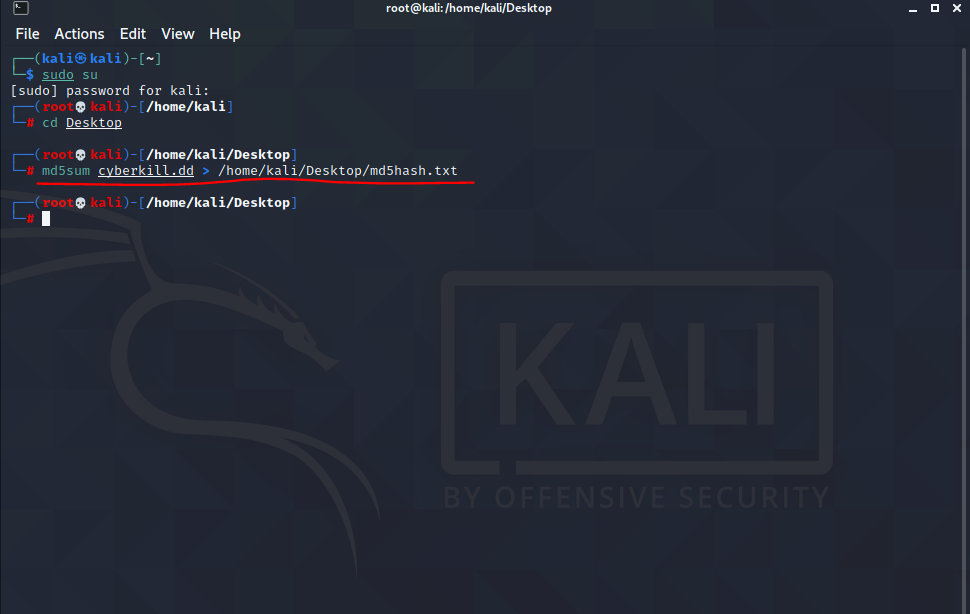
**DIGITAL FORENSICS PROJECT**

A family has recently reported that their daughter has gone missing for over a week. The field officers have seized evidence and an image of the evidence is available with the evidence file link. Download the evidence file and match the hash values to the hashlog.txt. The job is to analyze the evidence and solve the case The following tasks have been designed to get an overall understanding of the digital forensics process. The task is to recover all the files and report your findings and finally document the findings.

**Task 1**: Generate the MD5 and SHA1 hash values of the evidence file and redirect them to a text file. Include a screenshot and also the hash values.



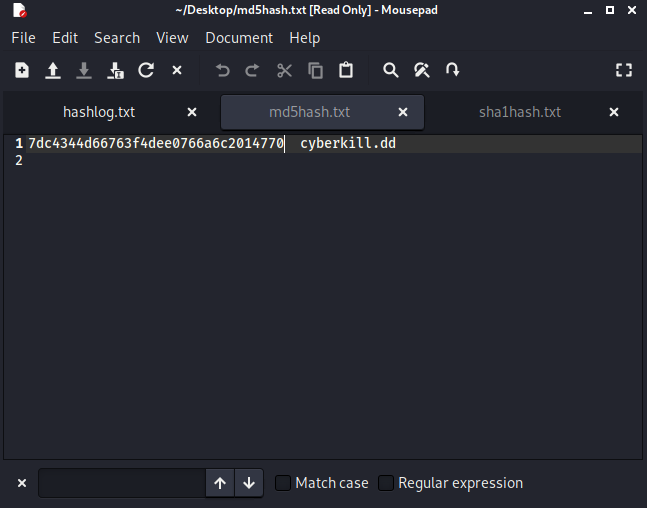
TheCommand i have used for generating MD5 hash value is **md5sum** **cyberkill.dd > /home/kali/Desktop/md5hash.txt**



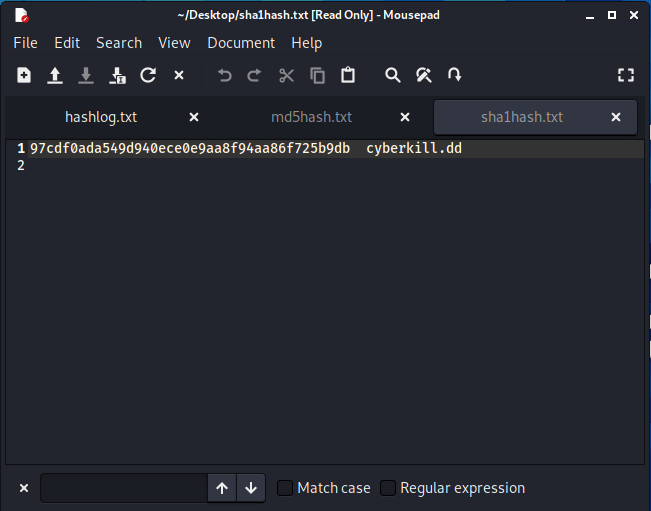
TheCommand i have used for generating Sha1 hash value is **sha1sum** **cyberkill.dd > /home/kali/Desktop/sha1hash.txt**



After entering the commands, two text files containing hash values have been created.

