



CY2002

Digital Forensics

Assignment 01 **Hands-On Projects**

Submitted by: Abdul Sami Qasim

Roll number: 22I-1725

Date: 30th August 2024

Table of Contents

• Introduction	4
• Details and Steps	4
Project 1-1.....	4
Statement:	4
Task 1:	4
Task 2:	4
Task 3:	5
Task 4:	5
Task 5:	6
Task 6:	6
Task 7:	7
Task 8:	7
Project 1-2.....	7
Statement:	7
Task 1:	7
Task 2:	8
Task 3:	8
Task 4:	8
Task 5:	9
Task 6:	9
Task 7:	9
Task 8:	11
Task 9:	11
Task 10:	12
Task 11:	12
Project 1-3.....	12
Statement:	12
Task 1:	13
Task 2:	13
Task 3:	13
Task 4:	14
Task 5:	14
Task 6:	15

Task 7:	15
Task 8:	15
Task 9:	17
Task 10:	17
Task 11:	17
Task 12:	17
Task 13:	18
Task 14:	18
Project 1-4.....	19
Statement:	19
Task 1:	19
Task 2:	19
Task 3:	20
Task 4:	20
Task 5:	20
Task 6:	21
Task 7:	21
Task 8:	21
Task 9:	21
Project 1-5.....	22
Statement:	22
Task 1:	22
Task 2:	22
Task 3:	22
Task 4:	22
Task 5:	23
Task 6:	23
Task 7:	23
Project 1-6.....	24
Statement:	24
Task 1:	24
Task 2:	24
Task 3:	24
Task 4:	25
Task 5:	25

Task 6:	26
Task 7:	26
Task 8:	26
Task 9:	27
Task 10:	27
Task 11:	27
Task 12:	28
Task 13:	28
• Summary	30
• References	30

• Introduction

This is the first assignment of our course in which we're tasked to do the 6 hands on projects given at the end of Chapter 1 from the book "Guide to Computer Forensics and Investigations: Processing Digital Evidence".

All of these projects are to be done on the software "Autopsy" which is available online (for free).

• Details and Steps

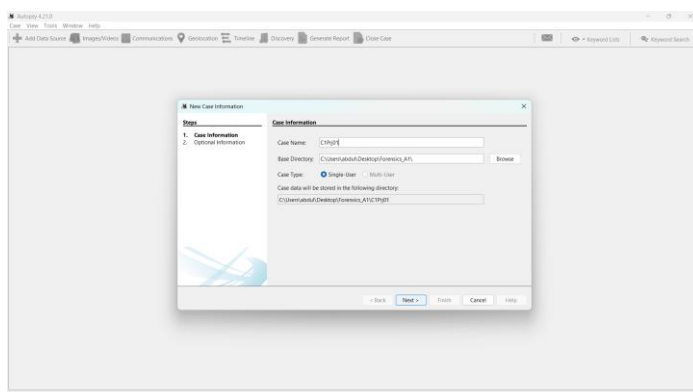
Project 1-1

Statement:

The case in this project involves a suspicious death. Joshua Zarkan found his girlfriend's dead body in her apartment and reported it. The first responding law enforcement officer seized a USB drive. A crime scene evidence technician skilled in data acquisition made an image of the USB drive with FTK Imager and named it C1Prj01.E01. Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station. You have received the image file from the detective assigned to this case. He directs you to examine it and identify any evidentiary artifacts that might relate to this case.

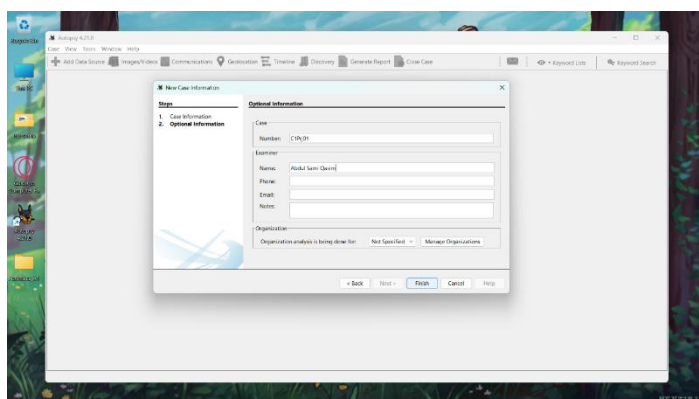
Task 1:

Entering the case name.

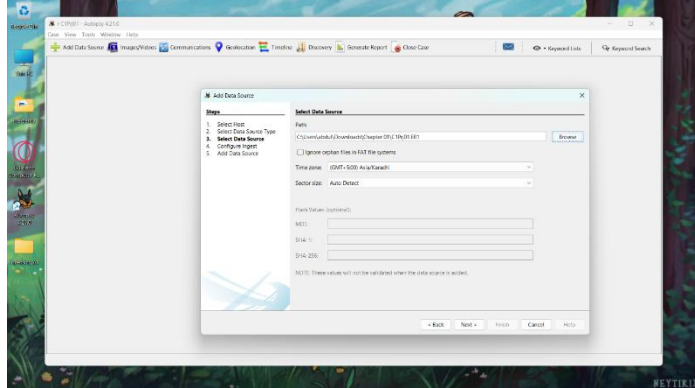
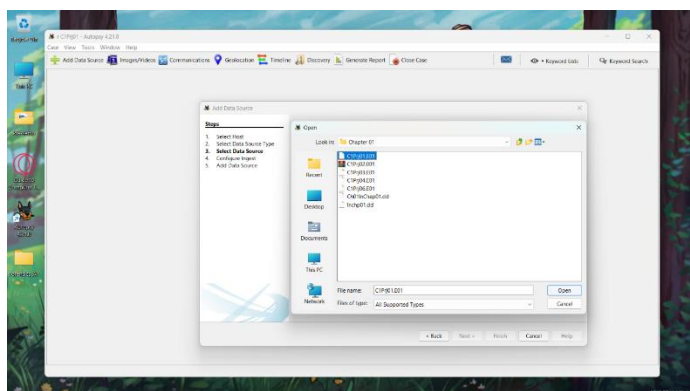
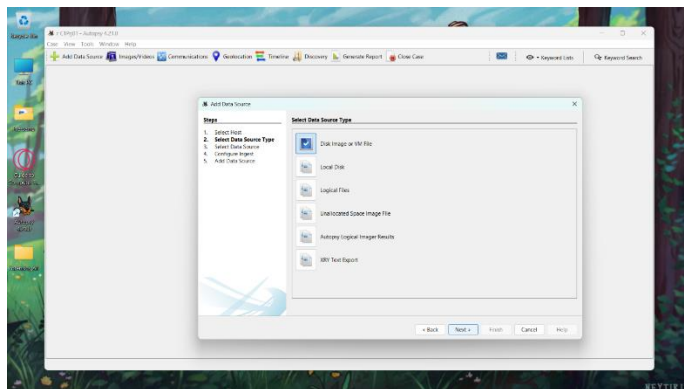


Task 2:

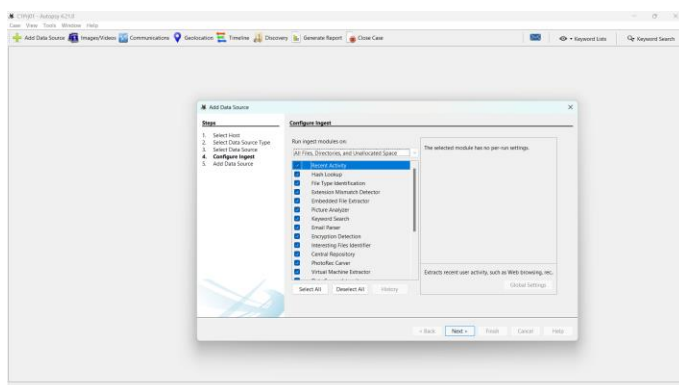
Entering the case number.



