

# Digital Forensics

SRN : PES1UG20CS825

NAME : PREM SAGAR J S

SEC : 'H'

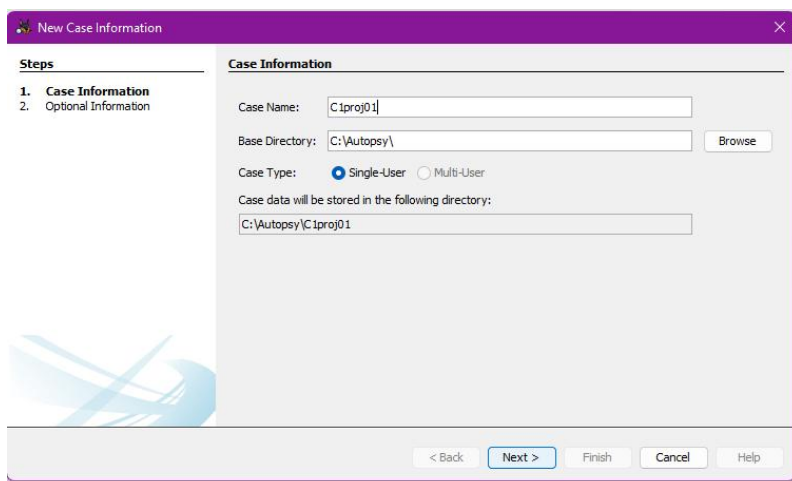
## Lab Assignment - 6

### Task 1 :

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, a 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. To process this case, follow these steps to evaluate what's on the image of the USB drive:

1. Start Autopsy for Windows, and click the Create New Case icon. In the New Case Information window, enter C1Prj01 in the Case Name text box, and click Browse next to the Base Directory text box. Navigate to and click your work folder, and then click Next.



2. In the Additional Information window, type C1Prj01 in the Case Number text box and your name in the Examiner text box, and then click Finish.

Examiner

Name: PREM SAGAR JS

Phone: 7892051977

Email: ajgamestar3@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

3. In the Select Data Source window, click the Select data source type list arrow, and click Disk Image or VM file. Click the Browse button next to the “Browse for an image file” text box, navigate to and click your work folder and the C1Prj01.E01 file, and then click Open. Click Next.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

☐ Specify new host name

☐ Use existing host

< Back Next > Finish Cancel Help

Add Data Source

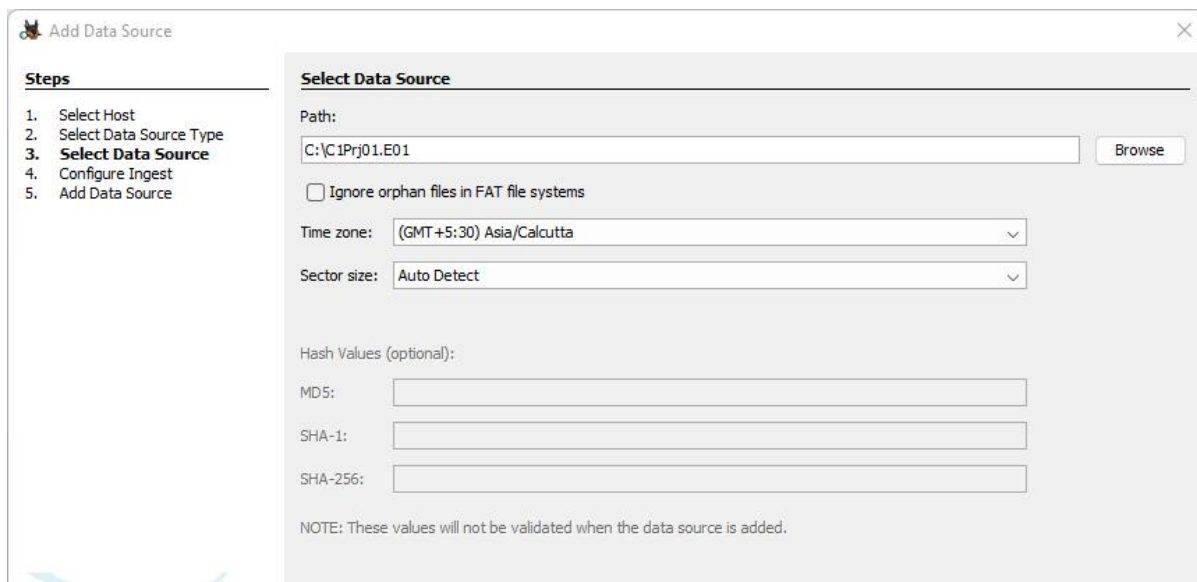
Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

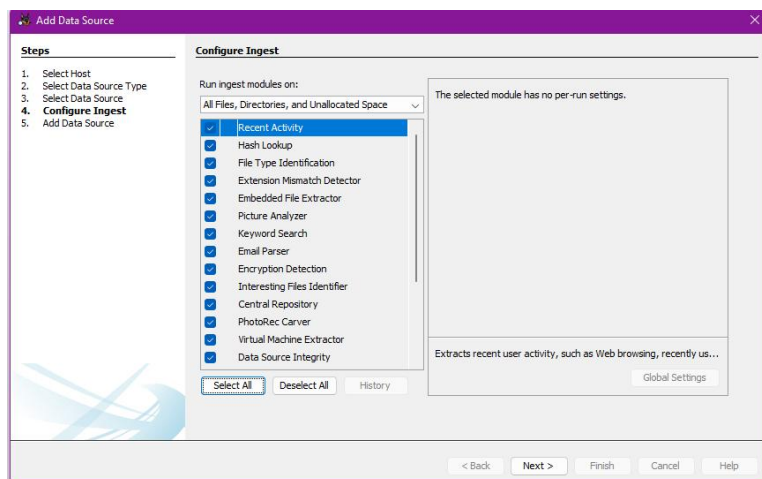
Select Data Source Type

- ☒ Disk Image or VM File
- ☐ Local Disk
- ☐ Logical Files
- ☐ Unallocated Space Image File
- ☐ Autopsy Logical Imager Results
- ☐ XRY Text Export

