

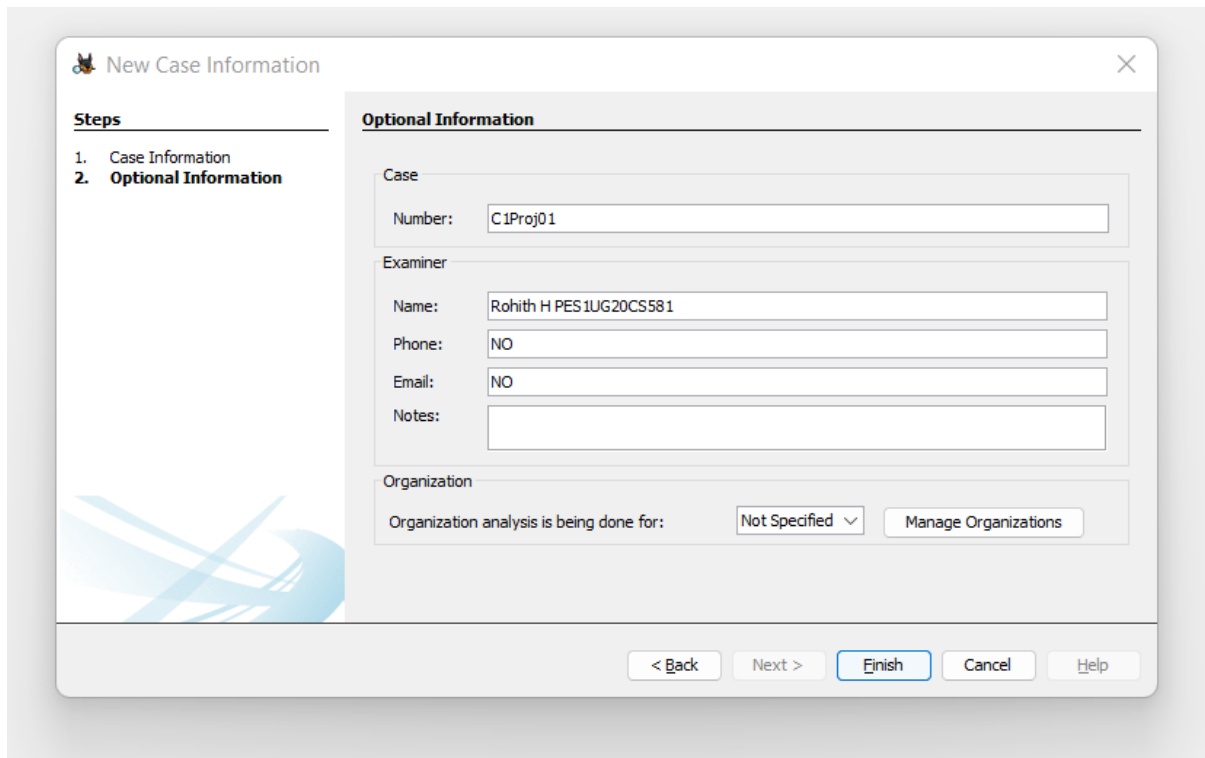
PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06

Task -01



The screenshot displays a software window titled "New Case Information" with a close button (X) in the top right corner. On the left side, there is a "Steps" panel with two items: "1. Case Information" and "2. Optional Information", where the second item is currently selected. The main area of the window is titled "Optional Information" and contains several input fields organized into sections: "Case" with a "Number:" field containing "C1Proj01"; "Examiner" with fields for "Name:" (containing "Rohith H PES1UG20CS581"), "Phone:" (containing "NO"), "Email:" (containing "NO"), and "Notes:" (an empty text area); and "Organization" with a label "Organization analysis is being done for:" followed by a dropdown menu showing "Not Specified" and a "Manage Organizations" button. At the bottom of the window, there is a row of five buttons: "< Back", "Next >", "Finish" (which is highlighted with a blue border), "Cancel", and "Help".