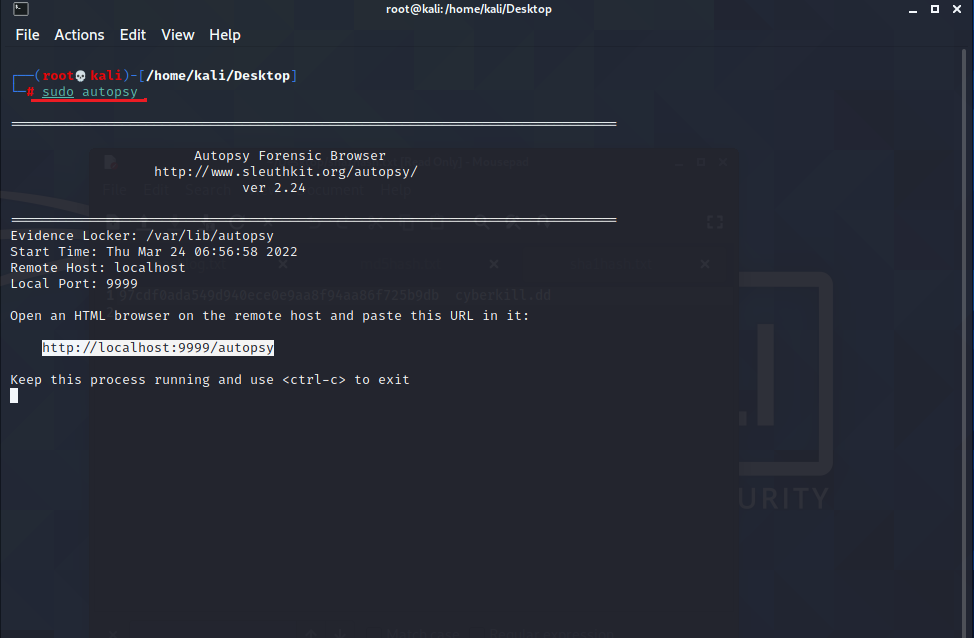


The md5 hash value is **7dc4344d66763f4dee0766a6c2014770.**

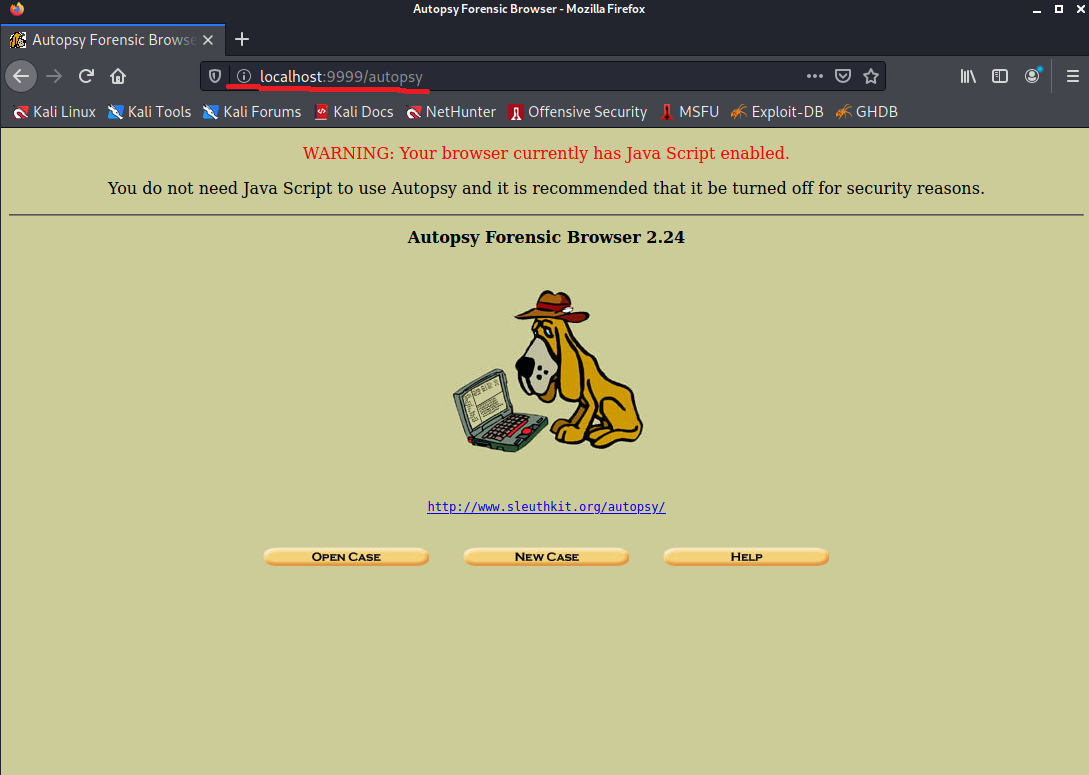


And sha1 hash value is **97cdf0ada549d940ece0e9aa8f94aa86f725b9db.**

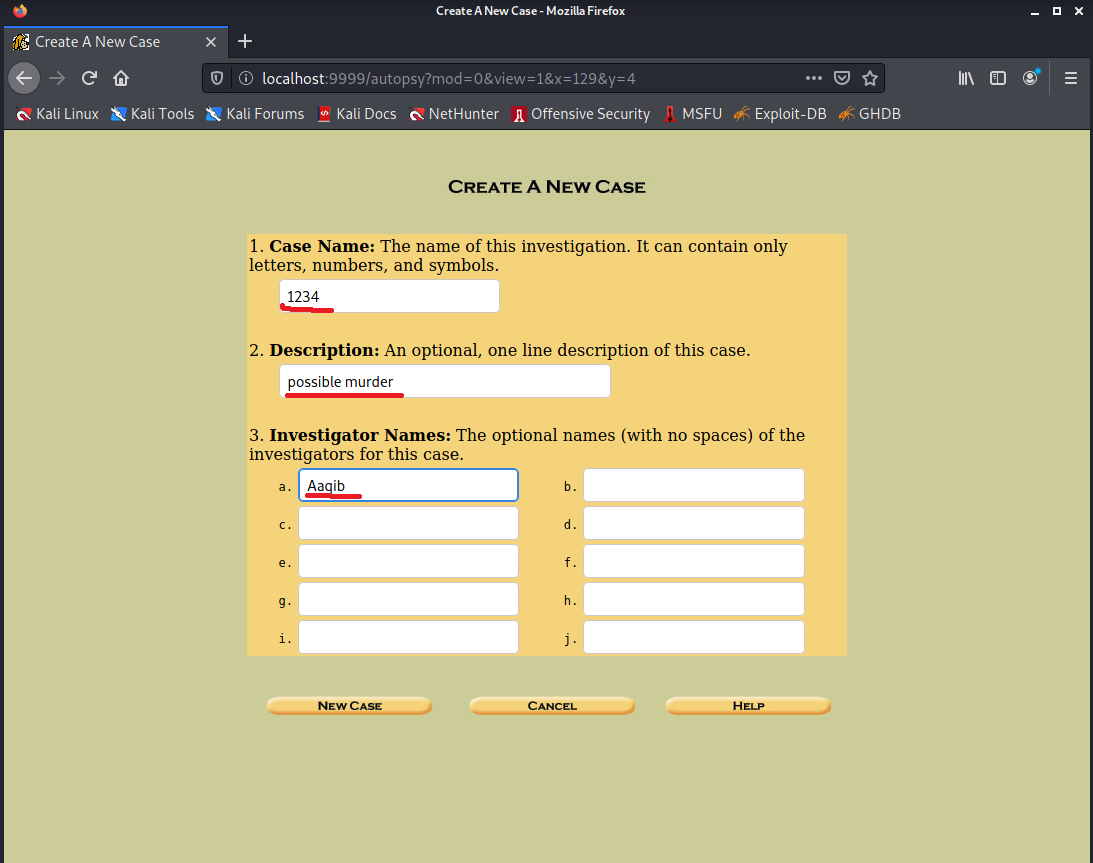
**Task 2**: Recover the files using autopsy browser and include a screenshot.



