SIT282 Computer Crime and Digital Forensics
ASSIGNMENT 1

Report Title: Forensic Investigation of Donald Price Case

Table of Contents:

Investigator Name: ***Nirosh Ravindran***

1. DIGITAL FORENSIC PROCEDURE

1.1. Evidence Form (Figure 1-11 of the text)

Digital Sentinel Forensic Team *This form is to be used for only one piece of evidence.* *Fill out a separate form for each piece of evidence.*			
Case No:	*Case_2024_00001*	*Unit Number:*	*Unit_0001*
Investigator:	*Nirosh Ravindran*		
Nature of Case:	*Missing artwork investigation*		
Location where evidence was obtained:	*Joachim's Art Gallery, Melbourne, Australia*		
Item # *ID*	*Description of evidence*	*Vendor Name*	*Model No/Serial No.*
ID_0001_0001	*CD-ROM*	*Unknown*	*Unknown*
Evidence Recovered by:	*Nirosh Ravindran*	*Date & Time:*	*28/04/2024 @ 10:32:25*
Evidence Placed in Locker:	*Original CD_ROM was placed in the locker.* *Copy of CD-ROM is placed in the virtual machine*	*Date & Time*	*28/04/2024 @ 11:30:11* *28/04/2024 @ 12:40:45*
Evidence Processed by	*Description of Evidence*		*Date & Time*
Nirosh Ravindran			
	Obtained the digital evidences from the Art Gallery by following all the protocols and chain of custody.		*28/04/2024 @ 10:32*
	Transported the evidence to the lab in a safe container		*28/04/2024 @ 10:45*
	Opened the evidence container and made a copy of it		*28/04/2024 @ 11:08*
	Kept the original evidence into the safe locker		*28/04/2024 @ 11:30*
	Met with my senior investigator to determine the type of the case		*01/05/2024 @ 08:40*
	Started to examine the copied CD-ROM		*02/05/2024 @ 12:40*
			*Page _1_ of _1_*

1.2. Description of Forensic Workstation and Image Download Procedure

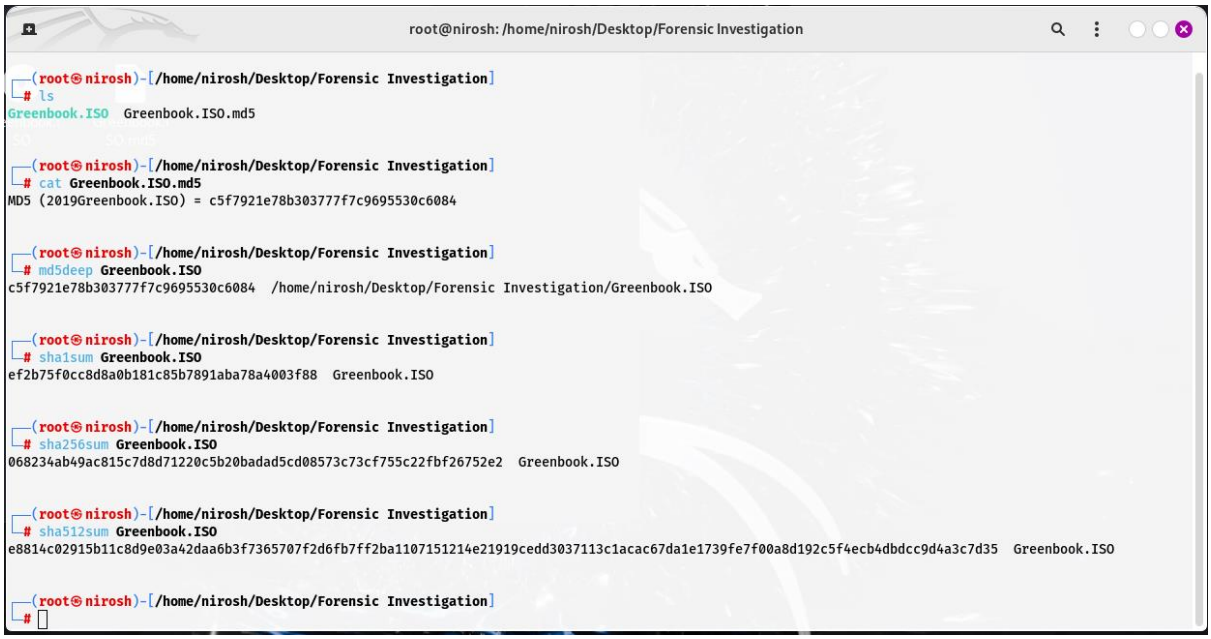
- The forensic workstation is an isolated environment (kali Linux) equipped with necessary forensic investigation tools. Power supply with battery backup, Extra power and data cables, High-end video card, Monitor, External Thunderbolt. The ISO image file was downloaded securely from the provided link using a trusted connection.

1.3. At Least Two SHA-based Hash Function Values of the ISO Image

- SHA1SUM Greenbook.iso - ef2b75f0cc8d8a0b181c85b7891aba78a4003f88

- SHA256SUM Greenbook.iso - 068234ab49ac815c7d8d71220c5b20badad5cd08573c73cf755c22fbf26752e2

- SHA512SUM Greenbook.iso - e8814c02915b11c8d9e03a42daa6b3f7365707f2d6fb7ff2ba1107151214e21919cedd3037113c1acac67da1e1739fe7f00a8d192c5f4ecb4dbdcc9d4a3c7d35



1.4 Explanation of need for Multiple Hash Values to Verify Validity of Image File

- Multiple hash values ensure integrity verification of the image file. It increases the reliability of the of the image file, in case if someone had altered it, the hash value will be different of the original one, so, we can identify that the copied version has been altered and the investigation can be carried on accordingly by taking another copy of the original evidence that is not altered.

1.5 Explanation of Procedure used Before Accessing Image File in VM

- Installed forensic tools, OSes (windows 10, kali linux, and ubuntu) and file systems on the virtual machine and necessary devices.
- Mounted the ISO image to the VM as a logical drive.
- Created a forensic image of the ISO file before accessing it.

2. DESCRIPTION OF BINARY DETAILS

2.1. Table 1: Properties of the Undeleted Files Found on the ISO Image

File Name	*Physical Size (KB)*	*MD5 Hash*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\1.HTML	*12*	*2a9d47cd337565ecbcd4556b85d675b2*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\1.JPG	*117*	*1831b1f5e0e5a22a1f9d5cbab2099f1b*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\2.JPG	*127*	*ae9ef080a292374a866d659abd55712f*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\3.JPG	*180*	*d3060c3925e2f21274c5d04ce465ef08*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\4.JPG	*120*	*30c58285a32ac6ff2232fe09cf8a11dd*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\5.JPG	*228*	*853bd591239b0225bbce59fdd7da1bc6*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\GREENBOOK.TC	*81,920*	*39e0cc888b3d96fb07c411b4d52da1fa*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\GREENBOOK_1937.PDF	*5288*	*1bcbf60d6f2629a35dabcb4bcf1b2071*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\1.html	*12*	*2a9d47cd337565ecbcd4556b85d675b2*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\1.jpg	*117*	*1831b1f5e0e5a22a1f9d5cbab2099f1b*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\2.jpg	*127*	*ae9ef080a292374a866d659abd55712f*

Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\3.jpg	*180*	*d3060c3925e2f21274c5d04ce465ef08*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\4.jpg	*120*	*30c58285a32ac6ff2232fe09cf8a11dd*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\5.jpg	*228*	*853bd591239b0225bbce59fdd7da1bc6*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\greenbook.tc	*81,920*	*39e0cc888b3d96fb07c411b4d52da1fa*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\Greenbook-1937.pdf	*5288*	*1bcbf60d6f2629a35dabcb4bcf1b2071*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\1.html	*12*	*2a9d47cd337565ecbcd4556b85d675b2*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\1.jpg	*117*	*1831b1f5e0e5a22a1f9d5cbab2099f1b*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\2.jpg	*127*	*ae9ef080a292374a866d659abd55712f*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\3.jpg	*180*	*d3060c3925e2f21274c5d04ce465ef08*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\4.jpg	*120*	*30c58285a32ac6ff2232fe09cf8a11dd*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\5.jpg	*228*	*853bd591239b0225bbce59fdd7da1bc6*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\Greenbook-1937.pdf	*5288*	*1bcbf60d6f2629a35dabcb4bcf1b2071*
Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\greenbook.tc	*81,920*	*39e0cc888b3d96fb07c411b4d52da1fa*

2.2. Description of Programs to be used to Perform Investigation

- ***Md5deep*** *– to find the md5 based hash value of the image*
- ***Sha1sum*** *- to find the sha1 based hash value of the image*
- ***Sha256sum*** *- to find the sha256 based hash value of the image*
- ***Sha512sum*** *- to find the sha512 based hash value of the image*
- ***FTKImager*** *– used to create iso image files and find hash functions, find the filenames inside the iso image.*
- ***Autopsy*** *– used to find the md5 hash values for the files inside the image*
- ***HxD*** *– to find hex values of the files to find any hidden files within another file. For example, an jpeg file is hidden inside a pdf.*

3. OUTCOMES OF DIGITAL FORENSIC INVESTIGATION

3.1. Description and Justification of Key Words Used to Search ISO Image

I tried few key words to search:
art *– since it was an art work missing, I used the word "art" to find anything related to art work.*

Credit *– the missing artwork might be sold, so Donald might have received a credit or money. So, to find anything related to that I used that word.*

Boats- *since the art work was about two boats, I used the word boats to find anything about boats.*

Artwork *– the case is about a missing artwork, so I used that word to find anything related to art work*

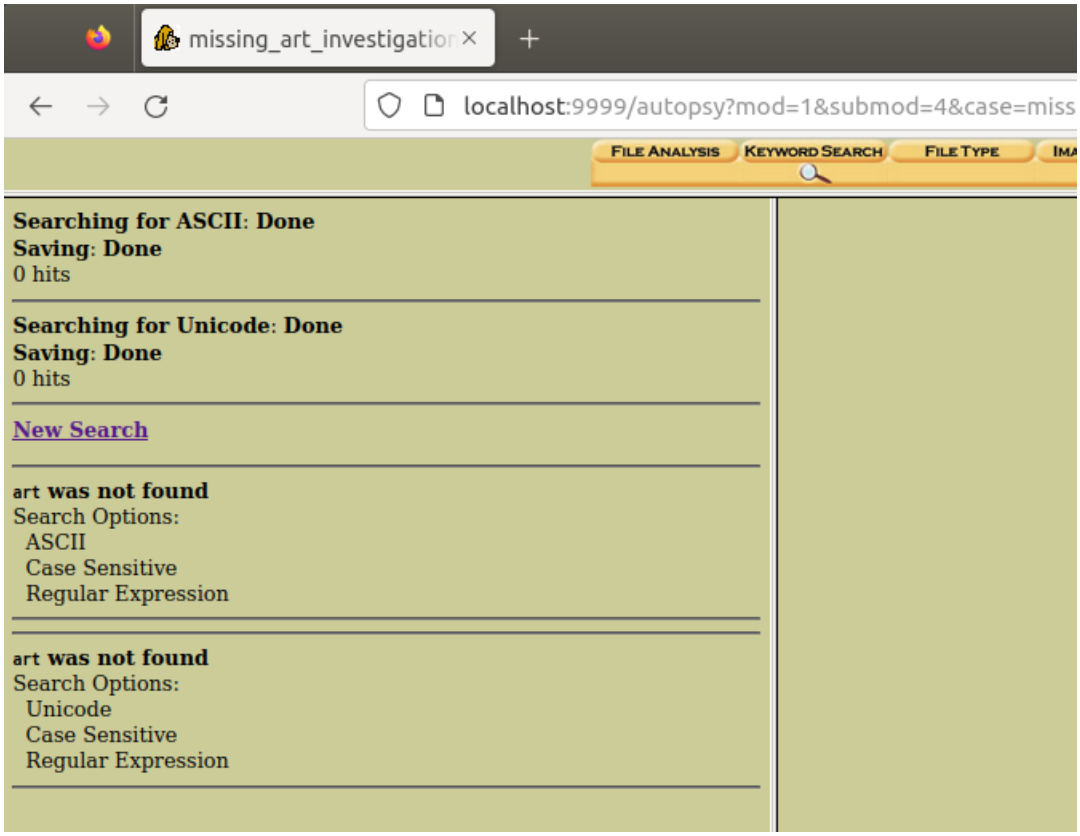
Watercolor *– the artwork was drawn by water color, so I used that word hoping that to find anything related to the missing artwork*

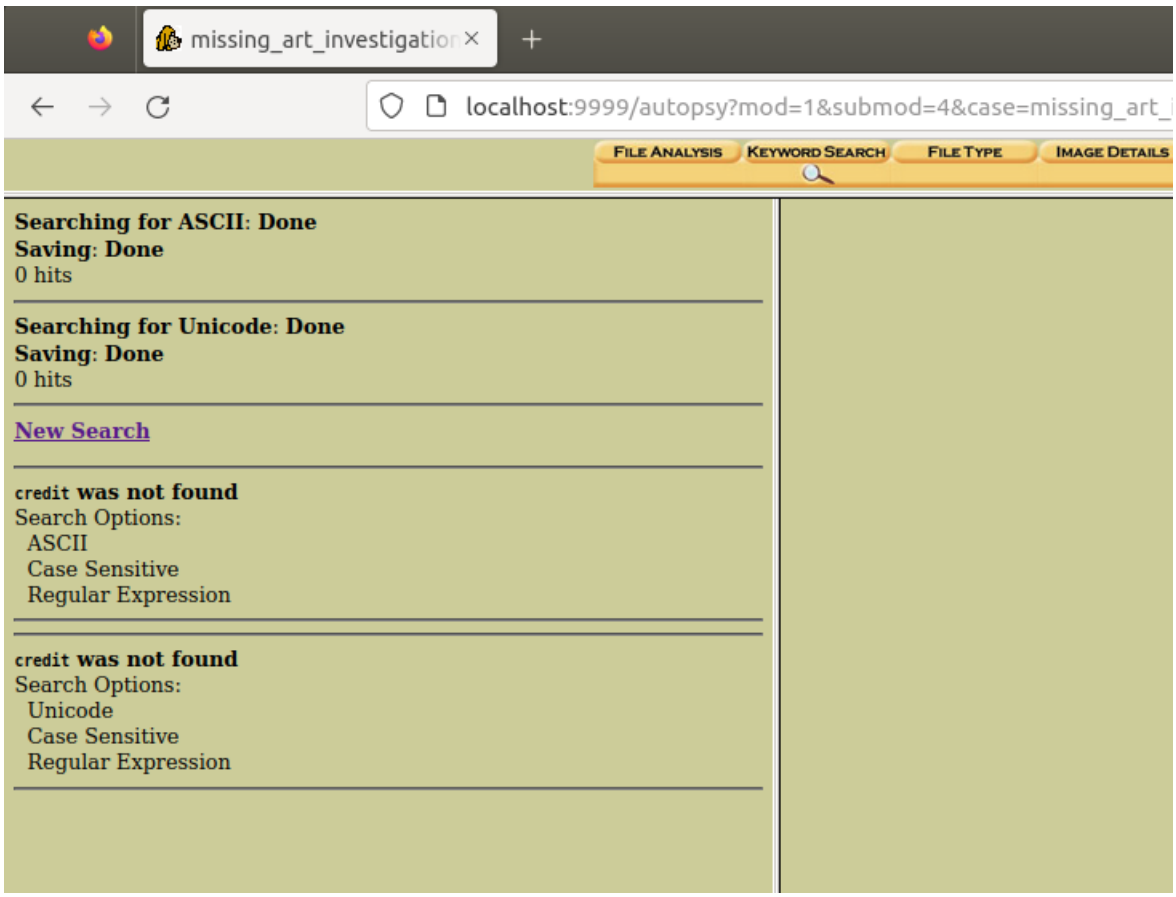
Museum *– since the artwork went missing from a museum, I used this word to find something related to the missing artwork*

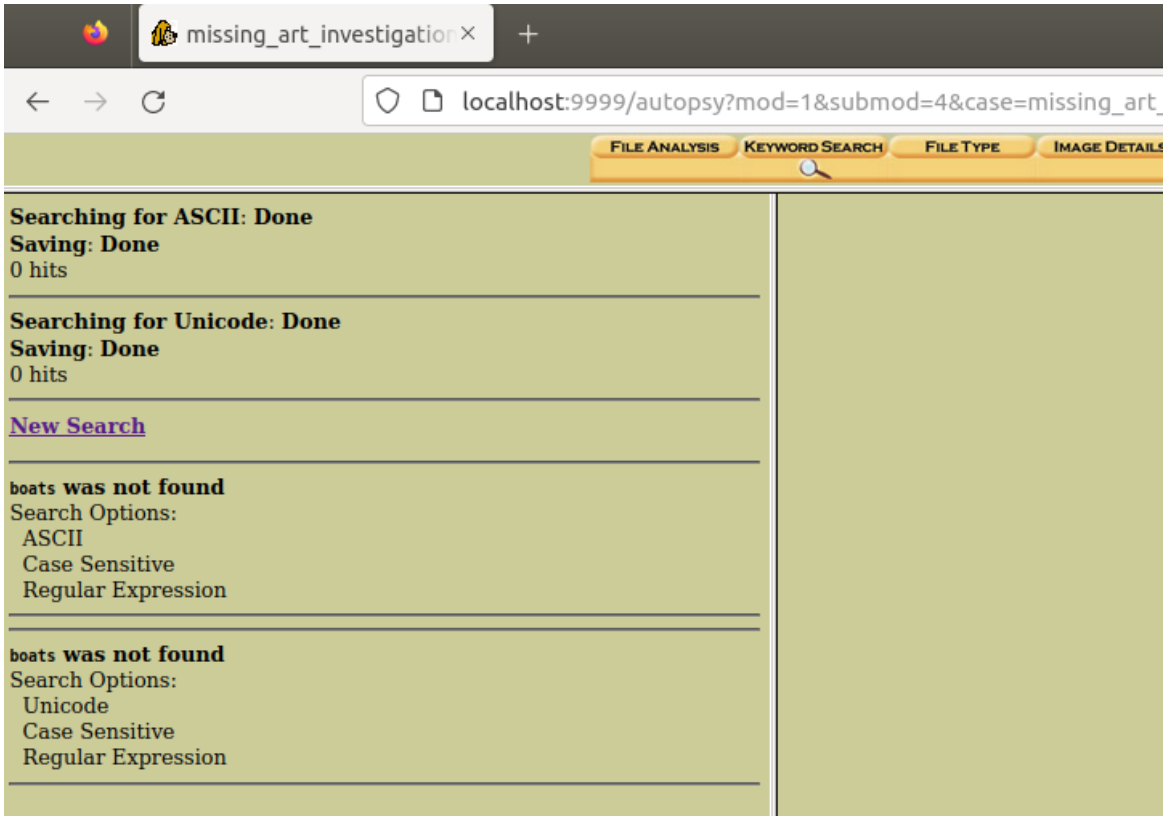
Donald price *– since he is the main suspect, I used his name itself to find any kind of suspicious activity he had performed*

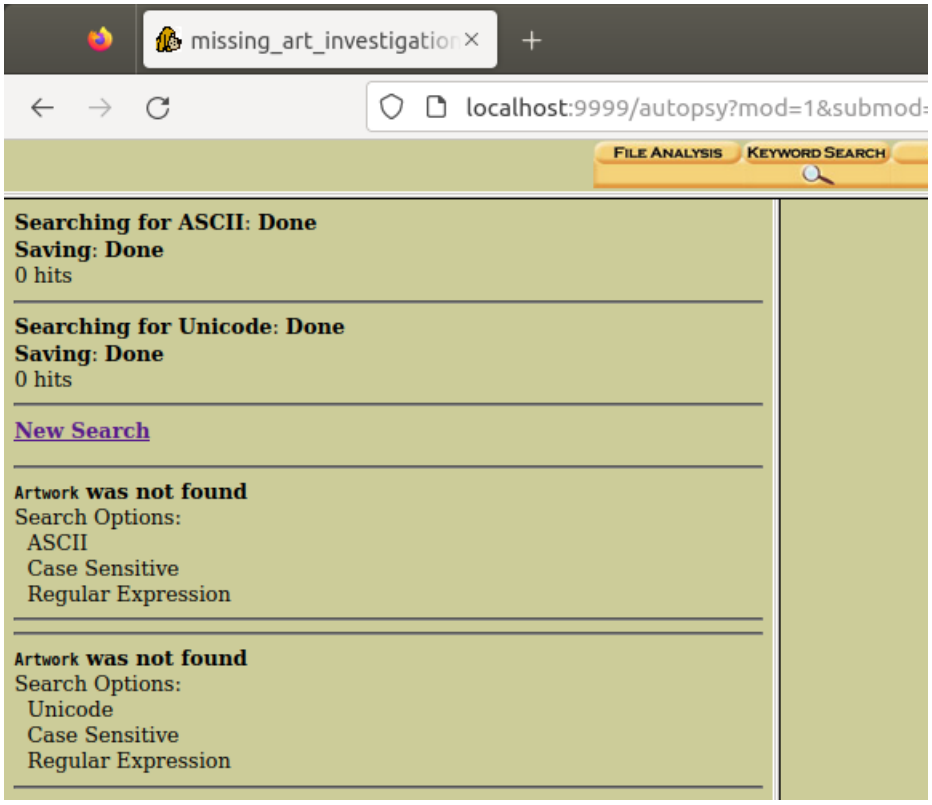
Cash *– I used this because the missing artwork might have gone up for a sale, so there might be cash involved, so to find anything related to that, I used it.*

