Assignment# 1

Digital forensics

Ahmad Abdullah Mujhaid i221609

2024

Contents

[Introduction 2](#_Toc176382369)

[Details and Steps 2](#_Toc176382370)

[Project 1 2](#_Toc176382371)

[Project 2 3](#_Toc176382372)

[Project 3 4](#_Toc176382373)

[Project 4 5](#_Toc176382374)

[Project 5 6](#_Toc176382375)

[Project 6 7](#_Toc176382376)

[Summary 10](#_Toc176382377)

[References 10](#_Toc176382378)

# Introduction

This assignment is based on the Forensics Tool ‘Autopsy’ used to analyze images of hard drives, USB etc. We are using the book “Guide To Computer Forensics” and practising its exercises given at the end of chapter 1 excluding the cases.

# Details and Steps

In this section, I have noted all the steps I performed to solve the project and find the necessary evidence.

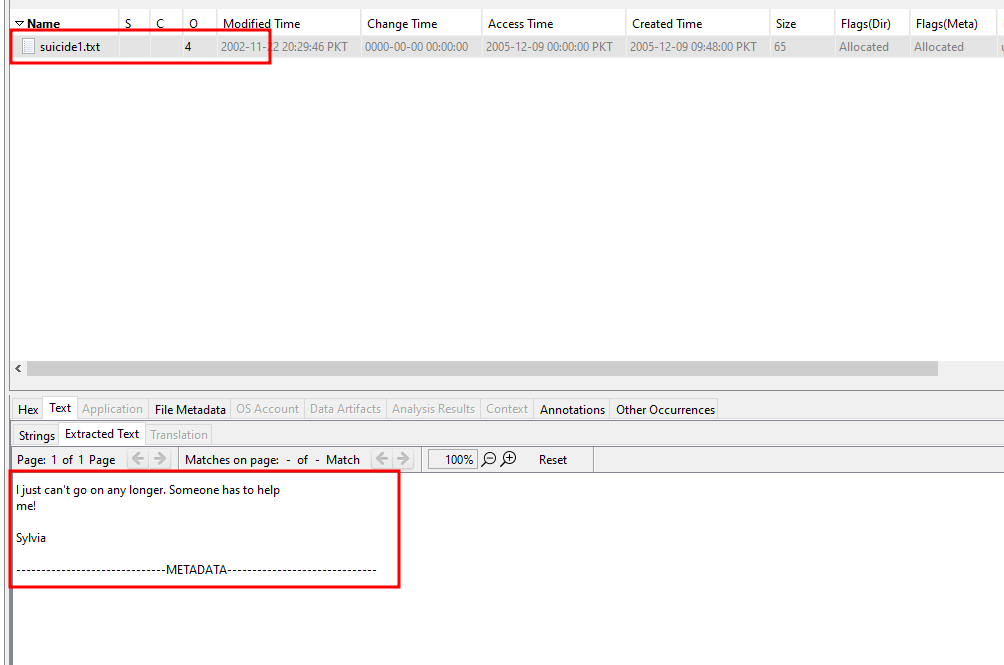
## Project 1

Just as guided in the book which was actually pretty easy to follow I opened the first Project file which looked like this.

A screenshot of a computer

Description automatically generated

It was surprising to use Autopsy with so much ease. The UI is pretty much self-explanatory so I didn’t need to follow the steps given in the book to come across this text file which had a ‘suicide.txt’. This is proof that Joshua’s girlfriend killed herself in this heartbreaking note.