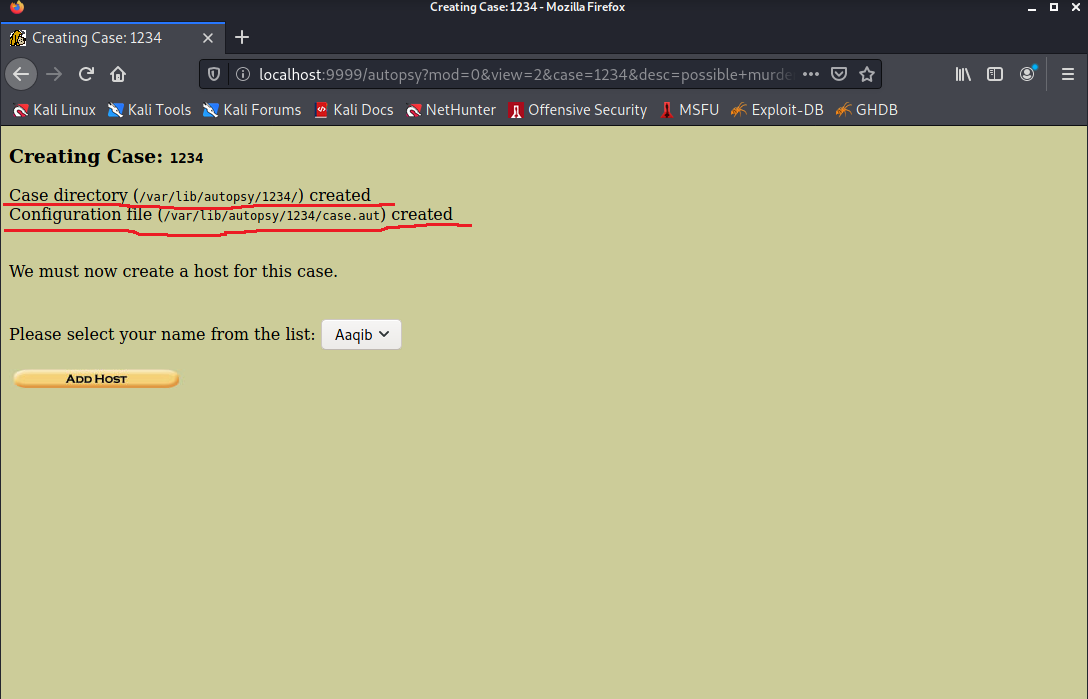
Command I have used for opening autopsy browser is **sudo autopsy.**



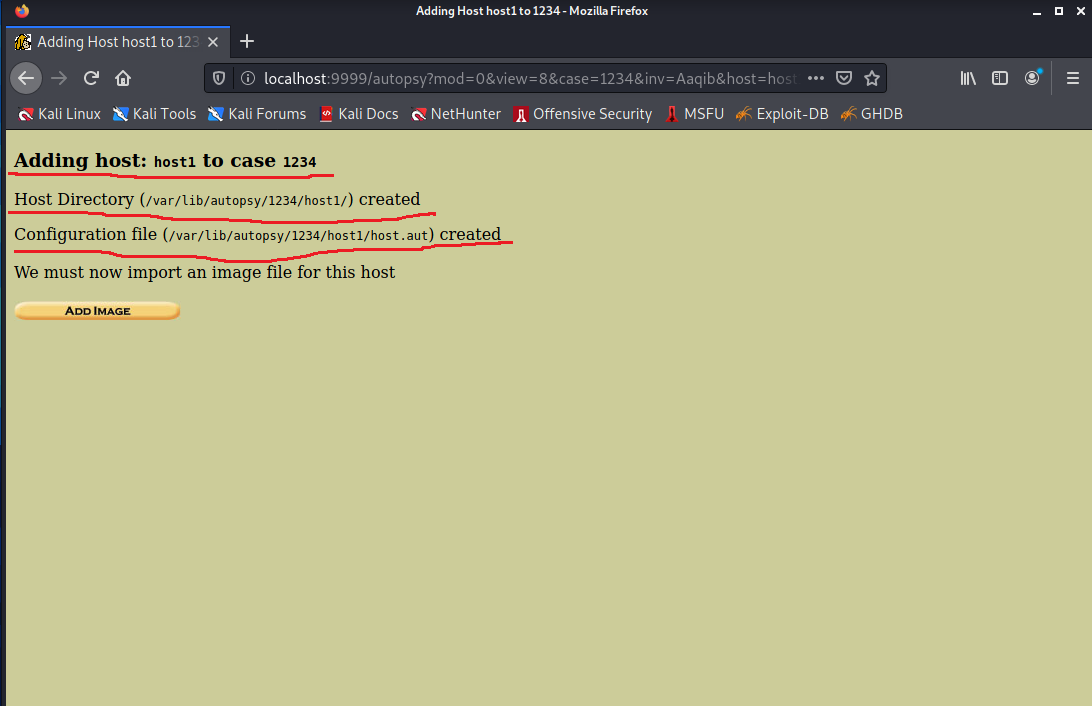
Copying the HTML link and pasting it in my browser.