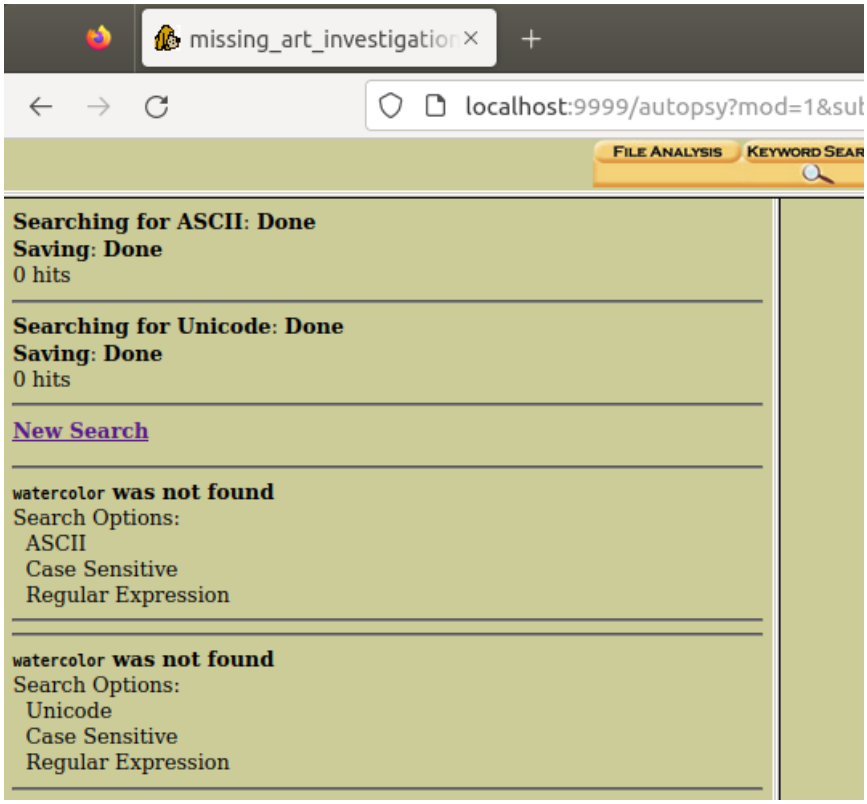
but none of the key words produced any visible and significant output that is useful to the case

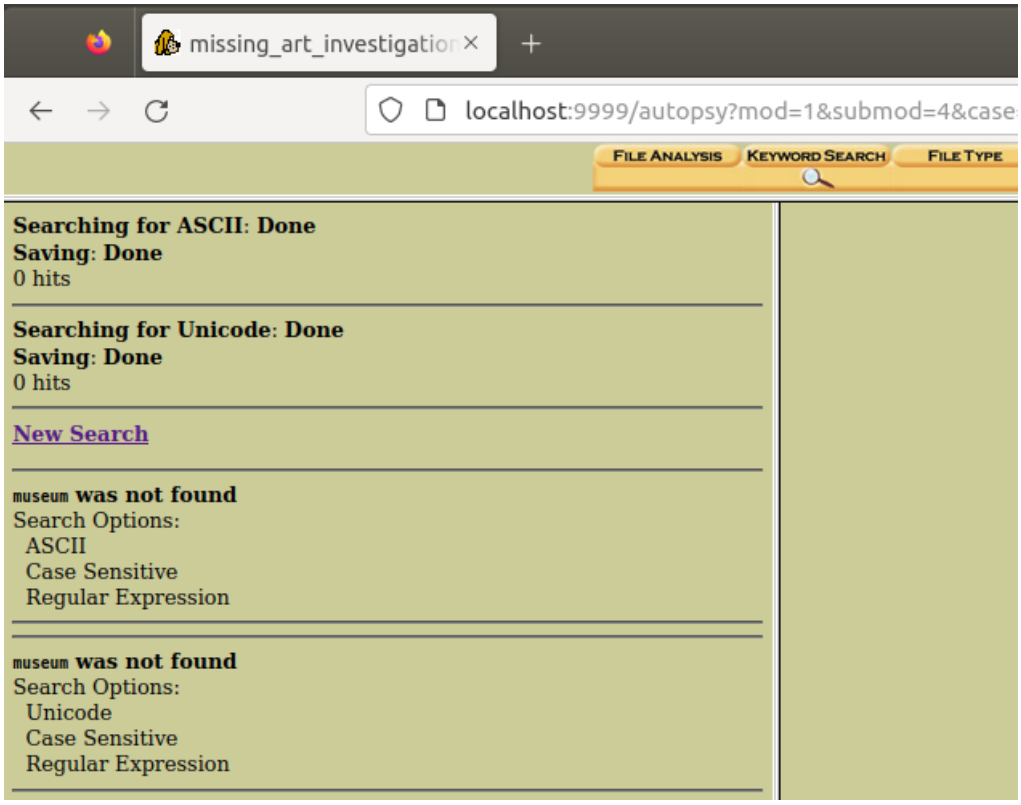

missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=4&case=miss
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
art was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
art was not found
Search Options:
Unicode
Case Sensitive
Regular Expression

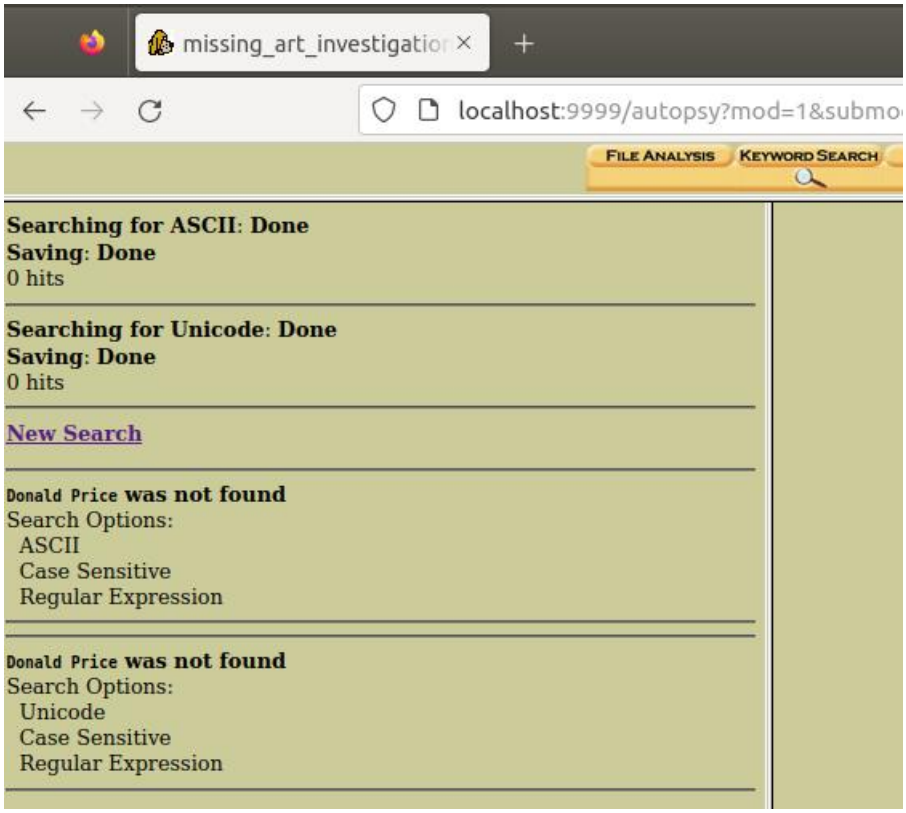

missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=4&case=missing_art_
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
credit was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
credit was not found
Search Options:
Unicode
Case Sensitive
Regular Expression

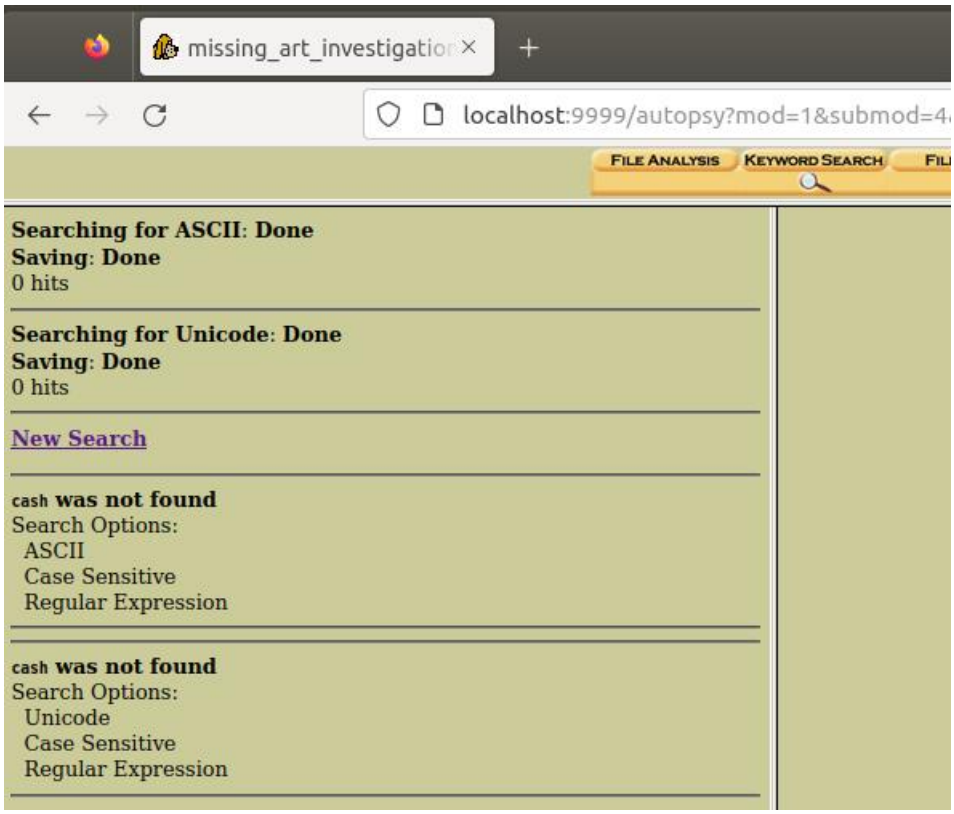

missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=4&case=missing_art_
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
boats was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
boats was not found
Search Options:
Unicode
Case Sensitive
Regular Expression


missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=
FILE ANALYSIS
KEYWORD SEARCH
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
Artwork was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
Artwork was not found
Search Options:
Unicode
Case Sensitive
Regular Expression


missing_art_investigatio
localhost:9999/autopsy?mod=1&sub
FILE ANALYSIS
KEYWORD SEAR
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
watercolor was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
watercolor was not found
Search Options:
Unicode
Case Sensitive
Regular Expression

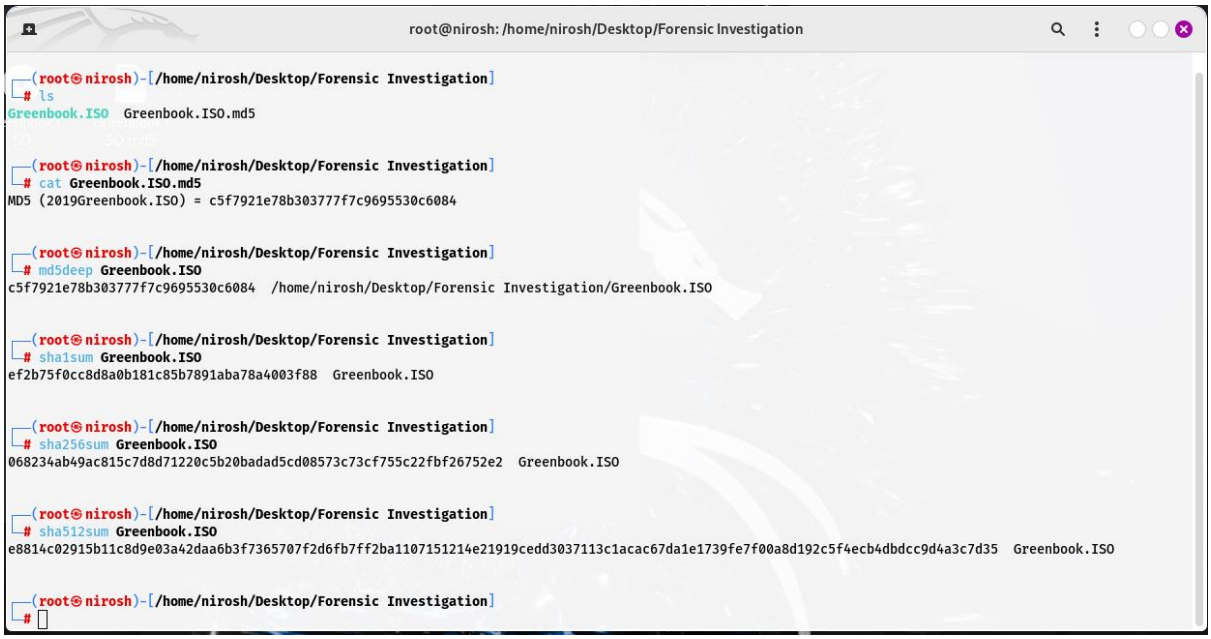

missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=4&case
FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
museum was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
museum was not found
Search Options:
Unicode
Case Sensitive
Regular Expression


missing_art_investigatio
localhost:9999/autopsy?mod=1&submo
FILE ANALYSIS
KEYWORD SEARCH
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
Donald Price was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
Donald Price was not found
Search Options:
Unicode
Case Sensitive
Regular Expression


missing_art_investigatio
localhost:9999/autopsy?mod=1&submod=4
FILE ANALYSIS
KEYWORD SEARCH
Searching for ASCII: Done
Saving: Done
0 hits
Searching for Unicode: Done
Saving: Done
0 hits
New Search
cash was not found
Search Options:
ASCII
Case Sensitive
Regular Expression
cash was not found
Search Options:
Unicode
Case Sensitive
Regular Expression

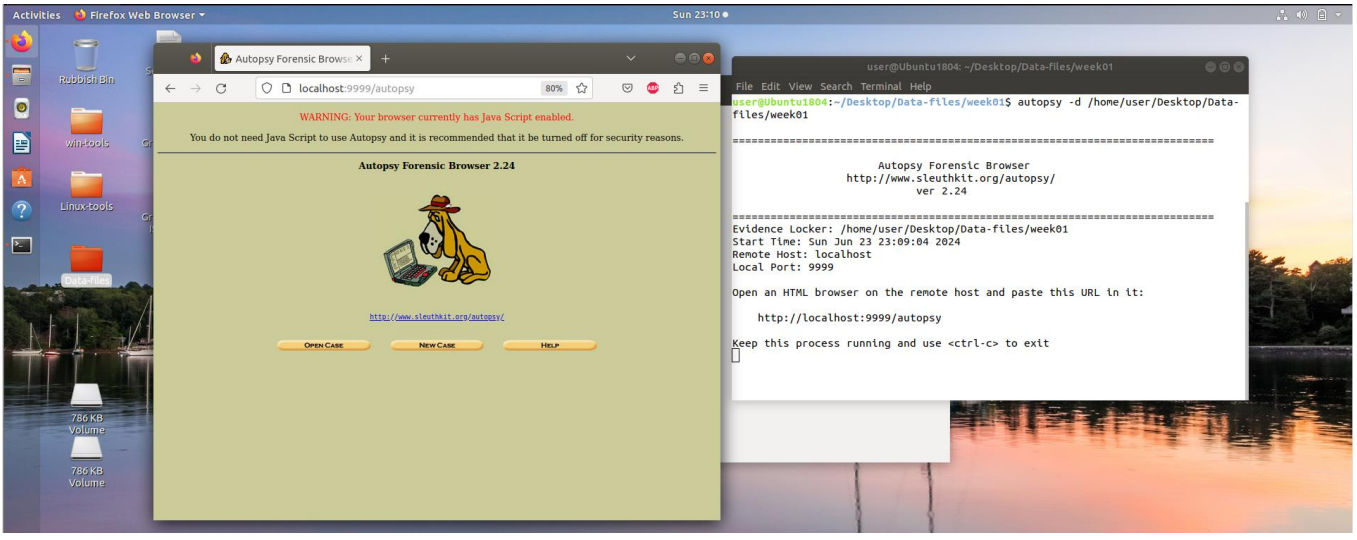
3.2. Document Procedure Including Appropriate Commands and Screenshots

1. first I had to confirm the iso image is reliable by checking the md5 hash value of the original image file and the md5 hash value that was given by the tutor using the kali linux machine. I used the md5deep to find the hash value of the original iso image and compared it with the given md5 hash value. Then I confirmed that the image is the same and not a tampered one. Then I also found the hash values of different sha based function values.

