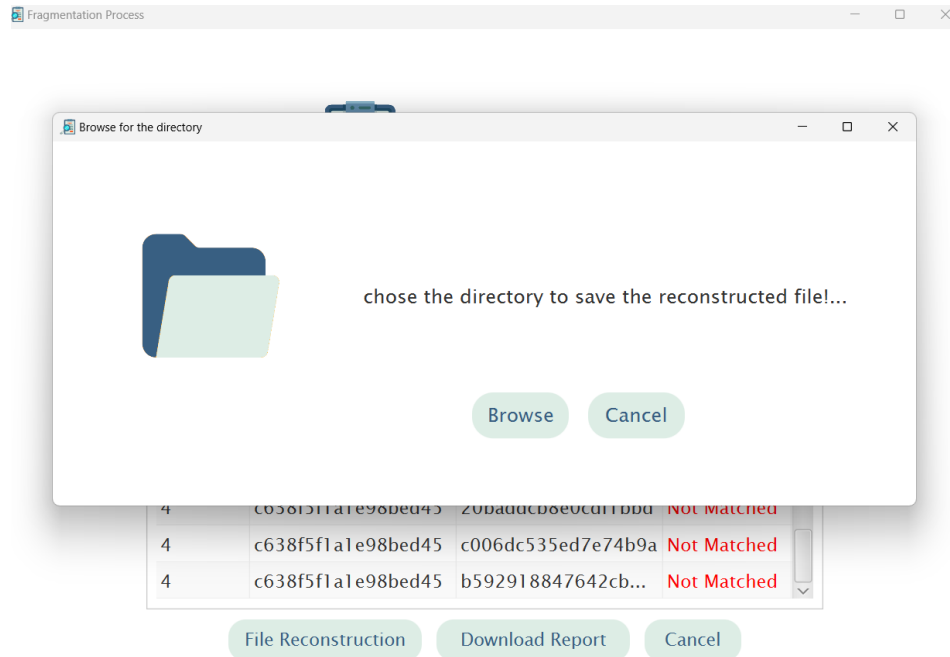
Figure (16): Hash-Based Search

If the file was successfully constructed the user then are shown the following scene:
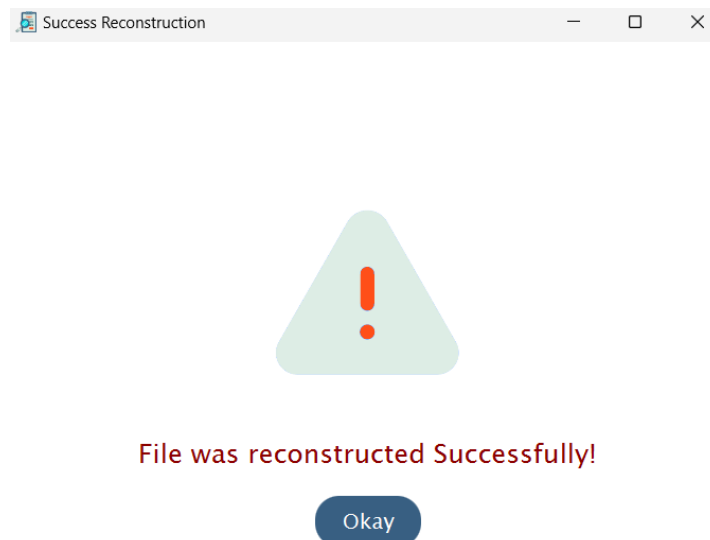
Figure (17): Hash-Based Search