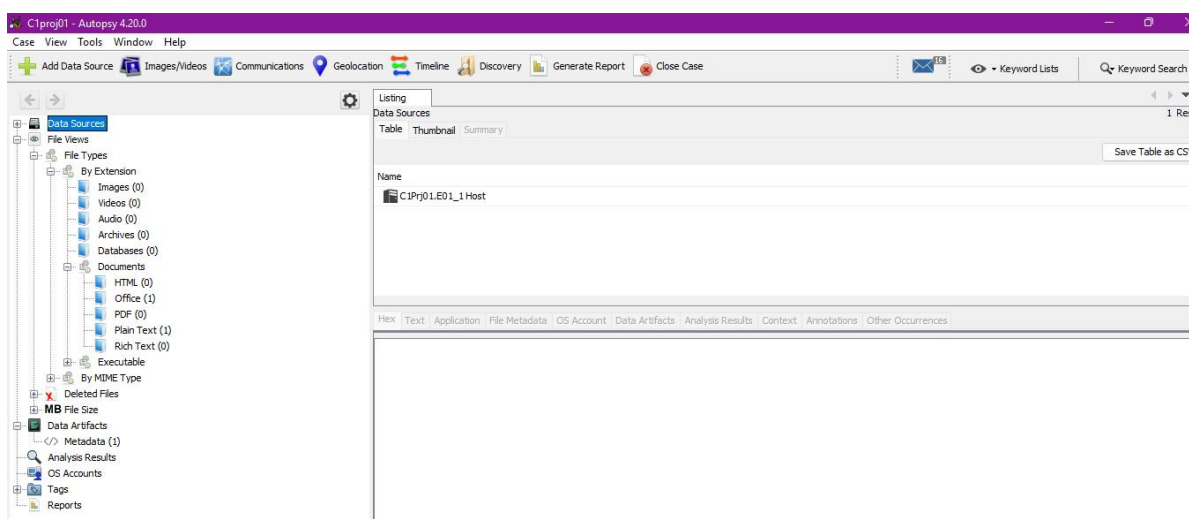
< Back Next > Finish Cancel Help



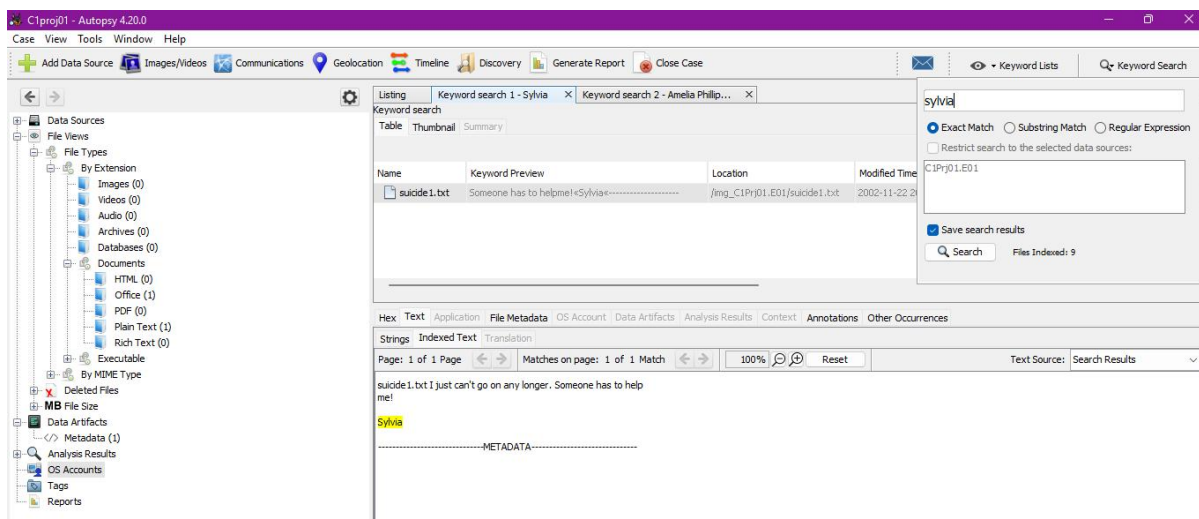
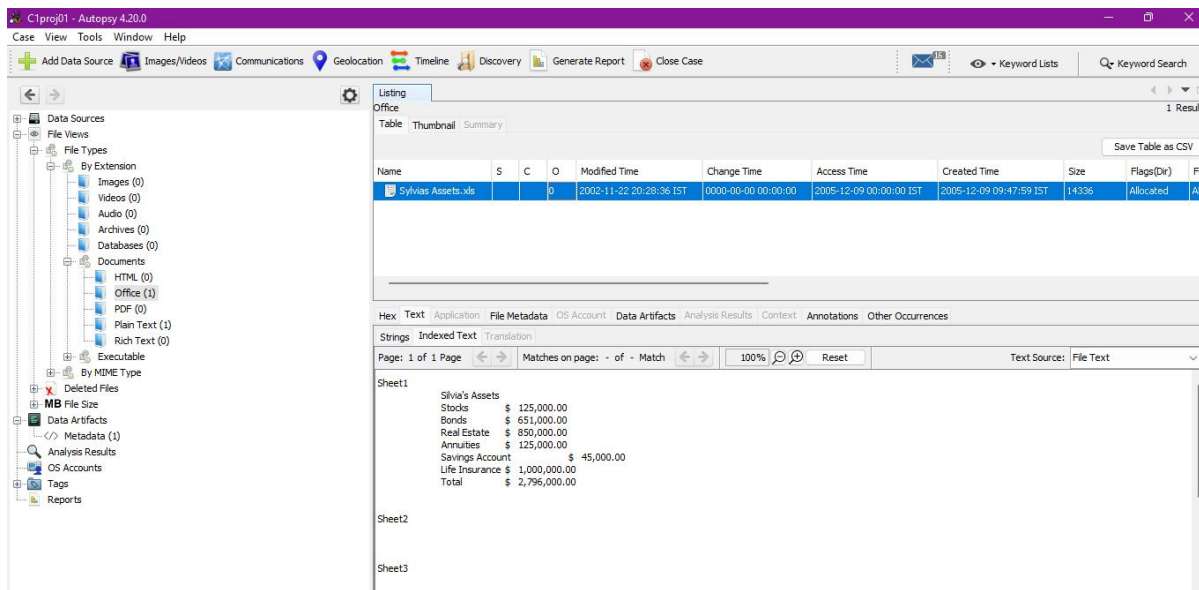
4. In the Configure Ingest Modules window, click Select All. Click Next and then Finish.