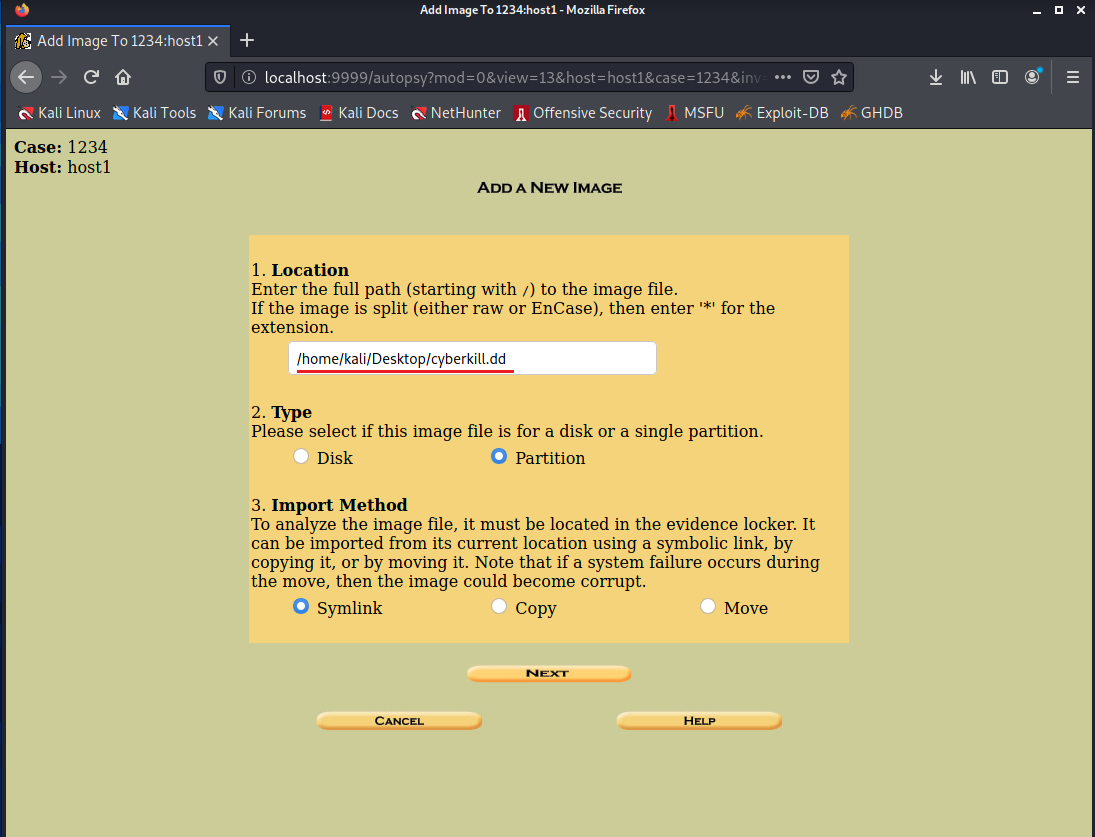
I have selected a new case and then as the highlights show I have entered case name, description, investigator name.



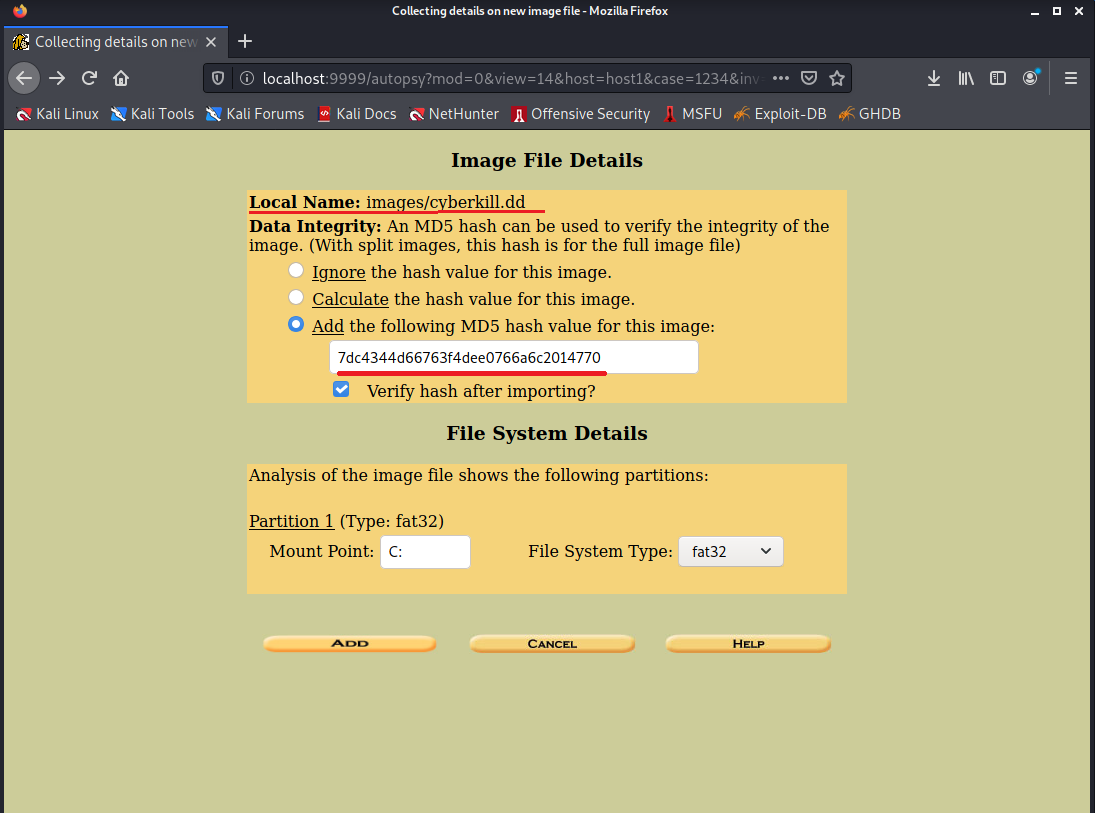
Highlights showing where the case directory has been saved and configuration file has been created. Then I’ve added host.