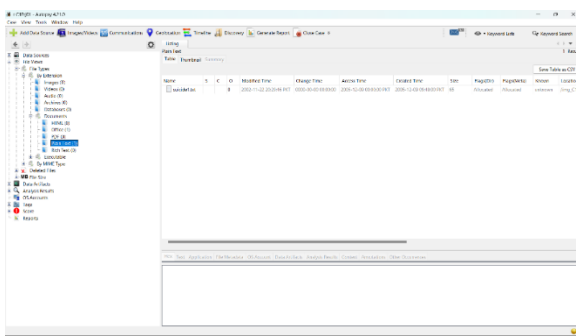
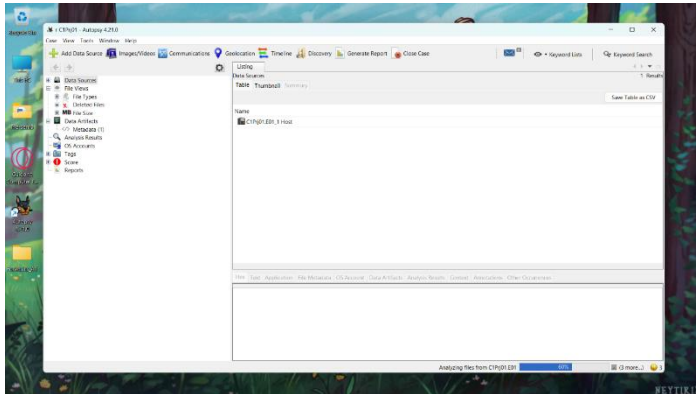
Task 3:
Selecting the disk image to be analyzed in Autopsy.



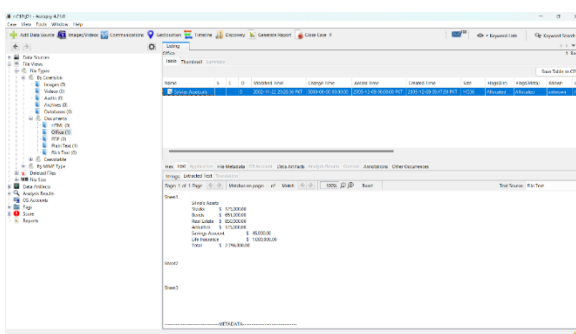
Task 4:
Configuring Ingest Modules (select all of them).

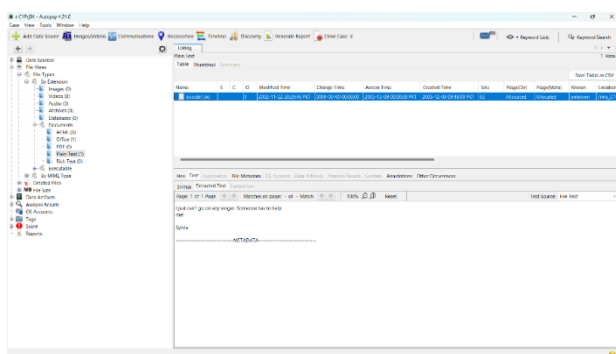


This tasks involved, opening up the documents folder. In order to do so, I at first collapsed the tree structure on the left side, then I opened up file types, by extension and that led me to the documents I needed to access.

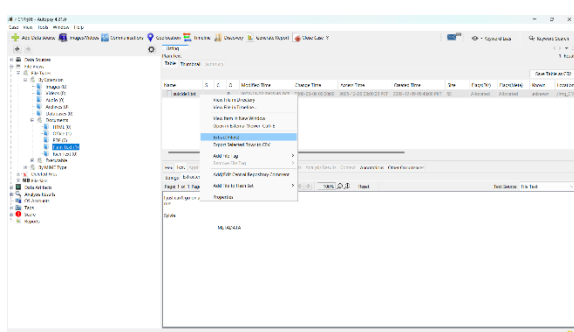


I had to analyze the files that would be of my interest in this task. So, I looked at the two documents that I could find, one was a .xls sheet and the other was a note stored in plaintext (named as suicide1.txt)





Task 7:
I extracted both the files.



Task 8:
Key findings from this case include two files, one being of sylvias assets (Sylvias Assets.xls) and the other being a suicide note (suicide1.txt), in which someone is asking for help.

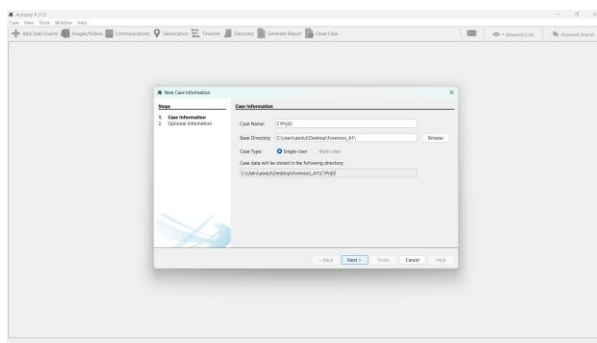
Sylvias assets reached a total of \$2,796,000.00 in which, life insurance amounts to \$1,000,000.00. Also, there are some real estate assets amounting to \$850,000.00 in the assets sheet. The person in question seems to be asking for help after that. The sheet was accessed before the suicide note, there's a difference of 1 minute and 10 seconds in the last modified time stamps of these two files.