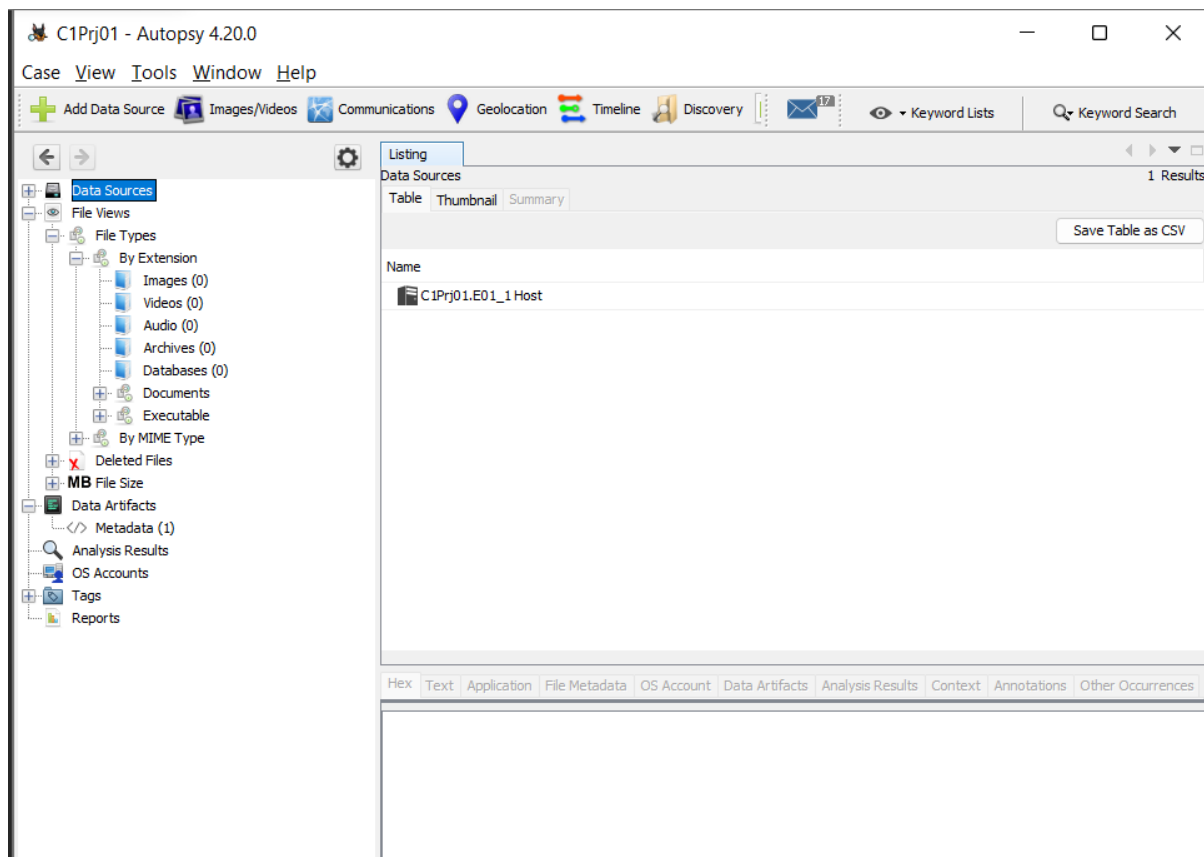
The Above Screenshot just represents the creation of the New Case C1Proj01.

PES1UG20CS581

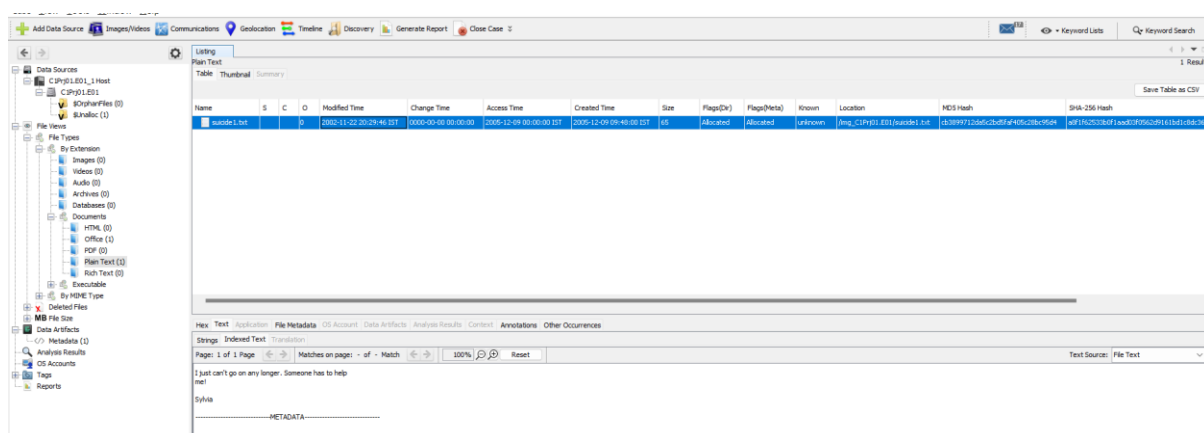
ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06



Main two panes that provide information about the case details are shown in the screenshot up top. All of the directories and files, including the deleted files from the extracted image, are displayed in a tree structure in the tree viewer pane.