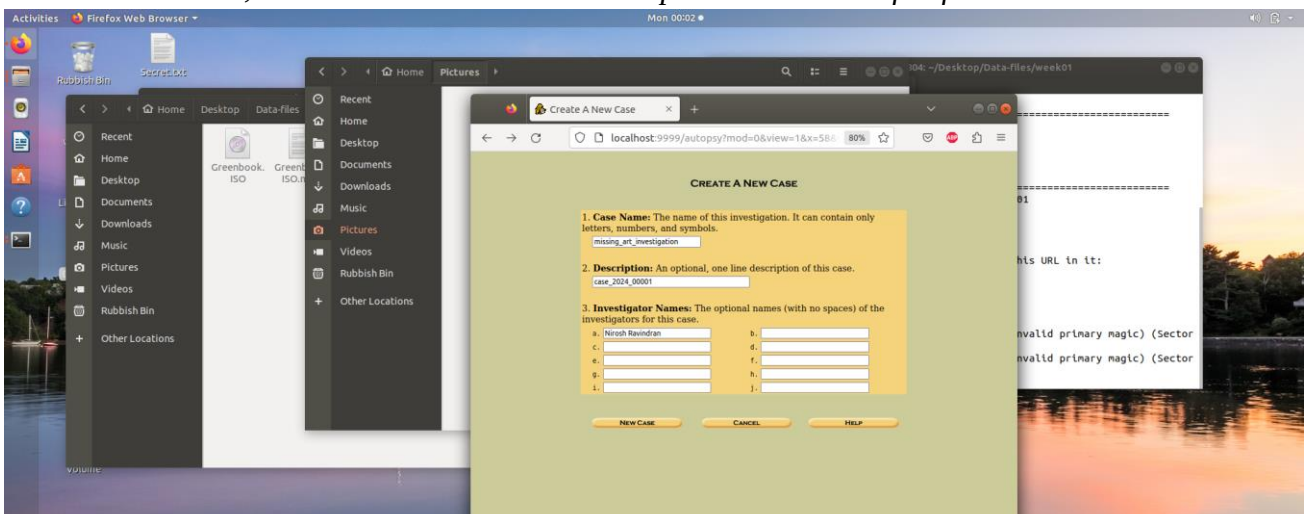


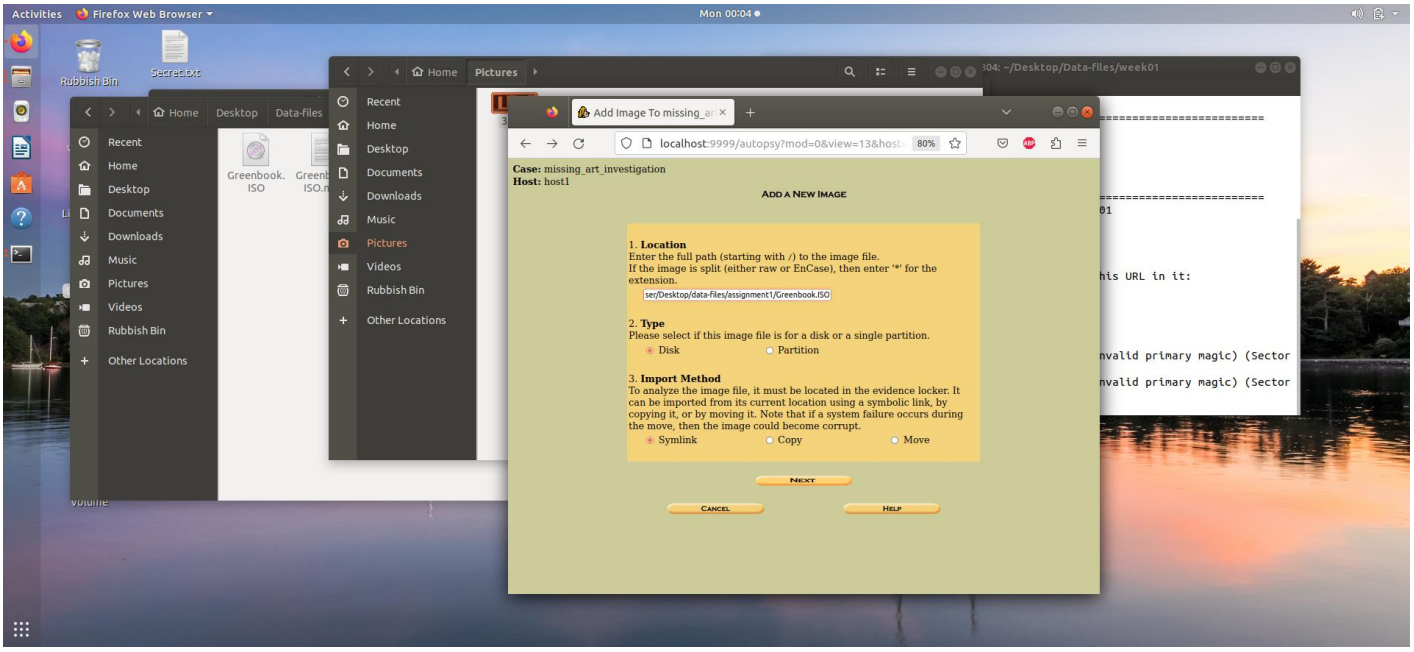
2. Then I started the tool autopsy and added the image file to and analysed the files inside it using the ubuntu machine that was provided by the tutor.

```
user@Ubuntu1804: ~/Desktop/Data-files/week01
File  Edit  View  Search  Terminal  Help
user@Ubuntu1804:~/Desktop/Data-files/week01$ autopsy -d /home/user/Desktop/Data-files/week01

================================================================================

                        Autopsy Forensic Browser
                    http://www.sleuthkit.org/autopsy/
                                ver 2.24

================================================================================
Evidence Locker: /home/user/Desktop/Data-files/week01
Start Time: Sun Jun 23 23:09:04 2024
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

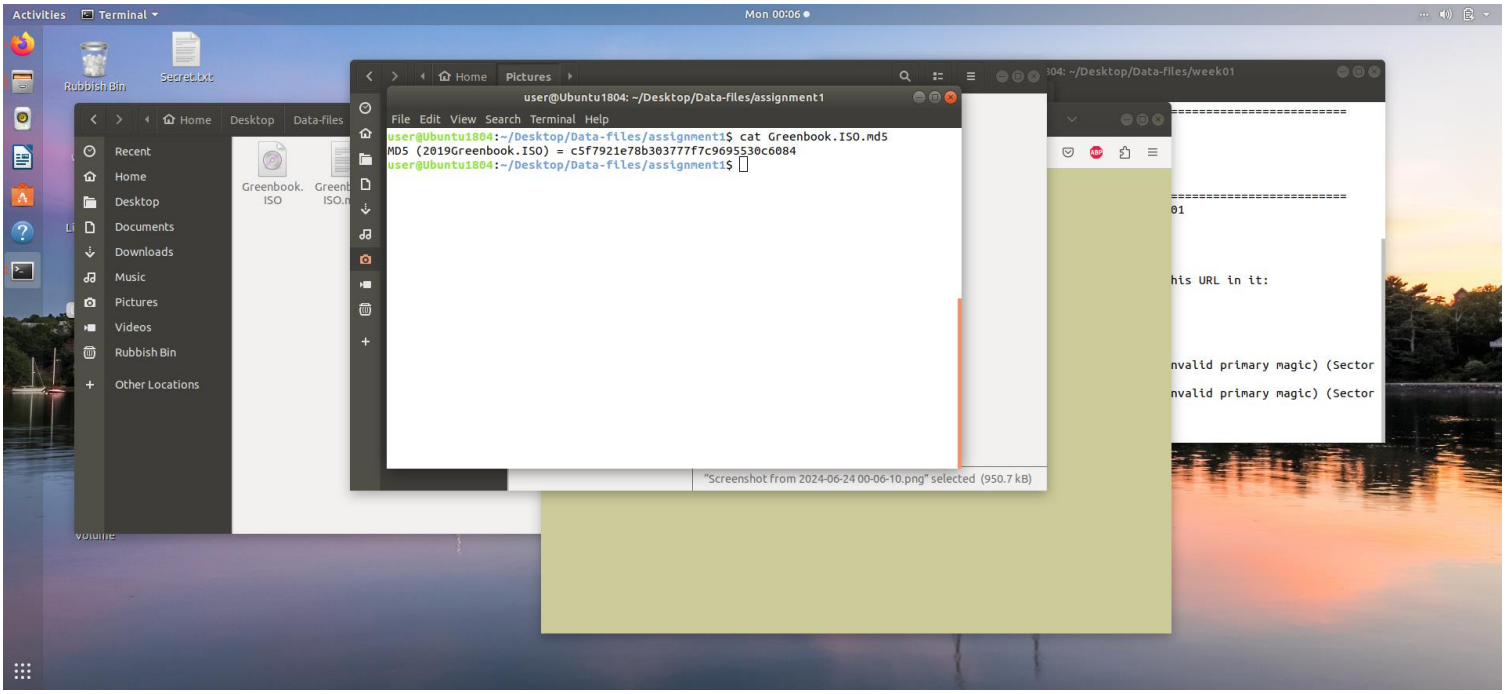


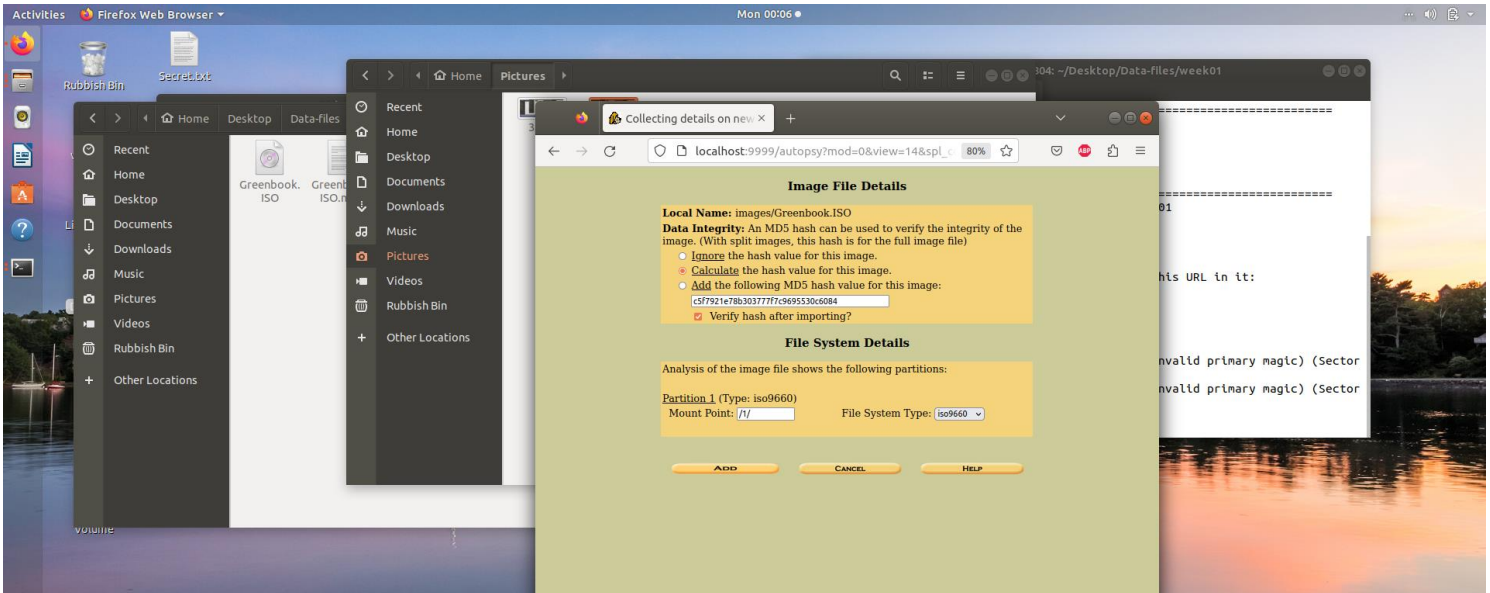
3. First, I entered the case details and opened a new case file for that

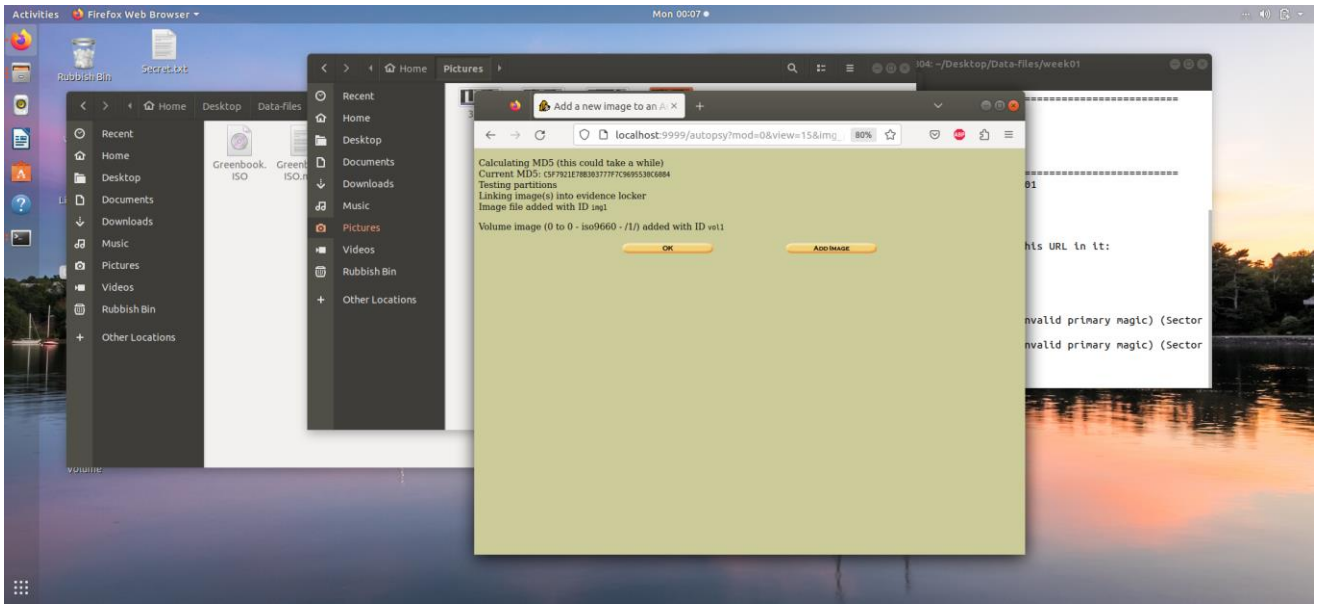


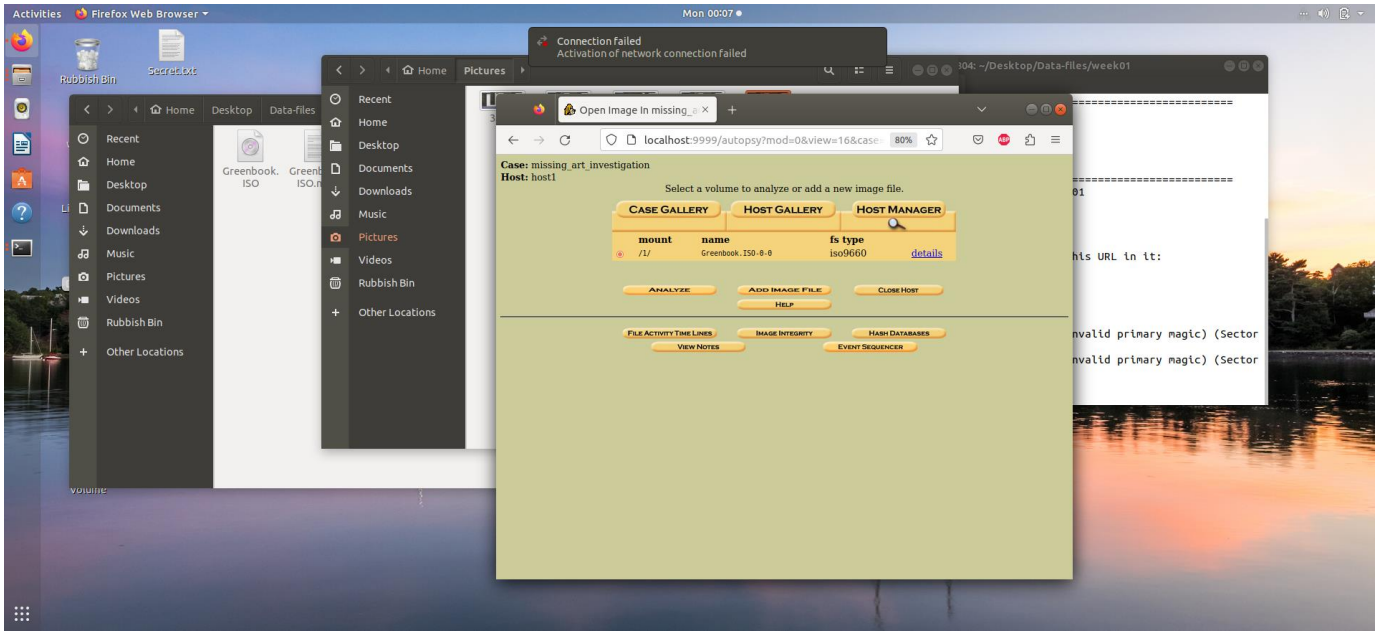


4. To verify the integrity of the file, I gave the md5hash value of the image to verify when the image is being verified by Autopsy.

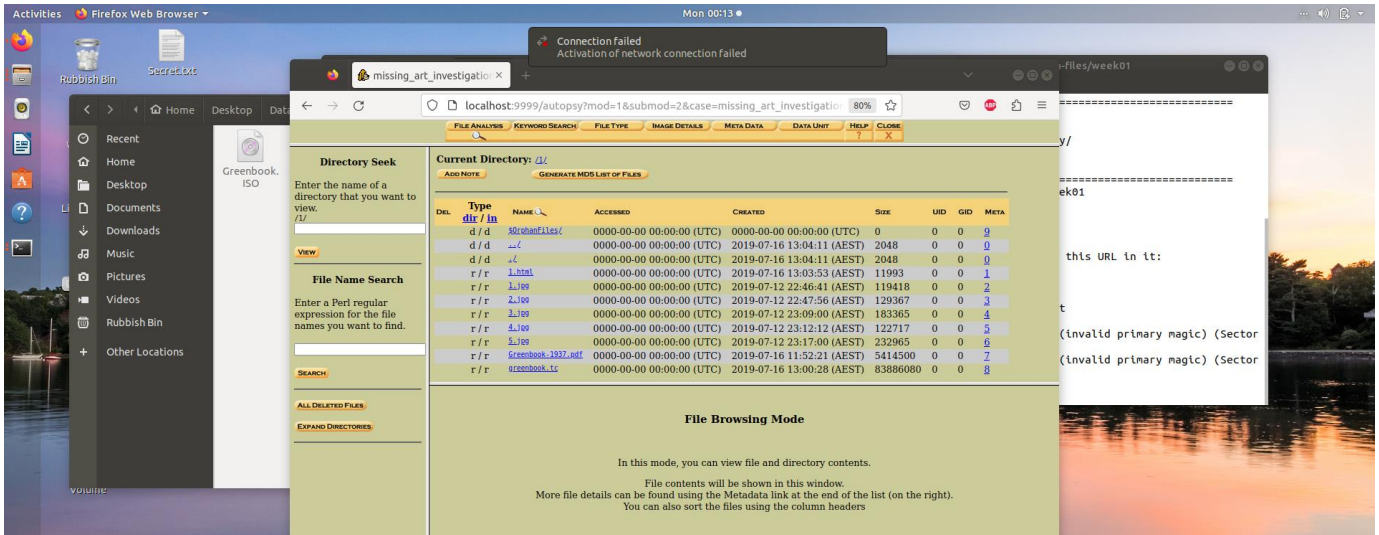




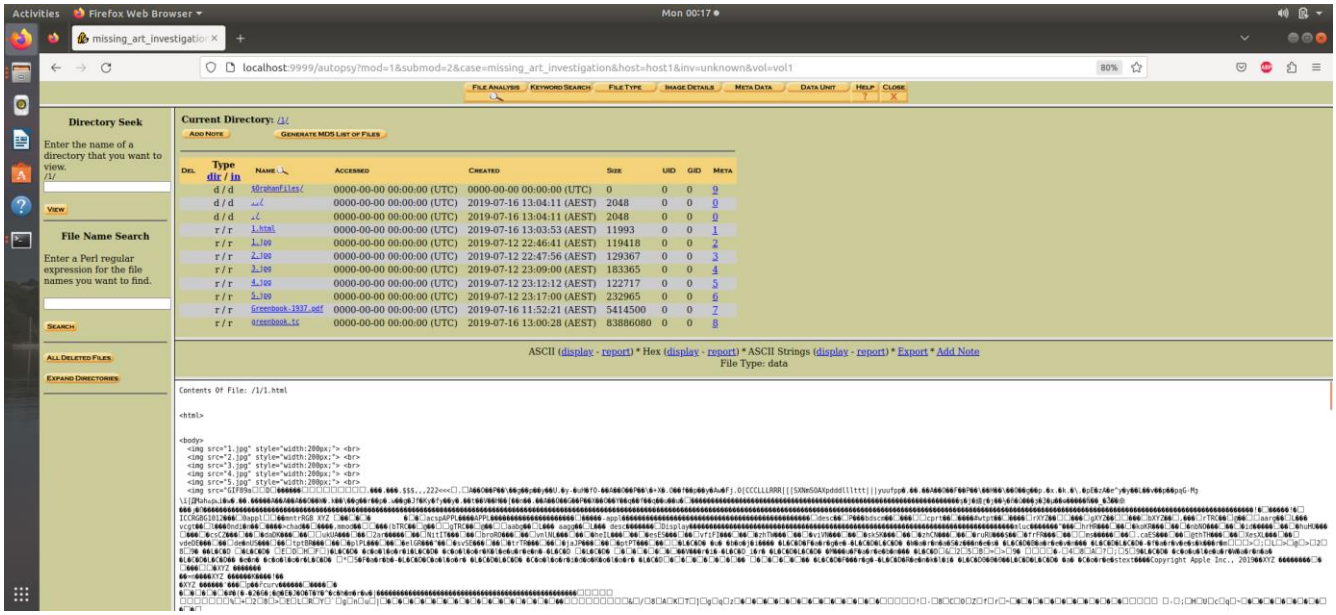


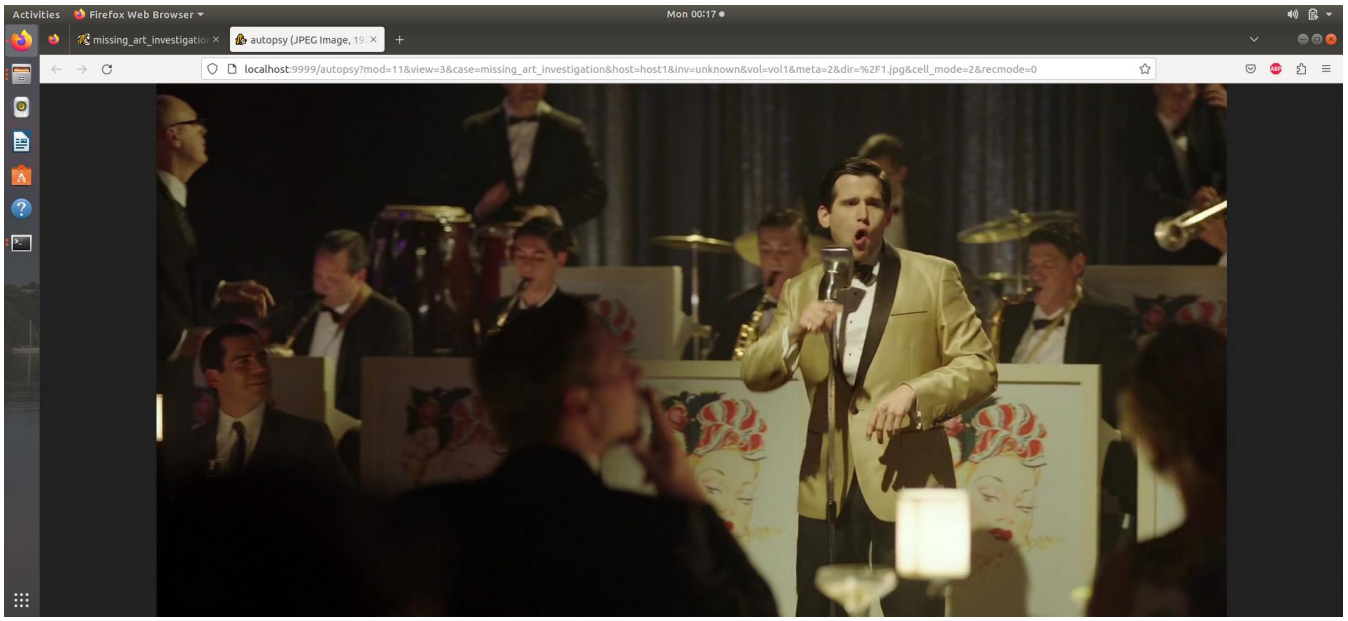


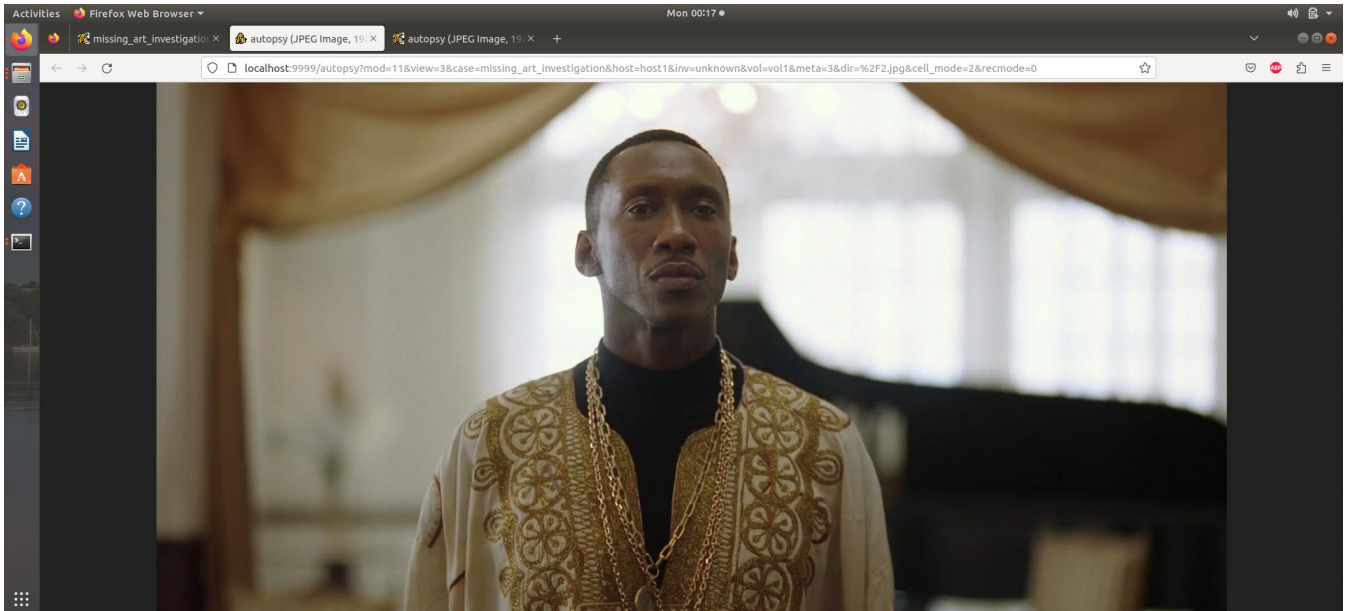
5. Now the case is ready to be analysed

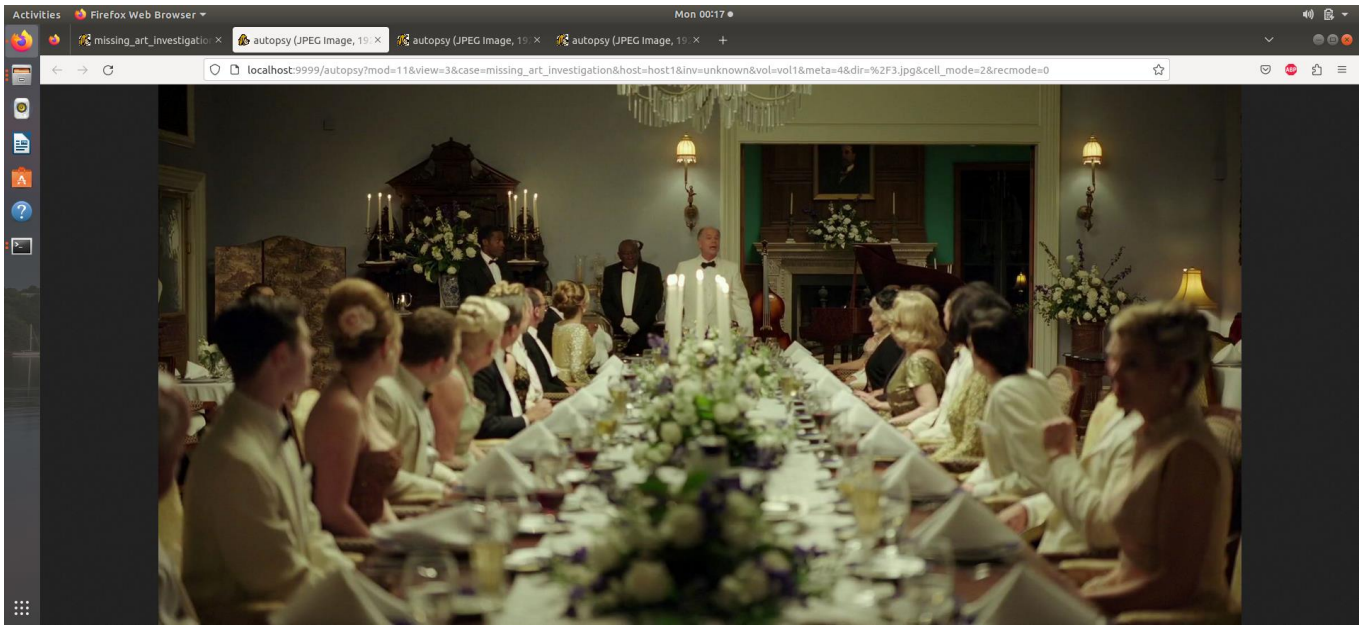


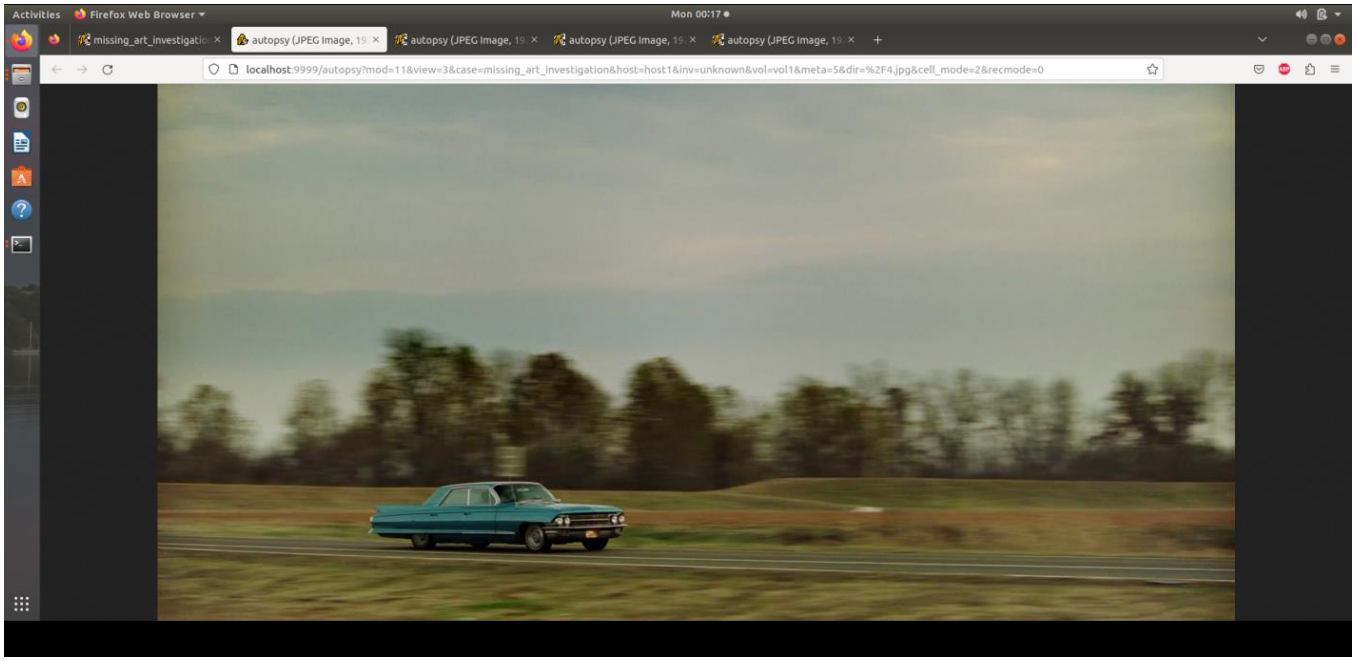
6. Then I went through the files inside the image, the html file, jpg files, the pdf file and the truecrypt file as well.

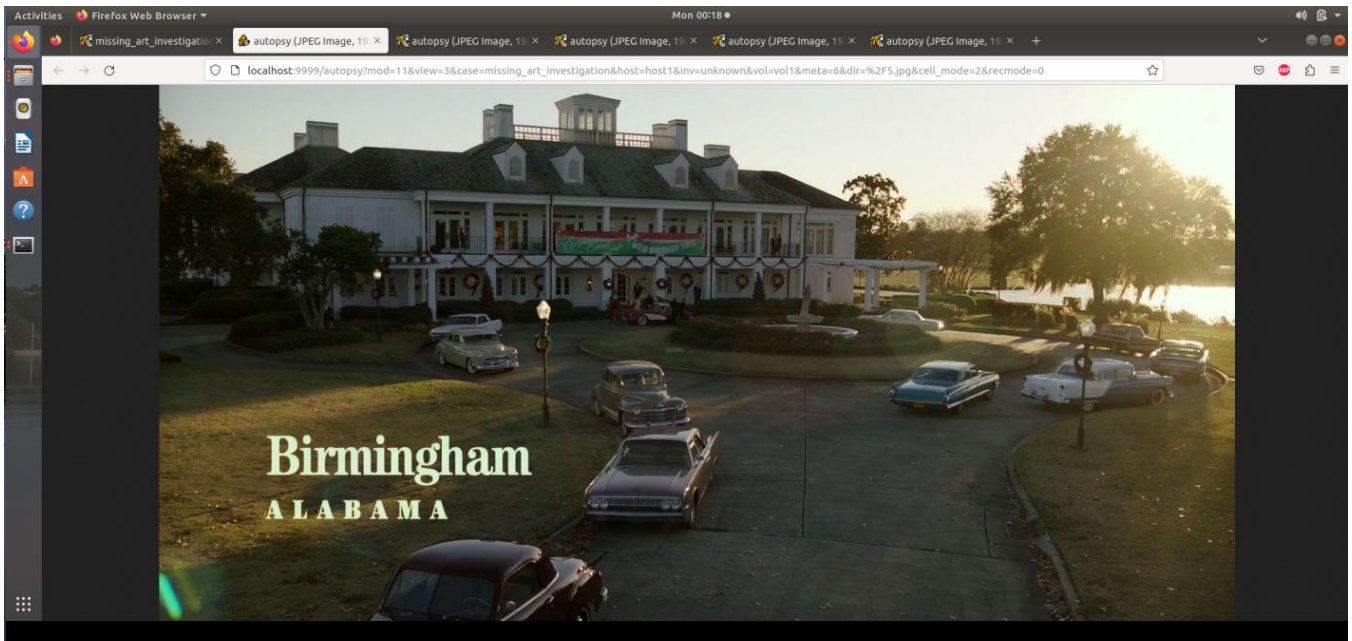




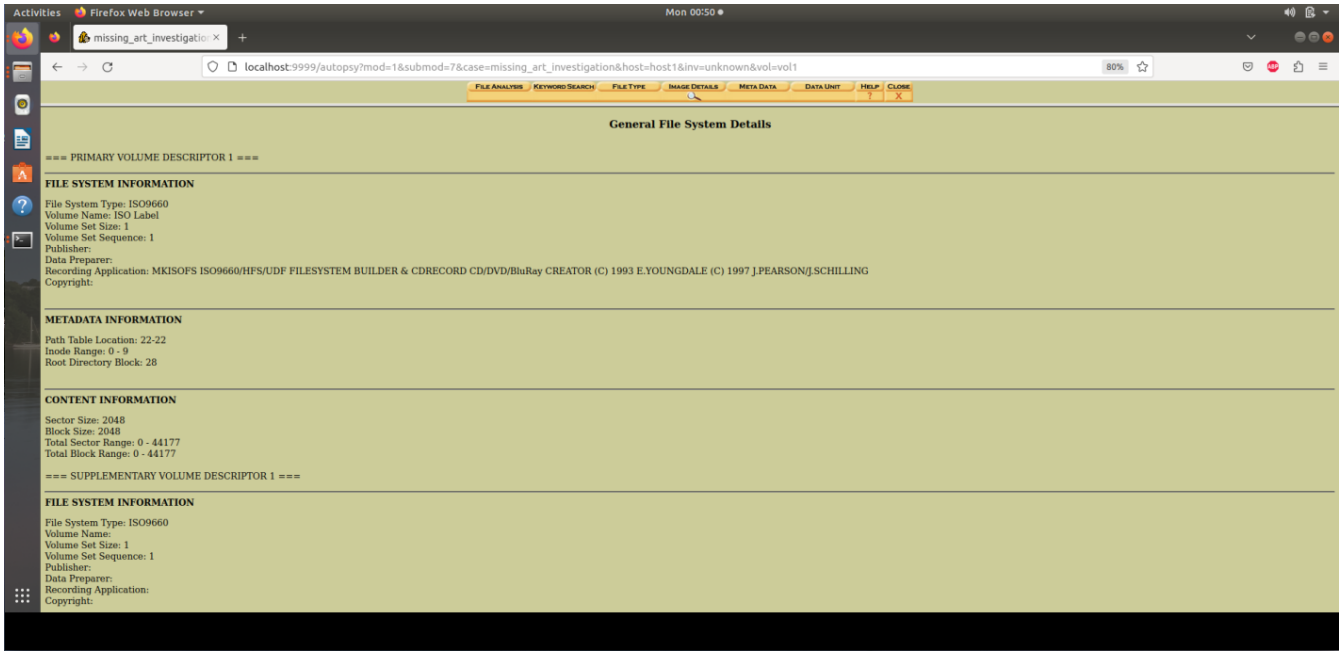



Activities
Firefox Web Browser
Mon 00:17
missing_art_investigatio
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
localhost:9999/autopsy?mod=11&view=3&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1&meta=4&dir=%2F3.jpg&cell_mode=2&recmode=0

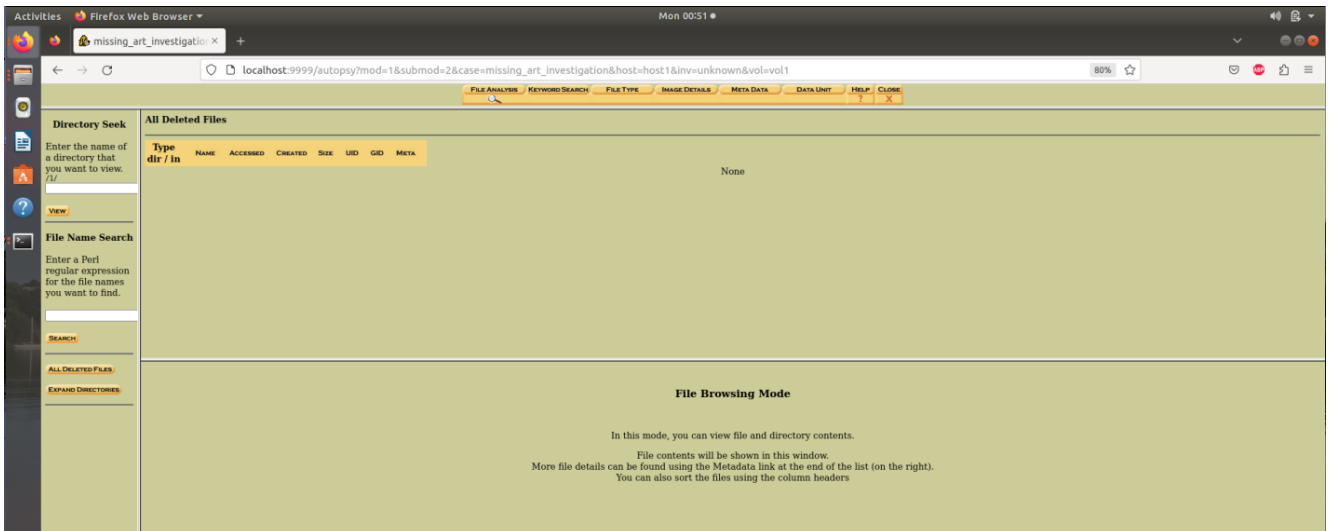

Activities
Firefox Web Browser
Mon 00:17
missing_art_investigatio
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
localhost:9999/autopsy?mod=11&view=3&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1&meta=5&dir=%2F4.jpg&cell_mode=2&recmode=0


Activities
Firefox Web Browser
Mon 00:18
missing_art_investigatio
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
autopsy (JPEG Image, 19
localhost:9999/autopsy?mod=11&view=3&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1&meta=6&dir=%2F5.jpg&cell_mode=2&recmode=0
Birmingham