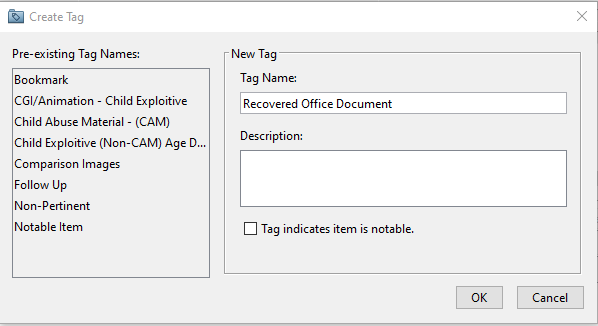
## Project 2

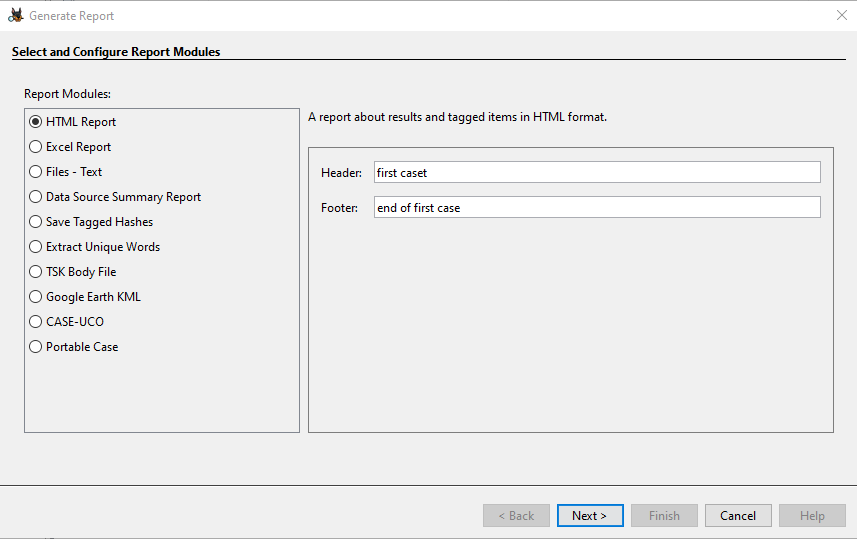
For this project, we simply needed to search the word ‘confidential’ in the keyword search on the upper right corner and we were given files that contained the instance of the word ‘confidential’.