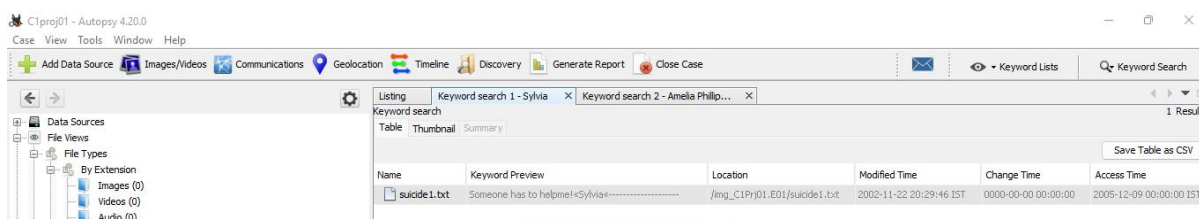
5. In the Tree Viewer pane, expand Views, File Types, By Extension, and Documents.

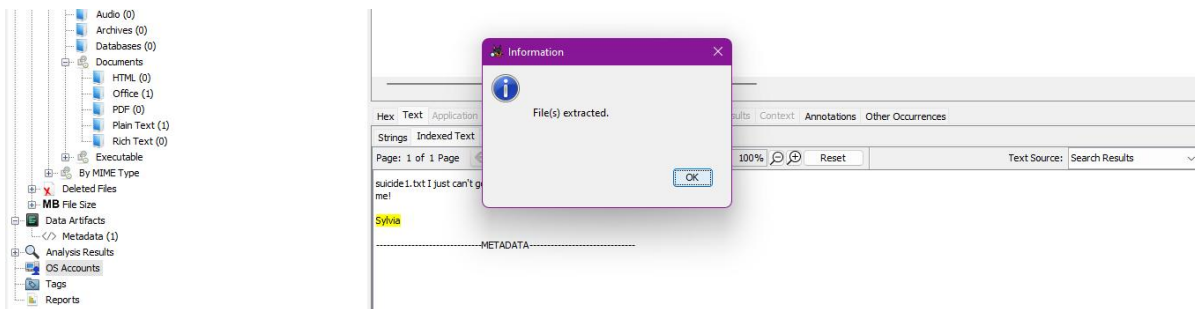


6. Examine each subfolder under Documents. Determine which folder might contain files of interest to this case.

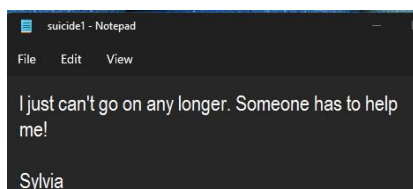


7. If you found any files related to the case, select the files as a group, right-click the selection, and click Extract File(s). In the Save dialog box, click Extract files to save the files.





