1.Complete Hands-on Projects 1-1, 1-2, 1-3,1-4, 1-5, and 1-6. Textbook pages 55-61. For each project, write a short description of what the project is about; include 2 or 3 pictures of the relevant steps (up to you what to select). Create one document with all your answers saved as a doc or pdf. Name the file as follows: lastnameHands-on1.pdf.

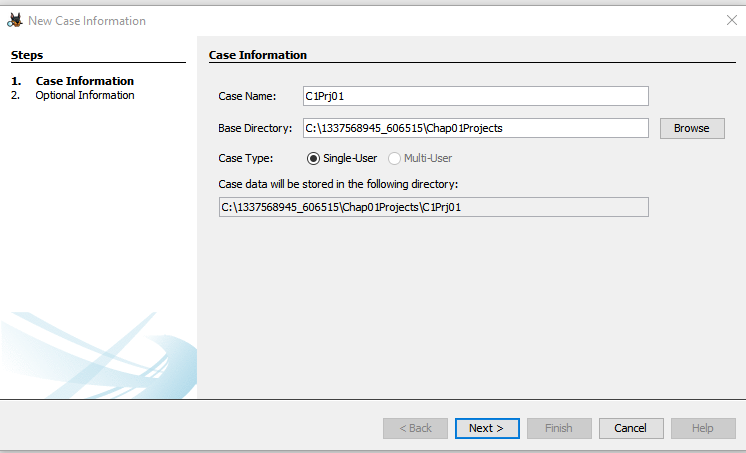
**Hands-On Project 1-1**

The case in this project involves a suspicious death. Joshua Zarkan found his girlfriend’s dead body in her apartment and reported it.

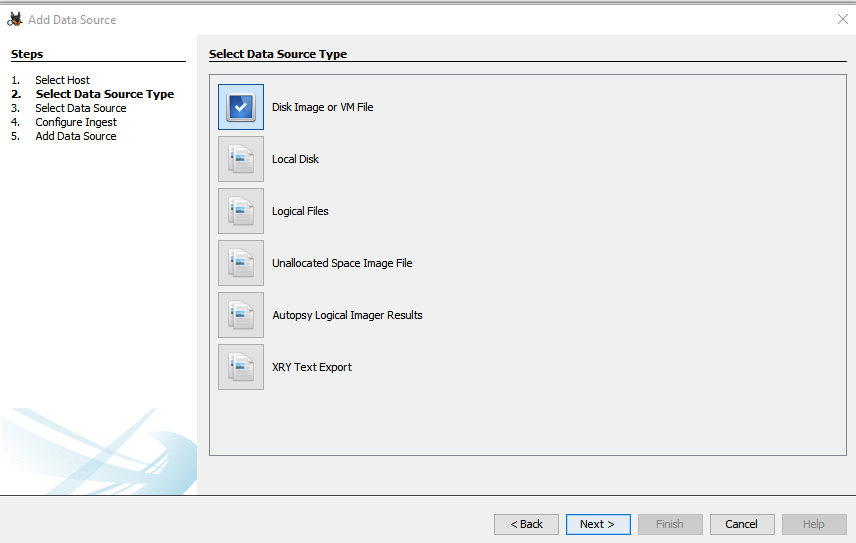
* The first responding law enforcement officer seized a USB drive.
* A crime scene evidence technician skilled in data acquisition made an image of the USB drive with FTK Imager and named it C1Prj01.E01.
* Following the acquisition, the technician transported and secured the USB drive and placed it in a secure evidence locker at the police station.
* You have received the image file from the detective assigned to this case and he directs you to examine it and identify any evidentiary artifacts that might relate to this case.