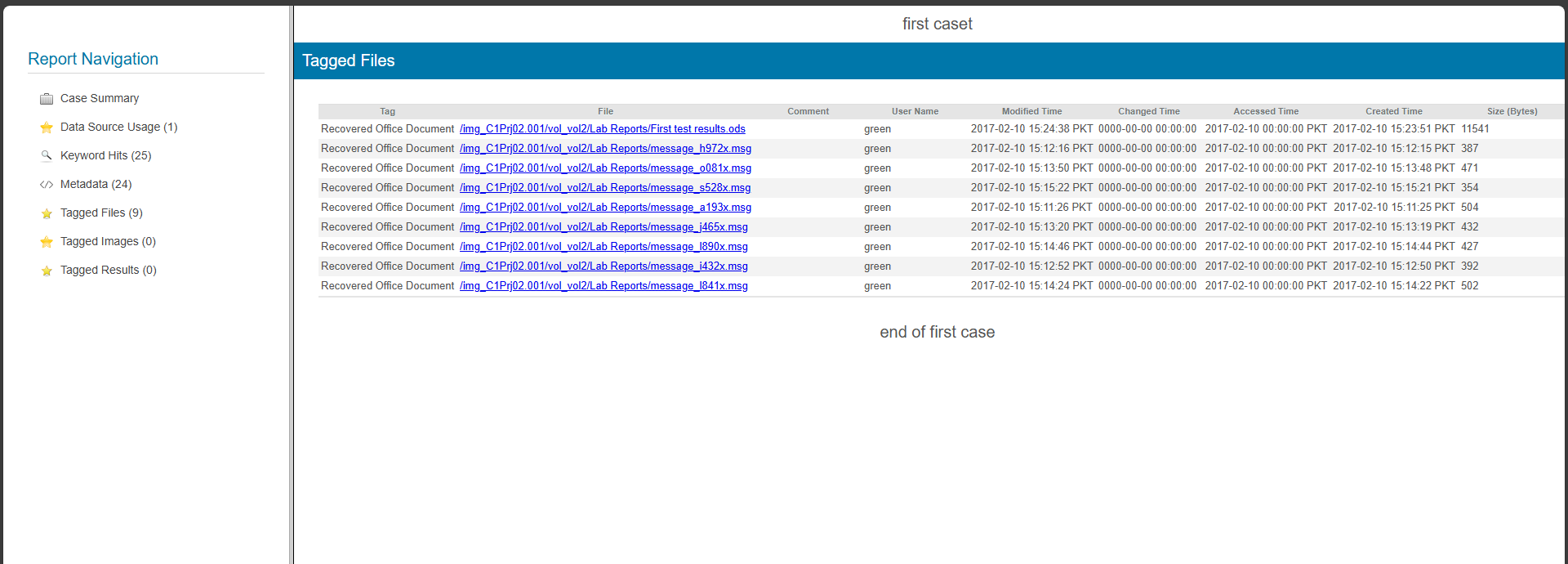
A screenshot of a computer

Description automatically generated

After that, we need to make a new tag named ‘Recovered Office Document’ so we are able to find it easily in the report generated by Autopsy.