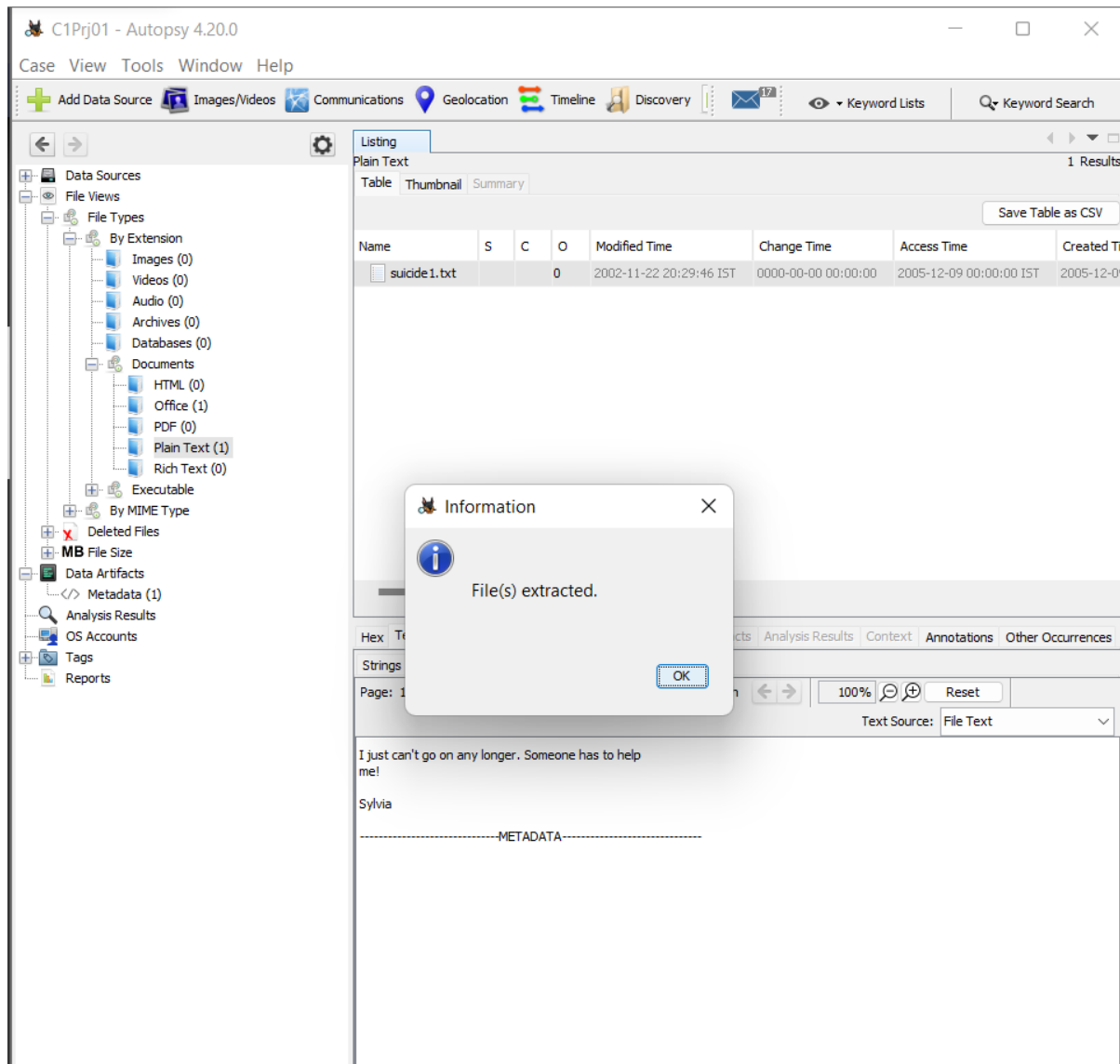
An image of the victim's computer's plain text file is displayed in the screen shot above. Given that it provides us with all of the files' metadata, this image may be crucial evidence in the case. Flags show whether or not the files have been removed. Unallocated means the file has been removed.

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06



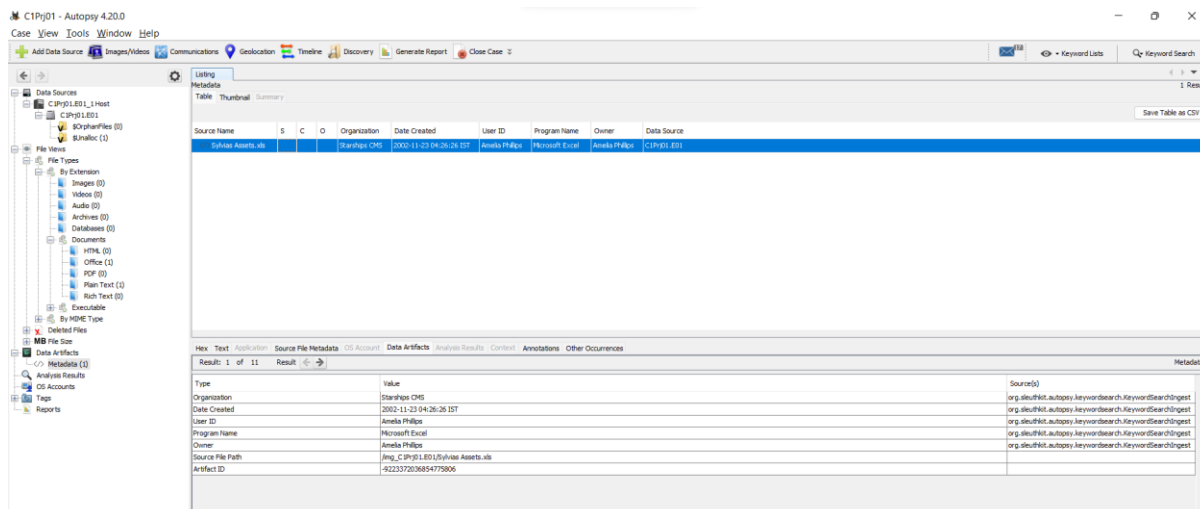
Autopsy has the ability to also produce and gives the hexadecimal view of the files. By extracting them we can do further analysis without altering or changing the image file.