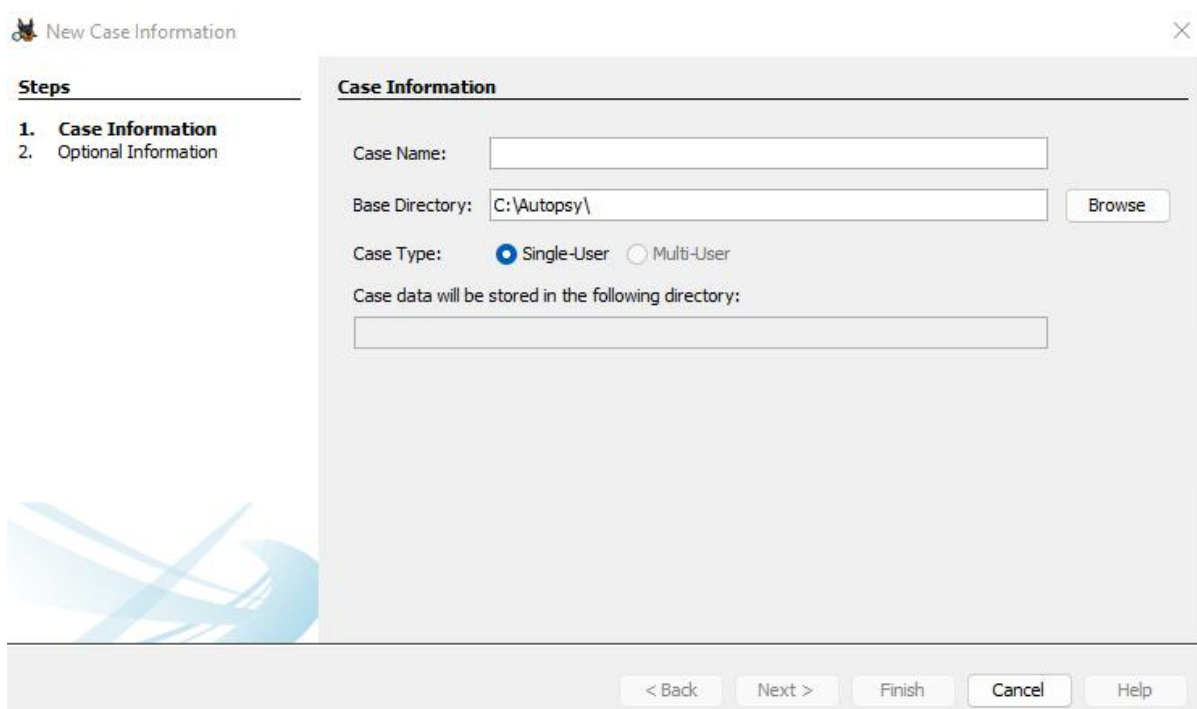
Suicide1.txt



## TASK 2 :

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.

1. Start Autopsy for Windows. Click the Create New Case icon. In the New Case Information window, enter C1Prj04 in the Case Name text box, and click Browse next to the Base Directory text box. Navigate to and click your work folder, and then click Next.



2. In the Additional Information window, type C1Prj04 in the Case Number text box and your name in the Examiner text box, and then click Finish.

Examiner

Name: PREM SAGAR JS

Phone: 7892051977

Email: sjgamestar3@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Host

Hosts are used to organize data sources and other data.

☒ Generate new host name based on data source name

☐ Specify new host name

☐ Use existing host

< Back Next > Finish Cancel Help

3. In the Select Data Source window, click the Select data source type list arrow, and click Disk Image or VM file. Click the Browse button next to the “Browse for an image file” text box, navigate to your work folder and click the C1Prj04.E01 file, and then click Open. Click Next.

Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source

Select Data Source Type

☒ Disk Image or VM File

☐ Local Disk

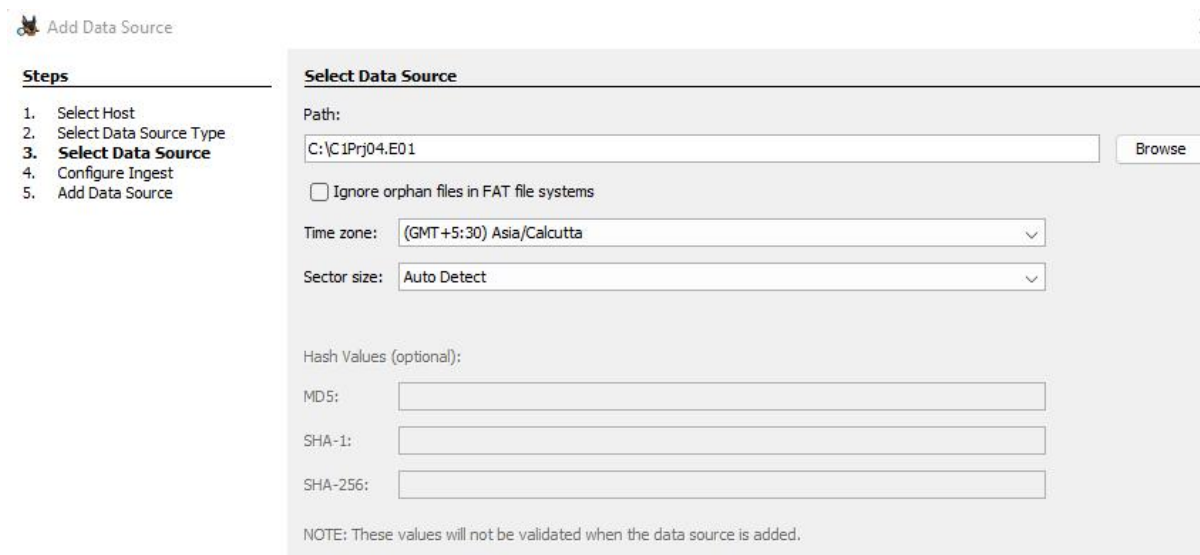
☐ Logical Files

☐ Unallocated Space Image File

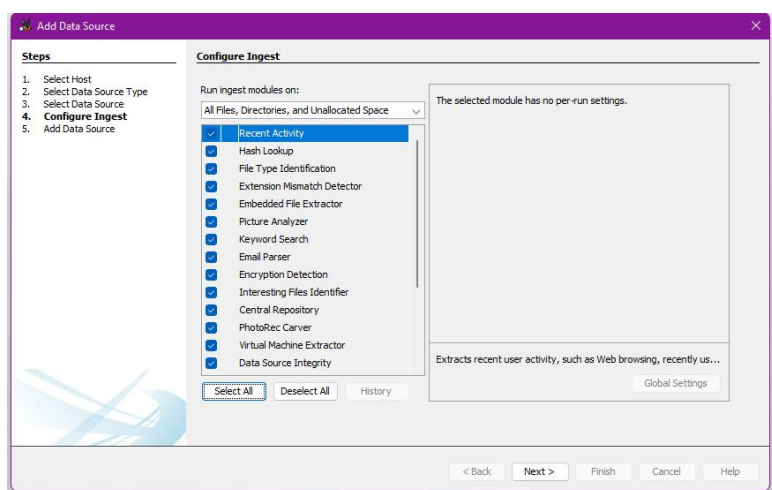
☐ Autopsy Logical Imager Results

☐ XRY Text Export

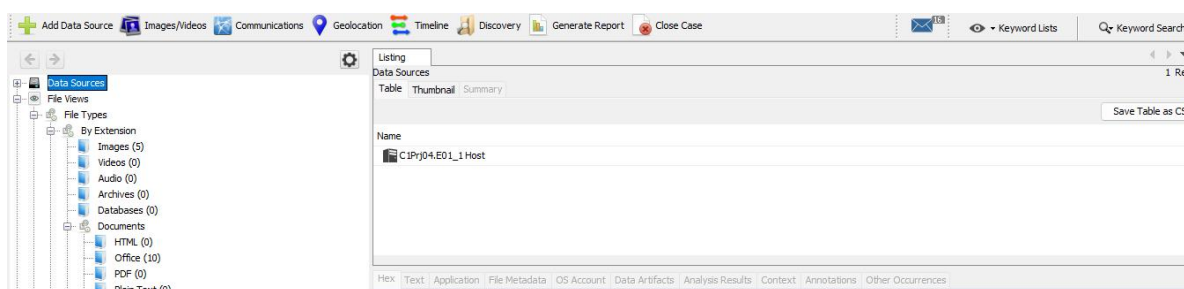
< Back Next > Finish Cancel Help



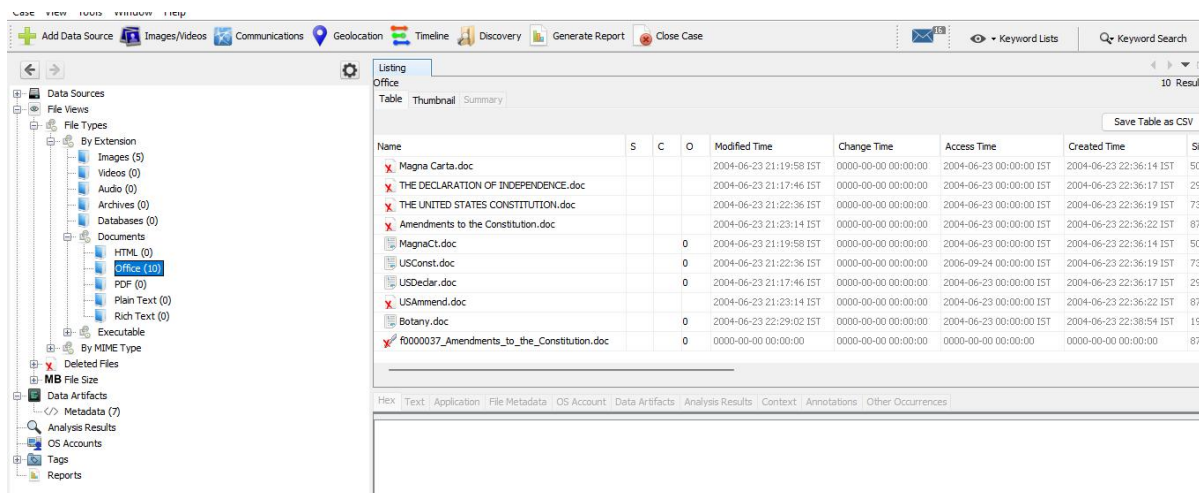
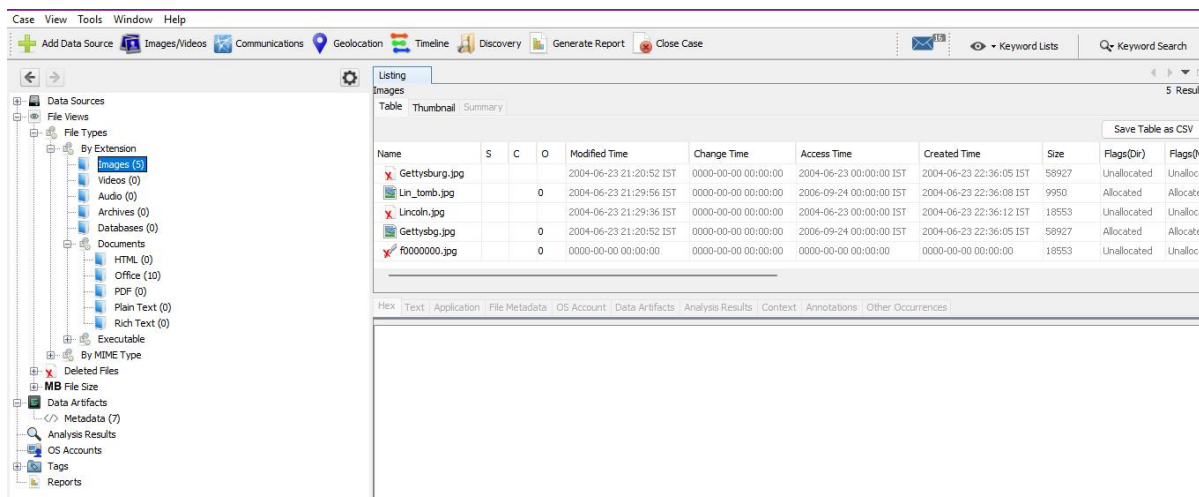
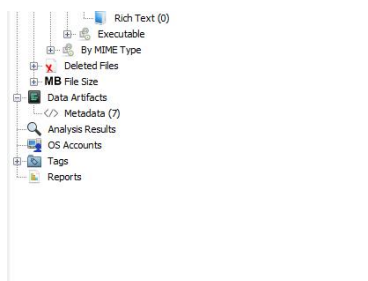
4. In the Configure Ingest Modules window, click Select All. Click Next and then Finish.