Solution

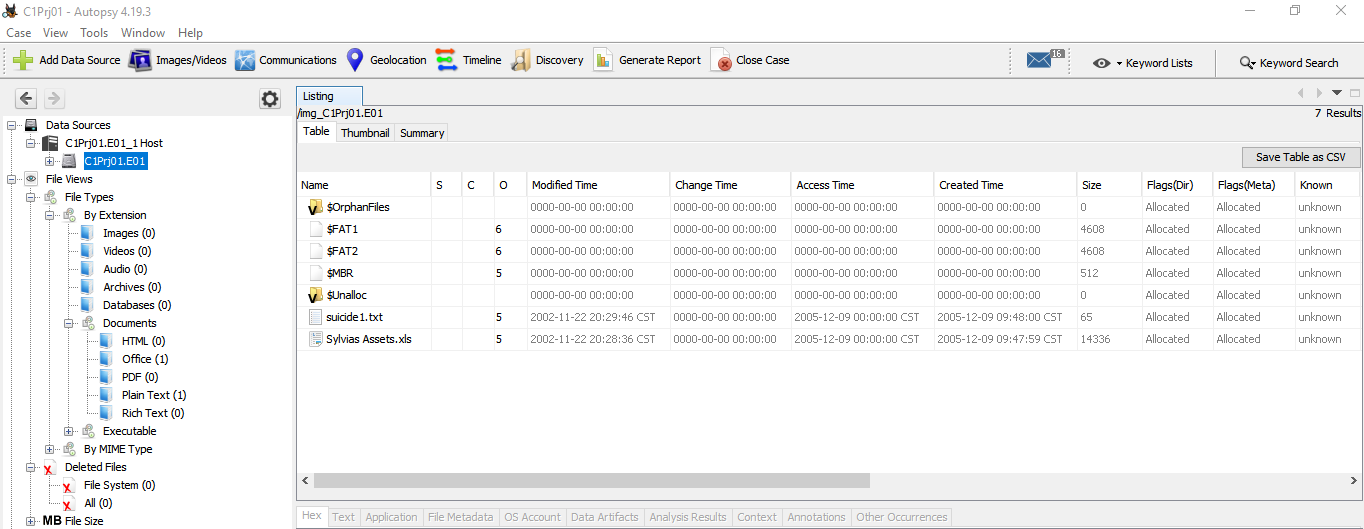
Create a Case Directory



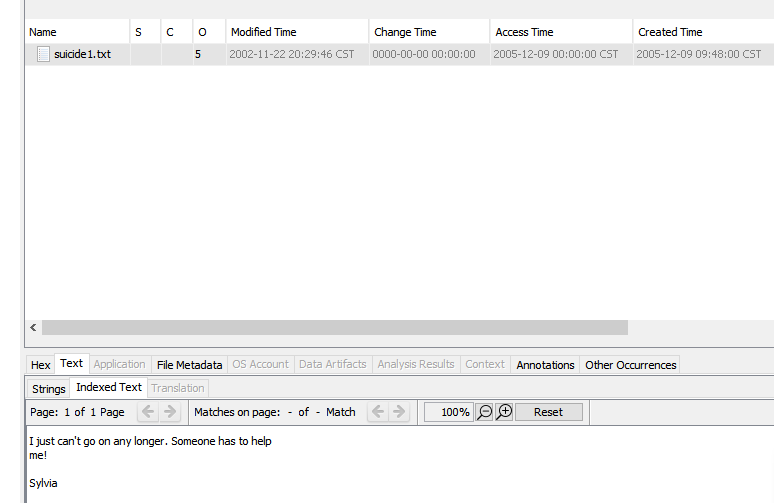
Add Data Source



Extract documents



Suicide1.txt



**Report**

The report reports on the death of Sylvia : -

* A suicide notes: “ I can’t go on any longer Somebody should help me! Sylvia”.
* Victim’s assets: Assets of the sylvia which is in the .xls design



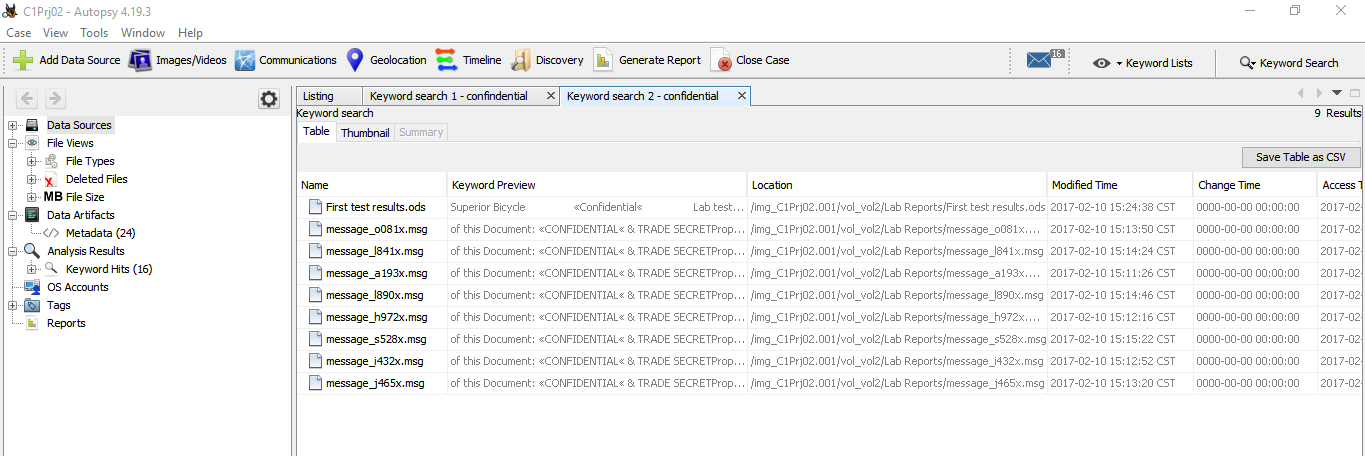
**Hands-On Project 1-2**

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.