ALABAMA

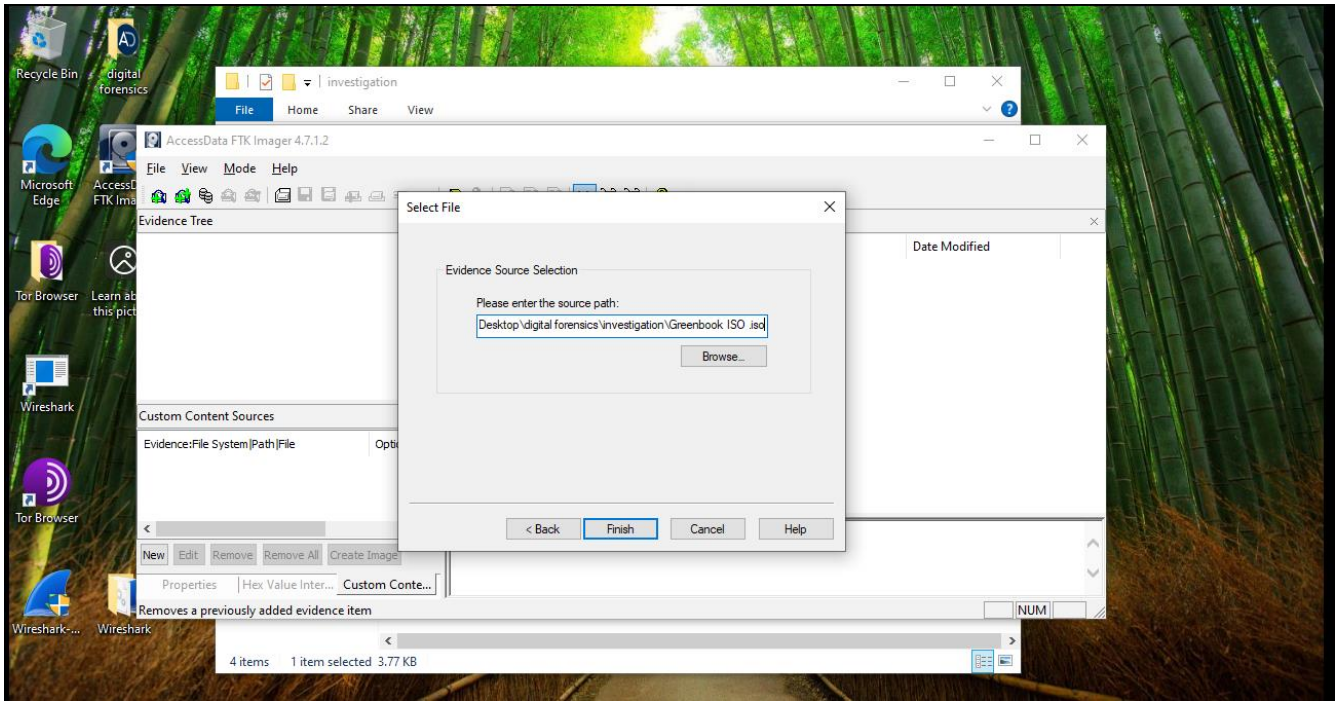
7. Then I went through the general file systems

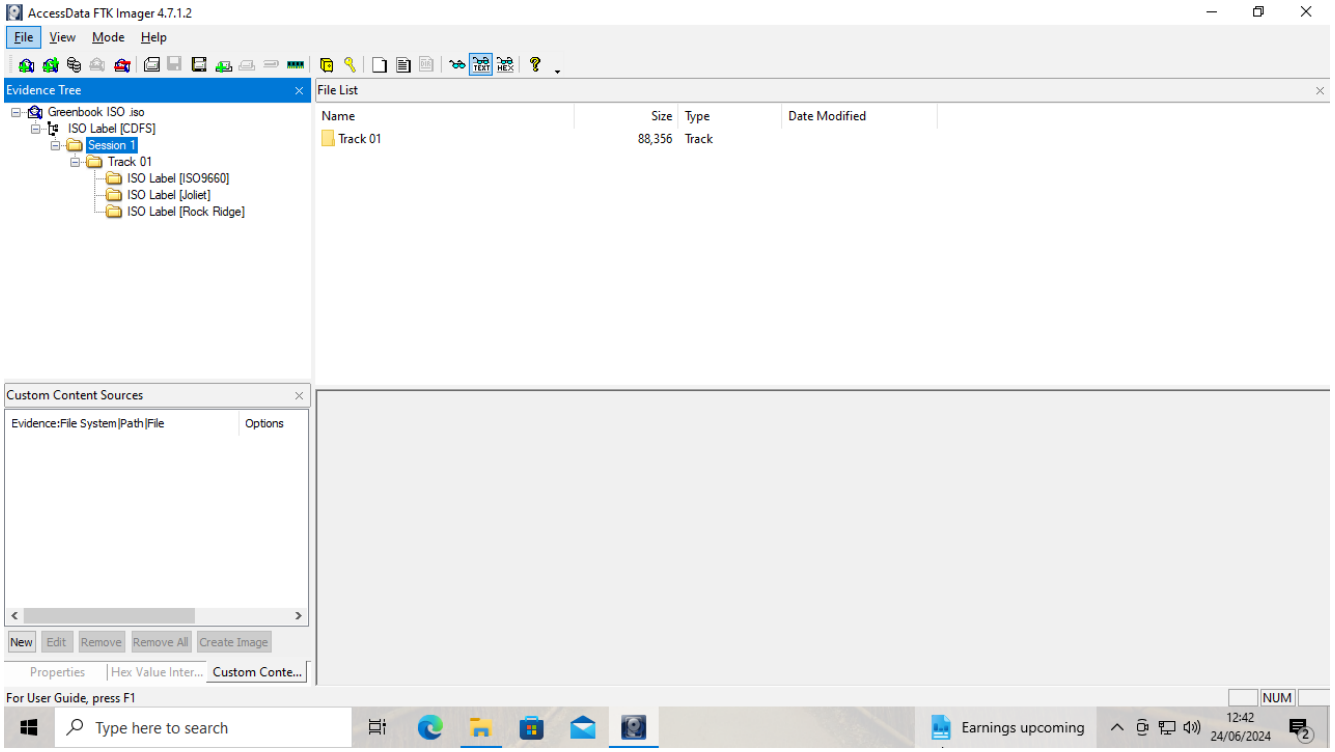


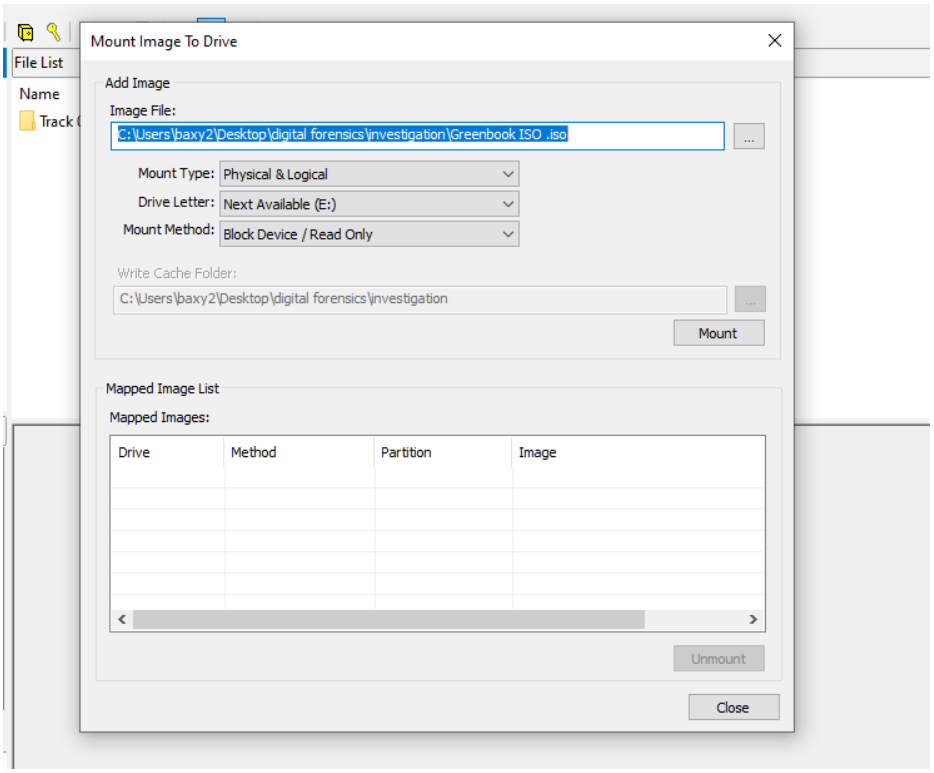
8. Then tried to look out at some deleted files, but couldn't find them.

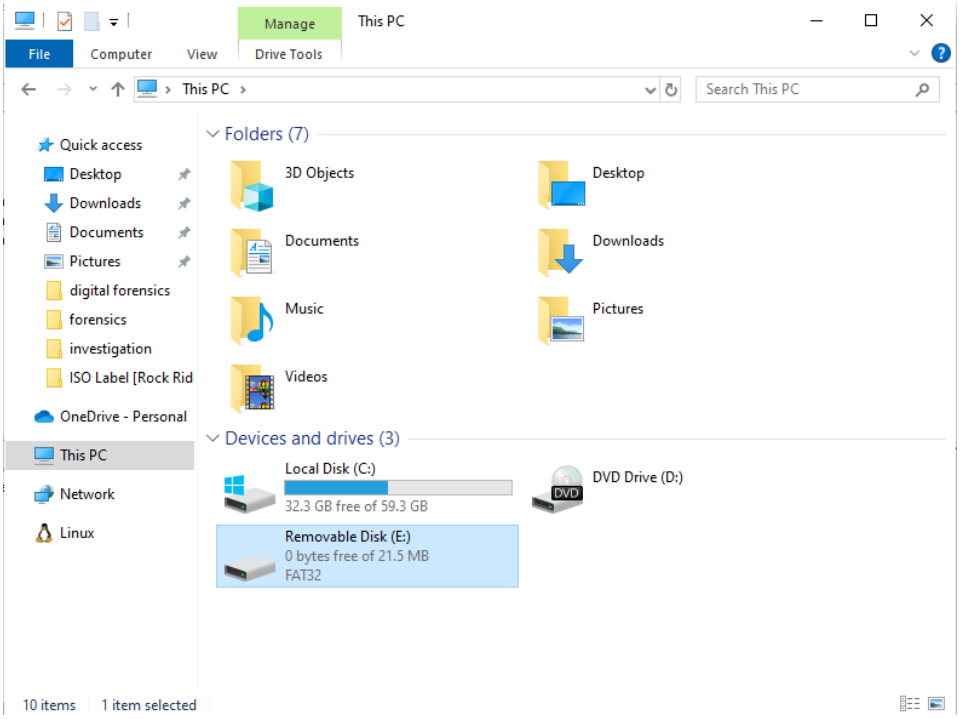


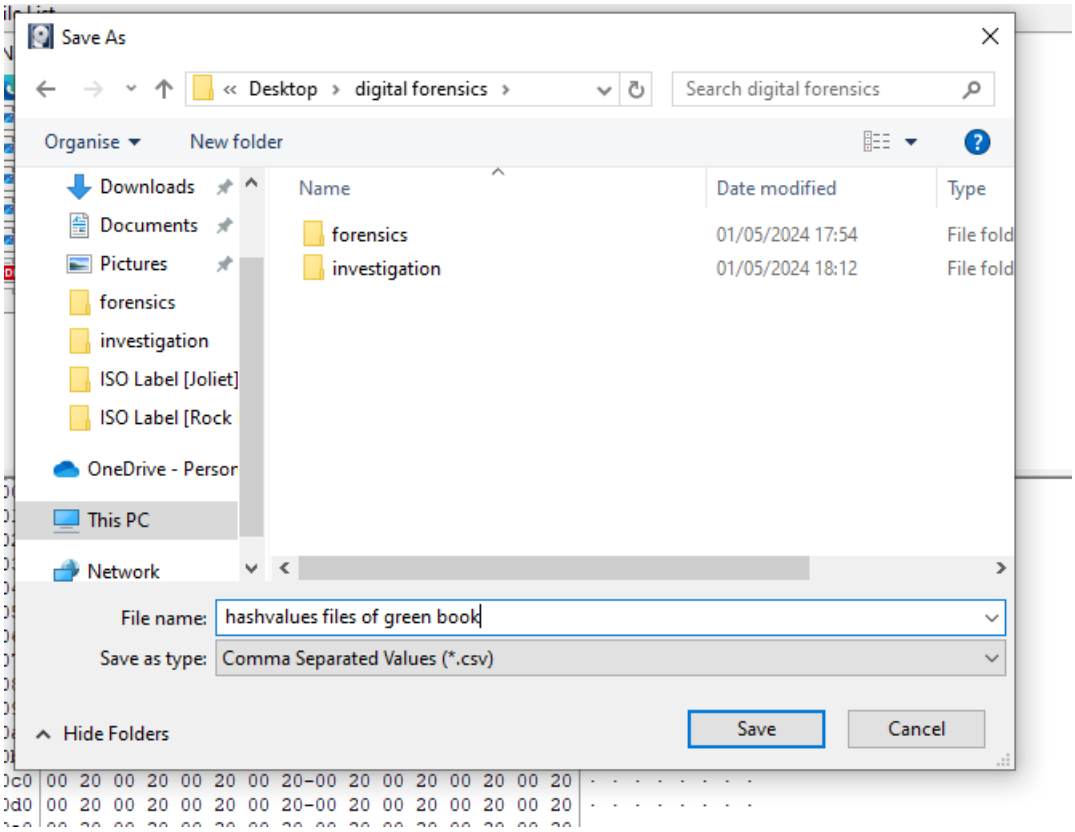
9. Now I used the FTK imager to analyse the image much further by mounting the image to the machine and finding all the md5 hash values for each file in the image along with the file size.






File List
Name
Track (
Mount Image To Drive
Add Image
Image File:
C:\Users\baxy2\Desktop\digital forensics\investigation\Greenbook ISO .iso
Mount Type:
Physical & Logical
Drive Letter:
Next Available (E:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
C:\Users\baxy2\Desktop\digital forensics\investigation
Mount
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
Unmount
Close


Manage
This PC
File
Computer
View
Drive Tools
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
digital forensics
forensics
investigation
ISO Label [Rock Rid
OneDrive - Personal
This PC
Network
Linux
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (3)
Local Disk (C:)
32.3 GB free of 59.3 GB
DVD Drive (D:)
DVD
Removable Disk (E:)
0 bytes free of 21.5 MB
FAT32
10 items
1 item selected



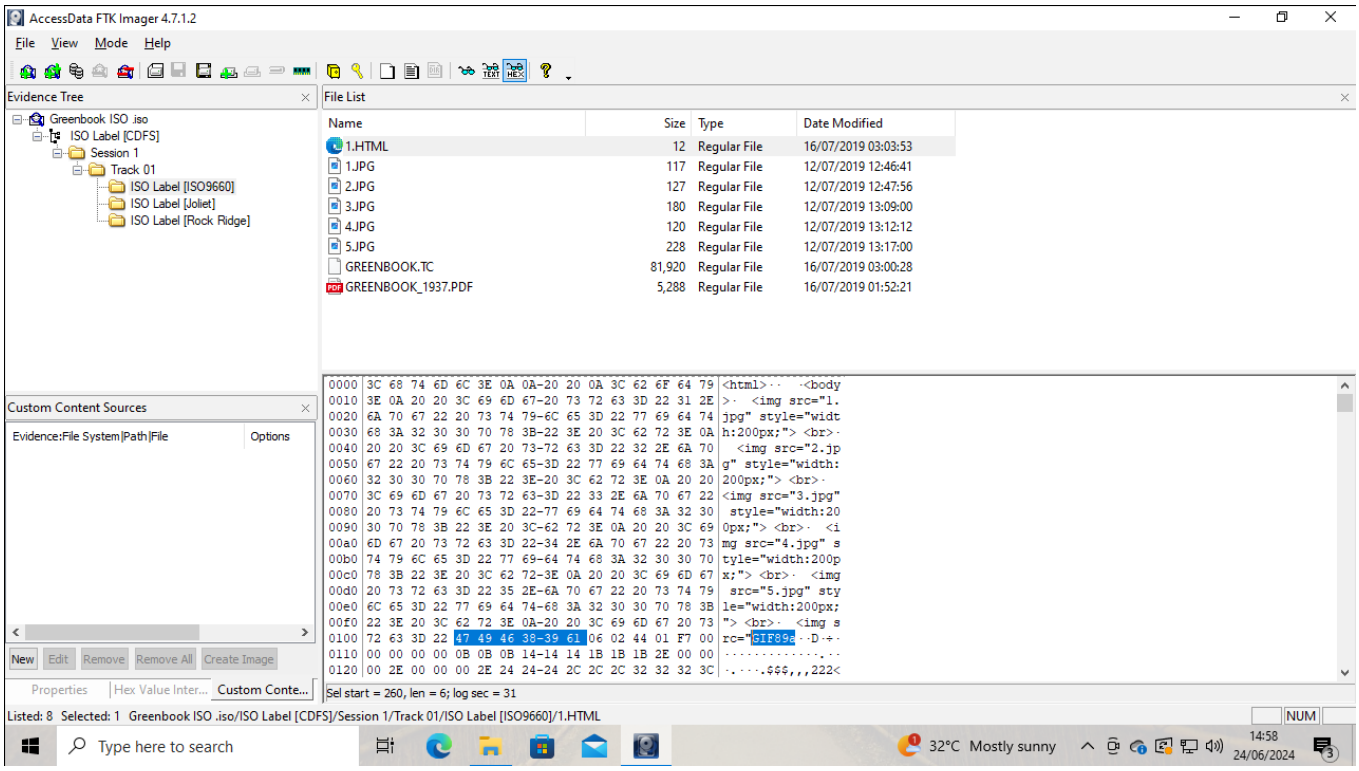
10. The md5 and sha based hash value for all the files in the

File Edit View

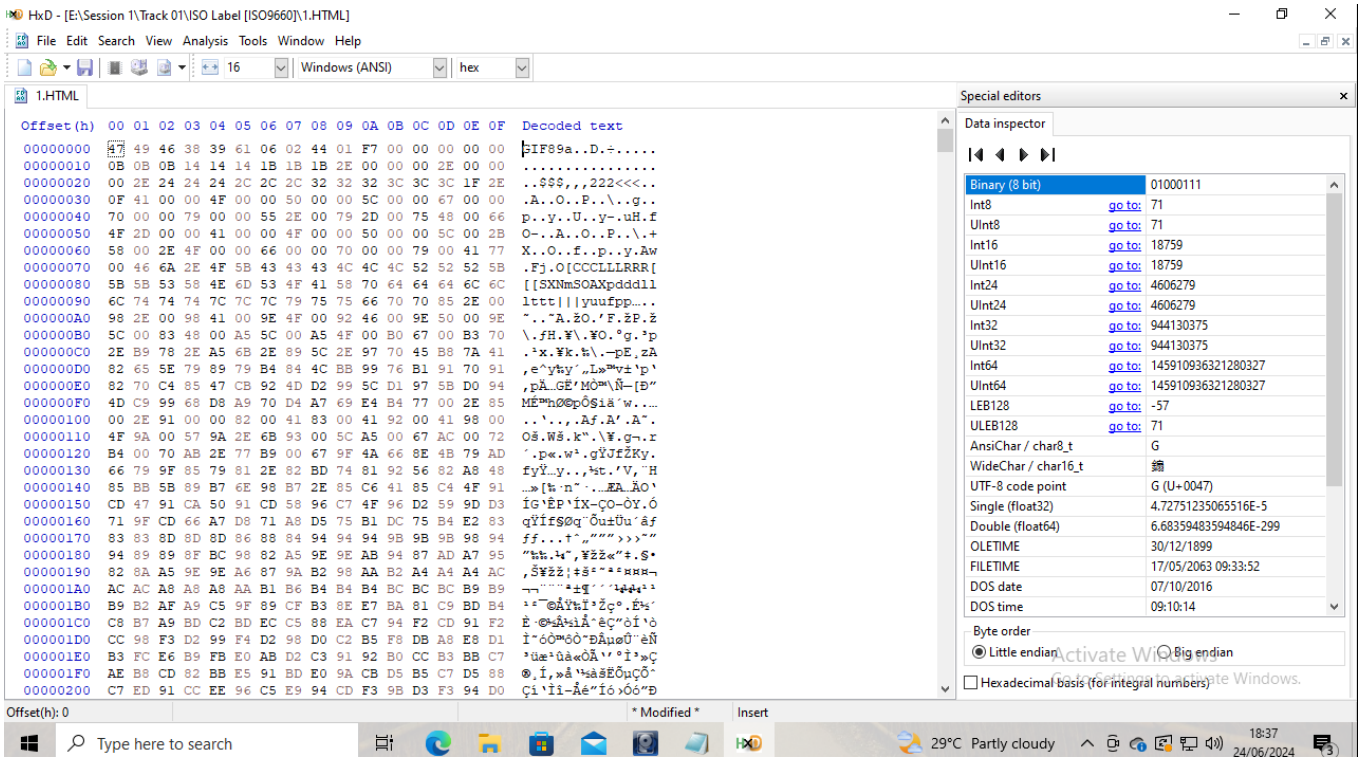
MD5	SHA1	FileNames
2a9d47cd337565ecbcd4556b85d675b2	2088912a1c7ea54d2fbd4540d0ba1fbd748b1c47	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\1.HTML
1831b1f5e0e5a22a1f9d5cbab2099f1b	133b871f9fbfe164c4c3ef66f772c67627606eb6	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\1.JPG
ae9ef080a292374a866d659abd55712f	d95551b859539e961e55db757d57505b1084ae3d	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\2.JPG
d3060c3925e2f21274c5d04ce465ef08	51e50e8e53dfa51c59a33637dd9f43f3a1b243c1	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\3.JPG
30c58285a32ac6ff2232fe09cf8a11dd	2f41da33c4a1716808faaa9a8f42a8483bf757f7	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\4.JPG
853bd591239b0225bbce59fdd7da1bc6	0dbf190c43472e9703fc507e08eb6447f3f5c8b4	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\5.JPG
39e0cc888b3d96fb07c411b4d52da1fa	51876d6af053134bc873b801bc06647159fdb2c8	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\GREENBOOK.TC
1bcbf60d6f2629a35dabcb4bcf1b2071	294e93d0348743c8ebfec8c173193e2d2f94a679	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [ISO9660]\GREENBOOK_1937.PDF