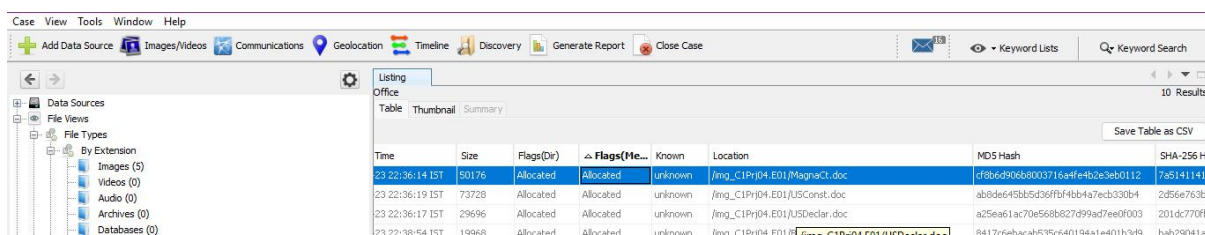
5. In the Tree Viewer pane, expand Views, File Types, and By Extension. Under By Extension are several subfolders representing file types, as you've seen in previous projects. Next to each file type subfolder is a number enclosed in parentheses, which shows the number of files of this type Autopsy found. Click subfolders with numbers greater than zero to view the files.



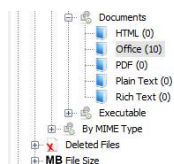




6. When you click on any file you will see a list of property headers in the Result Viewer pane, here scroll to the right, if necessary until the Flags(Meta) column is in view. Sort the column by clicking the Flags(Meta) header, which displays all allocated files to the top of the list.

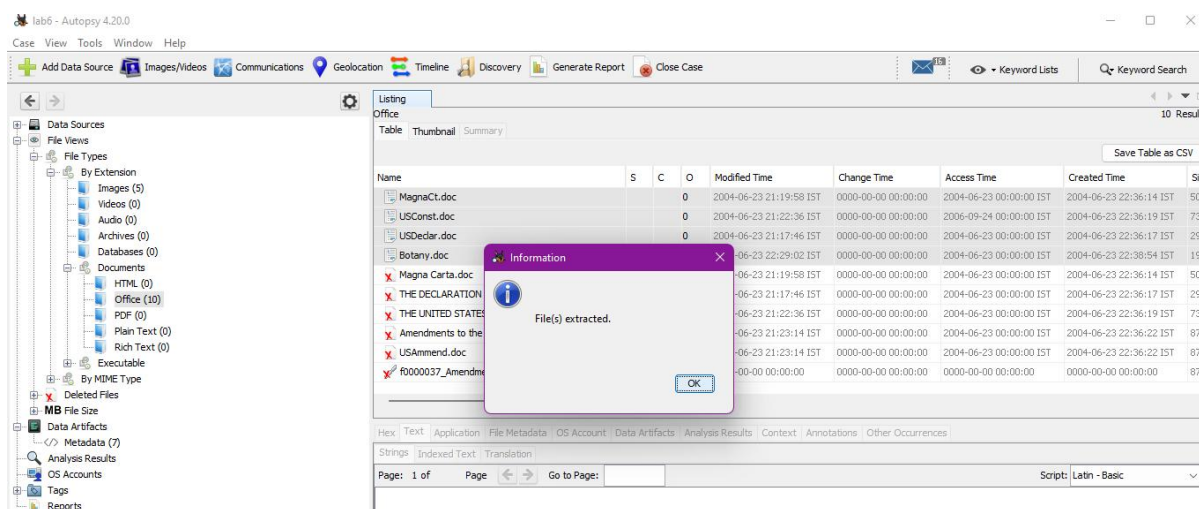
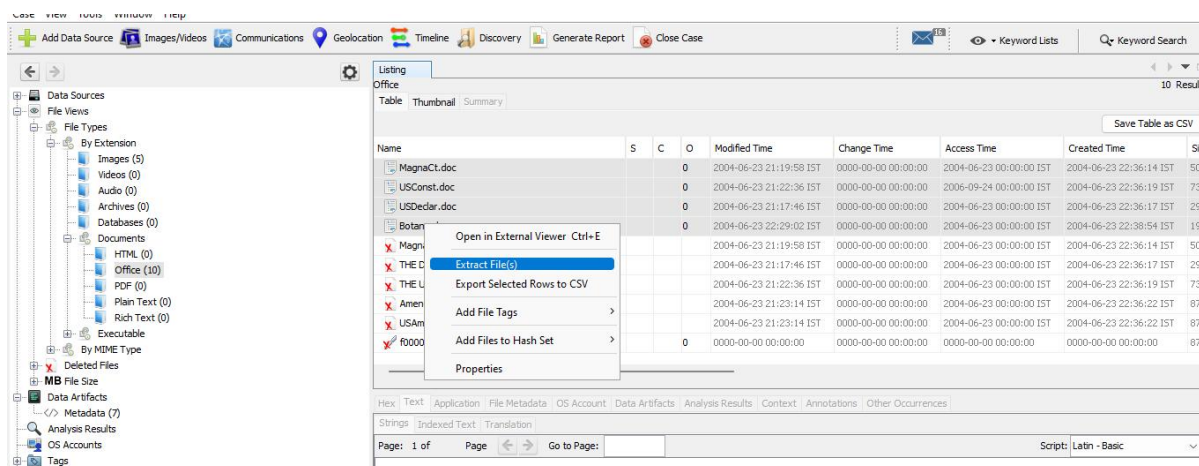