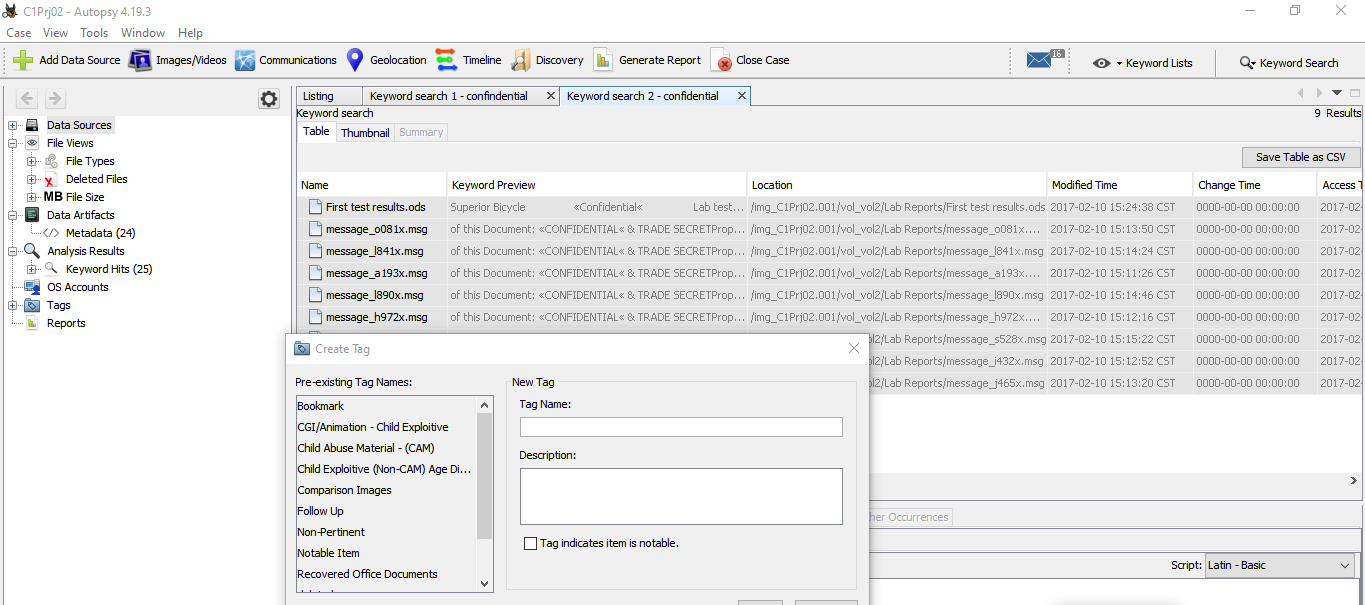
Solution

Screenshots: -

Search for Keyword “Confidential”:



Tag all the files:



Generating Report in Exel

Graphical user interface, application, table, Excel

Description automatically generated

**Report:**

In the given information source when looking for the watchword "classified" there is a rundown of records that are having the catchphrase. Furthermore, the tag for the rundown of records is "Recuperated Office Documents"

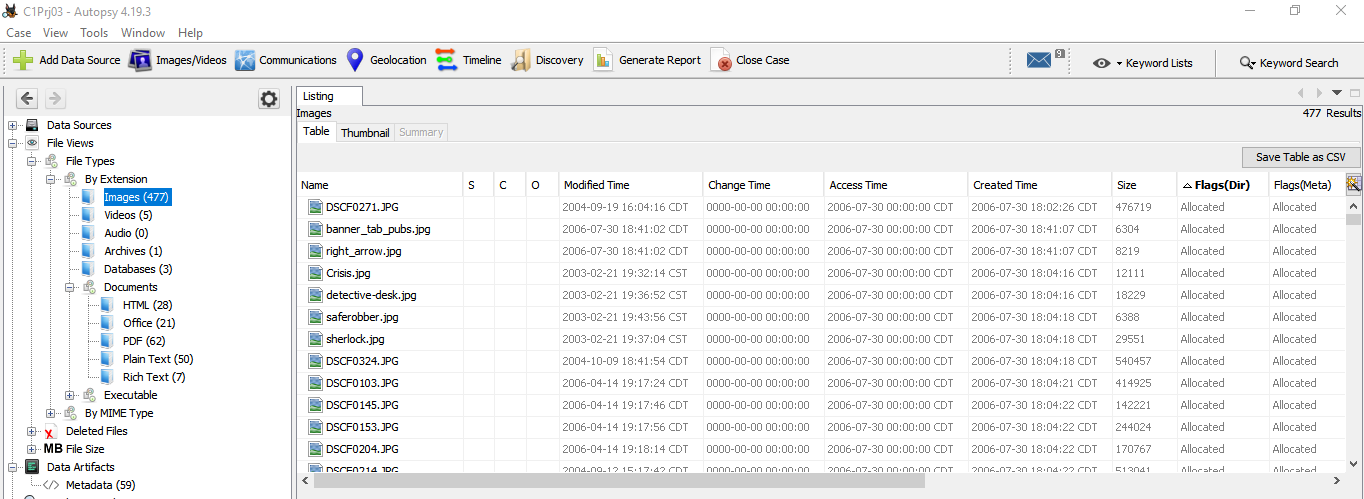
**Hands-On Project 1-3**

You’re an IT security specialist for Superior Sailmakers, a company making sails for sloops and yawls. It sells rigging and sails to many sailboat makers who are competing against one another. Ms. Olsen 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.