The file is shown in the directory chosen as shown in the following figure:
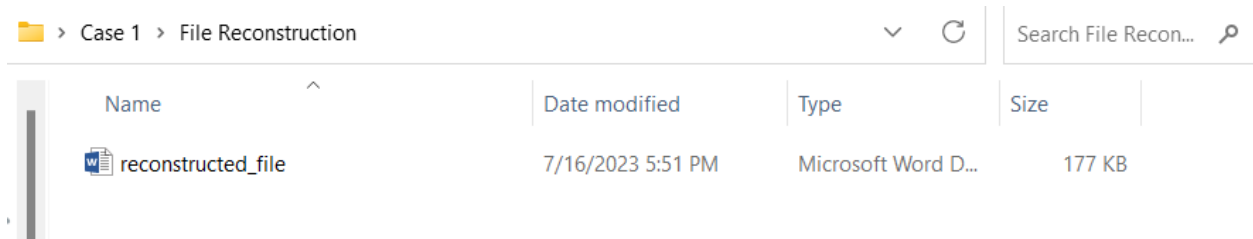
Figure (18): the reconstructed file

Now let's see and open the file to check if it was successfully reconstructed
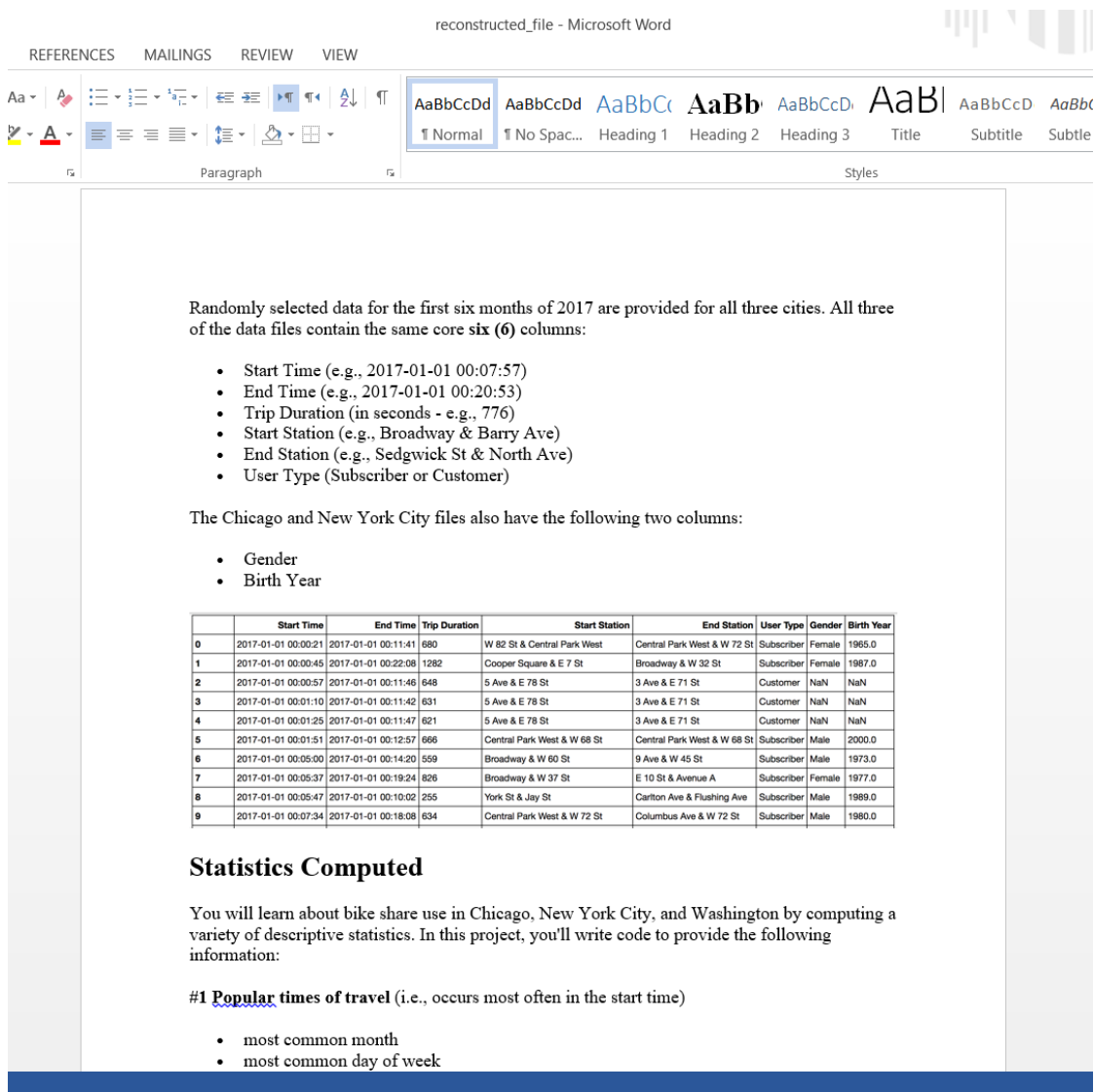
Figure (19): the reconstructed file