Project 1-2

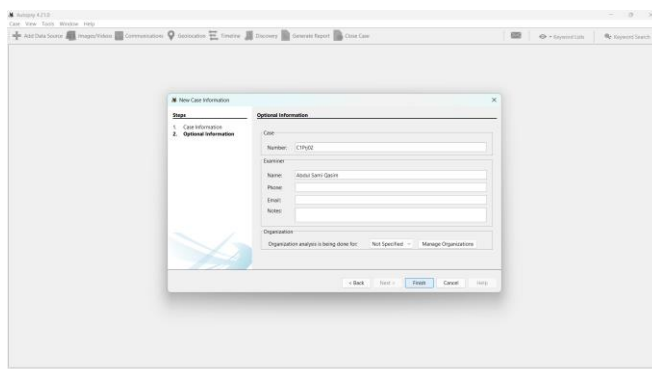
Statement:

In this project, you work for a large corporation's IT Security Department. Your duties include conducting internal digital investigations and forensics examinations on company computing systems. A paralegal from the Law Department, Ms. Jones, asks you to examine a USB drive belonging to an employee who left the company and now works for a competitor. The Law Department is concerned that the former employee might possess sensitive company data. Ms. Jones wants to know whether the USB drive contains anything relevant. In addition, she tells you that the former employee might have had access to confidential documents because a co-worker saw him accessing his manager's computer on his last day of work. These documents consist of nine files containing the word "confidential." She wants to know whether the USB's bit-stream image file has these documents

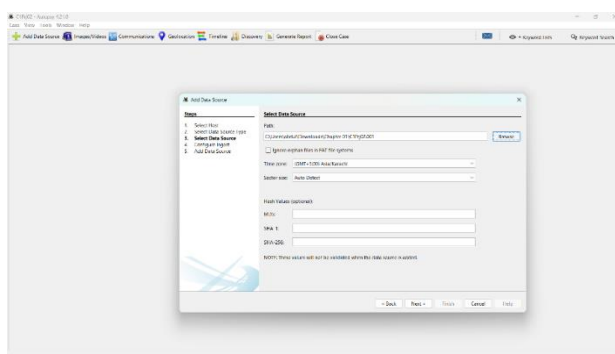
Task 1:
Entering the case name.



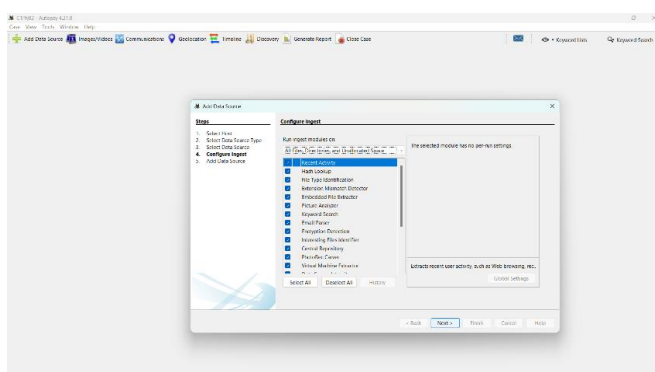
Task 2:
Entering the case number.

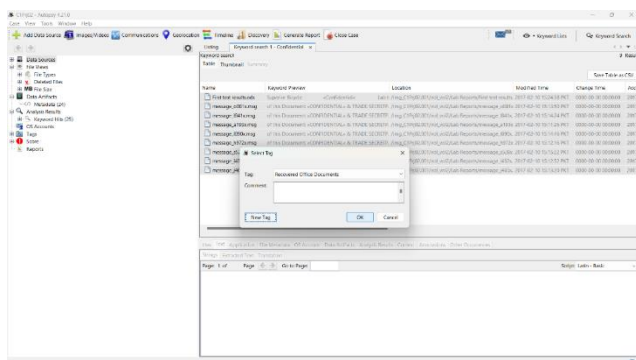
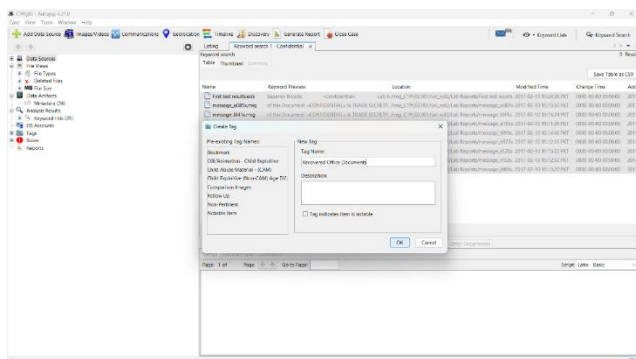
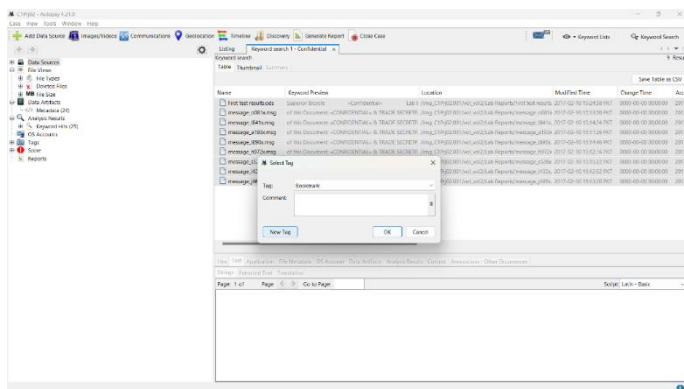
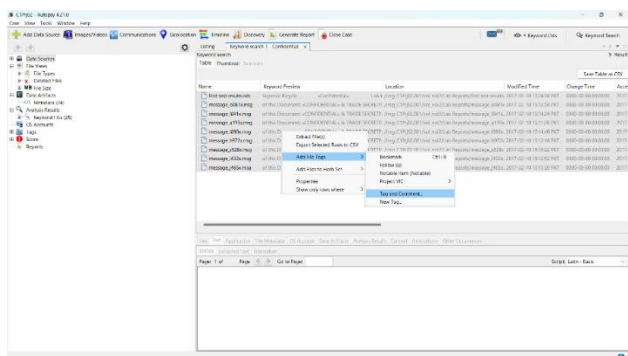


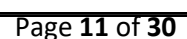
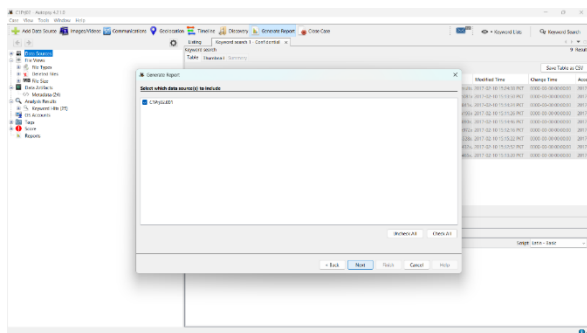
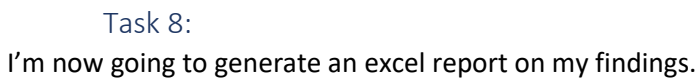
Task 3:
Selecting the disk image to be analyzed in Autopsy.



Task 4:
Configuring Ingest Modules (select all of them).