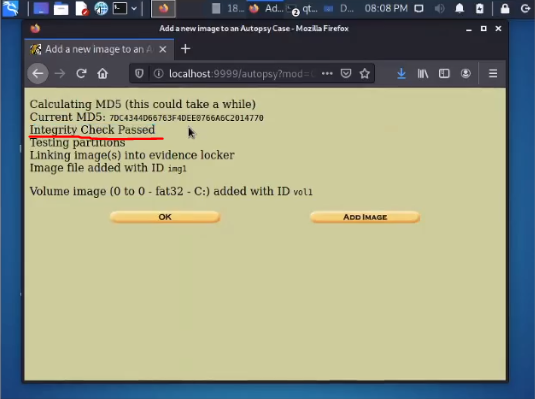
Highlights shows where the Host Directory and configuration file has been saved. Then it asked me to Add Image.



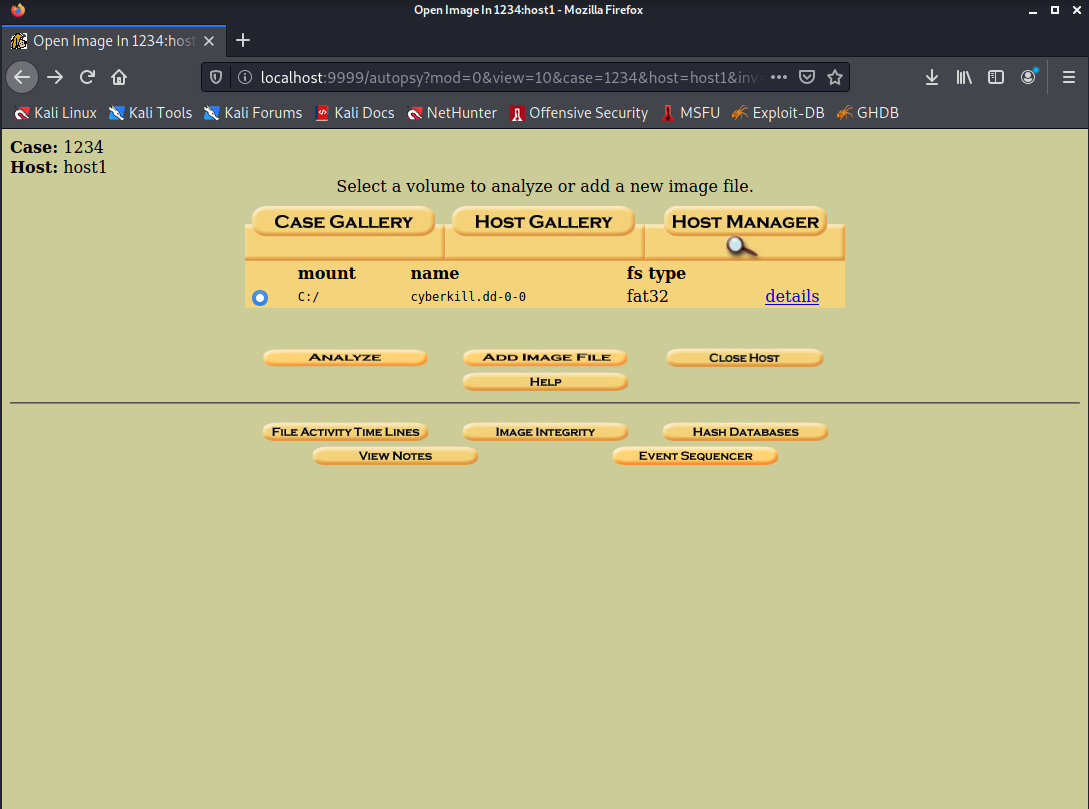
Then I have entered the path where dd file has been kept which is **/home/kali/Desktop/cyberkill.dd**. Then I have selected image file as partition type and import method as Symlink.



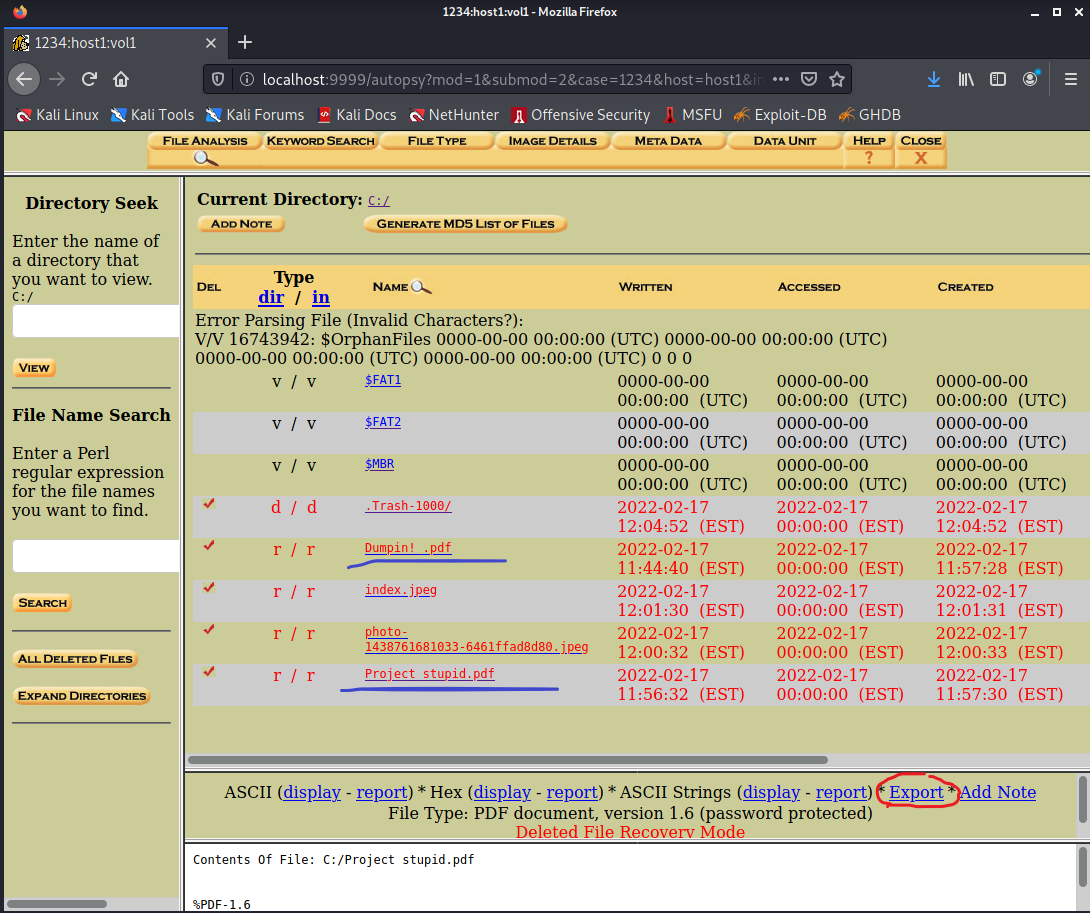
To ensure the evidence file is not modified I have Added MD5 hash value.