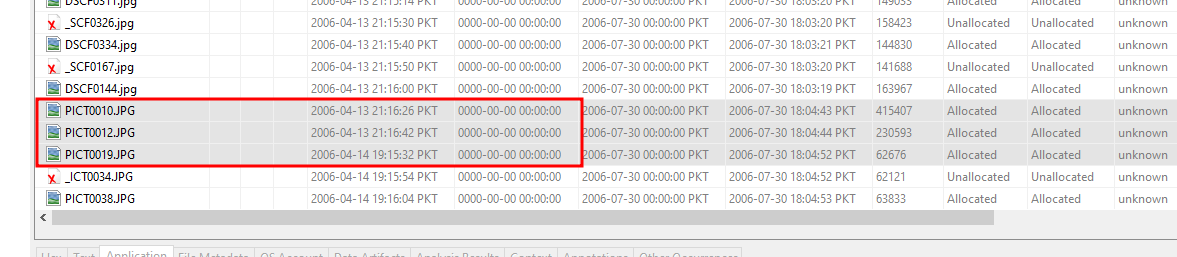




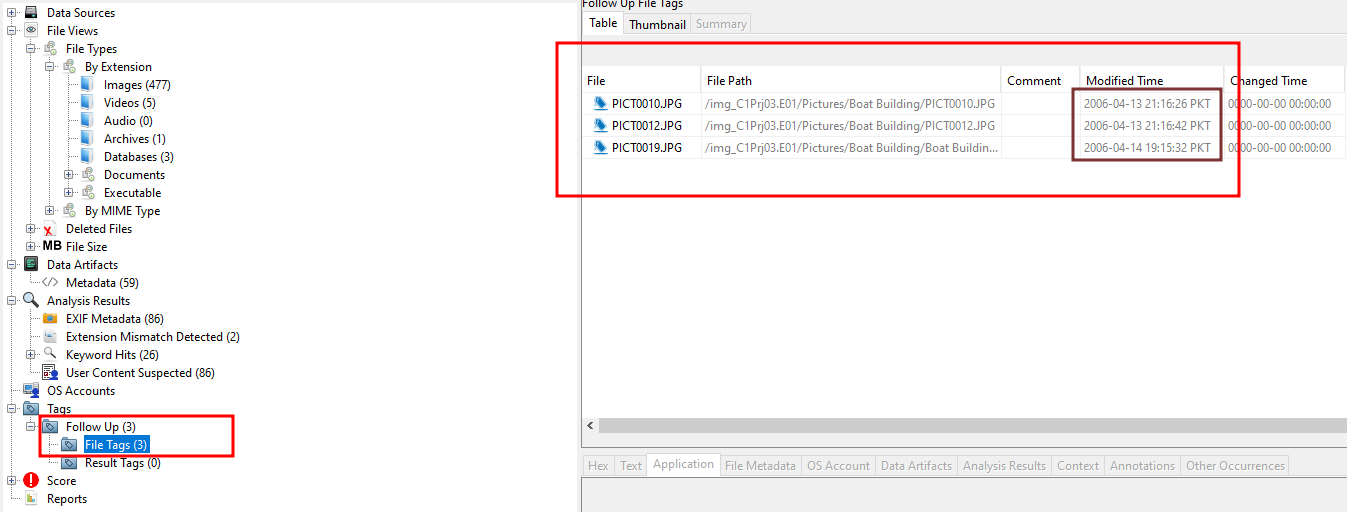


## Project 3

This project required us to find proof that Ralph Williams illegally used confidential files from his previous company to get a job in his next company. All we needed to was sort the dates and look for boat images for April 2006. We found 3 images showing the design of the boats which proved that Ralph did use the images for his personal benefit.

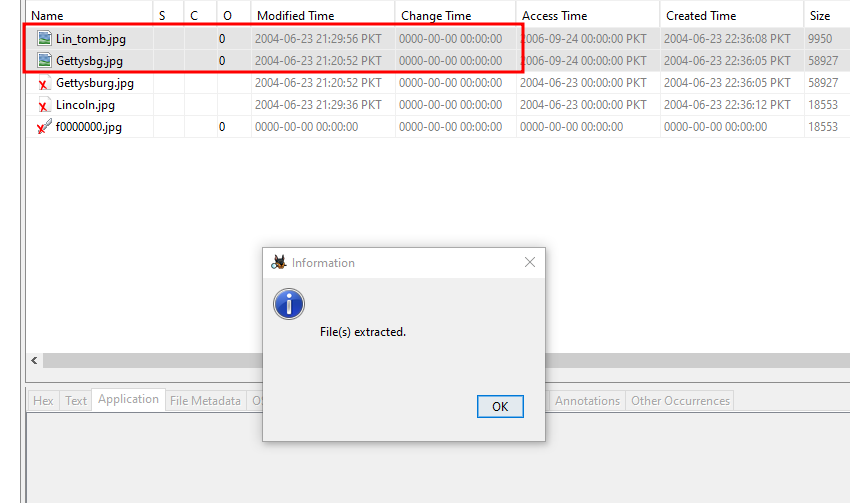


Next, we added the tag to easily find them without looking for them again.