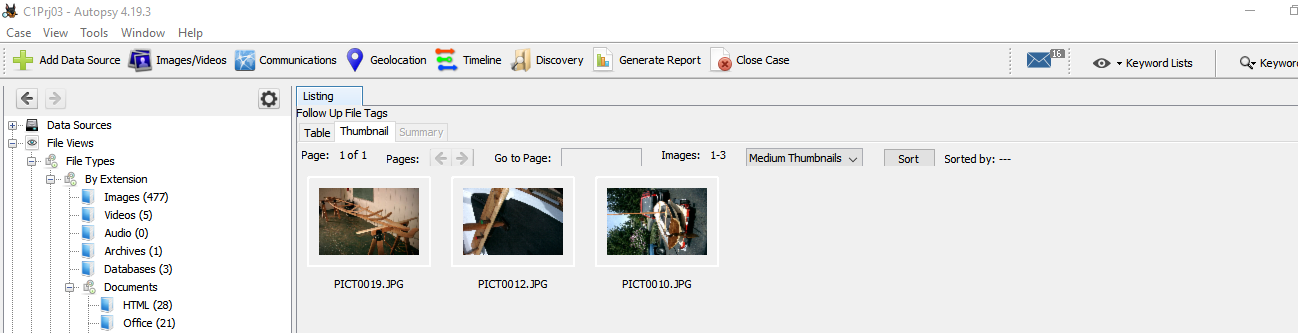
Solution

Screenshot

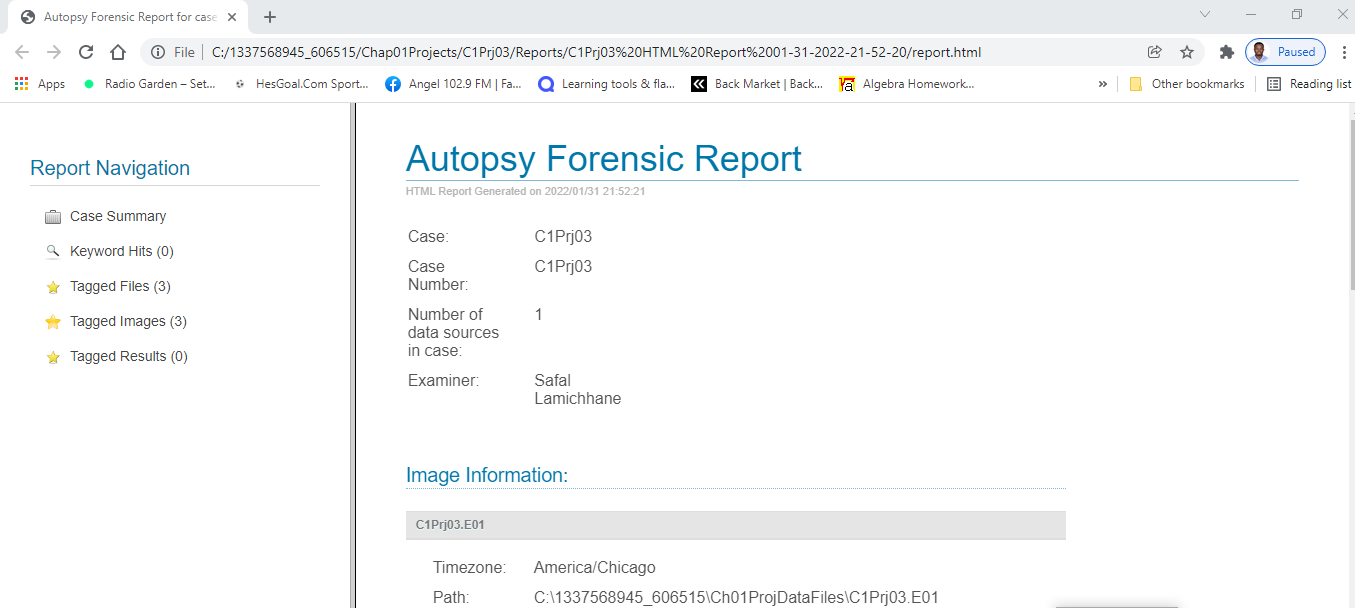
Listing images from data source of usb image:



To view tagged photo:



Generate Report:



There are a couple of pictures from 2006 April and not every one of them relates to boats or portions of boats.

There is a sum of 477 pictures in the USB drive.