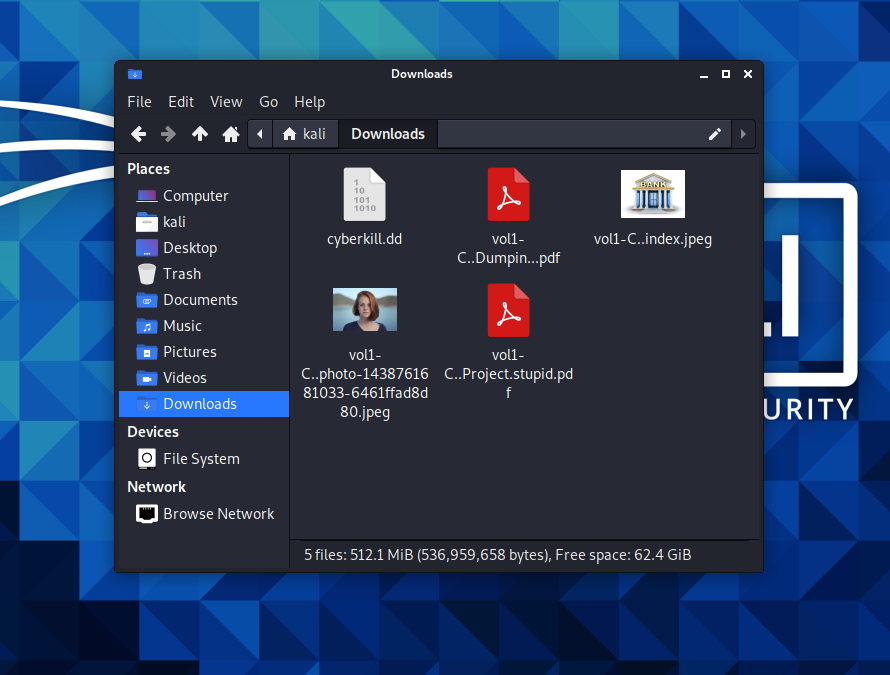
Highlights show that the integrity check passed, that means hash value has not been tampered.



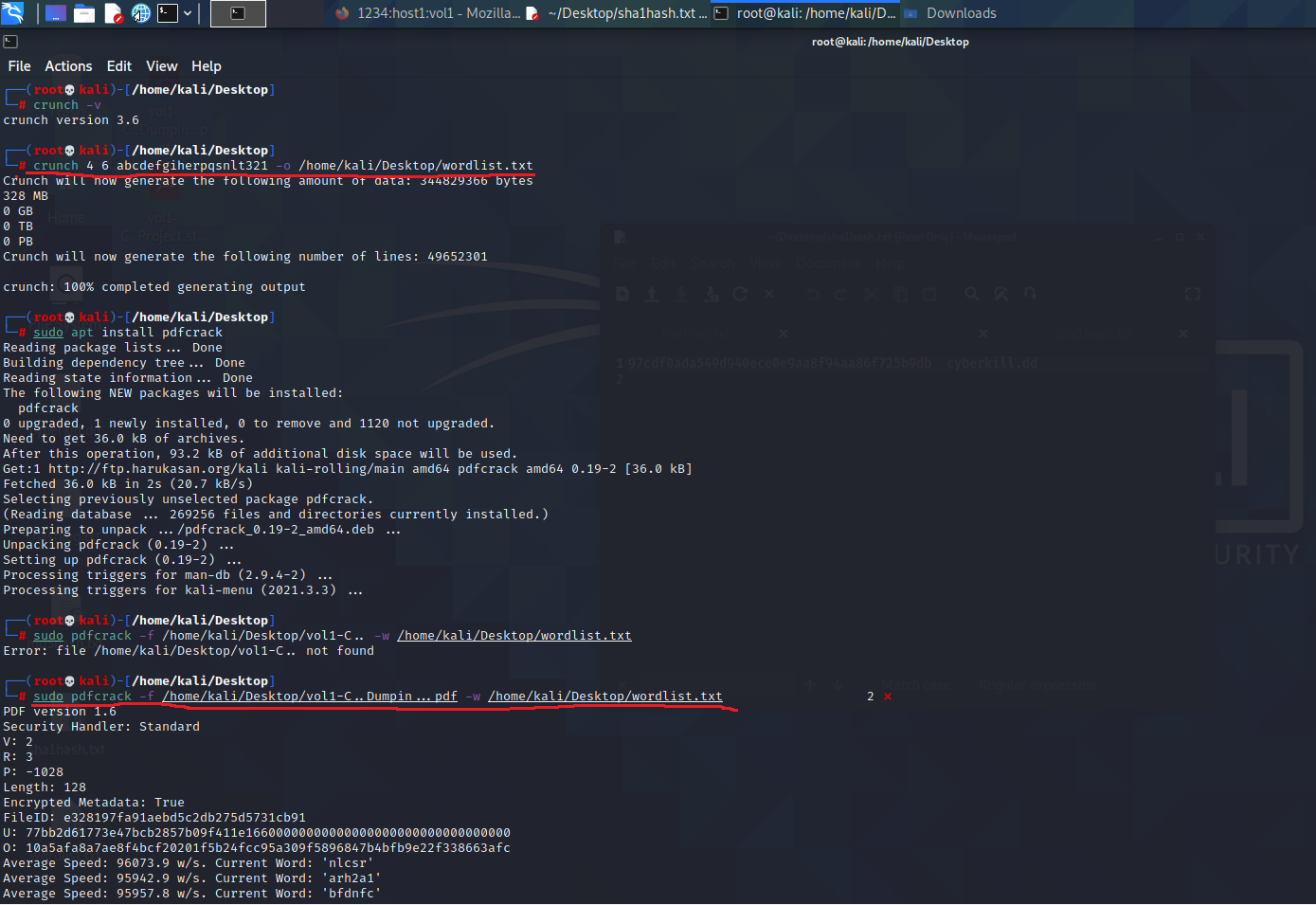
I have selected given image file to analyze.