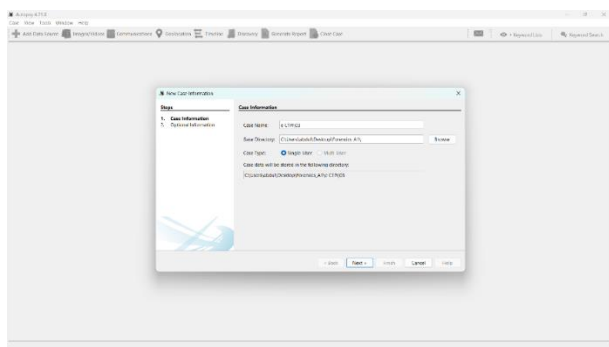




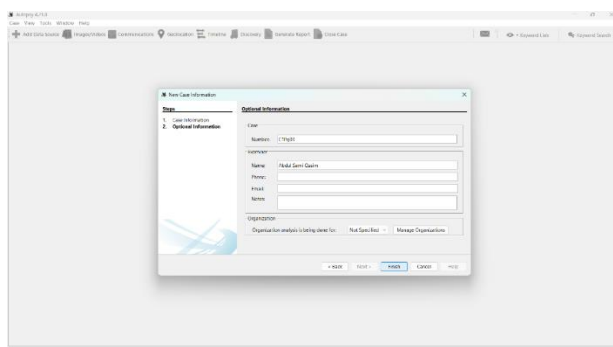


in the Human Resources Department notifies you that she got an anonymous letter with an old USB drive. The letter states that a former employee, Ralph Williams, had photos belonging to ACE Sailboats that contained trade secrets from April 2006. The letter also states that after Mr. Williams ended his employment at Superior Sailmakers in January 2007, he used the photos on the USB drive to get hired by Smith Sloop Boats, a competitor of ACE Sailboats. Both sailboat manufacturers are customers of Superior Sailmakers. Ms. Olsen tells you that another specialist has already made an image of the USB drive in the Expert Witness format (with an .E01 extension). She wants you to examine its contents for any photograph files to determine whether the anonymous complaint is true. After your examination, you need to generate a report that Ms. Olsen will send to the Legal Department. The Legal Department will then determine whether any violations of trade secret or intellectual property laws might have occurred.

Task 1:
Entering the case name.



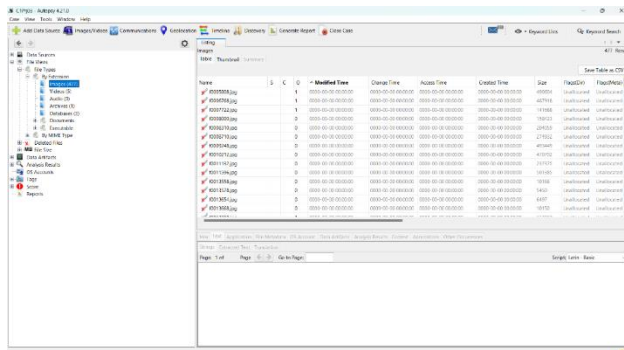
Task 2:
Entering the case number.



Task 3:
Selecting the disk image to be analyzed in Autopsy.

Task 6:

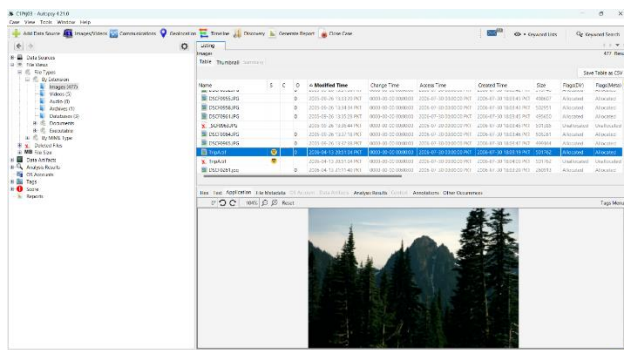
Clicked on the modified time header to get the photos in a chronological order to easily examine them.



The screenshot shows the X-Forensics application window. The 'Data Sources' pane on the left lists various file systems. The main pane displays a table of files with columns: Name, S, C, D, Modified Time, Change Time, Access Time, Created Time, Size, PageID, and PageMeta. The files are sorted by Modified Time in descending order. The table contains 17 rows of file entries, including files like 'E:\100000.jpg', 'E:\100001.jpg', etc.

Task 7:

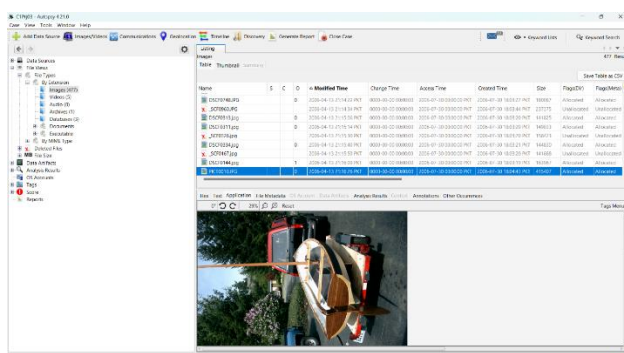
Looking for images/files that are either created or modified in April 2006.



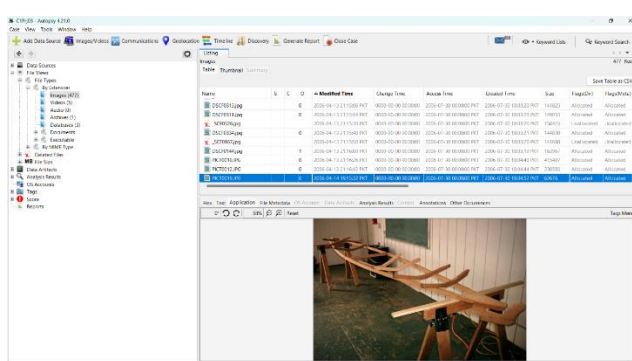
The screenshot shows the X-Forensics application window. The 'Data Sources' pane on the left lists various file systems. The main pane displays a table of files with columns: Name, S, C, D, Modified Time, Change Time, Access Time, Created Time, Size, PageID, and PageMeta. The files are sorted by Modified Time in descending order. The table contains 17 rows of file entries, including files like 'E:\100000.jpg', 'E:\100001.jpg', etc. Below the table, a preview of a landscape image is shown.

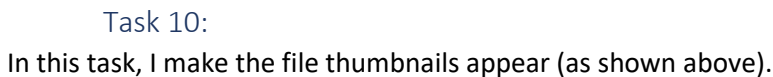
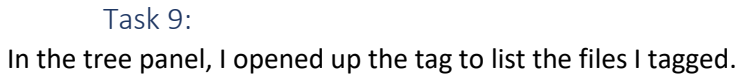
Task 8:

Scrolling through all the images and tagging the images that contain a boat (tagged them with the follow up quick tag).

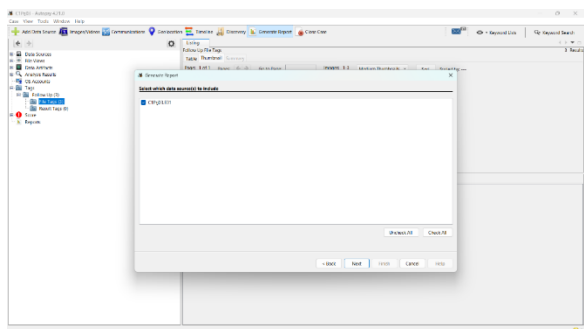


The screenshot shows the X-Forensics application window. The 'Data Sources' pane on the left lists various file systems. The main pane displays a table of files with columns: Name, S, C, D, Modified Time, Change Time, Access Time, Created Time, Size, PageID, and PageMeta. The files are sorted by Modified Time in descending order. The table contains 17 rows of file entries, including files like 'E:\100000.jpg', 'E:\100001.jpg', etc. Below the table, a preview of a boat image is shown.



