

SIT282 Computer Crime and Digital Forensics
ASSIGNMENT 1

Report Title: Forensic Investigation of Donald Price Case

Table of Contents:

1. Digital Forensic Procedure

1.1 Evidence Form

1.2 Description of Forensic Workstation and Image Download Procedure

1.3 SHA-based Hash Function Values of the ISO Image

1.4 Explanation of Need for Multiple Hash Values

1.5 Procedure Before Accessing Image File in VM

2. Description of Binary Details

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

2.2 Description of Programs for Investigation

3. Outcomes of Digital Forensic Investigation

3.1 Description and Justification of Key Words

3.2 Documented Procedure and Screenshots

3.3 Search Results and Conclusions

4. Legal Implications

4.1 Violation Against Cybercrime Act 2001 and Crimes Act 1958

4.2 Justification for Investigation Type

Investigator Name: Nirosh Ravindran

1. DIGITAL FORENSIC PROCEDURE

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

Digital Sentinel Forensic Team <i>This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.</i>			
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.	Date & Time	28/04/2024 @ 11:30:11
	Copy of CD-ROM is placed in the virtual machine		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

The screenshot shows a terminal window with a root shell on a Kali Linux system. The user has run several commands to calculate different hash values for the 'Greenbook.ISO' file:

- ls: Shows the file 'Greenbook.ISO' in the current directory.
- cat Greenbook.ISO.mds: Prints the MD5 hash of the file, which is c5f7921e78b303777f7c9695530c6084.
- md5deep Greenbook.ISO: Prints the MD5 hash again, confirming it's the same as the previous command.
- sha1sum Greenbook.ISO: Prints the SHA-1 hash, which is ef2b75f0cc8d8a0b181c85b7891aba78a4003f88.
- sha256sum Greenbook.ISO: Prints the SHA-256 hash, which is 068234ab49ac815c7d8d71220c5b20badad5cd08573c73cf755c22fbf26752e2.
- sha512sum Greenbook.ISO: Prints the SHA-512 hash, which is 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 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*

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

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

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_investigation × +

localhost:9999/autopsy?mod=1&submod=4&case=missing_art_investigation

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](#)

art was not found
Search Options:
 ASCII
 Case Sensitive
 Regular Expression

art was not found
Search Options:
 Unicode
 Case Sensitive
 Regular Expression

 missing_art_investigation × +

localhost:9999/autopsy?mod=1&submod=4&case=missing_art_investigation

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

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

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_investigation

localhost:9999/autopsy?mod=1&submod=4&case

FILE ANALYSIS KEYWORD SEARCH

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_investigation

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

A screenshot of a Firefox browser window titled "missing_art_investigation". The address bar shows "localhost:9999/autopsy?mod=1&submod=4". The main content area displays search results for the term "Donald Price".

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

A screenshot of a Firefox browser window titled "missing_art_investigation". The address bar shows "localhost:9999/autopsy?mod=1&submod=4". The main content area displays search results for the term "cash".

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.

The screenshot shows a terminal window titled "root@nirosh:/home/nirosh/Desktop/Forensic Investigation". The terminal history is as follows:

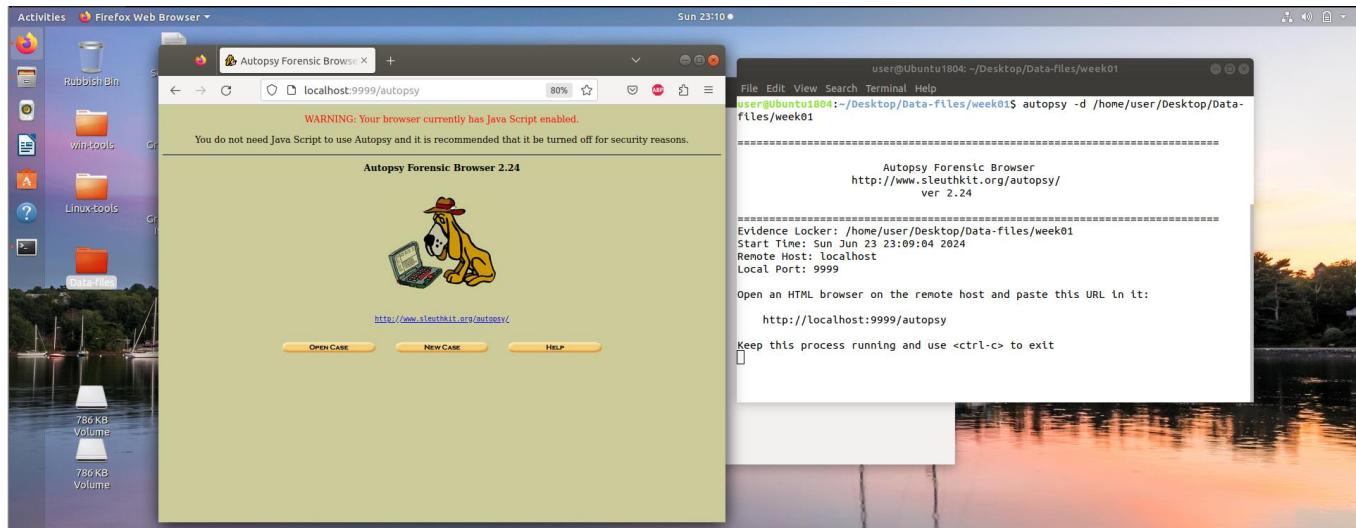
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
ls
Greenbook.ISO Greenbook.ISO.md5
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
cat Greenbook.ISO.md5
MD5 (2019Greenbook.ISO) = c5f7921e78b303777f7c9695530c6084
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
md5deep Greenbook.ISO
c5f7921e78b303777f7c9695530c6084 /home/nirosh/Desktop/Forensic Investigation/Greenbook.ISO
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
sha1sum Greenbook.ISO
ef2b75f0cc8d8a0b181c85b7891aba78a4003f88 Greenbook.ISO
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
sha256sum Greenbook.ISO
068234ab49ac815c7d8d71220c5b20badad5cd08573c73cf755c22fbf26752e2 Greenbook.ISO
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
sha512sum Greenbook.ISO
e8814c02915b11c8d9e03a42daa6b3f7365707f2d6fb7ff2ba1107151214e21919cedd3037113c1acac67da1e1739fe7f00a8d192c5f4ecb4dbdcc9d4a3c7d35 Greenbook.ISO
- (root@nirosh)-[~/home/nirosh/Desktop/Forensic Investigation]
#

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.