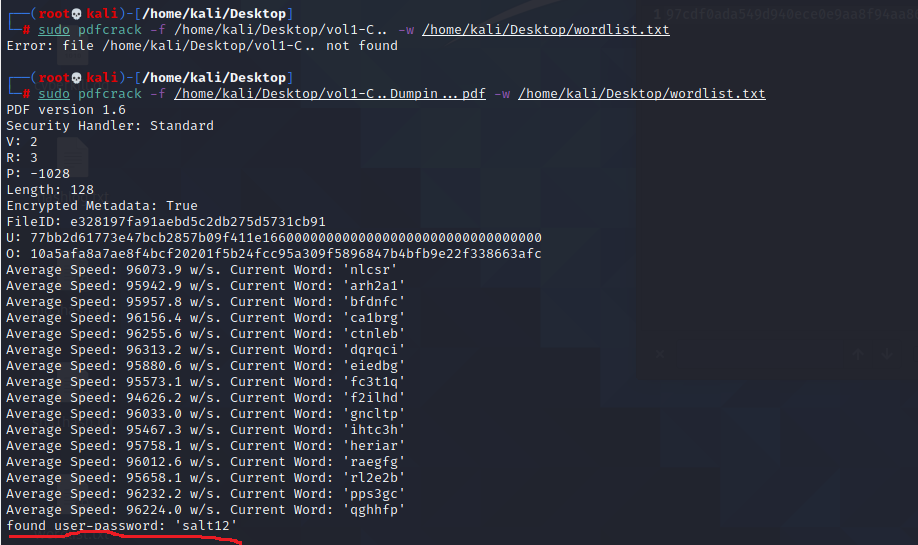
Then it redirected me to all the files stored. The files with red color are the deleted ones. Then I have clicked on two pdf’s which are highlighted and exported it to my virtual machine.



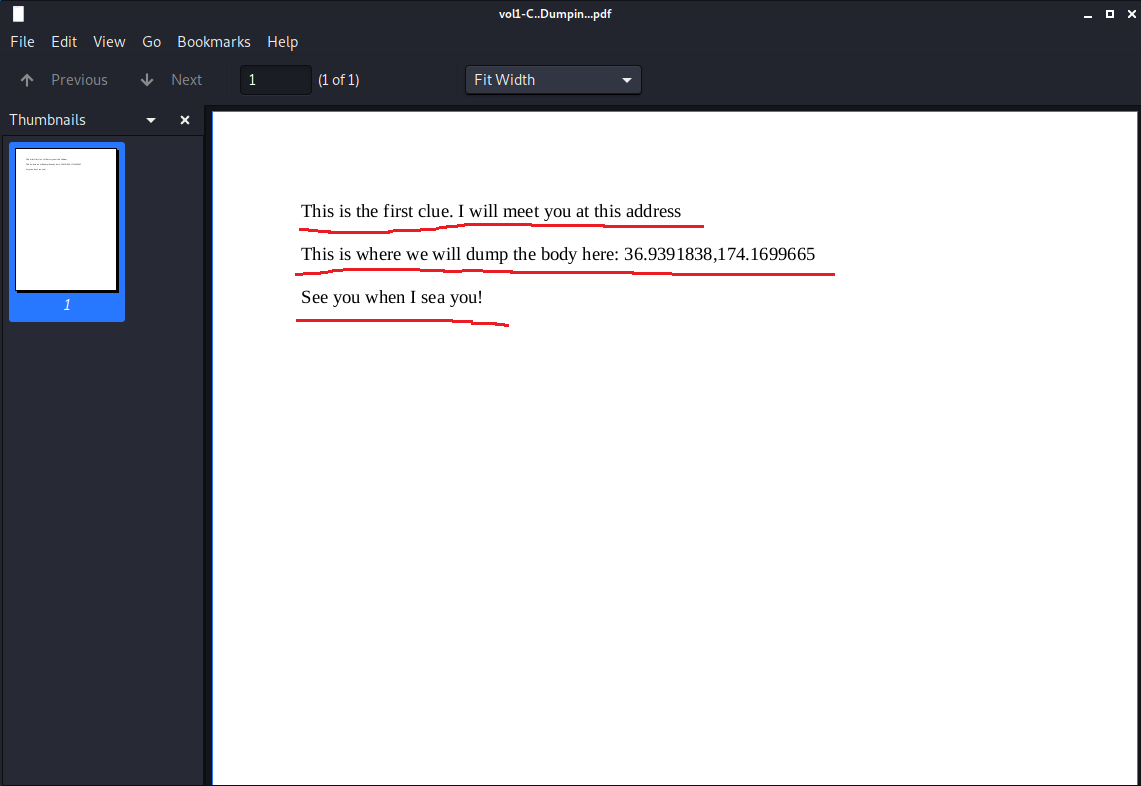
These are the deleted files which I have recovered from autopsy browser. The two pdf’s are password protected.