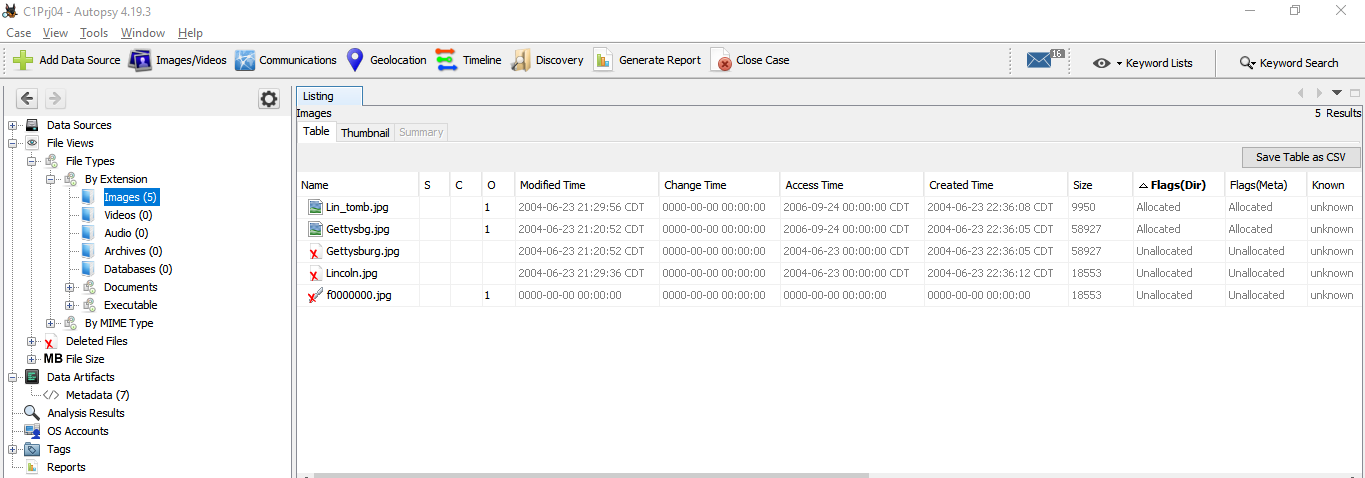
**Hands-On Project 1-4**

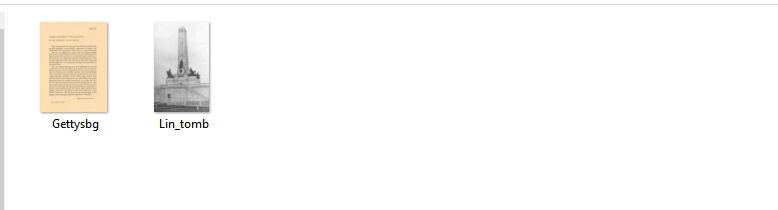
Sometimes discovery demands from law firms require you to recover only allocated data from a disk. This project shows you how to extract just the files that haven’t been deleted (that is, the allocated files) from an image.

Extracting allocated files from an image:

List of files that have been extracted from the usb image:

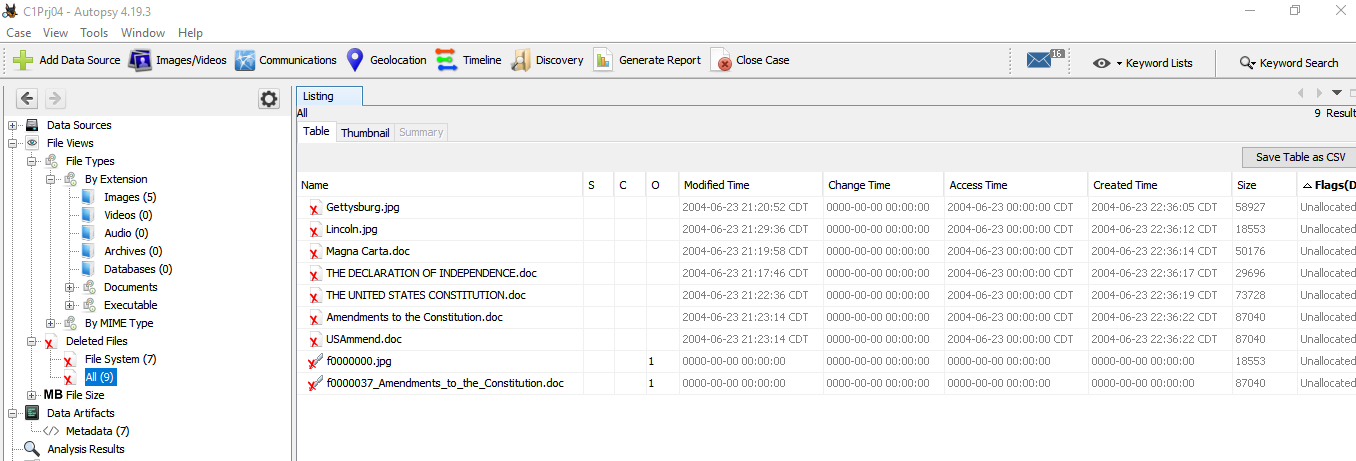
* Lin\_tomb.jpg
* Gettysbg.jpg



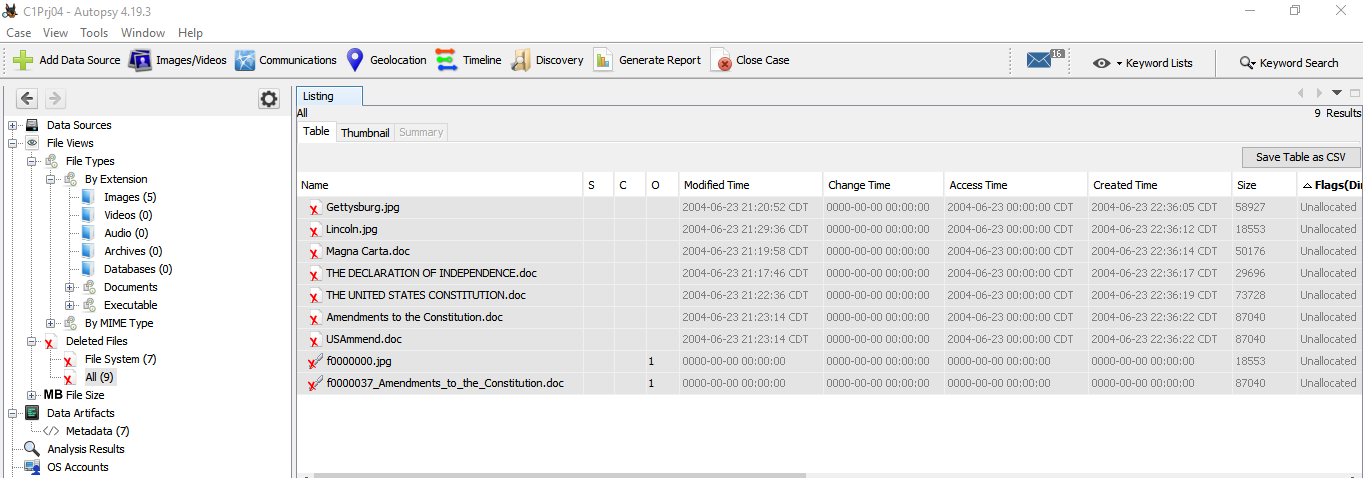


**Hands-On Project 1-5** This project is a continuation from the previous project. You create a report listing all the unallocated (deleted) files Autopsy finds.

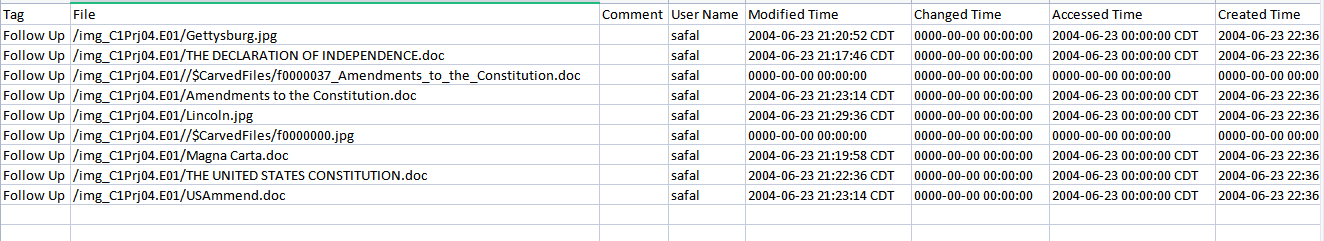
Extracting list of deleted files



Tagging all the deleted files in follow up:



Generating Report:



Below is the list of files that are deleted and broken in the given data source:

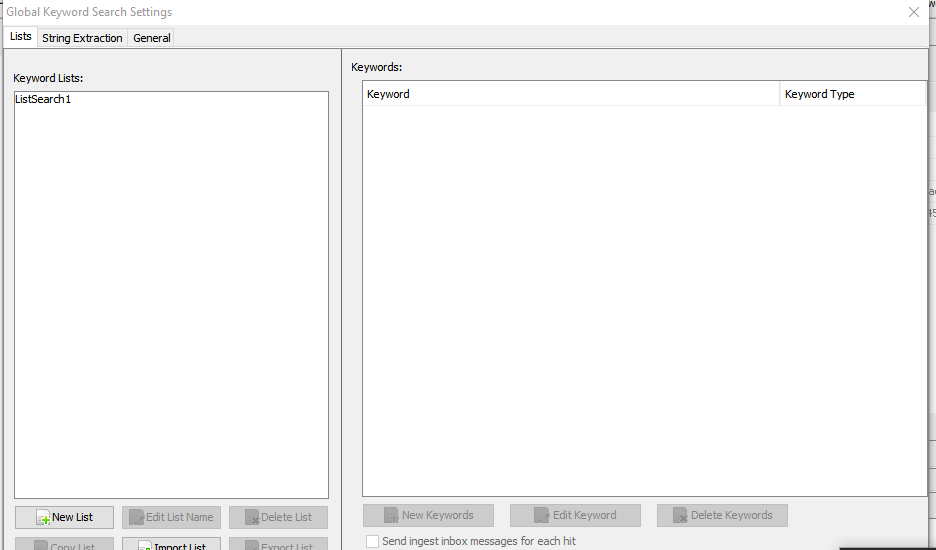
|  |
| --- |
| * /img\_C1Prj04.E01/Gettysburg.jpg |
| * /img\_C1Prj04.E01/THE DECLARATION OF INDEPENDENCE.doc |
| * /img\_C1Prj04.E01/Amendments to the Constitution.doc |
| * /img\_C1Prj04.E01/Lincoln.jpg |
| * /img\_C1Prj04.E01/Magna Carta.doc |
| * /img\_C1Prj04.E01/THE UNITED STATES CONSTITUTION.doc |
| * /img\_C1Prj04.E01/USAmmend.doc |