2a9d47cd337565ecbcd4556b85d675b2	2088912a1c7ea54d2fbd4540d0ba1fbd748b1c47	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\1.html
1831b1f5e0e5a22a1f9d5cbab2099f1b	133b871f9fbfe164c4c3ef66f772c67627606eb6	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\1.jpg
ae9ef080a292374a866d659abd55712f	d95551b859539e961e55db757d57505b1084ae3d	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\2.jpg
d3060c3925e2f21274c5d04ce465ef08	51e50e8e53dfa51c59a33637dd9f43f3a1b243c1	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\3.jpg
30c58285a32ac6ff2232fe09cf8a11dd	2f41da33c4a1716808faaa9a8f42a8483bf757f7	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\4.jpg
853bd591239b0225bbce59fdd7da1bc6	0dbf190c43472e9703fc507e08eb6447f3f5c8b4	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\5.jpg
39e0cc888b3d96fb07c411b4d52da1fa	51876d6af053134bc873b801bc06647159fdb2c8	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\greenbook.tc
1bcbf60d6f2629a35dabcb4bcf1b2071	294e93d0348743c8ebfec8c173193e2d2f94a679	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Rock Ridge]\Greenbook-1937.pdf
2a9d47cd337565ecbcd4556b85d675b2	2088912a1c7ea54d2fbd4540d0ba1fbd748b1c47	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\1.html
1831b1f5e0e5a22a1f9d5cbab2099f1b	133b871f9fbfe164c4c3ef66f772c67627606eb6	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\1.jpg
ae9ef080a292374a866d659abd55712f	d95551b859539e961e55db757d57505b1084ae3d	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\2.jpg
d3060c3925e2f21274c5d04ce465ef08	51e50e8e53dfa51c59a33637dd9f43f3a1b243c1	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\3.jpg
30c58285a32ac6ff2232fe09cf8a11dd	2f41da33c4a1716808faaa9a8f42a8483bf757f7	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\4.jpg
853bd591239b0225bbce59fdd7da1bc6	0dbf190c43472e9703fc507e08eb6447f3f5c8b4	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\5.jpg
1bcbf60d6f2629a35dabcb4bcf1b2071	294e93d0348743c8ebfec8c173193e2d2f94a679	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\Greenbook-1937.pdf
39e0cc888b3d96fb07c411b4d52da1fa	51876d6af053134bc873b801bc06647159fdb2c8	Greenbook.ISO\ISO Label [CDFS]\Session 1\Track 01\ISO Label [Joliet]\greenbook.tc

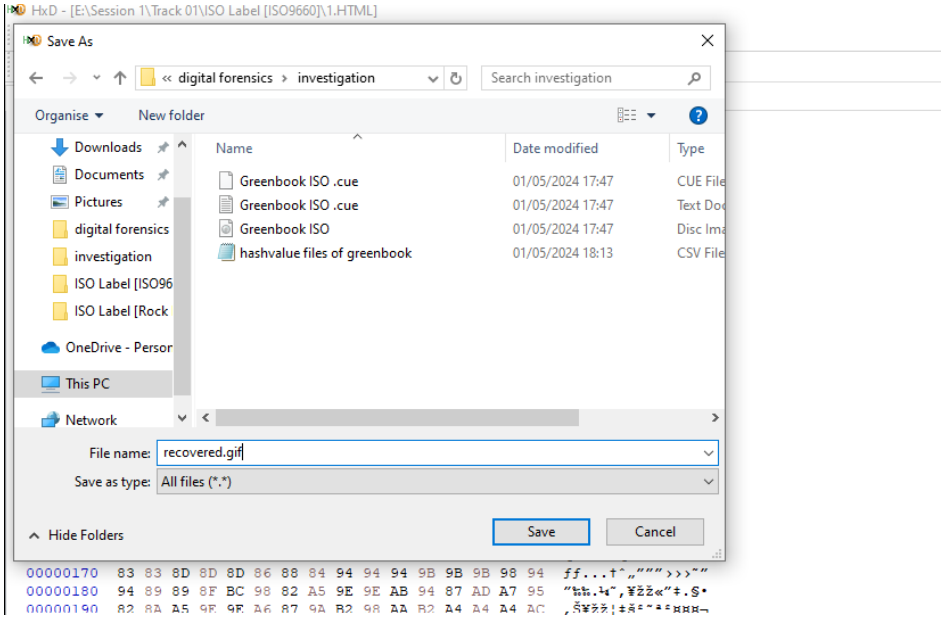
3.3. Details of Search Result and Conclusions

In the investigation, I found that there is a hex value given and a magic number (GIF89a) given in the html file that indicates a presence of a GIF file.

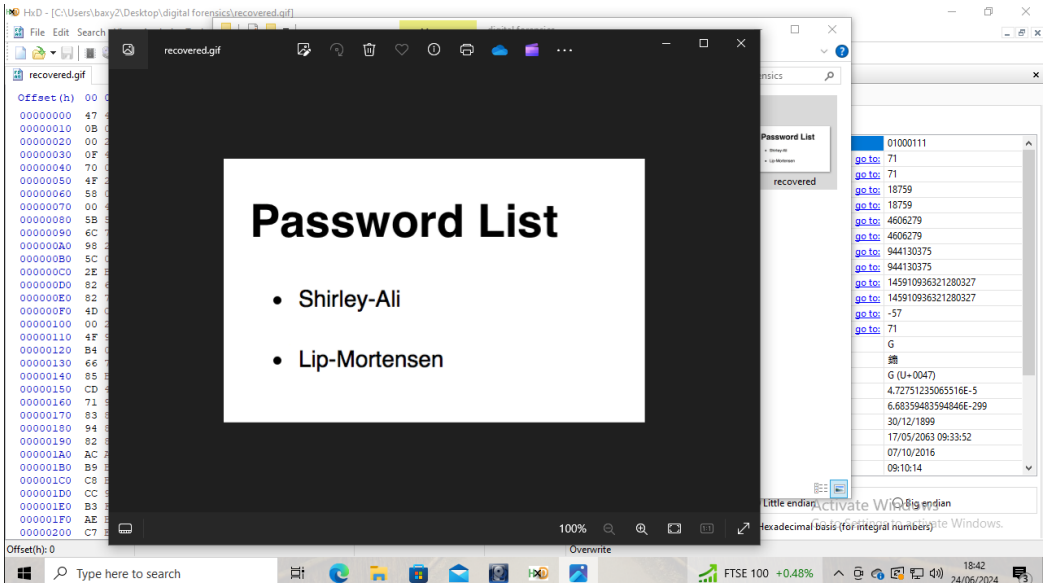