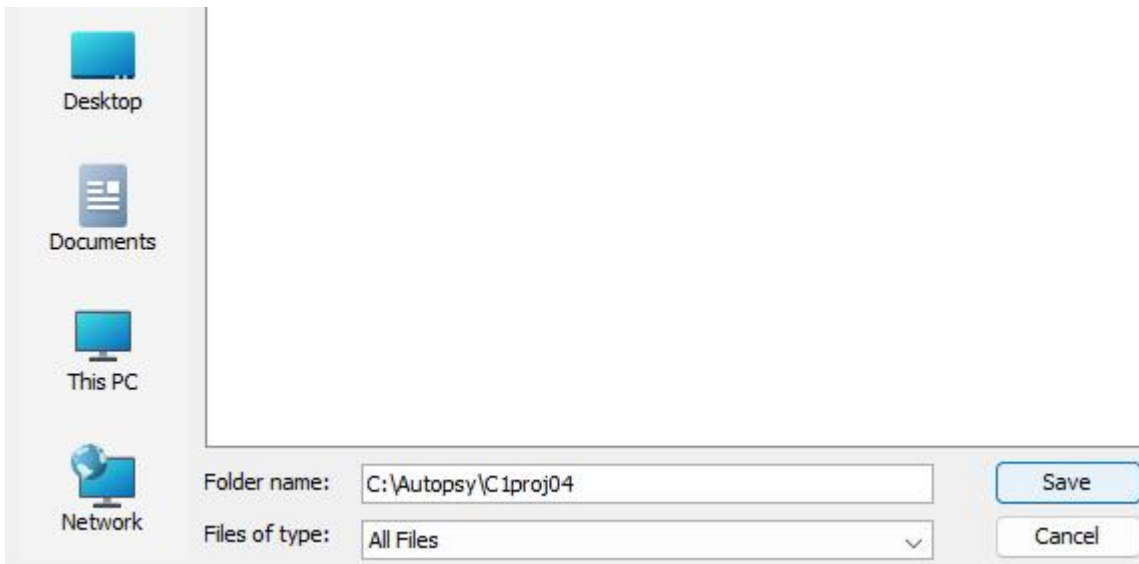
23 22:36:14 IST	50176	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/Magna Carta.doc	02ac35ba1752f9c8a35ce5adcf8f3e4d	7f45a34bad
23 22:36:17 IST	29696	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/THE DECLARATION OF INDEPENDENCE...	fb8ec22cfce8f9f14a49710b256ee	b92917c0c
23 22:36:19 IST	73728	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/THE UNITED STATES CONSTITUTION.doc	27f9e7dbf1669296d5a161a643e48b2	ba093d73c
23 22:36:22 IST	87040	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/Amendments to the Constitution.doc	a57ff86dc2226031cf7813341199e82	ff47ace3d5
23 22:36:22 IST	87040	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/USAmend.doc	a57ff86dc2226031cf7813341199e82	ff47ace3d5
00 00:00:00	87040	Unallocated	Unallocated	unknown	/img_C1Prj04.E01/CarvedFiles/1/f0000037_Amendments...	a57ff86dc2226031cf7813341199e82	ff47ace3d5

7. Scroll to the left until the Name column is visible. If there are allocated files, they will be at the top of this list. Ctrl+click each allocated file, right-click this selection, and then click Extract File(s).



8. In the Save dialog box, click Save to save the files automatically in Autopsy's case subfolder: Case-Name\Export.





9. Write a brief memo that lists all the files you exported. Leave Autopsy running for the next project.

There were four files namely

a)MagnaCt Rules, regulations, and the rights of King John's people are outlined in this document. In heir concerns, there are around 63 rules specified.

b)USConst

## THE AMERICAN CONSTITUTION

This document comprises the tax-related articles, clauses, and sections of the US constitution.

c) USDeclar This file includes all relevant data on the US Declaration of Independence.

d)Botany

I've been considering the New World Order as a result of these excellent materials. It is past time to abolish the current regimes. The events in the Botany Bay episode of Star Trek happened only a few decades too late. Imagine if the Atkin's diet really did result in a superior intellect as well as a superior physique.

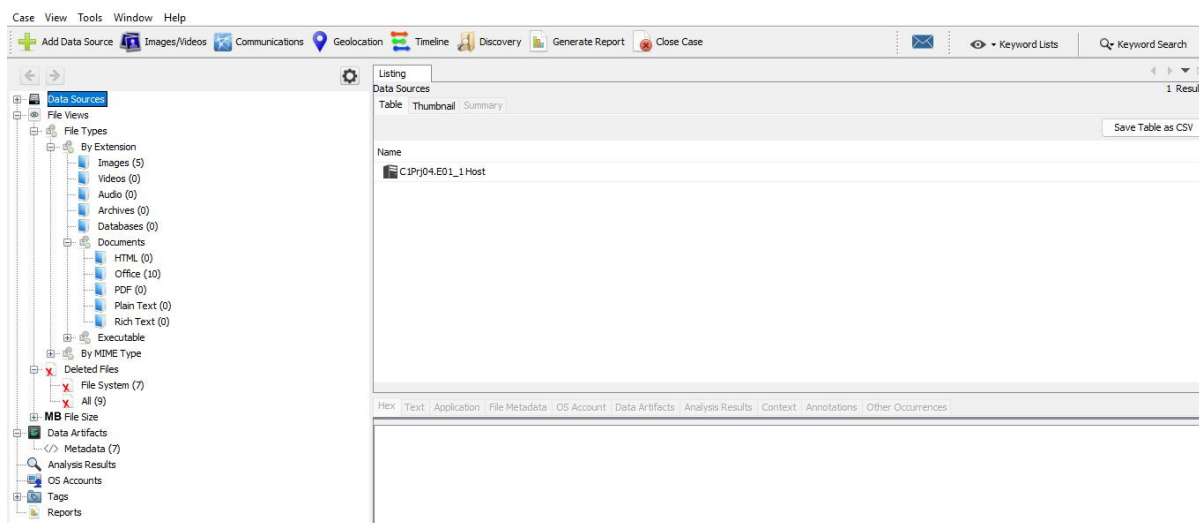
The moment has come for world rule. Forget about the conflicts.