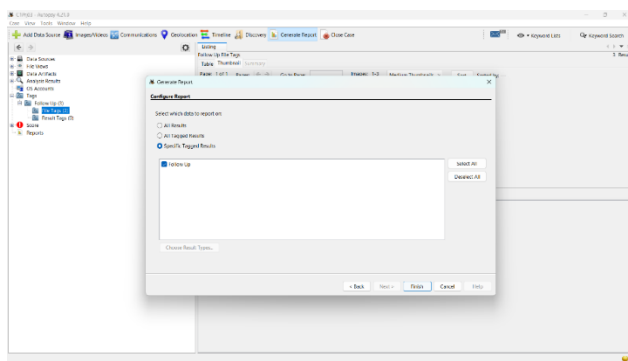


Task 11:
Generating the HTML report.

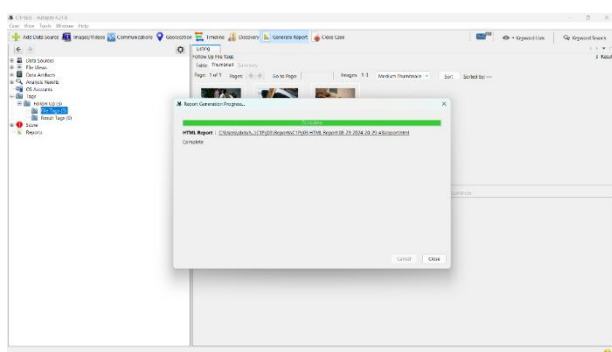


Task 12:

Selected the follow up tag so that only those files are analyzed in the report process.

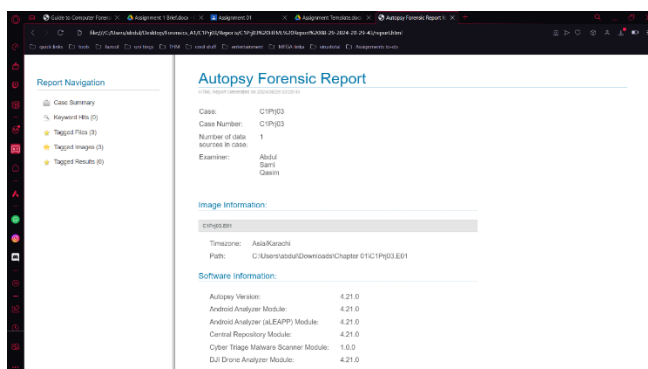


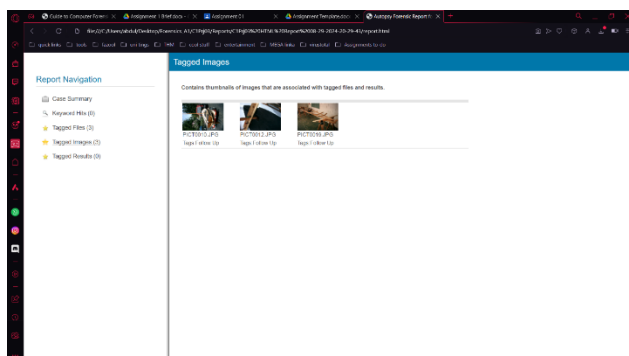
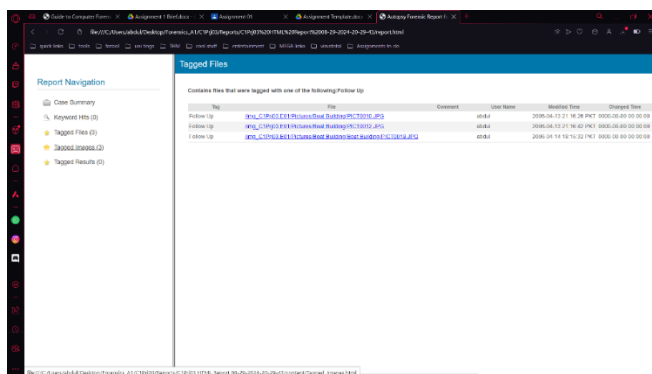
Task 13:
The report is being generated.



Task 14:
DATE: 30/8/24
TO: Ms. Olsen
FROM: Abdul Sami Qasim
SUBJECT: Findings on the Ralph Williams case

I have analyzed the image you've sent me, and I found three images of a boat in it, they are shown in the report below.





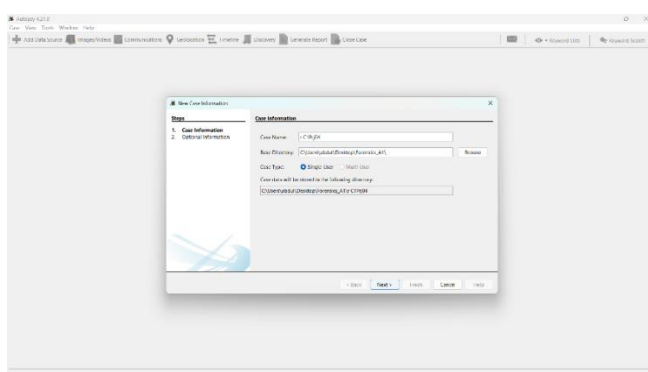
Project 1-4

Statement:

Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven't been deleted (that is, the allocated files) from an image.

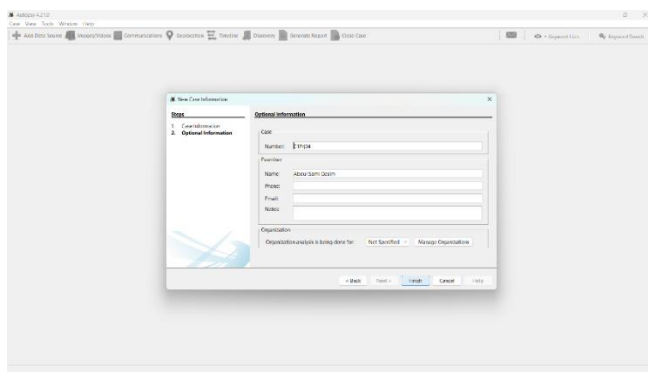
Task 1:

Entering the case name.