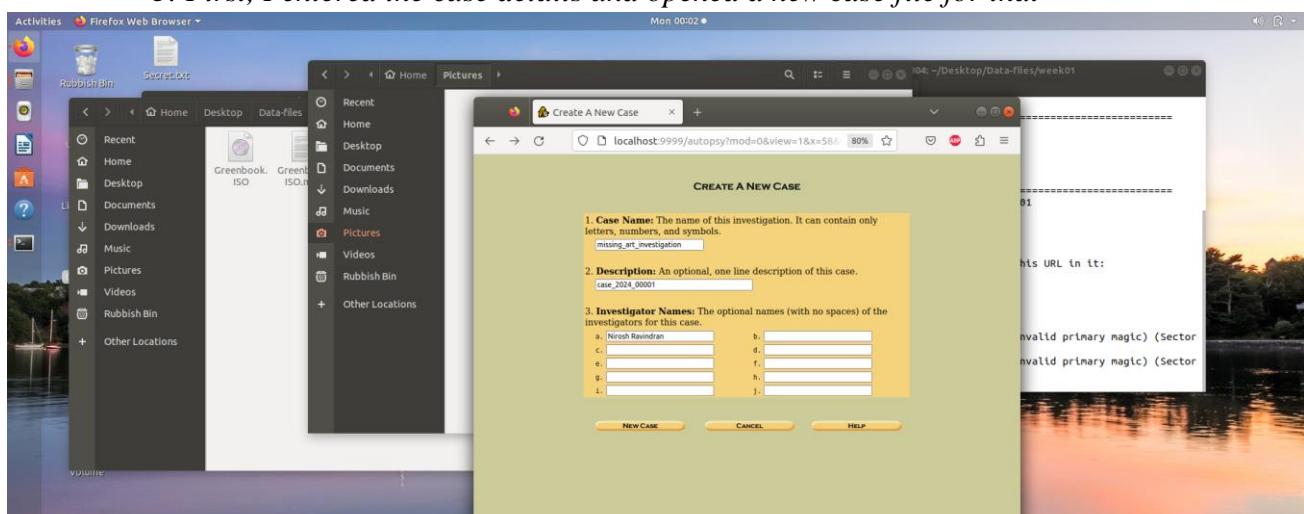
```
user@Ubuntu1804: ~/Desktop/Data-files/week01
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/week01$ autopsy -d /home/user/Desktop/Data-
files/week01
=====
Autopsy Forensic Browser
http://www.sleuthkit.org/autopsy/
ver 2.24
=====
Evidence Locker: /home/user/Desktop/Data-files/week01