So, I decided to change the format of the file by deleting all the hex values above the 47 45 46 38-39 61 and making it a GIF file header. Then, renamed that file to recovered.gif and saved it. Finally I got the gif file that was hidden in the html file.

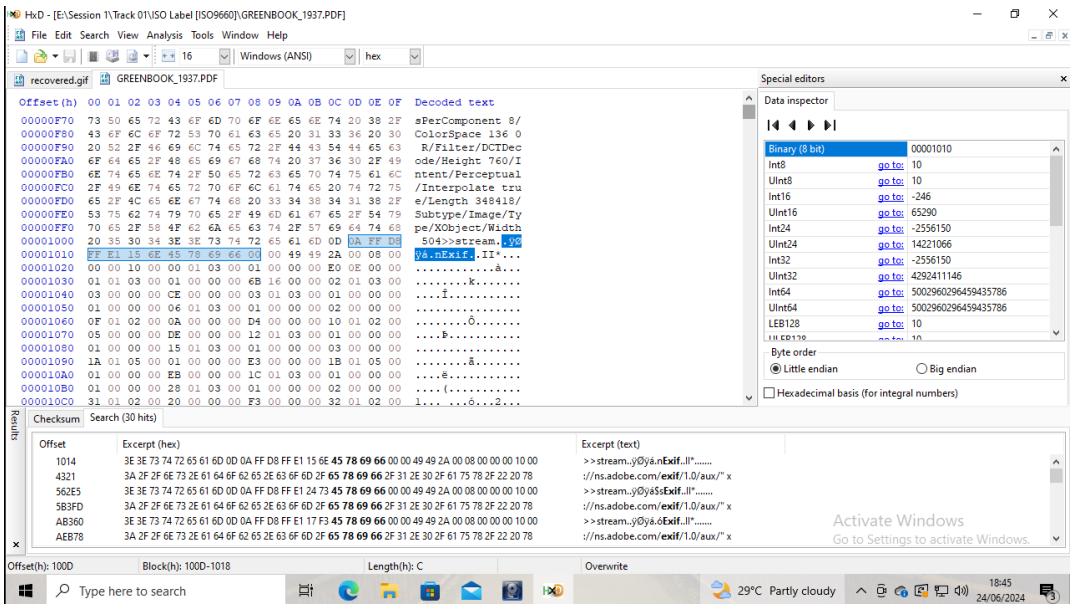




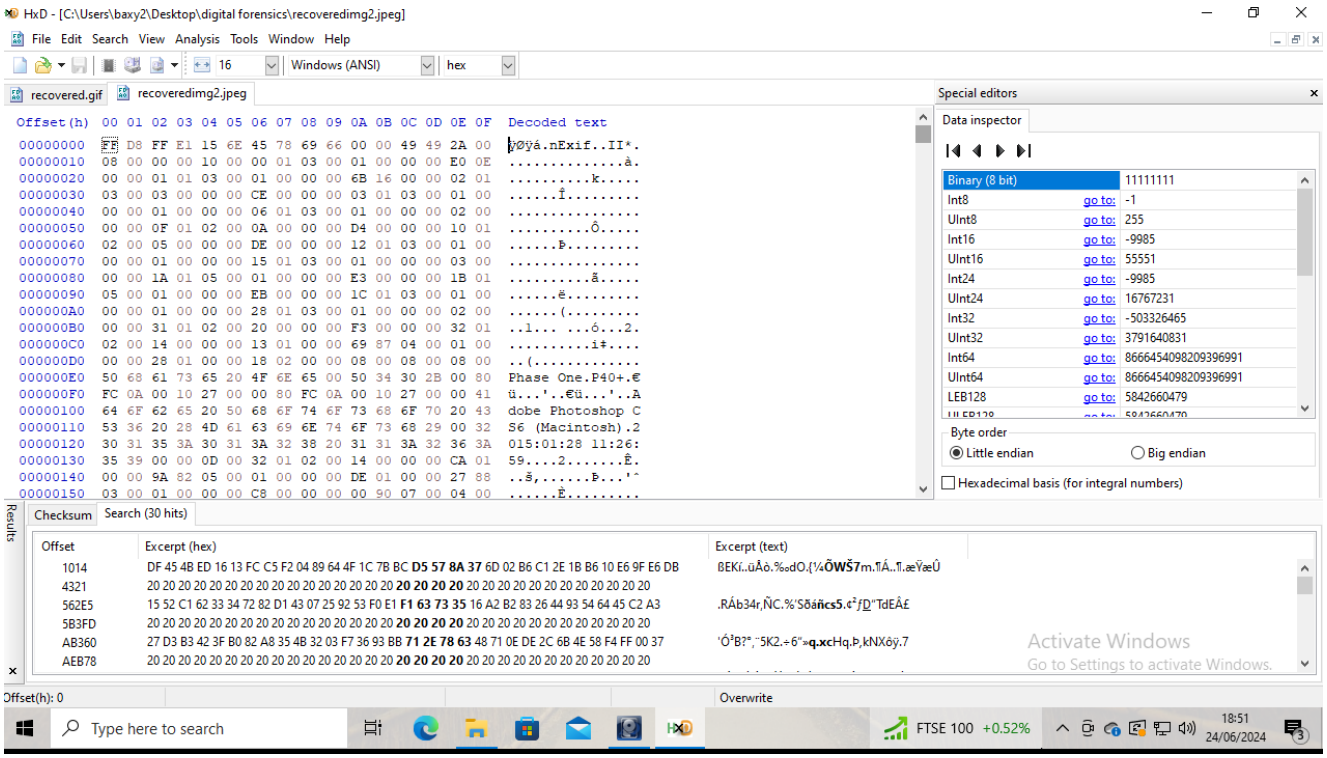
The recovered gif file contained a list of passwords. So, I investigated into other files much further to find out why these passwords are given.

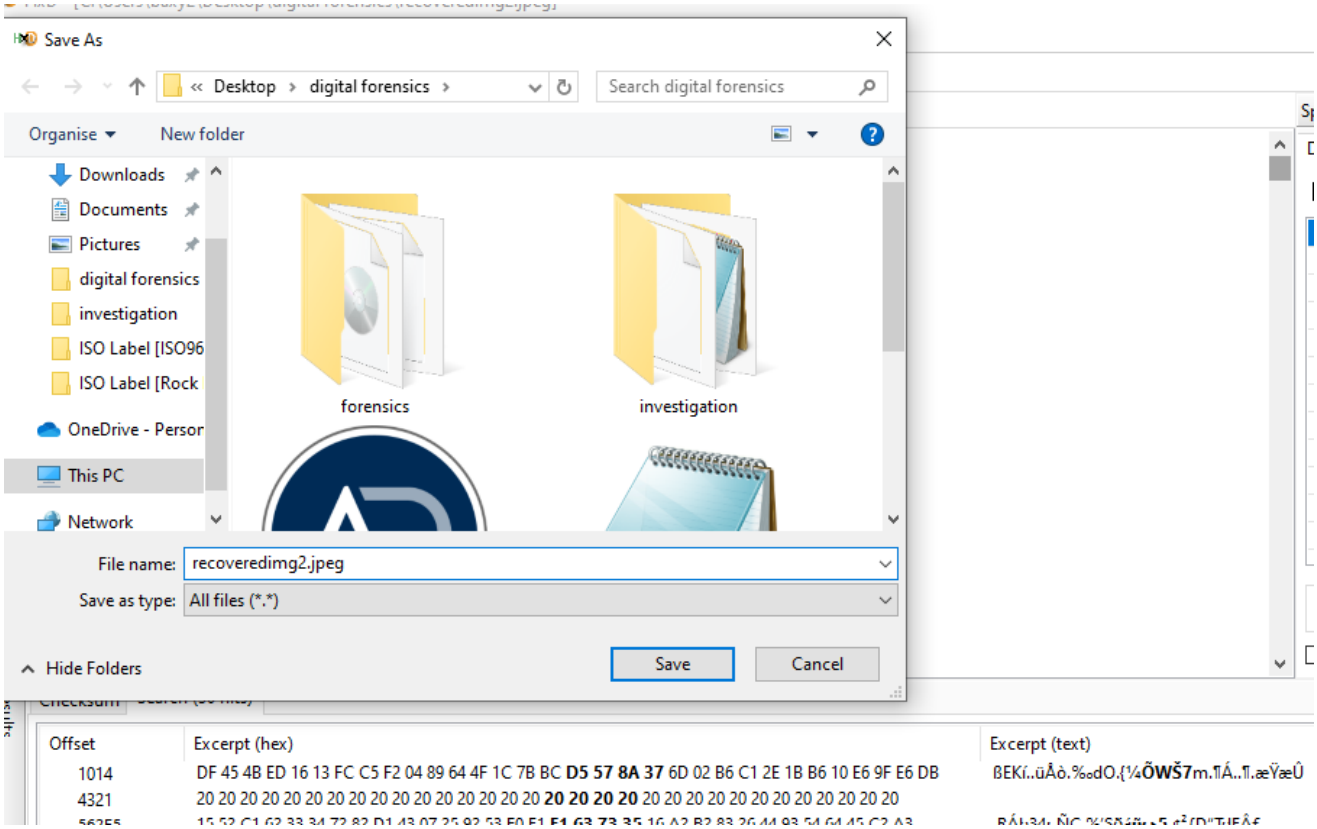


Then there was a PDF file, Greenbook.pdf, I opened it with the hex editor

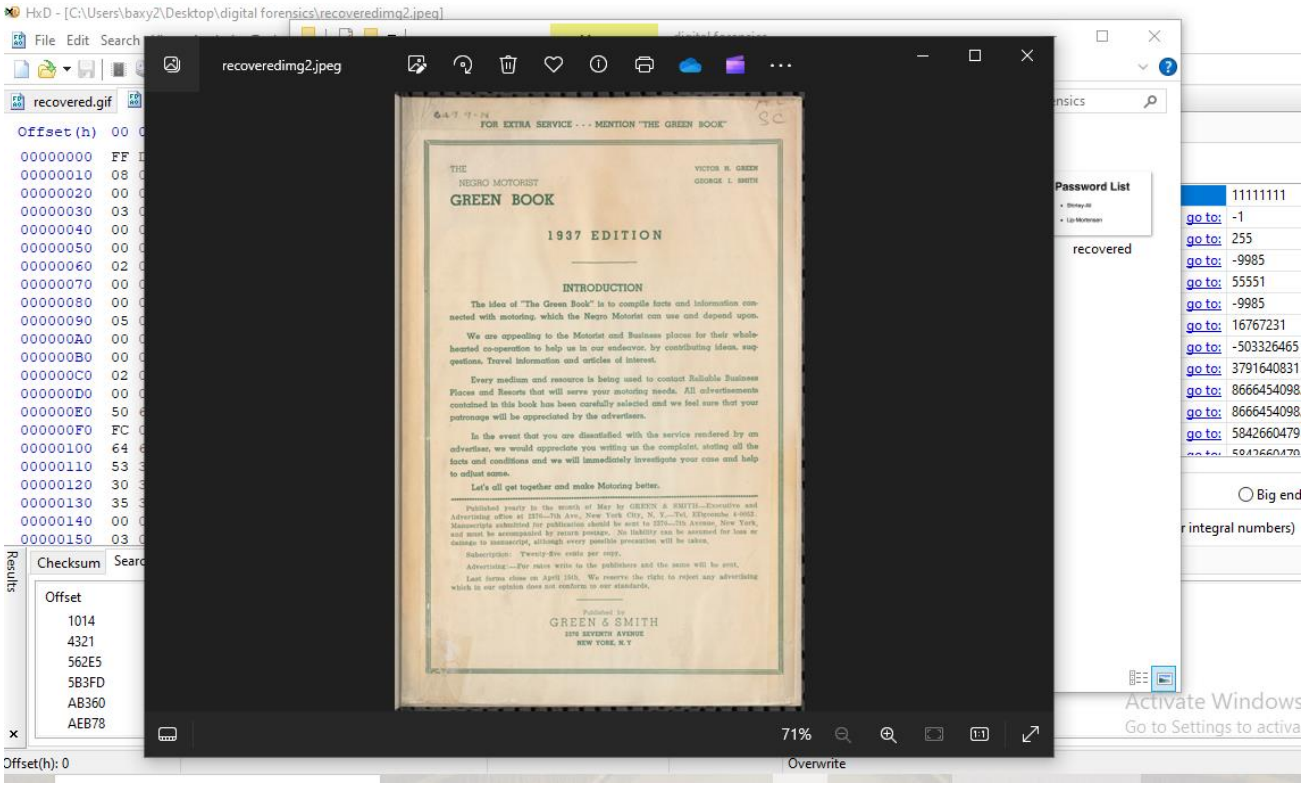


I found that there is an exif file hidden in this as well. So, to recover the exif file, I deleted the hex values above the 0A FF D8 to make the header a Exif file header. Then I saved the file as recovered2.jpeg.

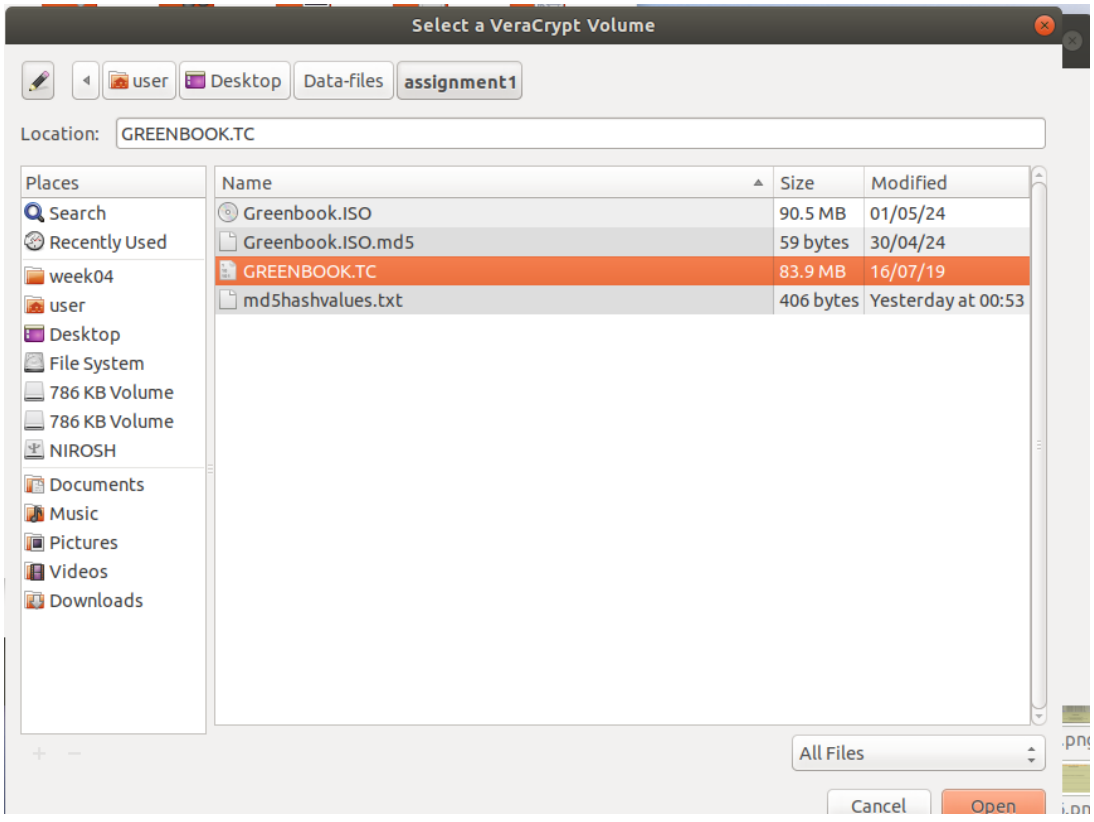




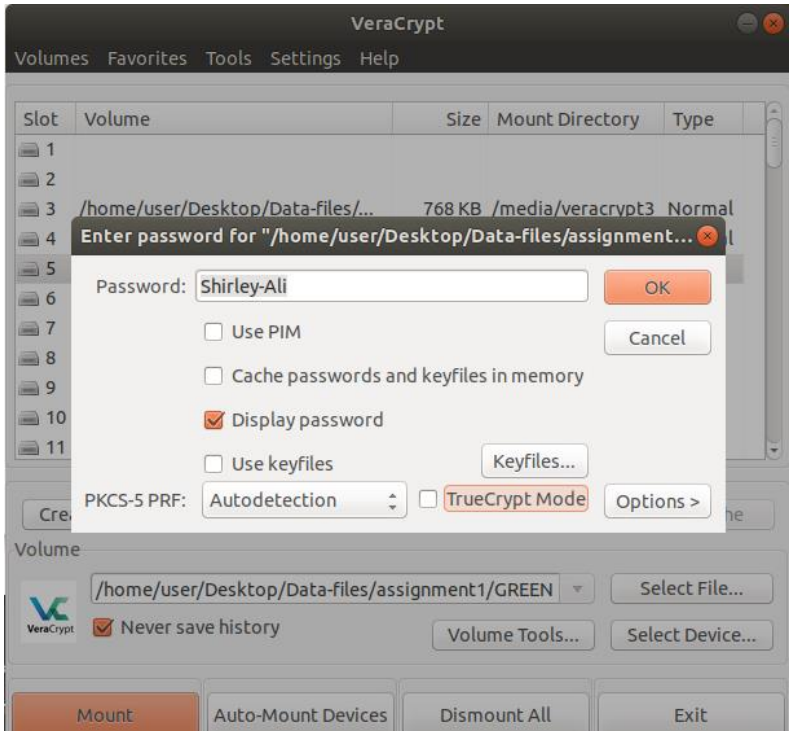
The recovered image shows about an introduction page to a book called GREEN BOOK



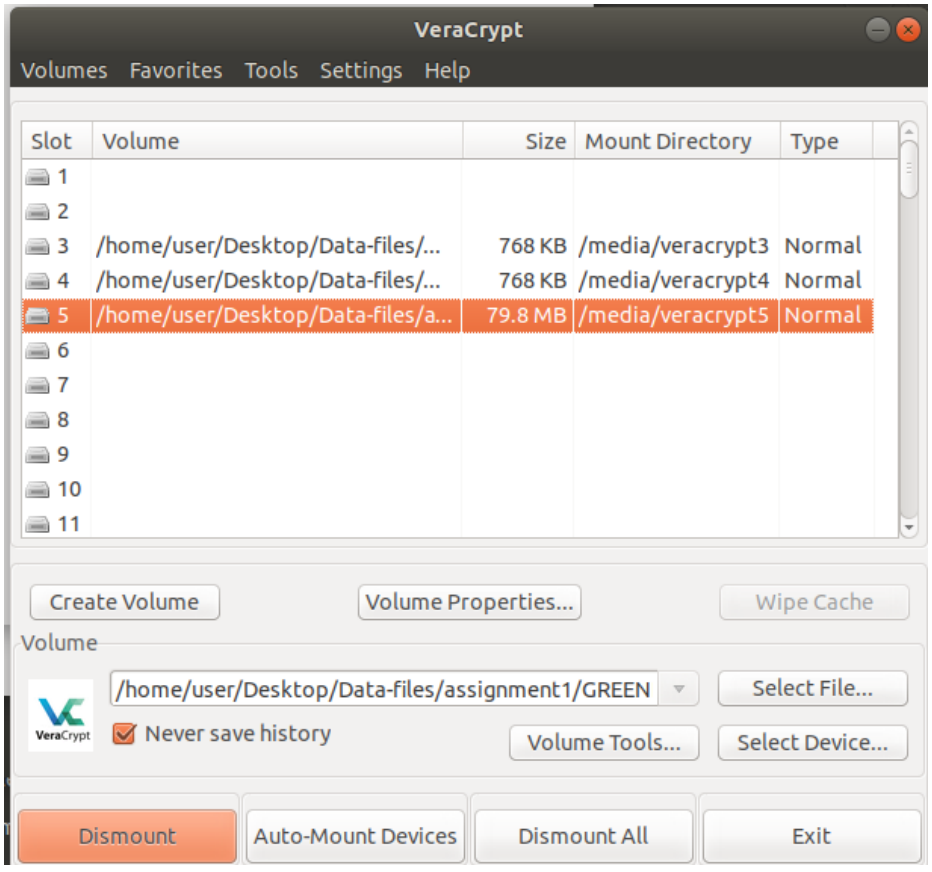
Now let's move on to GREENBOOK.tc file. This is a TrueCrypt file and it is encrypted. So, inorder to decrypt it, I'm using VeraCrypt to do that.



In order to decrypt this file, I have to first mount this file, for that, we will have to know the password that was used to encrypt it, since we have got the password file, I'm going to use the first password (Shirley-Ali) to decrypt it.

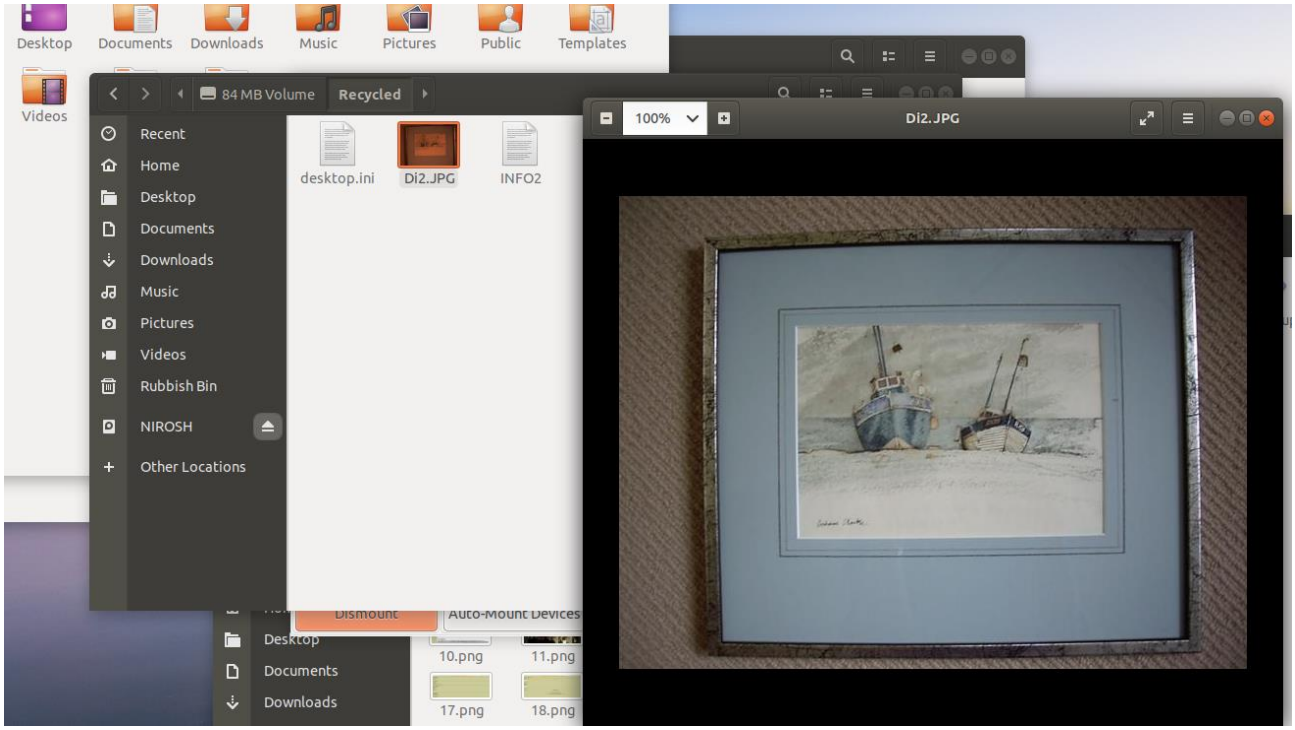


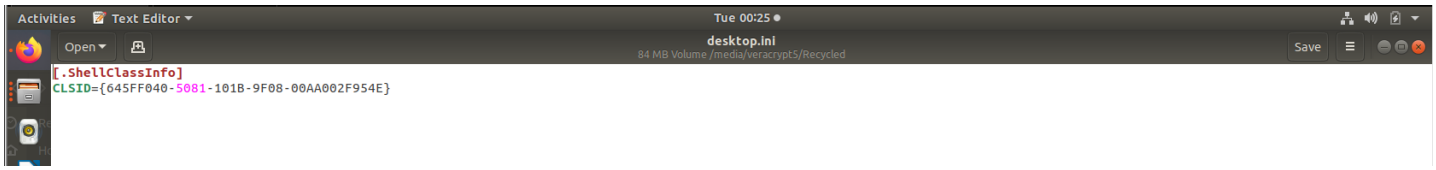
Then the password was correct and it got mounted and the decrypted files were recovered



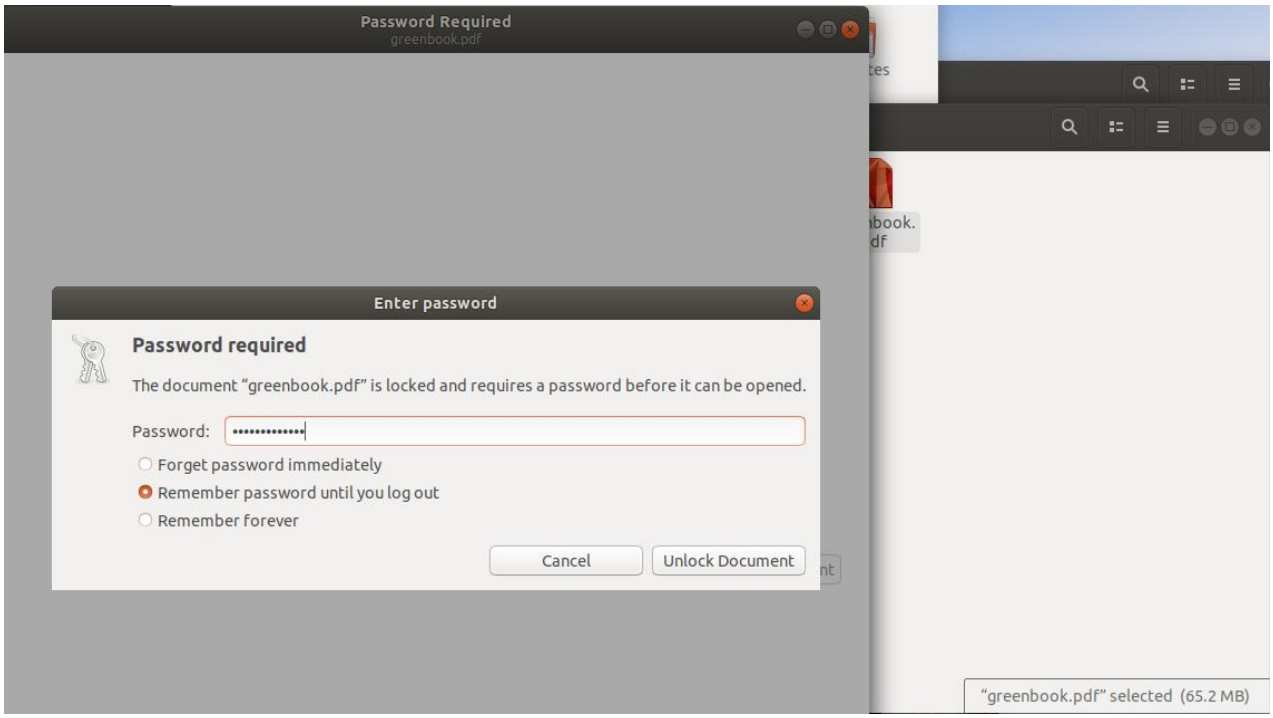
Then I went through the file, there in the Recycled folder I got the deleted items. Finally, there were 2 other pdfs, greenbook.pdf and credit.pdf.

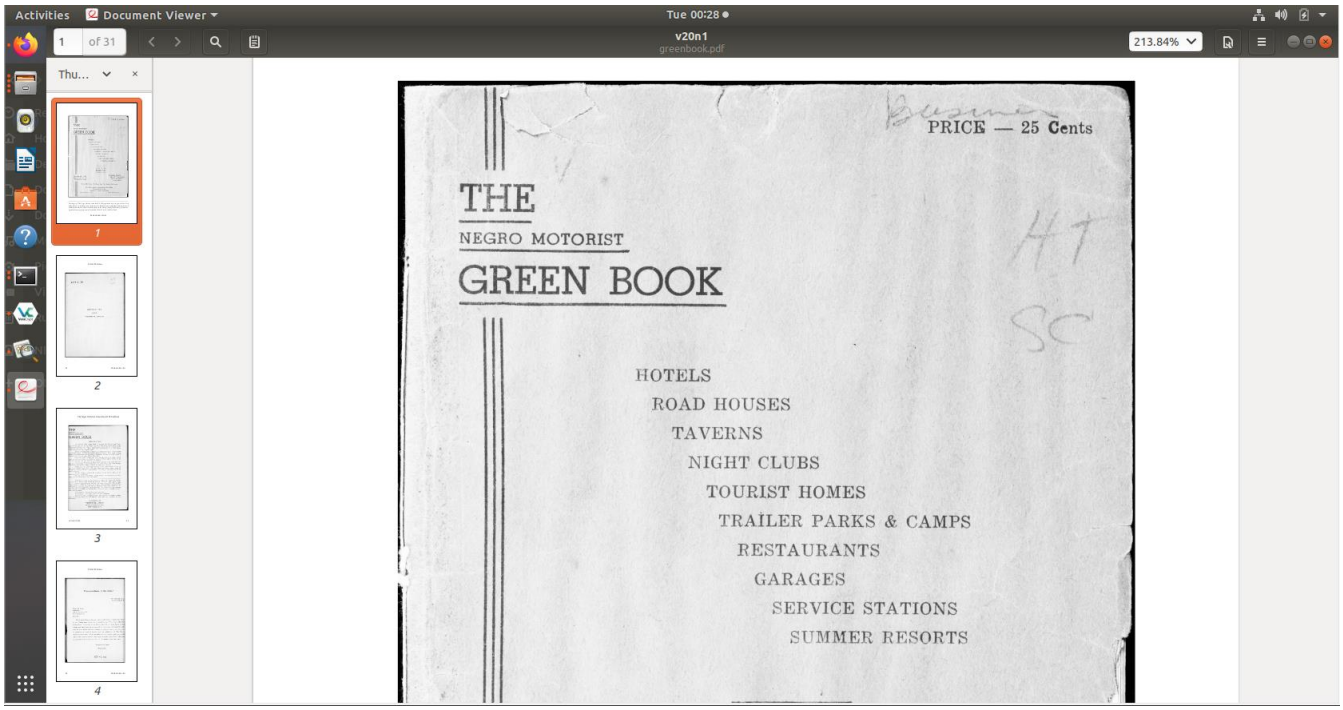
The Recycled folder contains the image of the two boats artwork, a binary file and an ordinary file.

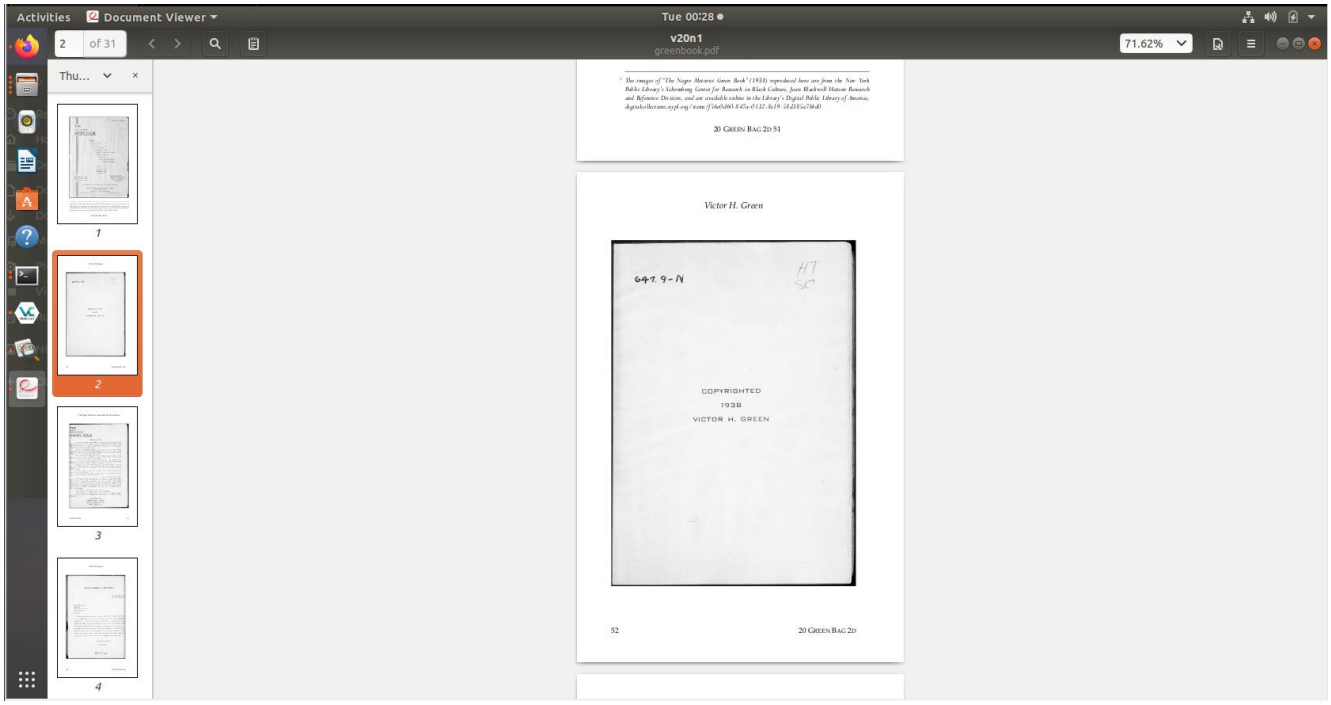




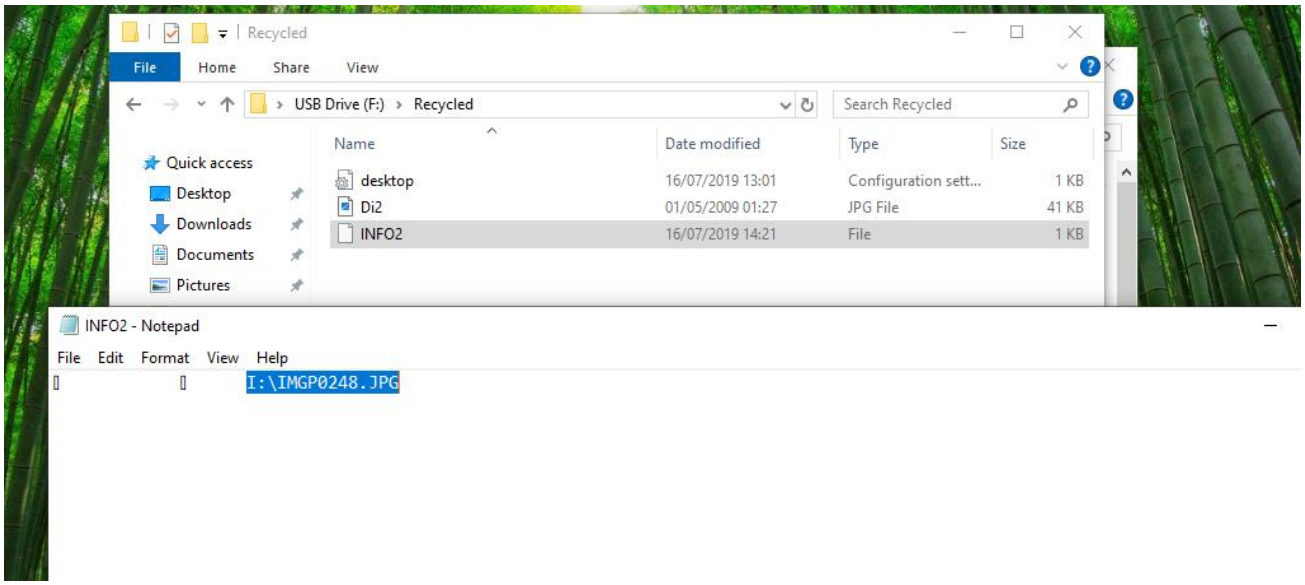
Now I tried access the Greenbook.pdf. Once I tried to do it, it asked for the password. I used the second password that was in the password list that I recovered earlier. The password was Lip-Mortensen. Then the pdf was about the Green Book.



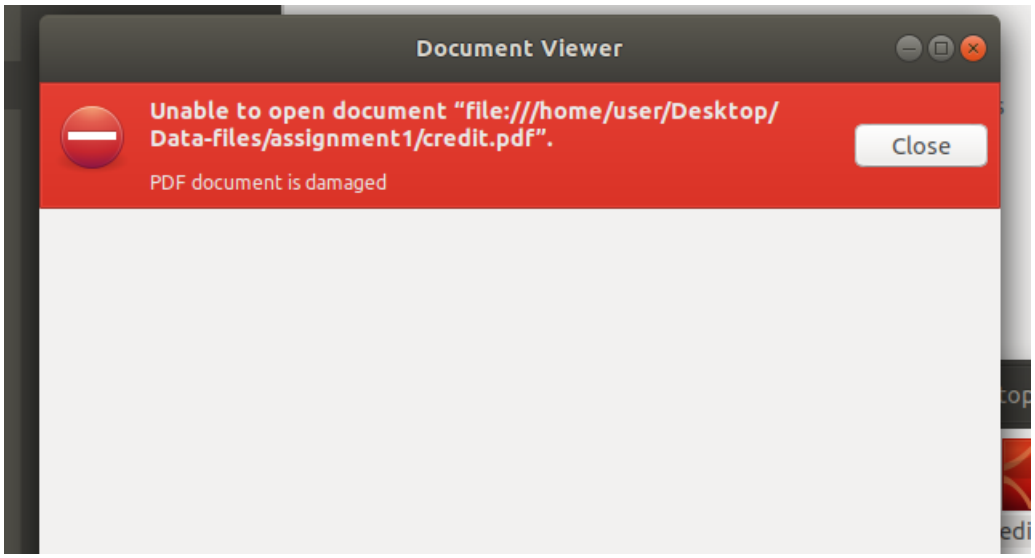




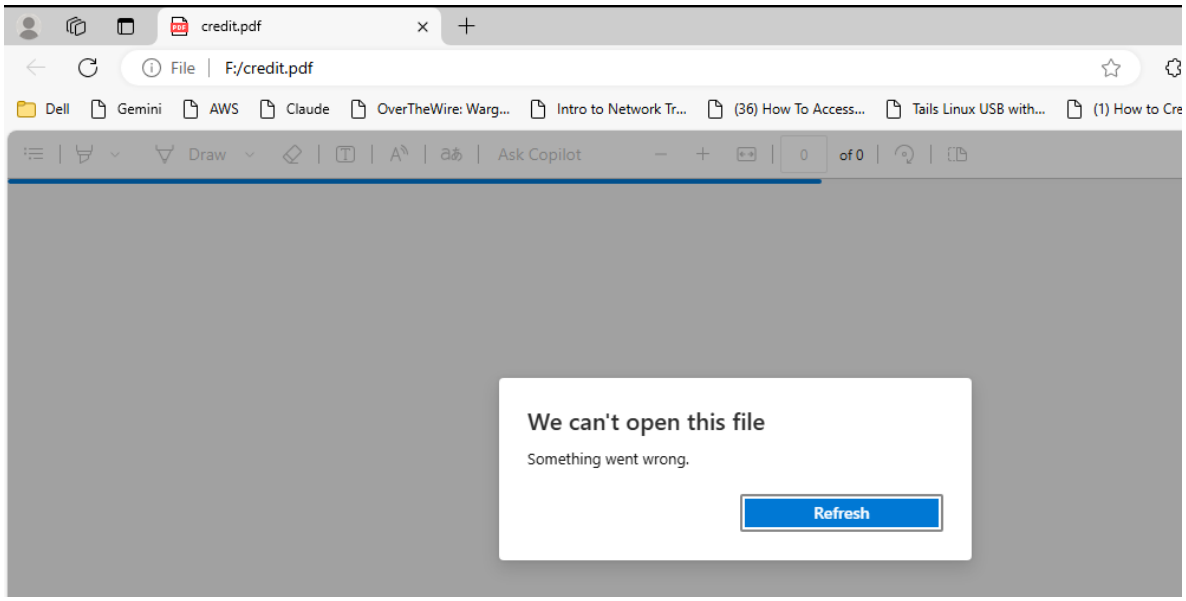
The INFO2 file contained a name of a jpeg file.



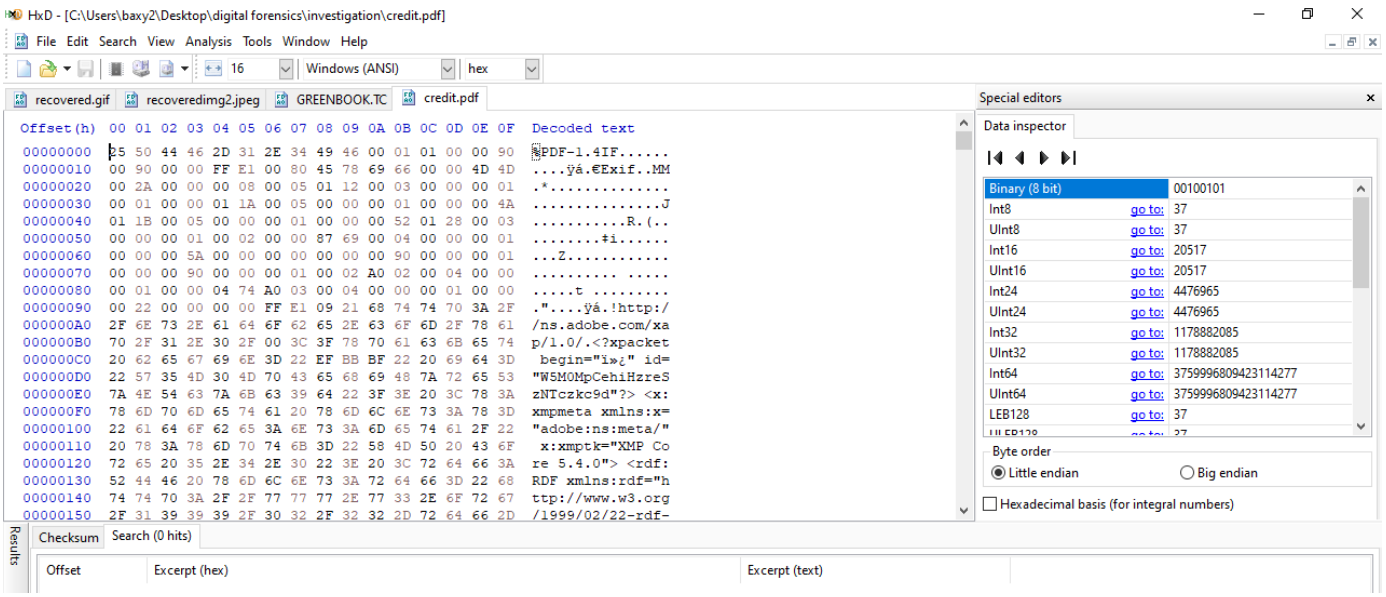
Then there was the pdf called Credit.pdf, when I tried to open it, it was corrupted, which means, it is not a pdf file but a different one.



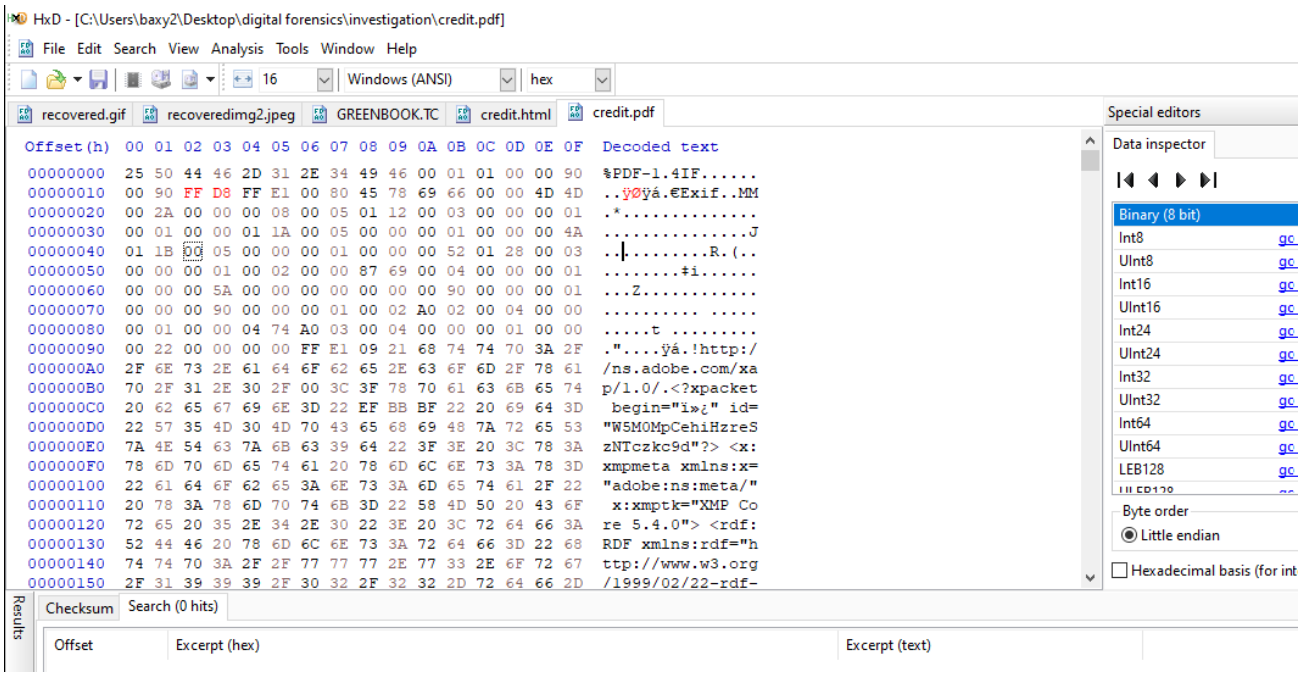
I tried to open it with the Microsoft edge, but didn't work.