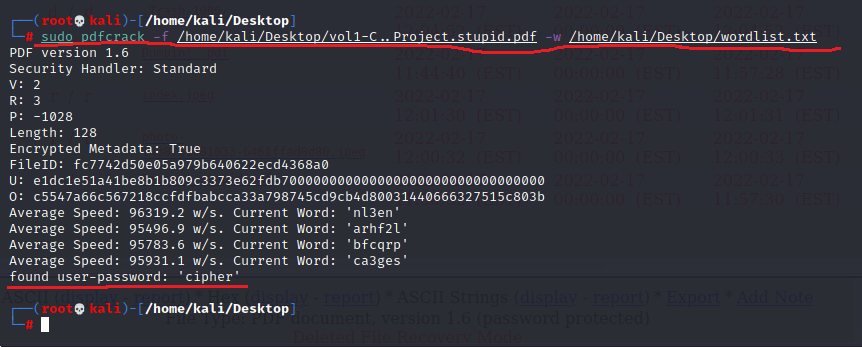
For cracking two pdf’s I have used crunch and pdfcrack. The command I have used for creating wordlist is **crunch 4 6 abcdefgiherpqsnlt321 -o /home/kali/Desktop/wordlist.txt.** Then it had created a text file containing list of all the possible combination of characters from the given combo **abcdefgiherpqsnlt321.**



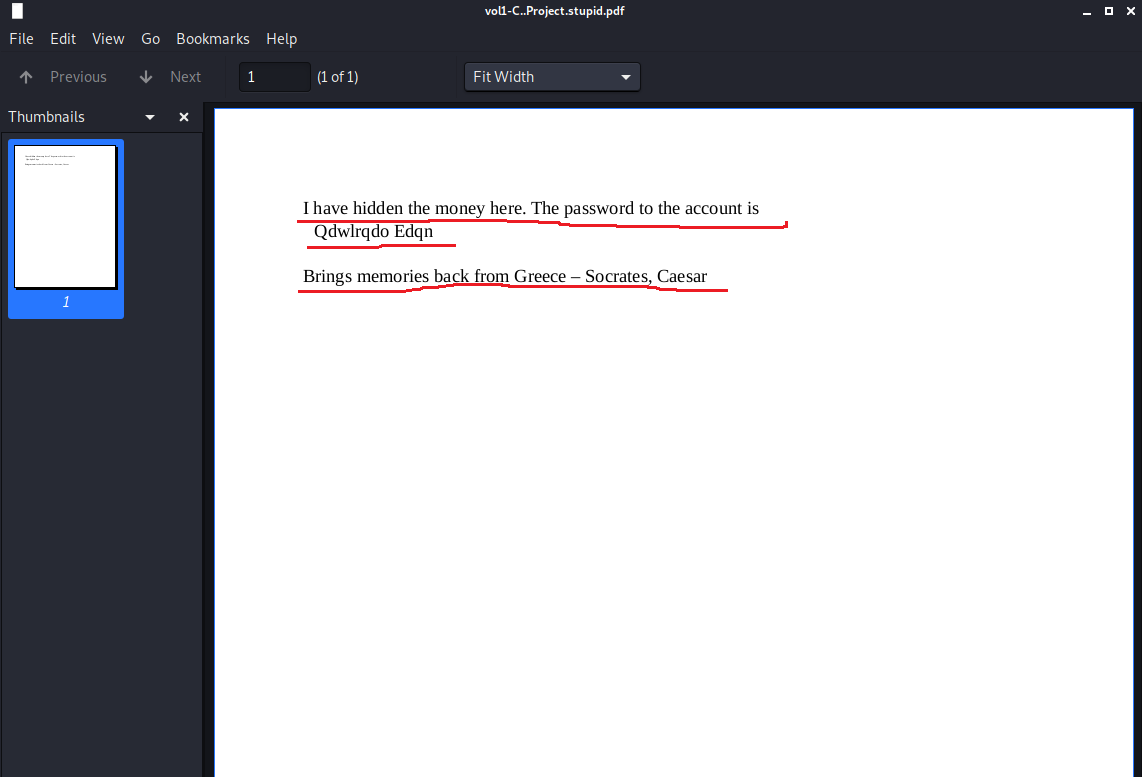
The command I have used for cracking password of the pdf is **sudo pdfcrack -f /home/kali/Desktop/vol1-c..Dumpin…pdf -w /home/kali/Desktop/wordlist.txt**. then it had cracked the password which is ‘salt12’.



Then I have entered the password. The highlights show the content of the pdf.



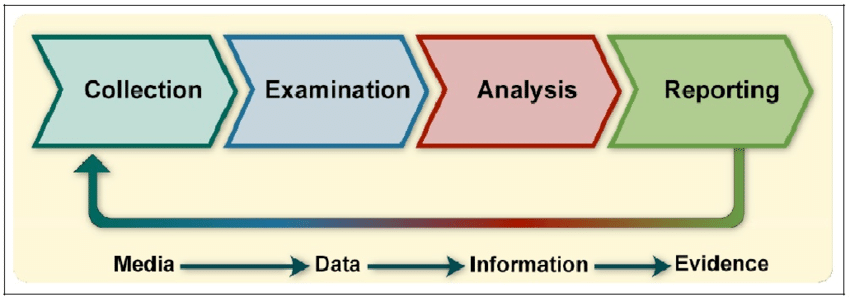
The command I have used for cracking password of the another pdf is **sudo pdfcrack -f /home/kali/Desktop/vol1-c..project.stupid.pdf -w /home/kali/Desktop/wordlist.txt**. then it had cracked the password which is ‘cipher’.



Entered the password and the highlights show the content of the pdf.

**Task 3:** Explain the various stages of the digital forensics process. Use the NIST or the SANS framework to explain these stages.

According to NIST, four-step process for digital forensics are:



1. **Collection**: identify, acquire and protect data related to a specific event. Where evidence is acquired with approval from authorities and in an acceptable manner.
2. **Examination**: this stage consists of processing the collected data and extracting relevant pieces of information from it.
3. **Analysis**: analyzing the extracted data to derive additional useful information. This is a crucial step and very useful because it includes information such as when files were MODIFIED, ACCESSED, CHANGED AND CREATED in a human readable format, known as MAC time evidence.
4. **Reporting**: report the results of the analysis which includes describing the actions performed, determining what other actions need to be performed, recommending improvements to policies. guidelines, procedures, tools, and other aspects of the forensic process

**Task 4**: Can the results obtained from using Kali Linux be admissible in court proceedings? Please justify your answer.

Yes. The digital forensics process involves collecting, analyzing and reporting on digital data in a way that is legally admissible. Digital evidence can also be used to prove whether a person has been involved in crimes that are unrelated to technology, such as murder.

Evidence is legally admissible when it:

* is offered to prove the facts of a case; and
* does not violate the Constitution or other legal statutes

The main repositories of digital evidence are computers, storage devices, telephones, networks, cloud servers and emails. However, as the Internet of Things develops, many other devices will provide digital evidence.