PES1UG20CS581

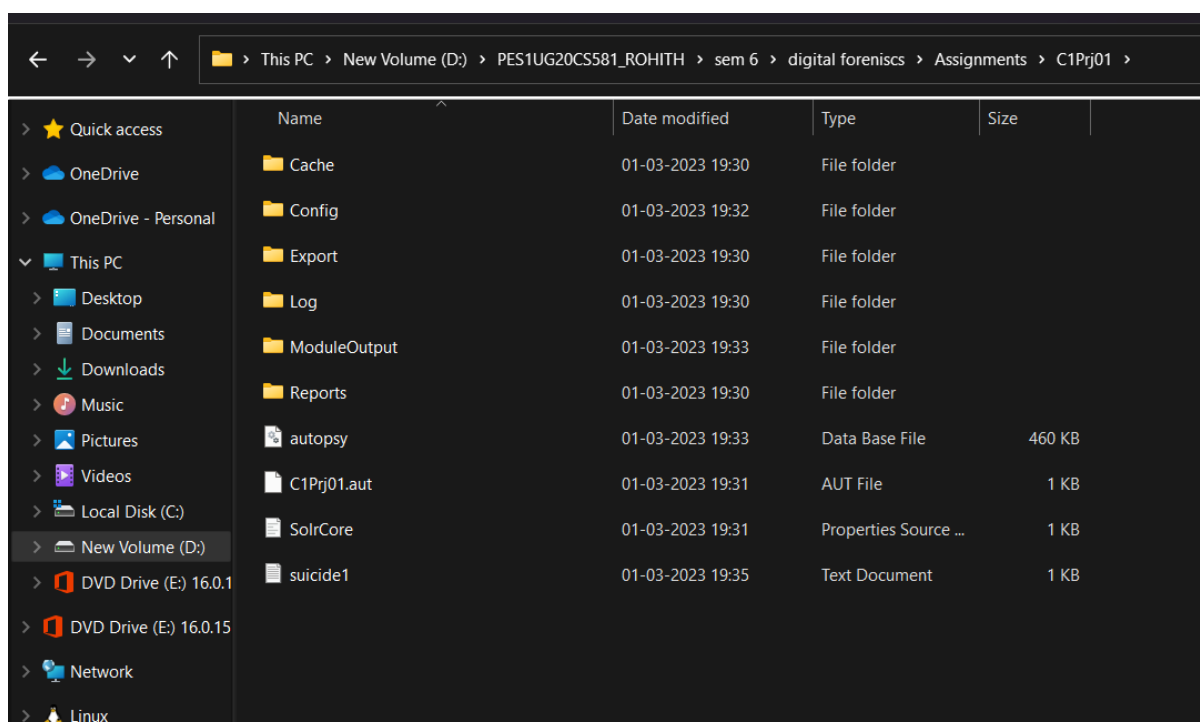
ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06



In the above Screenshot We can see the Metadata information of the another files which is found in the image file and we can see the Author and the Organization name also.



In the Above Screenshot we can see the extracted image in the Case folder after the extraction step is completed.

Report

From the above observations,, it could appear at first glance that this is a suicide case, but with deeper inspection, it becomes clear that the timings of the file are unclear.

Including this person could provide a case lead. We need to find out more about how these two people are related.

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06

Task -02

New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: C1Prj04

Examiner

Name: Rohith H PES1UG20CS581

Phone: NO

Email: NO

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back Next > Finish Cancel Help

This again is the information of the New Case C1Prj04

Listing

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(DV)	Flags(Meta)	Known	Location	MD5 Hash	SHA-256 Hash
Gettysburg.jpg				2004-06-23 21:29:52 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:05 IST	18927	Unallocated	Unallocated	unknown	Img_C1Prj04\Gettysburg.jpg	2855da4cf52174c1576af636c23224e	0009c053a227b950494
Lincoln.jpg				2004-06-23 21:29:56 IST	0000-00-00 00:00:00	2004-06-24 00:00:00 IST	2004-06-23 22:36:08 IST	18953	Allocated	Allocated	unknown	Img_C1Prj04\Lincoln.jpg	60579423c3c0b049477020a15a9b03f9	19a134726a056d6174e
f0000000.jpg				2004-06-23 21:29:52 IST	0000-00-00 00:00:00	2004-06-24 00:00:00 IST	2004-06-23 22:36:12 IST	18953	Unallocated	Unallocated	unknown	Img_C1Prj04\Lincoln.jpg	c2d25934b7613177e47d050ae51c4d	076342adef75d9917