Below are the corrupted files

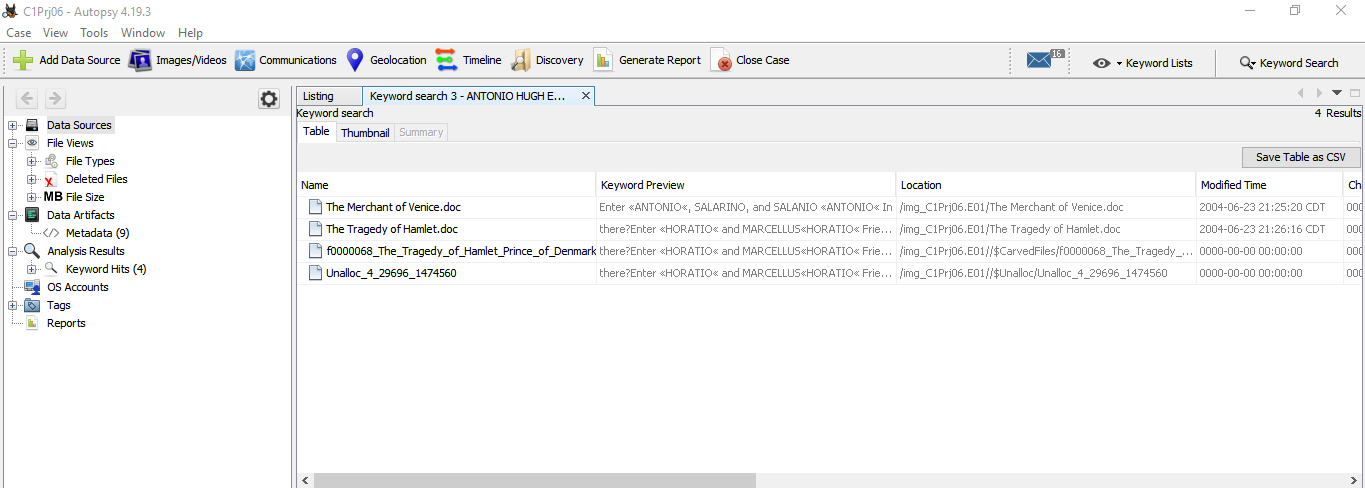
* /img\_C1Prj04.E01//$CarvedFiles/f0000000.jpg
* /img\_C1Prj04.E01//$CarvedFiles/f0000037\_Amendments\_to\_the\_Constitution.doc

Hands-On Project 1-6 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 name

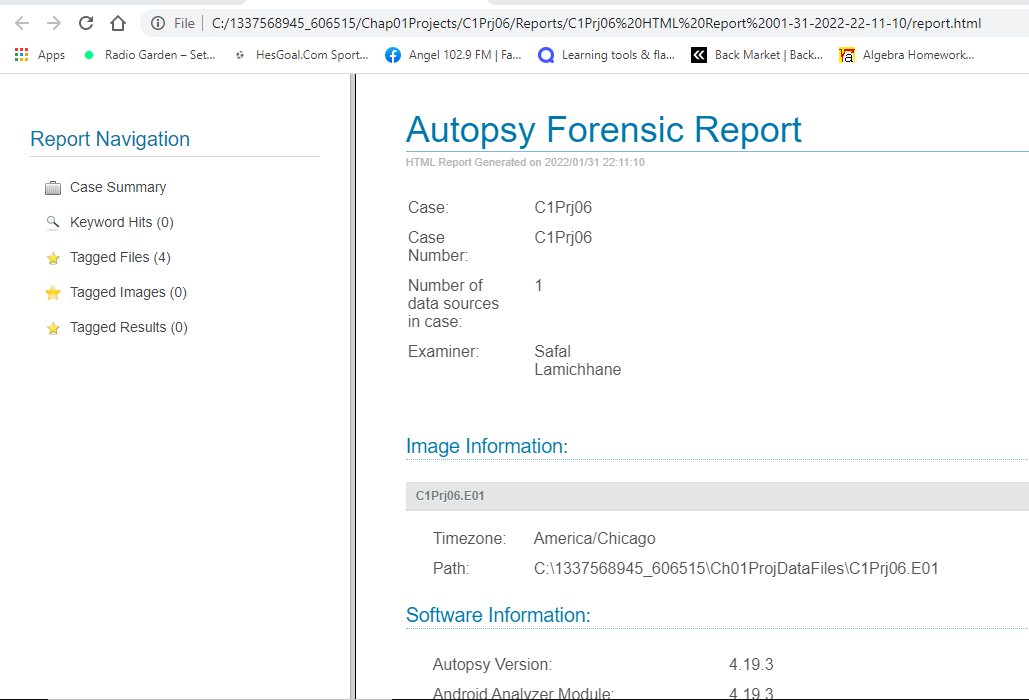
The Global Keyword Search Settings dialog box:



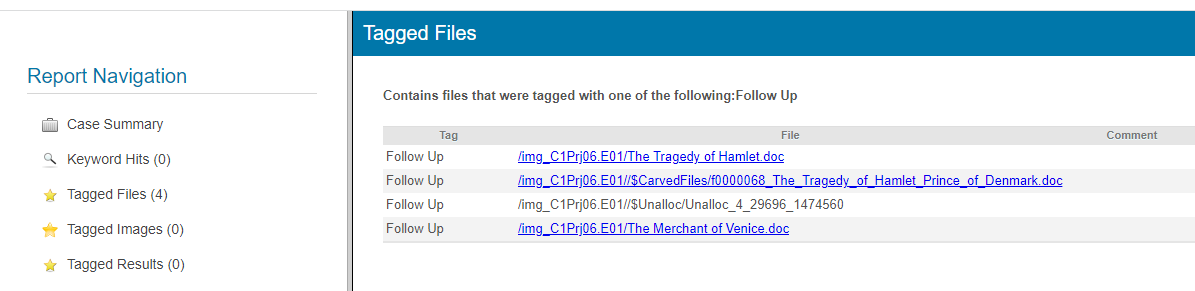
Search result for Keywords:



Generate report:



Tagged files:



List of Keywords:

|  |
| --- |
| * ANTONIO |
| * HUGH EVANS |
| * HORATIO |



2. Write a solution for the Case projects 1-1, 1-2,1-3, and 1-4 pages 62-63

1-1

For defining the nature of this case, the investigator should talk with all the people that are involved in the case. He should inquire about incident. As this case assessment also involve type and number of evidence found. So, investigator must ask questions from all those who are affected with the arson. He should contact the local people if he really wants to find out what happened and ask them about Mr. Kasey. He should find out characteristic of him and why other people think he is involved in this.

1-2

As we know that time is more important, and we need to find out if our work done has efficient or not. For that, I will gather the details about the total cost implied and the total hours worked and completed work in that specific area. Then just to make sure, I would ask the sub-contractor the same question about cost implied and hours worked. I also would get the information about who was the person who signed the first check. As we can see there is an overvaluation of the cost, I would call the person who is responsible in the accounting section and question him about the mismatch between the budgets. As we can see the check of $12750 was made in place of $10,750. As there is more value in check being signed, I would go to the root of that problem. I will also later question Jonathan about this problem. I would tell them to hand me the checkbook and the ledger. As more amounts could be either a human fault or a mistake or also could have been stolen by someone. I would try to find out what had happened. So, to find out if it was a mistake or an intended action, I would call all of them personally and set the interview in person. I would try to evaluate if someone is lying in that interview. After questioning them, I will try to reach out to the result accessing the situation and evaluate my findings. Lastly, I would get a conclusive end.

1-3

First that women should be asked several questions before the investigation should be started.

* If anyone has password of her computer
* Anyone else uses her computer
* Has she downloaded some attachments?
* Firewall installed on it
* If she noticed strange files on computer
* Does the PC have WIFI capabilities?
* What’s her proficiency with computers?

From this question, investigator would have good understanding and could see the possible scenarios that could have occur. It is important to secure the digital evidence and make sure that it remains unaltered. The imaging of the computer disk using write blocking tools should also be performed after that. This helps in collecting the proof that the information has not been modified after being collected. Then he should collect all digital evidence. The Ram should be examined so that he could find any digital evidence prior to shutting down computer.

After that, the examination of the evidence will be started. The investigator will catalogue all recovered evidence and verify it. After this analysis is performed to discover the contents of the disk. This process will include a review of the Windows registry too.

At last, the reporting of the evidence collected and about findings is done. The report can be both verbal when the investigator will present their findings in court.

1-4

The options we have are that we are able to retrieve the files, but we need to have the machine at first to start the process. We would inform about this topic to the user so and recover their files for certain fee. The employee needs to fill the form and let us know about the files that have been accidentally deleted. The form will also help us to know the name of the files that the employee would like to recover so that there will be no misunderstandings in the future.

This issue can happen to anyone even if someone is careful. The data retrieval is a three-step process.

* Questioning client
* Recovering data
* Information delivery to client

In first step we find out what operating system the employee was using and if it was a laptop or a desktop. What programs does the clients use to find out the type of file to be recovered.

For instance: If employee was using MS word then .doc would be included and so on.

Also, we can find out about the directory where the file was and the amount of the files that was deleted and so on. Once the information is gathered, the data can be recovered using a recovery software. There are many free recovery software’s that we use according to the files that we want t recover. EG: Scalpel, Magic Rescue. After the data is recovered, it is turned over to the client.