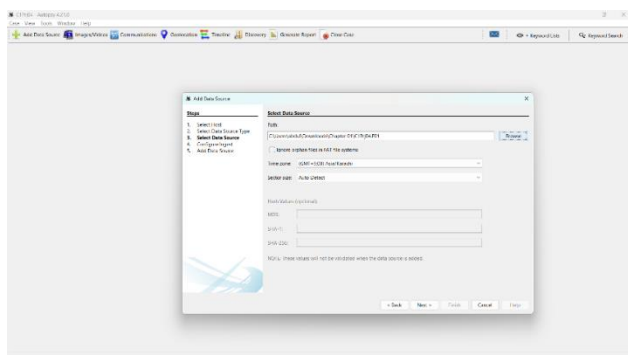
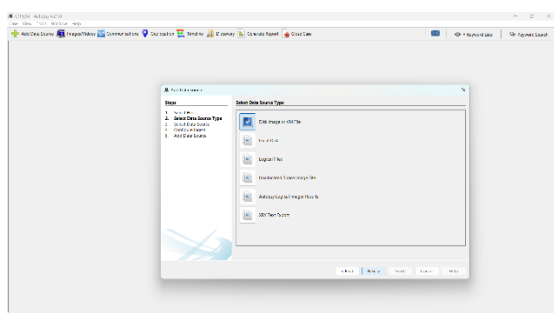


Task 2:

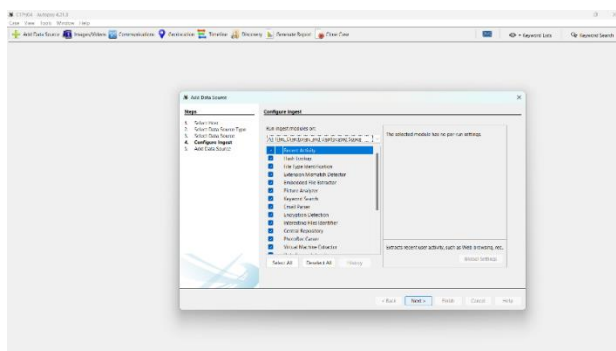
Entering the case number.



Task 3:
Selecting the disk image to be analyzed in Autopsy.



Task 4:
Configuring Ingest Modules (select all of them).



Task 5:
Opening views, file type, by extension to find out all the files present and analyzing them.

- 8-Lin_tomb.jpg
- 18-Gettysbg.jpg

Project 1-5

Statement:

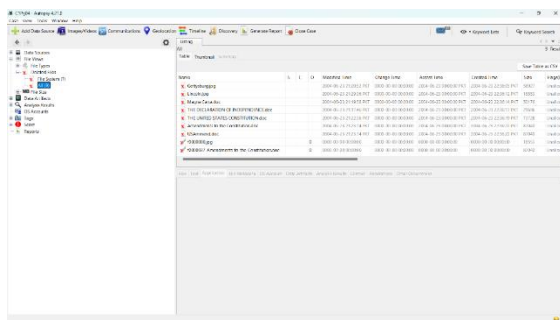
This project is a continuation from the previous project. You create a report listing all the unallocated (deleted) files Autopsy finds.

Task 1:

I didn't close the previous case.

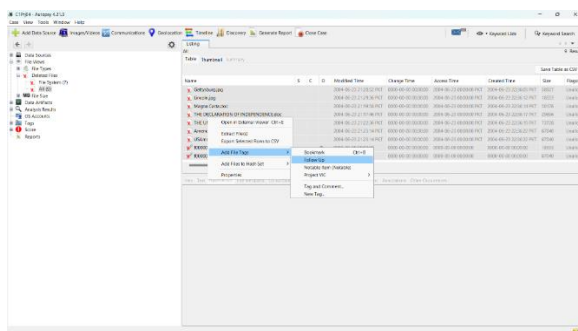
Task 2:

Opening views, file types, deleted, all. These files are to be analyzed.



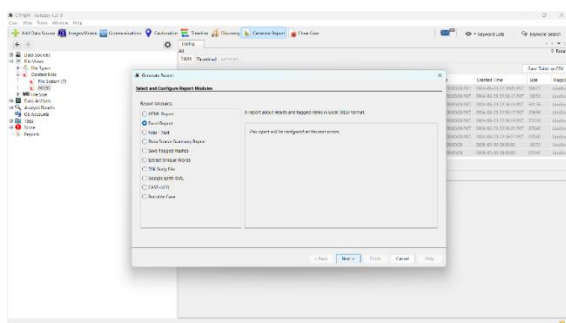
Task 3:

Selecting all the files in this folder and giving them the "Follow Up" quick tag.



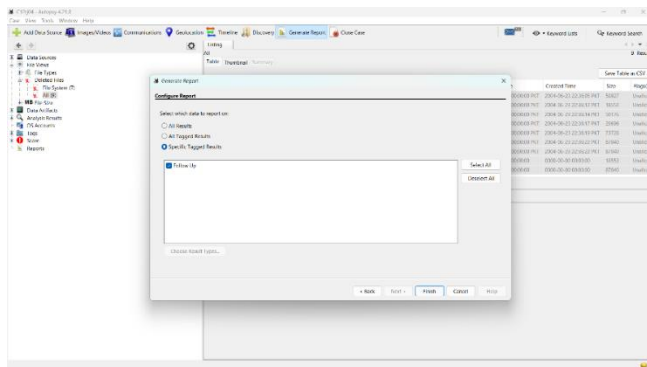
Task 4:

Generating an excel report.



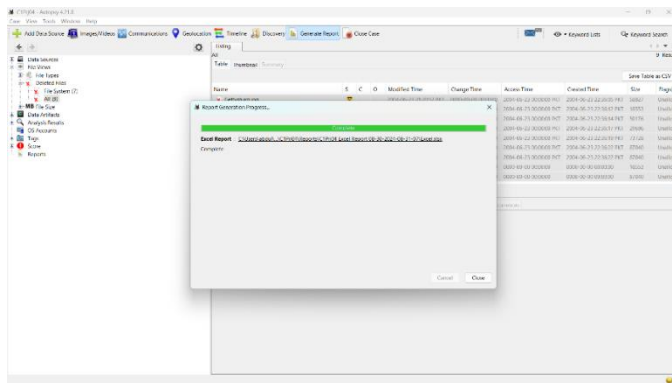
Task 5:

Selecting the “Follow Up” tag as I want to only analyze those files with that tag.



Task 6:

The report has been generated.



Task 7:

DATE: 30/8/24

TO: Unknown

FROM: Abdul Sami Qasim

SUBJECT: Deleted files found in given image

These are the deleted files that I found in the provided image:

- Gettysburg.jpg
- f0000000.jpg
- THE DECLARATION OF INDEPENDENCE.doc
- Amendments to the Constitution.doc
- Lincoln.jpg
- Magna Carta.doc
- THE UNITED STATES CONSTITUTION.doc
- USAmend.doc
- f0000037_Amendments_to_the_Constitution.doc

Project 1-6

Statement:

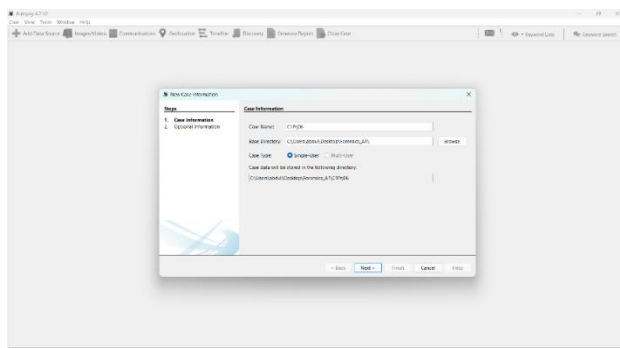
In this project, another investigator asks you to examine an image and search for all occurrences of the following keywords:

- ANTONIO
- HUGH EVANS
- HORATIO

After you complete these searches, the investigator wants a short report listing which files contain these names.