## TASK 3 :

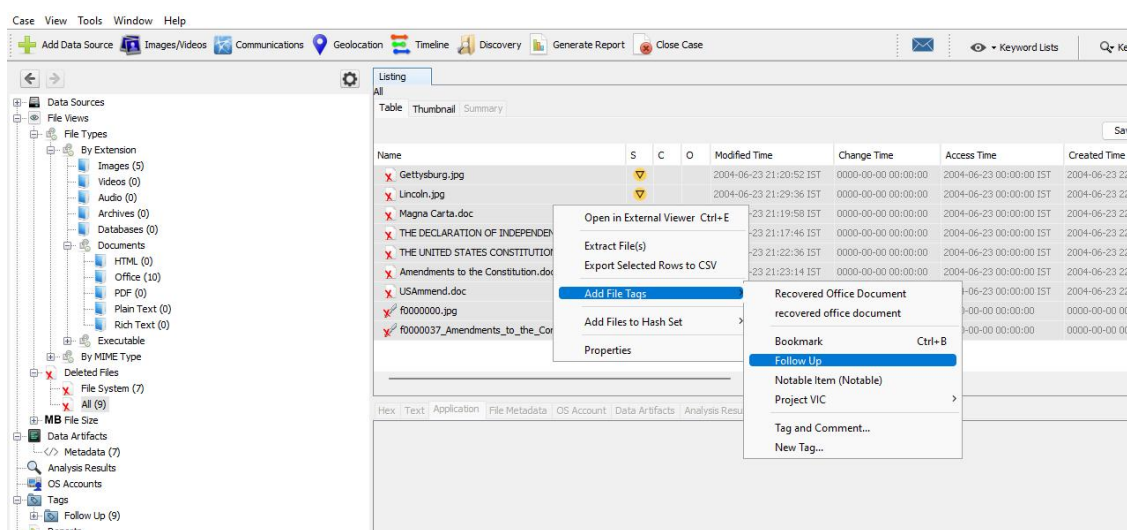
This project is a continuation from the previous project. You create a report listing all the unallocated (deleted) files Autopsy finds.

1. Start Autopsy for Windows and click the Open Recent Case icon, if necessary.

2. In the Tree Viewer pane, expand Views, File Types, Deleted Files, and All.



3. In the Result Viewer pane, Ctrl+click all files in the All subfolder. Right-click this selection, point to Tag File and then Quick Tag, and click Follow Up.



Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing

Table Thumbnail Summary

Save Table

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Amendments to the Constitution.doc	✓			2004-06-23 21:23:14 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:22
Gettysburg.jpg	✓			2004-06-23 21:20:52 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:09
Lincoln.jpg	✓			2004-06-23 21:29:36 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:12
Magna Carta.doc	✓			2004-06-23 21:19:58 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:14
THE DECLARATION OF INDEPENDENCE.doc	✓			2004-06-23 21:17:46 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:17
THE UNITED STATES CONSTITUTION.doc	✓			2004-06-23 21:22:36 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:19
USAmend.doc	✓			2004-06-23 21:23:14 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:22
R0000000.jpg	✓		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
R0000037_Amendments_to_the_Constitution.doc	✓		1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of Page Go to Page: Script: Latin - Basic

4. Click Generate Report at the top. In the Generate Report window, click the Results - Excel option button in the Report Modules section, and then click Next.

Generate Report

Select and Configure Report Modules

Report Modules:

☐ HTML Report

☒ Excel Report

☐ Files - Text

☐ Data Source Summary Report

☐ Save Tagged Hashes

☐ Extract Unique Words

☐ TSK Body File

☐ Google Earth KML

☐ CASE-UCO

☐ Portable Case

A report about results and tagged items in Excel (XLS) format.

This report will be configured on the next screen.

< Back Next > Finish Cancel Help

5. In the Configure Artifacts Report window, click the Tagged Results button, click the Follow Up check box, and then click Finish.

Generate Report

Configure Report

Select which data to report on:

☐ All Results

☒ All Tagged Results

☐ Specific Tagged Results

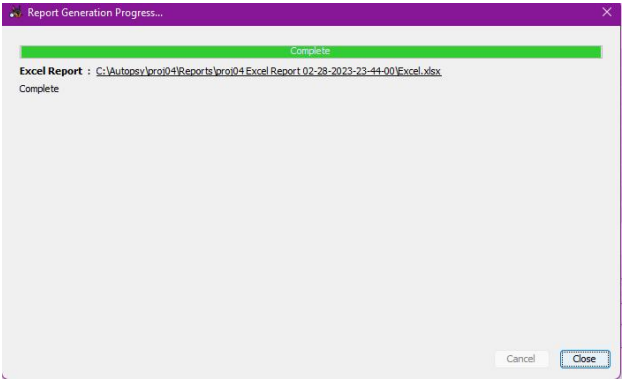
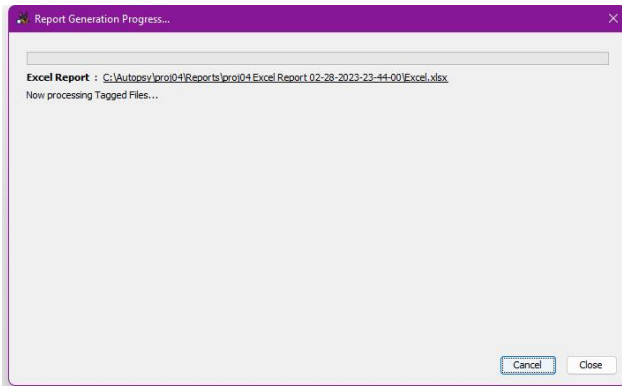
☒ Follow Up

Select All

Deselect All

Choose Result Types...

< Back Next > Finish Cancel Help



6. In the Report Generation Progress Complete window, click the Results – Excel pathname to open the Excel report. When you’ re finished, click Close in the Report Generation Progress window.

Summary		
Case Name:	C1proj04	
Number of data sources in case:	1	
Examiner:	Prem Sagar JS	

=====\*\*\*\*\*=====