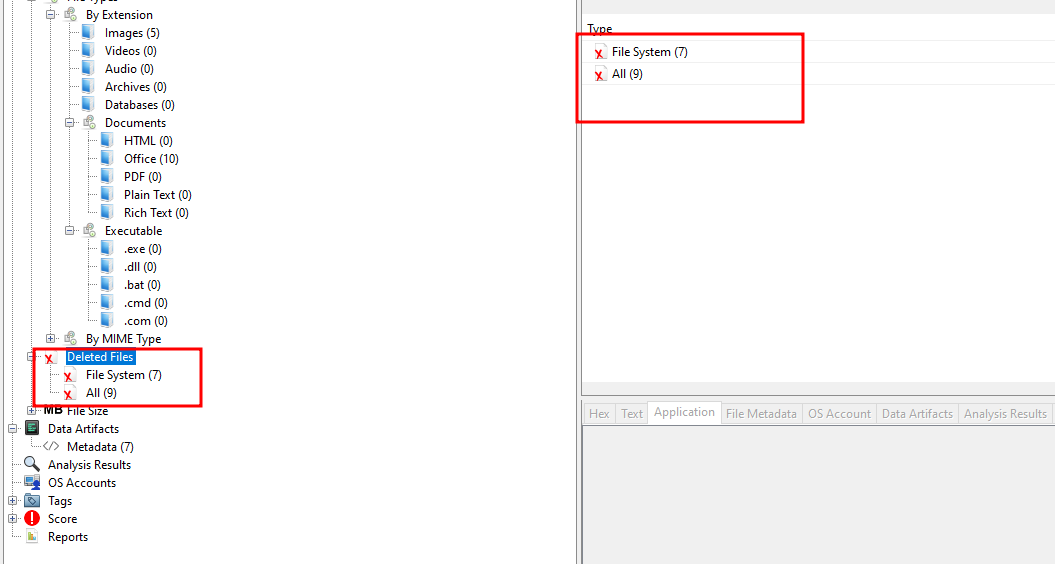
## Project 4

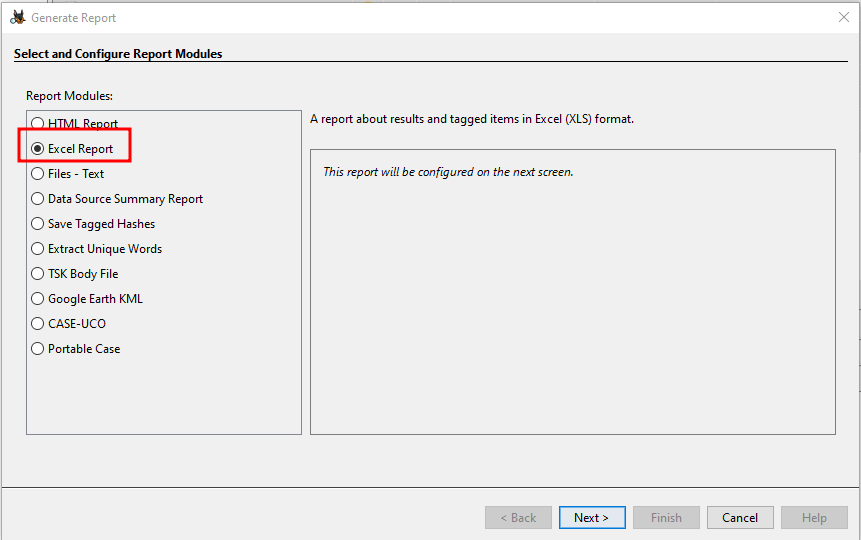
We extracted 2 images after sorting the files via the extension. We left the rest because they were deleted and in some countries it is not allowed by law to access deleted files without warrant.



## Project 5

We got the Warrant! Remember when we left deleted files and only extracted allocated(not deleted) files? Yeah, we got a warrant to analyze the deleted files. So, now we will analyze them and then generate a report of it.

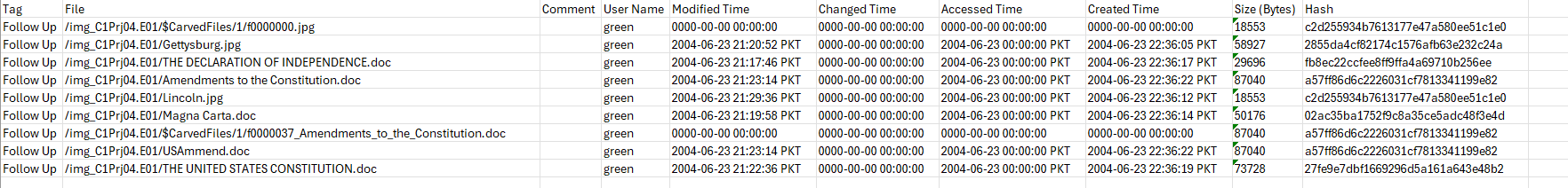




Checking “All Tagged Results” so that only the important things that we tagged are included in the report.

A screenshot of a computer

Description automatically generated



## Project 6

This project asks us to make a personalized search list by going to keyword list on top right and then clicking Manage Lists.