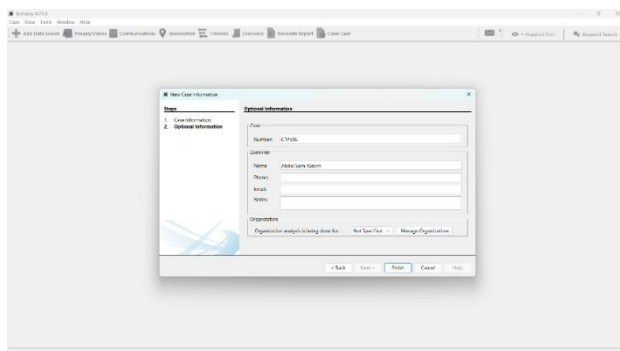
Task 1:

Entering the case name.



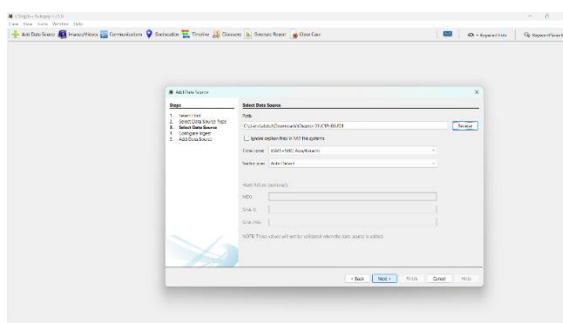
Task 2:

Entering the case number.

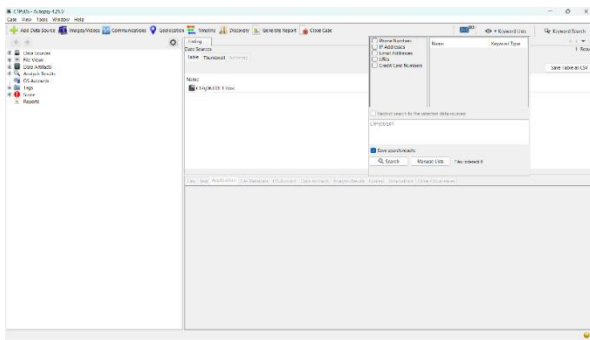


Task 3:

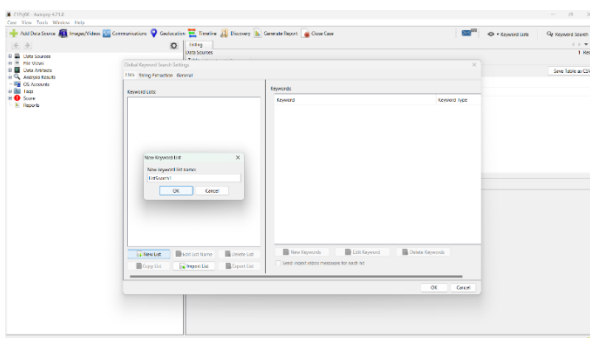
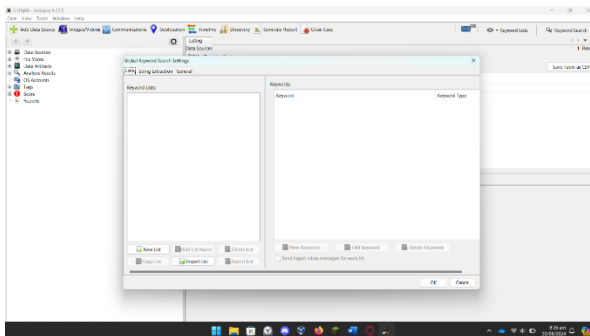
Selecting the disk image to be analyzed in Autopsy.



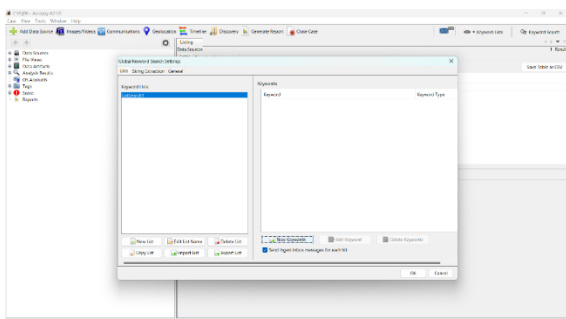
Page 25 of 30



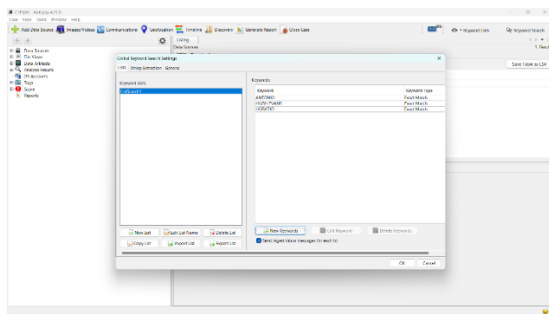
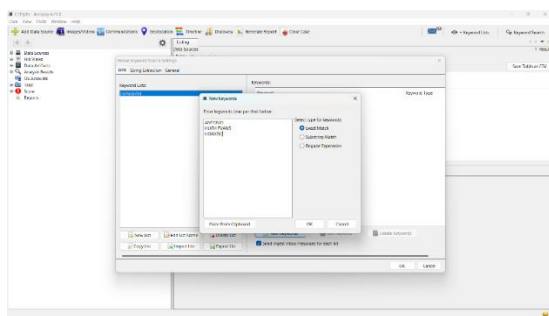
Task 6:
Adding a new list named "ListSearch1".



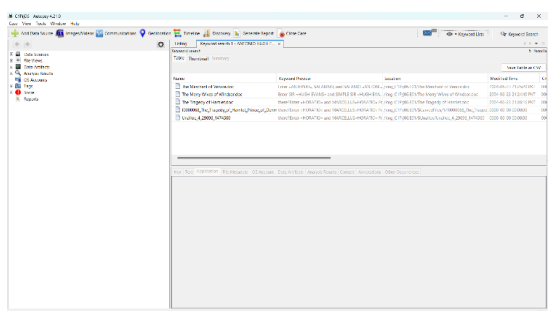
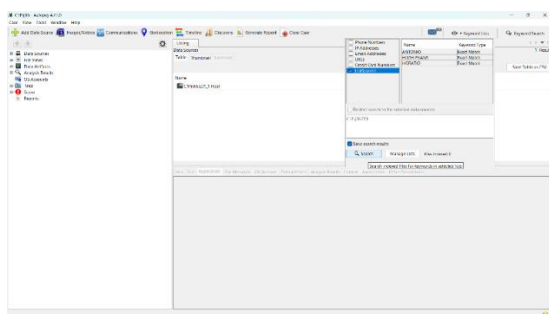
Task 7:
Selecting the "new keywords" option in the "ListSearch1" list in order to add the required keywords.