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

87% Reset

Tags Menu

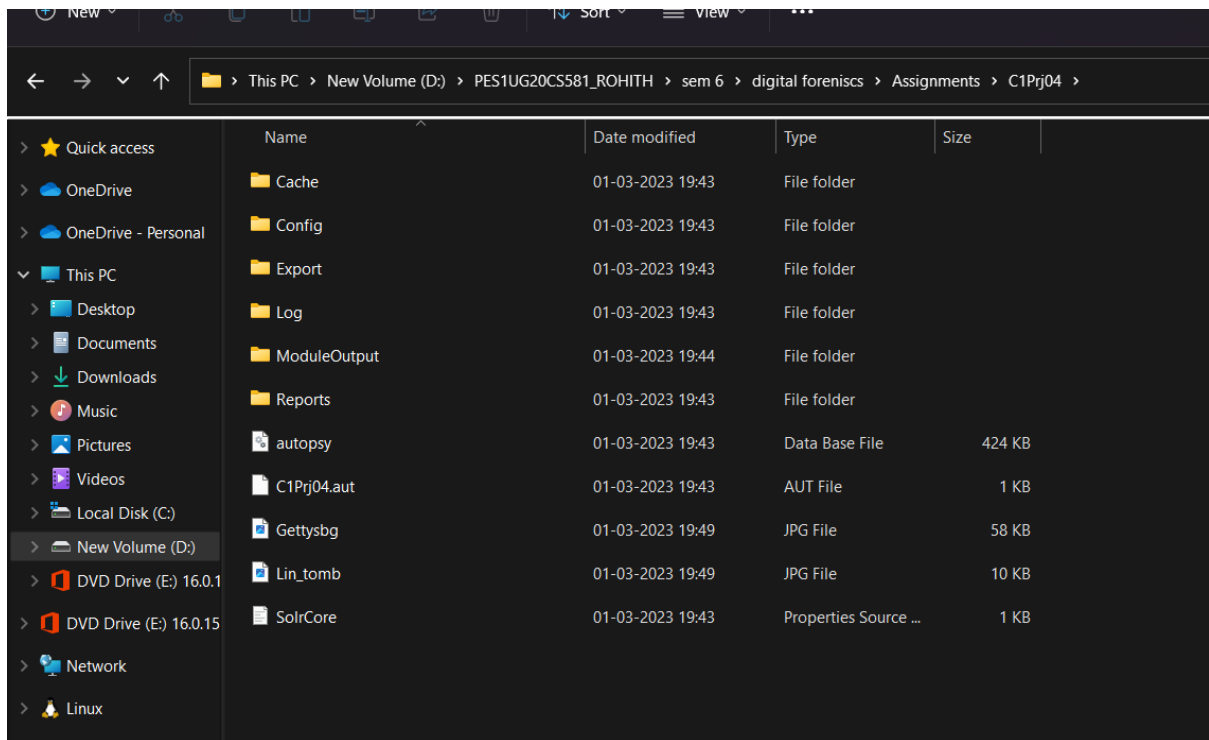
From the above screenshot we can see that we got the pictures / images which are related to the case . We also got the hashed images which would be critical in the investigation of the file and some of the files spaces are unallocated that means that the files /images has been deleted.

PES1UG20CS581

ROHITH H

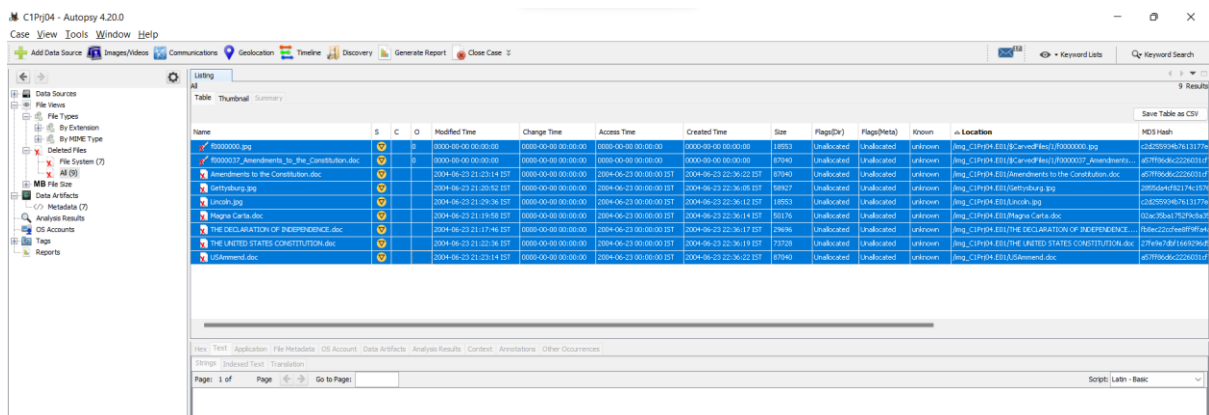
J SEC

DIGITAL FORENSICS ASSIGNMENT -06



The above screenshot shows the images that we extracted from the autopsy tool for this case.