A close-up of a computer screen

Description automatically generated

A screenshot of a computer

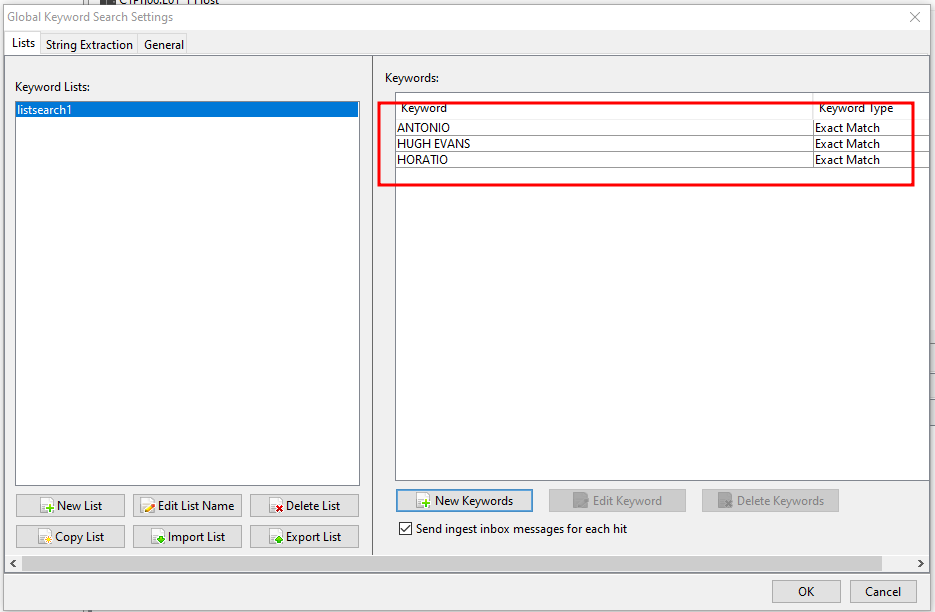
Description automatically generated

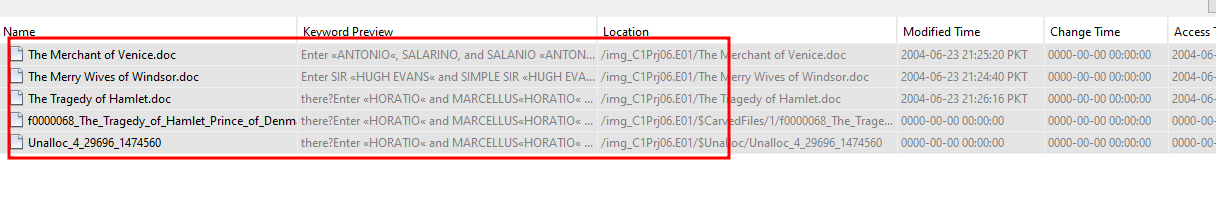
Next is clicking ‘New List’ and giving a name to your search list. After that, we need to add all the search words that we need to filter from the files on the right under keywords pane and then click ‘ok’.

A screenshot of a computer

Description automatically generated

Then we need to open keyword list again and select the personalized keyword list and then all the files with the keywords will be filtered.





A screenshot of a computer

Description automatically generated

# Summary

In conclusion, Autopsy is a very versatile utility to not only analyze an image for forensics purposes but also make it easy to analyze the files to find evidence such as Autopsy separates the files by extension. And after all the searching Autopsy also helps in generating report in more than one format.

# References

1. [Guide to computer forensics and investigations : processing digital evidence : Nelson, Bill, author : Free Download, Borrow, and Streaming : Internet Archive](https://archive.org/details/guidetocomputerf0005nels)
2. [Autopsy User Documentation: Autopsy User's Guide (sleuthkit.org)](https://sleuthkit.org/autopsy/docs/user-docs/4.21.0/)
3. [Cybersecurity Autopsy: Unveiling Digital Forensics (ccslearningacademy.com)](https://www.ccslearningacademy.com/what-is-autopsy-in-cybersecurity/)