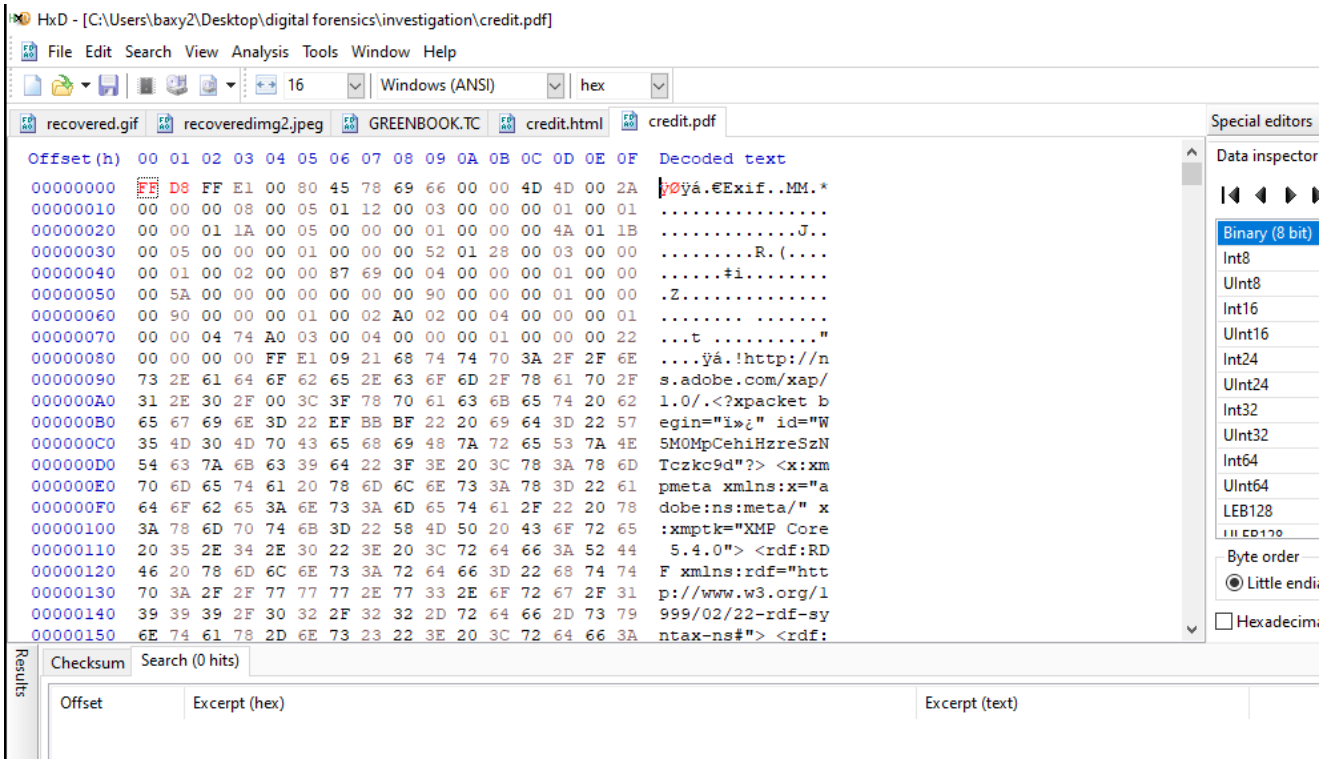


So, to figure out what this file really is, I opened the HxD editor and opened the credit.pdf file.

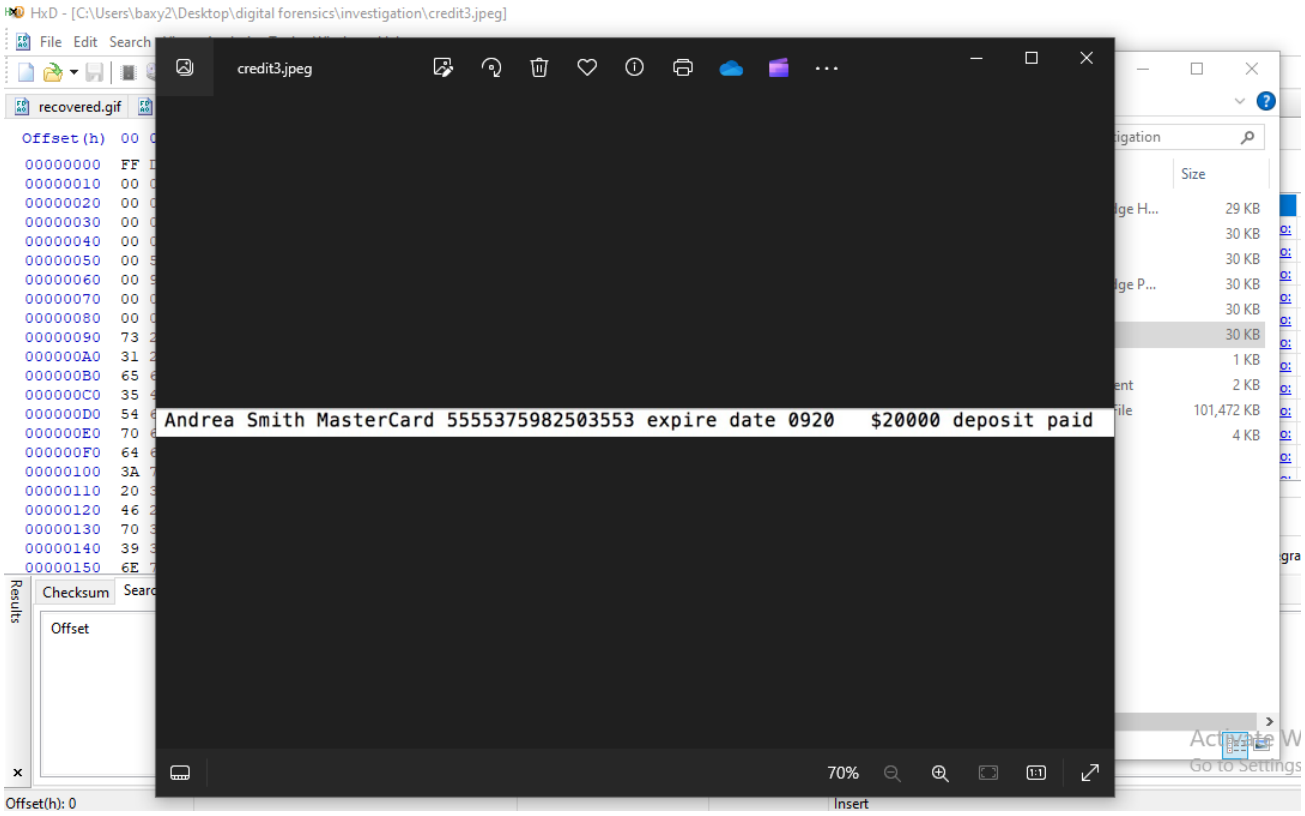


The hex editor showed that there is another Exif file embedded with it, so in order to retrieve it, I had to type in the correct header value for the Exif file and delete the header of the PDF file.





Then I saved the file called credit3.jpeg, since it has an exif file embedded along with it. Once I open the image, it was the bank details of the person called Andrea.



Conclusion

Standard forensic techniques were followed in the thorough examination of the CD-ROM that was taken from Donald Price's office. After safely configuring the digital forensic workstation, the CD-ROM's ISO image was downloaded and its integrity was confirmed using several SHA-based hash functions. In order to preserve data validity, a thorough record of the files and their attributes on the CD-ROM was completed. This included the MD5 hash values.

Key findings:

- *On the CD-ROM, a number of files were found, including pictures and records that were essential to the inquiry. Importantly, the existence of files like GREENBOOK_1937.PDF and GREENBOOK.TC offered strong proof.*

- *On the ISO image, a comprehensive keyword search was carried out, focusing on terms associated with the transactions and missing artwork. But nothing significant was found.*

- *Records of a business transaction in which Donald Price sold Andrea the lost artwork for $20,000 were among the evidence retrieved from the CD-ROM.*

The digital forensic data clearly demonstrates that Donald Price committed fraud when he sold Andrea the pilfered artwork for $20,000. He tried to hide what he had done by erasing his PC's hard drive, but the CD-ROM was found and examined by forensics. Donald Price is declared guilty of both theft and fraud in light of the overwhelming proof of his involvement and the financial transaction. Given the gravity of the acts committed, the case ought to be investigated as a criminal case.

The evidence produced was ensured to be reliable and admissible by a rigorous forensic process that followed legal and technological requirements. Donald Price's activities have caused Joachim's Art Gallery serious financial and reputational harm, necessitating more legal action.

4. LEGAL IMPLICATIONS

4.1. One Violation and Justification Against: Cybercrime Act 2001 and Crimes Act 1958