Task -03



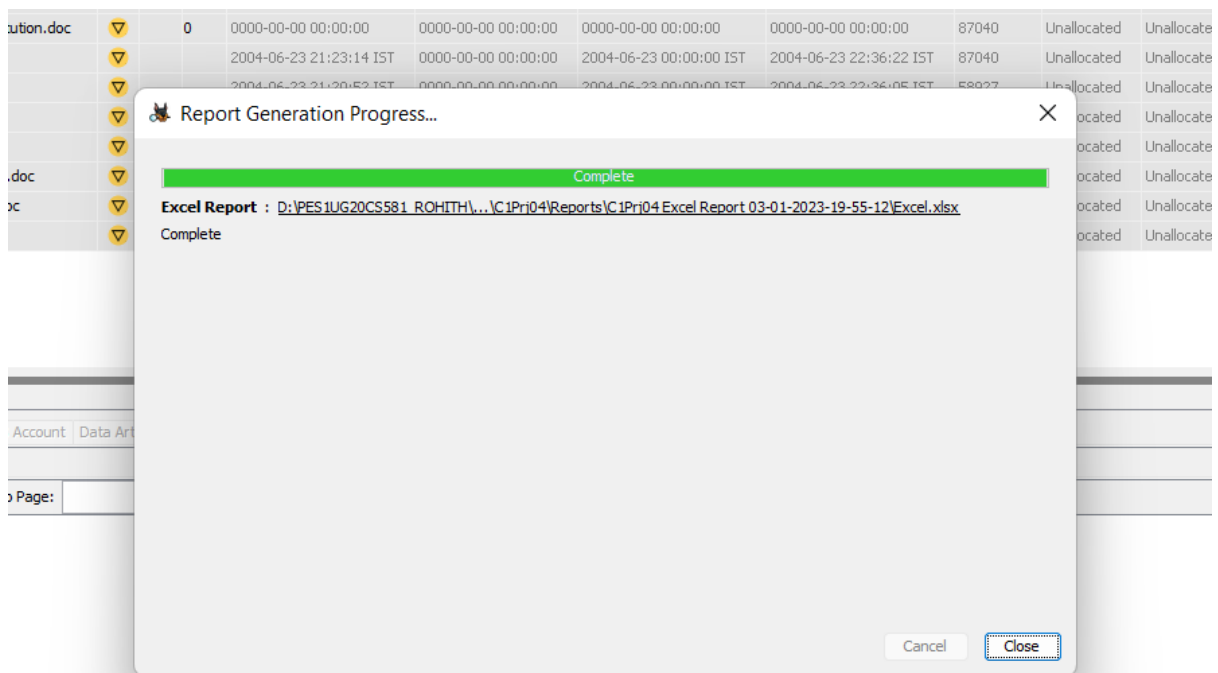
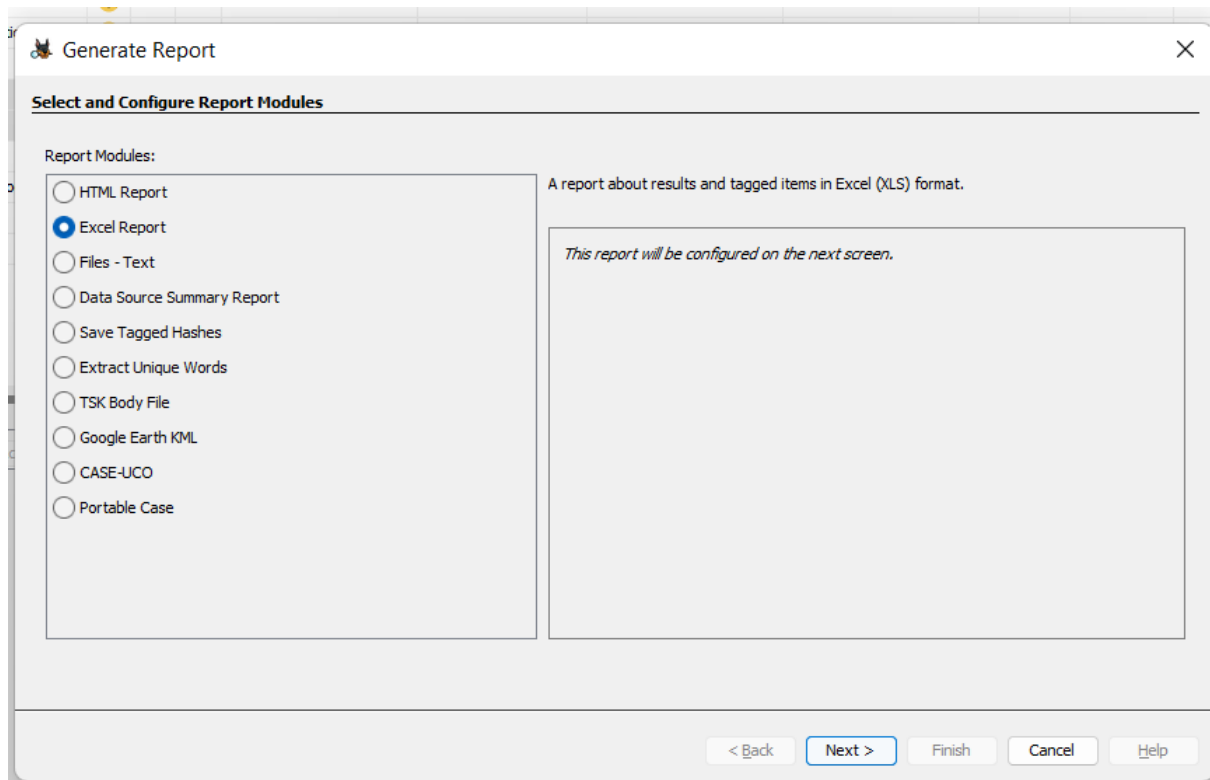
This screenshot provides the list of all the files that are been deleted and located in the unallocated location and first two files have no temporal information present in them.