The users are able to click on the download report button so that they can get the generated report of the fragmentation and the hashing and the reconstructing process. They will be asked to choose the directory they want to generate the report in.

Figure (20): Generate report of the process

If there was no problem with generating the report the program will let them know that.

Figure (21): Generate report of the process

Now checking the directory that the Report was chosen to be generated in the report file is successfully found there:

Figure (22): Generate report in the directory

report

Opening the report the user will find all the details of the hash based search


```
File Carving Information:
Original File Fragments:
- Fragment: Target File.docx_fragment_0
- Fragment: Target File.docx_fragment_1
- Fragment: Target File.docx_fragment_2
- Fragment: Target File.docx_fragment_3
*****************************************
Fragment Match Data:
- Fragment Number: 1
  Original File Hash: fc2b5b3437a4b88306
  Search Result File Hash: fc2b5b3437a4b88306
  Match or not: true

- Fragment Number: 1
  Original File Hash: fc2b5b3437a4b88306
  Search Result File Hash: c419f52ce8f909fd06
  Match or not: false

- Fragment Number: 1
  Original File Hash: fc2b5b3437a4b88306
  Search Result File Hash: 7babb43752fa4e04a0
  Match or not: false

- Fragment Number: 1
  Original File Hash: fc2b5b3437a4b88306
  Search Result File Hash: c638f5f1a1e98bed45
  Match or not: false

Fragment Number: 1
```
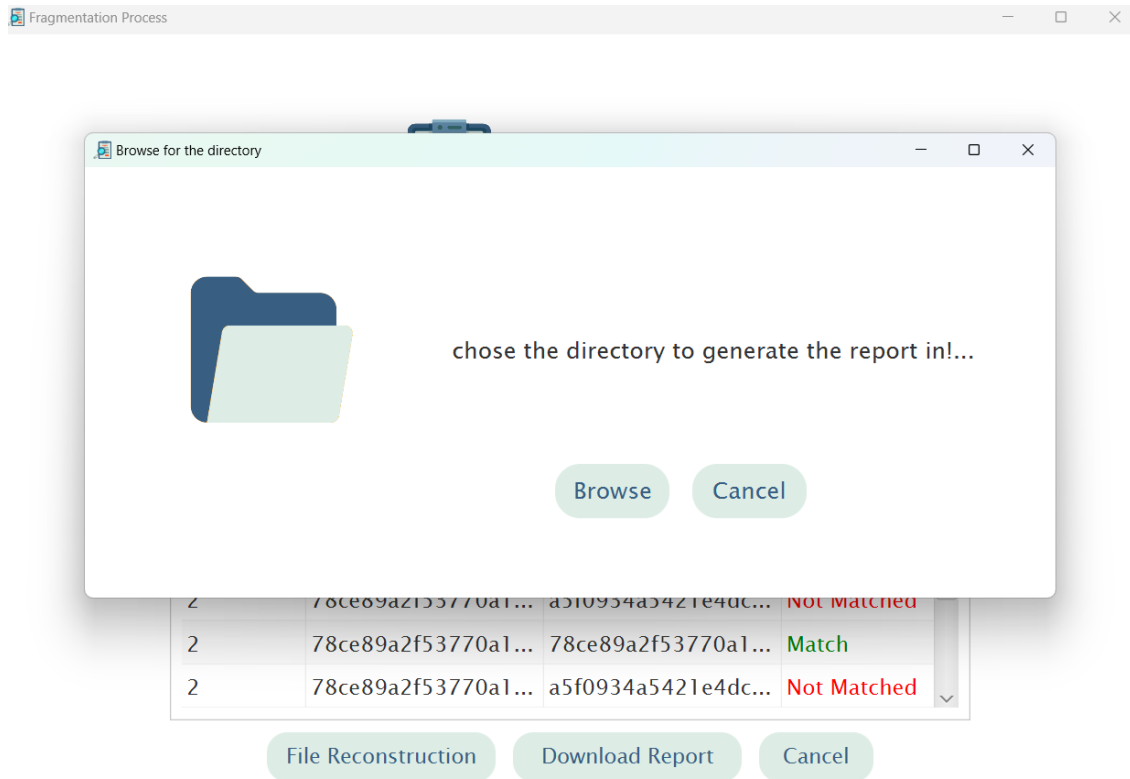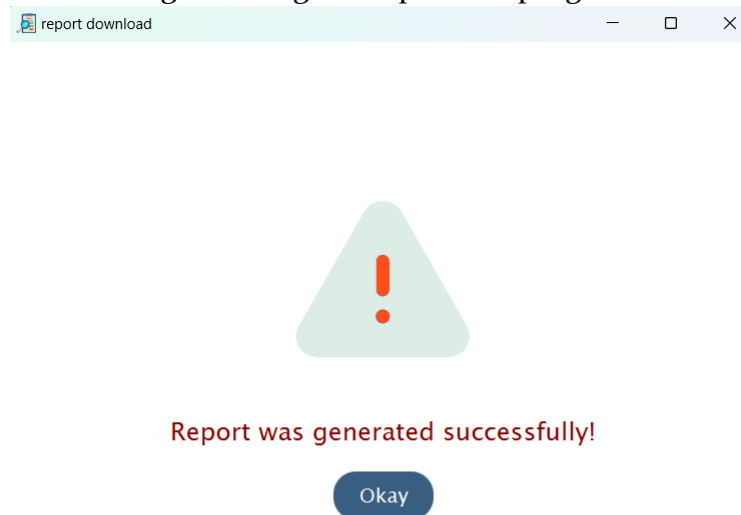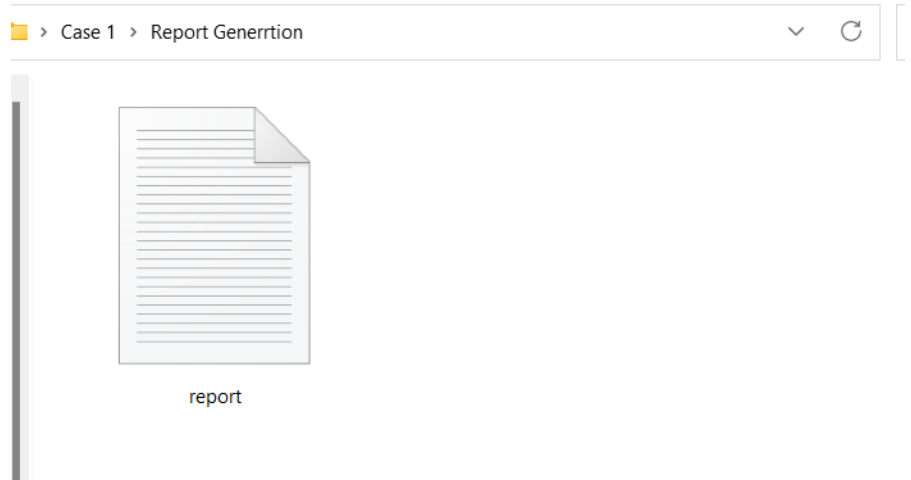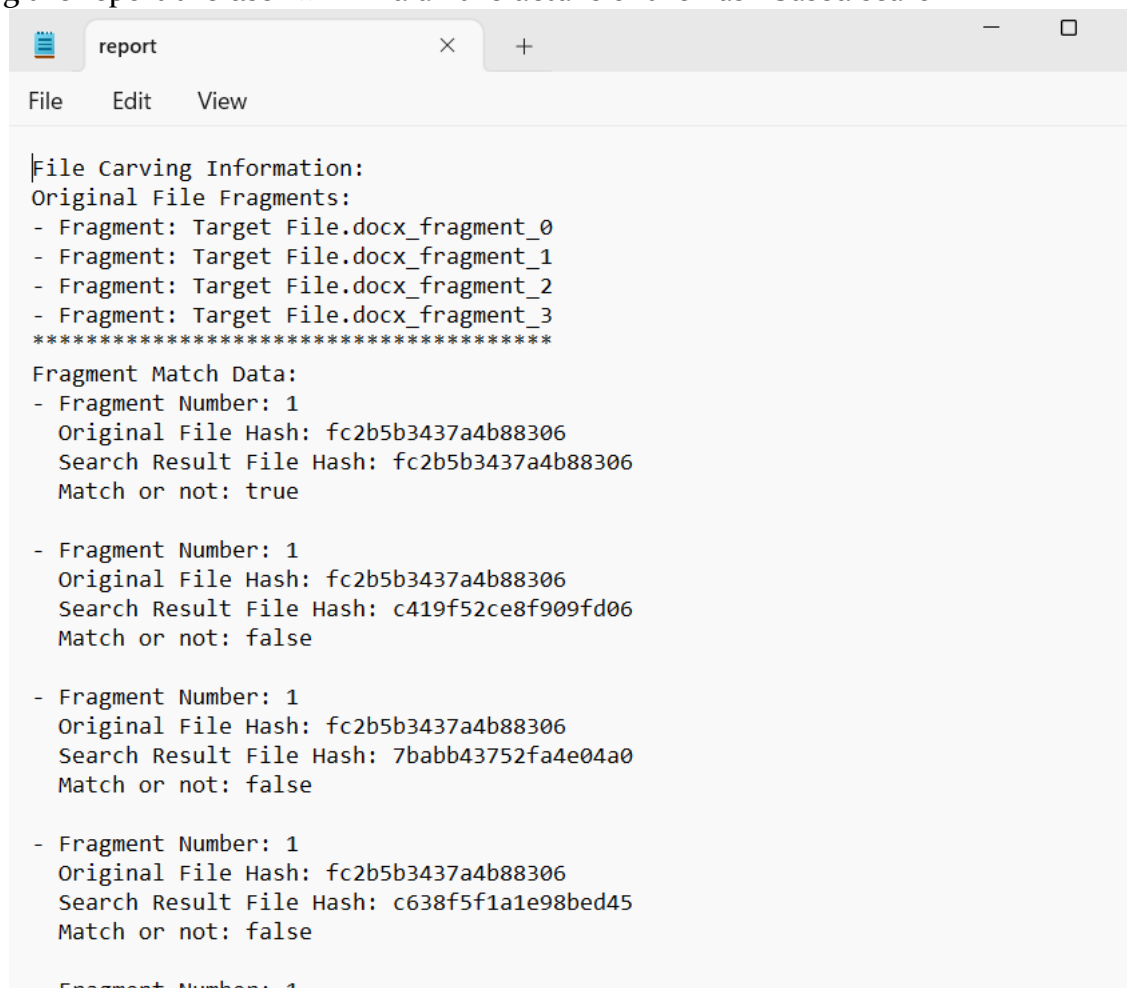
Figure (23): Generate report in the directory

Part 3

Enhancement Suggestion

In conclusion, "Java has been criticized by many online security experts, who have said it is vulnerable to hackers." So an enhancement suggesting might be not using Java for a digital forensics environment specifically that the digital forensics environment must be robust against any hacker or danger.

References

https://www.baeldung.com/java-copy-file

https://www.baeldung.com/sha-256-hashing-java

https://docs.oracle.com/javase/tutorial/essential/io/bytestreams.html

https://www.forensicfocus.com/forums/general/java-in-forensic-computing/

https://www.bbc.com/news/technology-35427685

https://www.tripwire.com/state-of-security/the-upcoming-death-of-the-java-plugin-has-been-announced-no-flowers-please