The Cybercrime Act 2001 is an Australian legislation that addresses various forms of cybercrime and criminal activities involving computers and digital technology. It aims to provide legal frameworks for investigating, prosecuting, and penalizing cyber-related offenses, ensuring the security and integrity of digital systems and information. The act covers a wide range of offenses, including unauthorized access to computer systems, data interference, cyber fraud, and online identity theft.

Violation: Mr. Price's act of wiping the hard disk of his office PC before investigators could be deployed constitutes a violation under the Cybercrime Act 2001. Specifically, it may fall under Section 477.1 - Unauthorized access, modification, or impairment with intent to commit a serious offence.

Justification: According to the Cybercrime Act 2001, unauthorized access, modification, or impairment of data with the intent to commit a serious offence is considered a criminal act. By wiping the hard disk, Mr. Price may have attempted to obstruct the investigation, which can be interpreted as an unauthorized modification of digital data with malicious intent.

The Crimes Act 1958 is a Victorian legislation in Australia that outlines criminal offenses and penalties within the state of Victoria. It covers a broad spectrum of criminal activities, including theft, assault, fraud, homicide, and property-related offenses. The act provides legal definitions of these offenses, along with the procedures for investigation, prosecution, and sentencing. It serves as a foundational legal framework for addressing criminal behavior and maintaining public safety within Victoria.

Violation: Mr. Price's involvement in the disappearance of the watercolour painting from Joachim's Art Gallery may constitute a violation under the Crimes Act 1958. Specifically, it may fall under Section 74 - Theft.

Justification: According to the Crimes Act 1958, theft is defined as intentionally and dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it. If Mr. Price is found to have unlawfully taken the watercolour painting, it would constitute theft under this act.

4.2. Justification as to whether this Case is Best Pursued as a Corporate or Criminal Investigation

- This case is best pursued as a criminal investigation due to the severity of violations and potential criminal activities involved.

References

Appendices – only use if you refer to additional information from the main body of your report.

- corporateName=Attorney-General's, S. (n.d.). *Cybercrime Act 2001*.

  https://www.legislation.gov.au/C2004A00937/latest/text

- *Crimes Act 1958*. (n.d.). https://www.legislation.vic.gov.au/in-force/acts/crimes-act-1958/304