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06



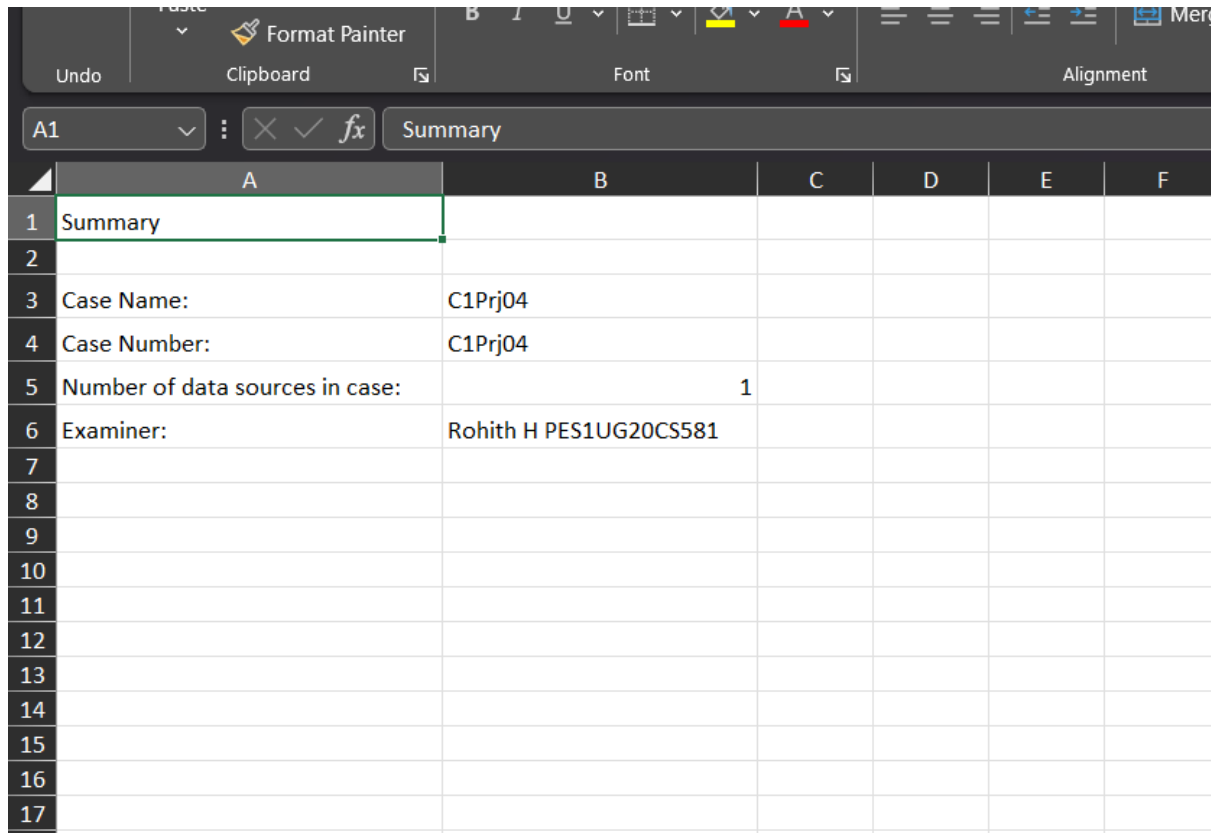
We extracted the excel sheet from the Autopsy tool .

PES1UG20CS581

ROHITH H

J SEC

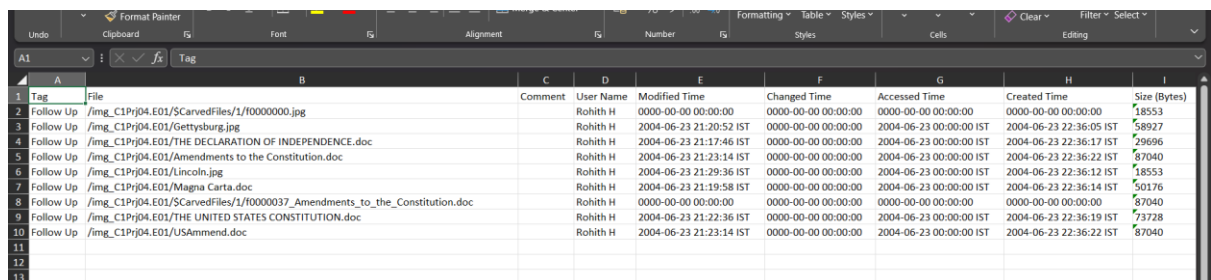
DIGITAL FORENSICS ASSIGNMENT -06



	A	B	C	D	E	F
1	Summary					
2						
3	Case Name:	C1Prj04				
4	Case Number:	C1Prj04				
5	Number of data sources in case:	1				
6	Examiner:	Rohith H PES1UG20CS581				
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						

As u can see that the Autopsy has the capability of creating/ generating the report from the image.

They represents those information in the excel files or documents or html format and many more.



Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)
1	Follow Up	/img_C1Prj04.E01/SCarvedFiles/1/0000000.jpg	Rohith H	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	18553
2	Follow Up	/img_C1Prj04.E01/Gettysburg.jpg	Rohith H	2004-06-23 21:20:52 IST	0000-00-00 00:00:00	2004-06-23 00:00:00 IST	2004-06-23 22:36:05 IST	58927
3	Follow Up	/img_C1Prj04.E01/THE DECLARATION OF INDEPENDENCE.doc	Rohith H	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 IST	29696
4	Follow Up	/img_C1Prj04.E01/Amendments to the Constitution.doc	Rohith H	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 IST	87040
5	Follow Up	/img_C1Prj04.E01/Lincoln.jpg	Rohith H	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 IST	18553
6	Follow Up	/img_C1Prj04.E01/Magna Carta.doc	Rohith H	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 IST	50176
7	Follow Up	/img_C1Prj04.E01/SCarvedFiles/1/0000037_Amendments_to_the_Constitution.doc	Rohith H	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	87040
8	Follow Up	/img_C1Prj04.E01/THE UNITED STATES CONSTITUTION.doc	Rohith H	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 IST	73728
9	Follow Up	/img_C1Prj04.E01/USAmend.doc	Rohith H	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 IST	87040
10								
11								
12								
13								

In the above screenshot we can see the information about the files that were deleted from the suspect machine that is from the image file, these are very useful when we are working with the large data/image size.

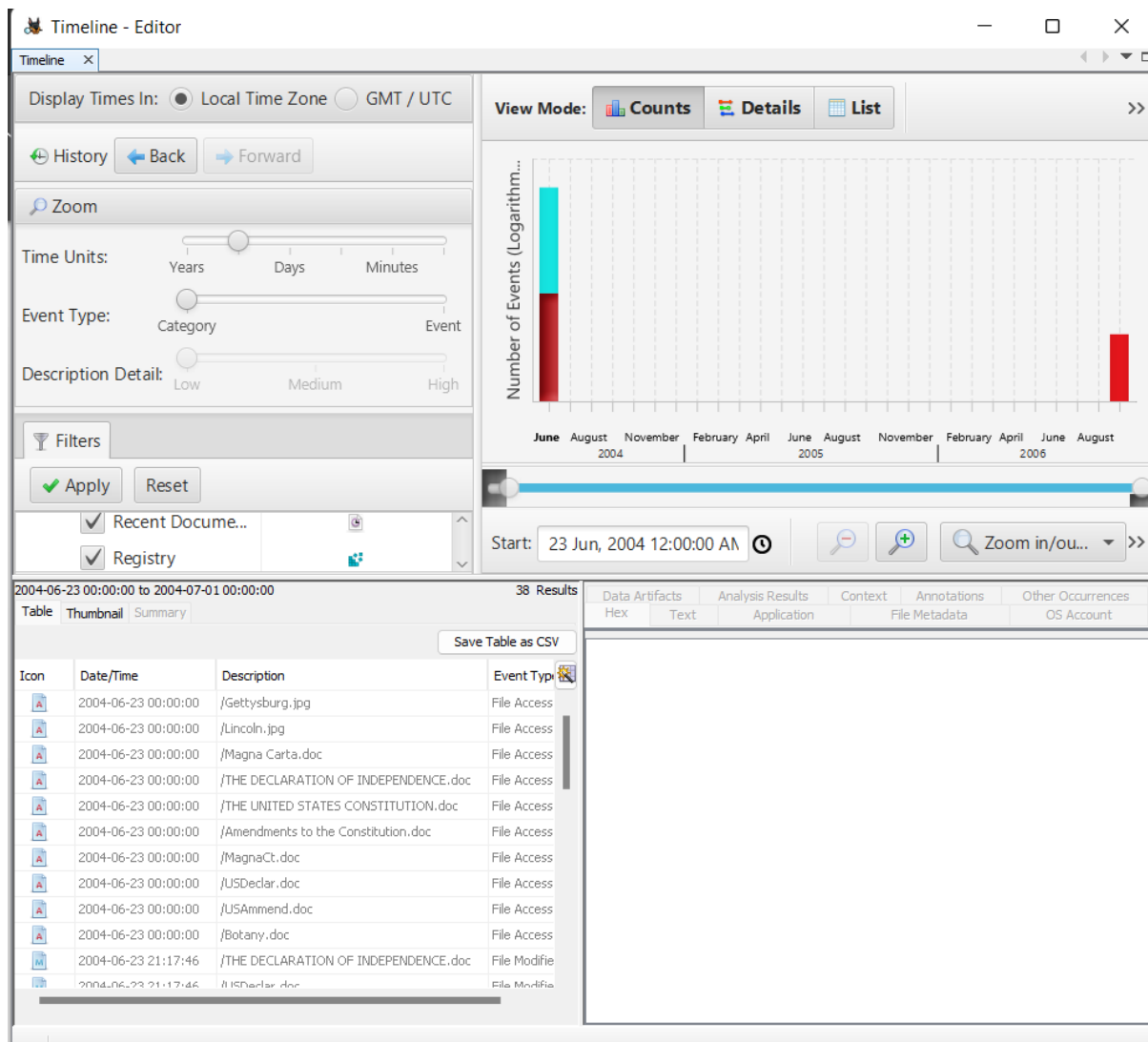
Timeline Analysis

PES1UG20CS581

ROHITH H

J SEC

DIGITAL FORENSICS ASSIGNMENT -06



The above screenshot shows the graphical representation of the timeline of the selected files in the image

Report (Task -02 and Task -03)

Finally observing all the files in the image we can say that the suspect/victim had a lot of information in his system which were related to the constitution and the president Abraham Lincoln.

The modified and the created and the accessed date are same which make the case more suspicious and we can conclude that the suspect/victim had some of the political awareness about the events that are occurred in the past.