Task 8:
Entering keywords "ANTONIO", "HUGH EVANS" and "HORATIO" in the search list.

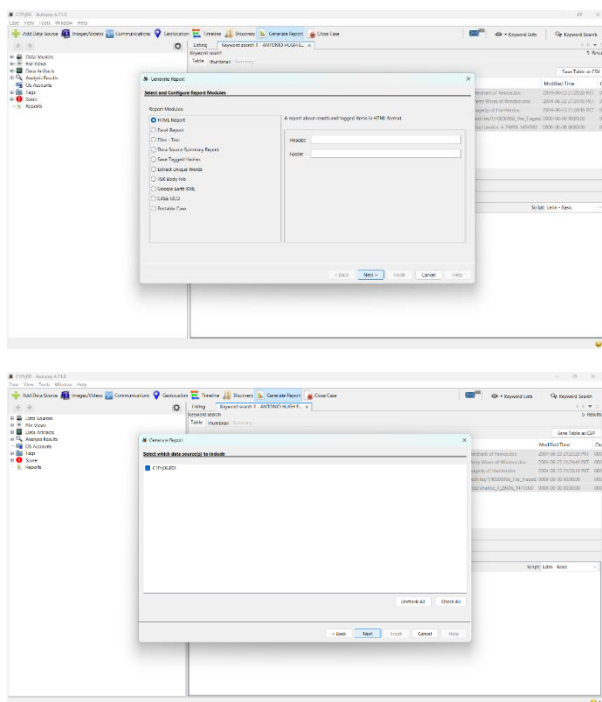


Task 9:
Searching for the keywords using the keyword list search button.

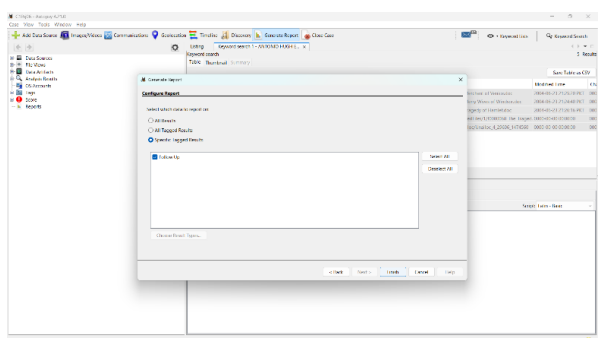


Task 10:
None of the searched files contained the word “confidential”.

Task 11:
Generating the HTML Report.



Task 12:
Selecting the “follow up” tag to only analyze the tagged files in the report.



Task 13:
DATE: 30/8/24
TO: another investigator
FROM: Abdul Sami Qasim
SUBJECT: Information of the files containing given keywords

Files with keyword “ANTONIO”

1. The Merchant of Venice.doc
 - File’s pathname and filename:
/img_C1Prj06.E01/The Merchant of Venice.doc
 - Modified date and time:
2004-06-23 21:25:20 PKT

- Create date and time:
2004-06-23 22:40:23 PKT
- File size (bytes):
72704

Files with keyword "HUGH EVANS"

1. The Merry Wives of Windsor.doc
 - File's pathname and filename:
/img_C1Prj06.E01/The Merry Wives of Windsor.doc
 - Modified date and time:
2004-06-23 21:24:40 PKT
 - Create date and time:
2004-06-23 22:40:27 PKT
 - File size (bytes):
164352

Files with keyword "HORATIO"

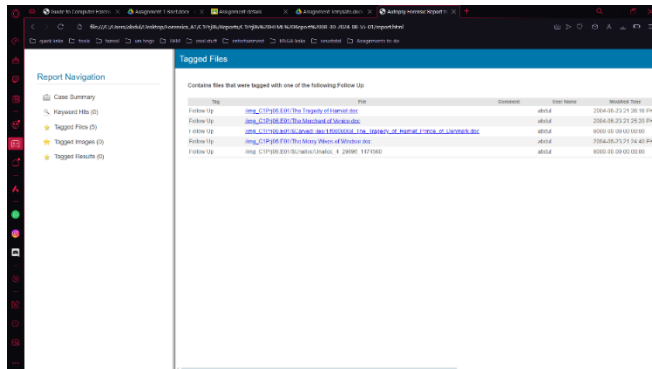
1. Unalloc_4_29696_1474560
 - File's pathname and filename:
/img_C1Prj06.E01/\$Unalloc/Unalloc_4_29696_1474560
 - Modified date and time:
0000-00-00 00:00:00
 - Create date and time:
0000-00-00 00:00:00
 - File size (bytes):
1019392
2. f0000068_The Tragedy of Hamlet Prince of Denmark.doc
 - File's pathname and filename:
/img_C1Prj06.E01/\$CarvedFiles/1/f0000068_The Tragedy of Hamlet Prince of Denmark.doc
 - Modified date and time:
0000-00-00 00:00:00
 - Create date and time:
0000-00-00 00:00:00
 - File size (bytes):
90112
3. The Tragedy of Hamlet.doc
 - File's pathname and filename:
/img_C1Prj06.E01/The Tragedy of Hamlet.doc
 - Modified date and time:

2004-06-23 21:26:16 PKT

- Create date and time:
2004-06-23 22:40:33 PKT

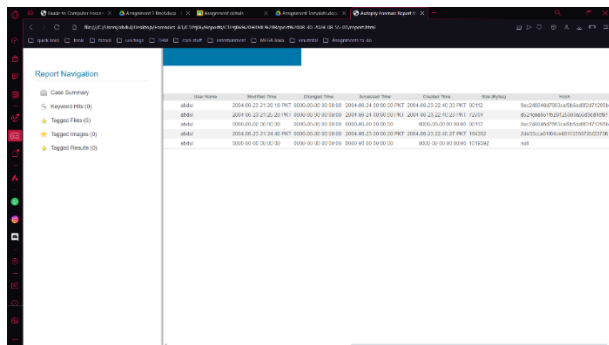
- File size (bytes):

90112



The screenshot shows the Autopsy software interface with the 'Tagged Files' report selected. The report lists files that were tagged with one of the following follow-up tags:

File	Comment	File Name	Modified Time
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	



The screenshot shows the Autopsy software interface with the 'Tagged Files' report selected. The report lists files that were tagged with one of the following follow-up tags:

File	Comment	File Name	Modified Time
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	
Follow Up: http://19198.83X/The Targets of Interest.doc	ab04	2004-06-23 21:26:16 PKT	

• Summary

This assignment made us perform 6 hands-on projects from the book “Guide to Computer Forensics and Investigations: Processing Digital Evidence”. These were projects that involved analysis of 5 different disk images that were provided to us. We were told to use the software “Autopsy” to perform analysis on these images. The projects involved analysis of deleted files, searching for keywords and generating reports on the findings.

• References

Nelson, B., Philips, A., & Stuart, C. (2018). *Guide to Computer Forensics and Investigations*.