Start Time: Sun Jun 23 23:09:04 2024
Remote Host: localhost
Local Port: 9999

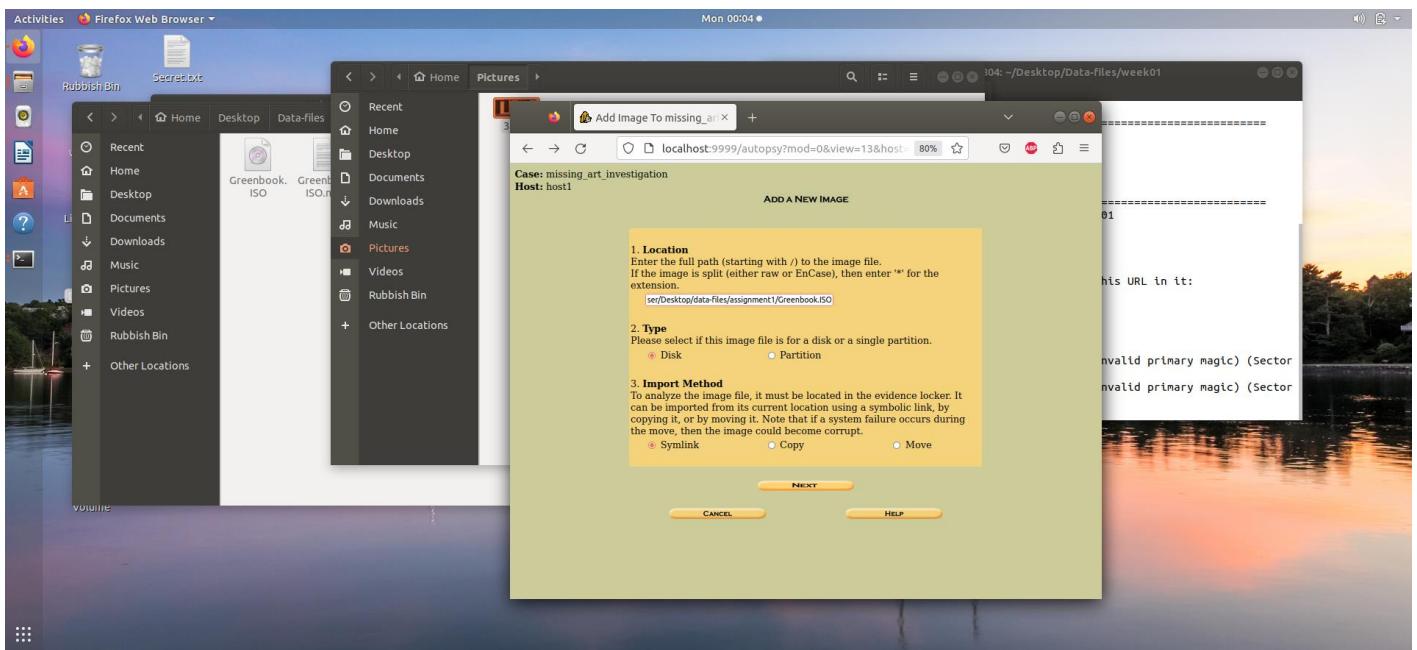
Open an HTML browser on the remote host and paste this URL in it:
http://localhost:9999/autopsy

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

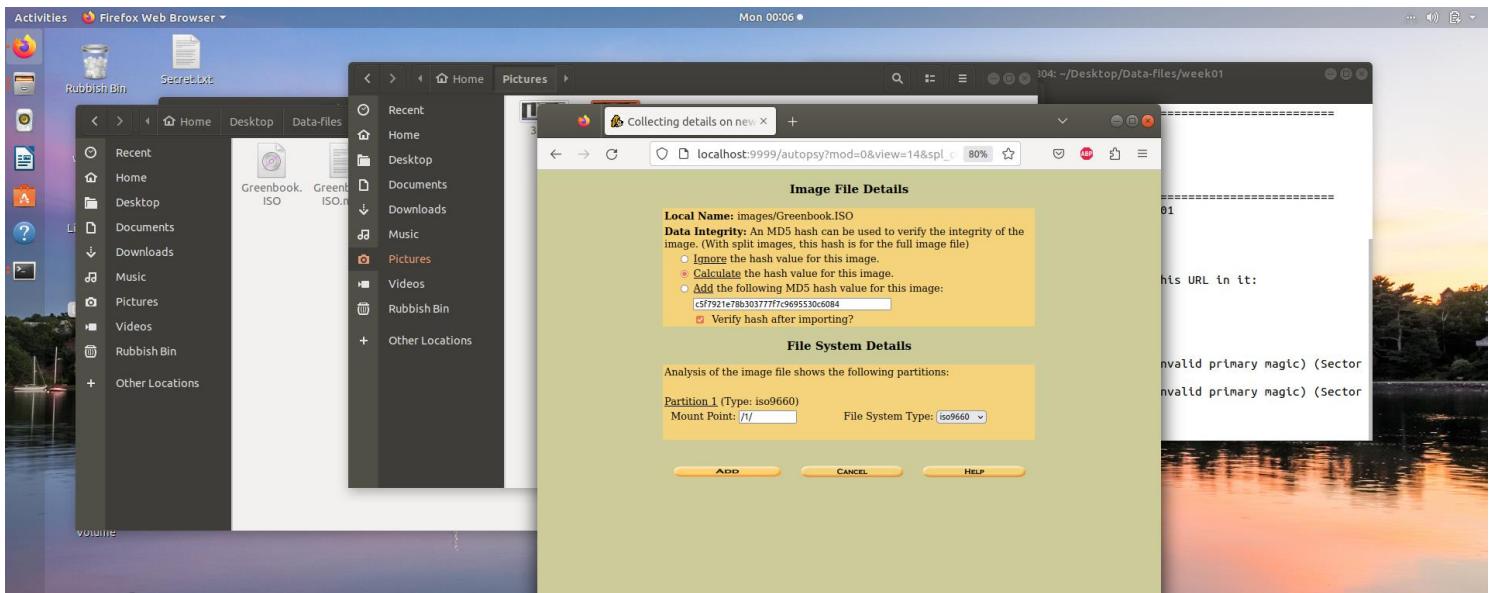
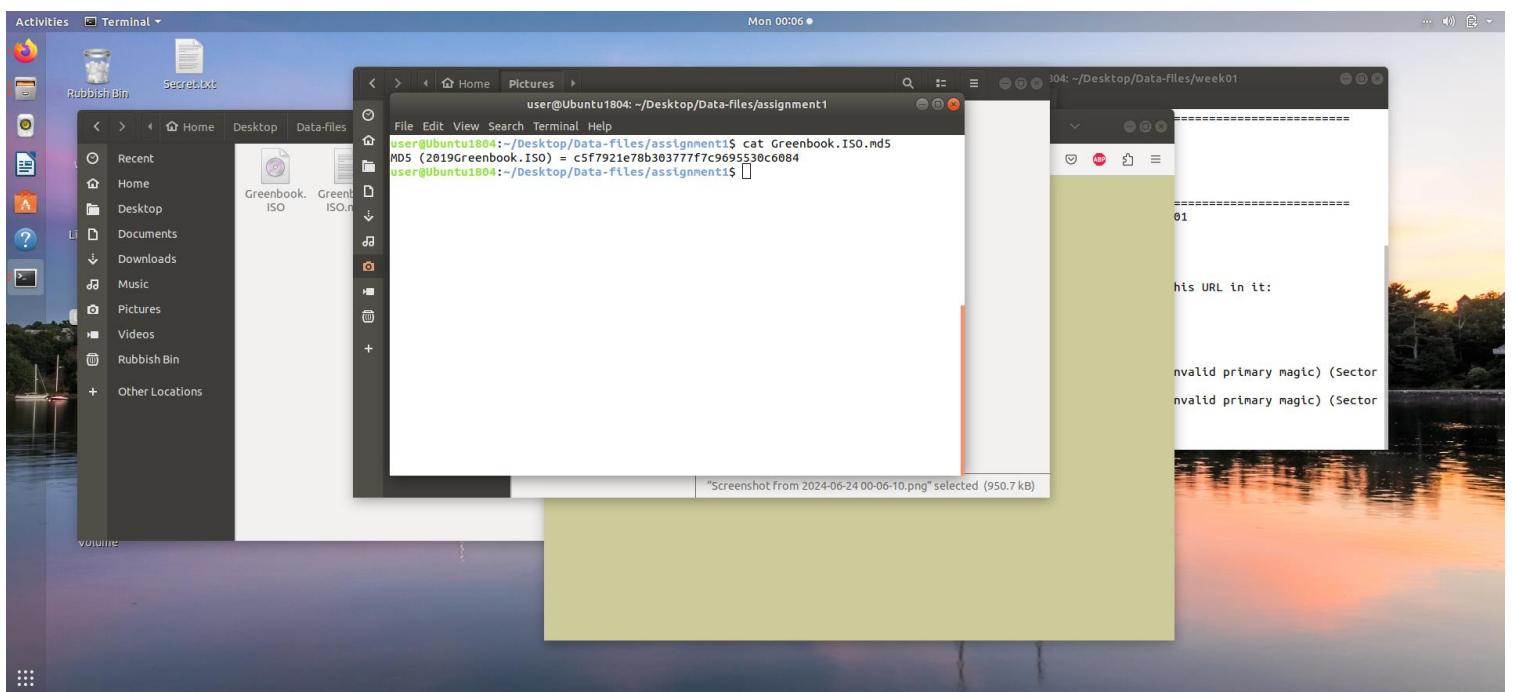


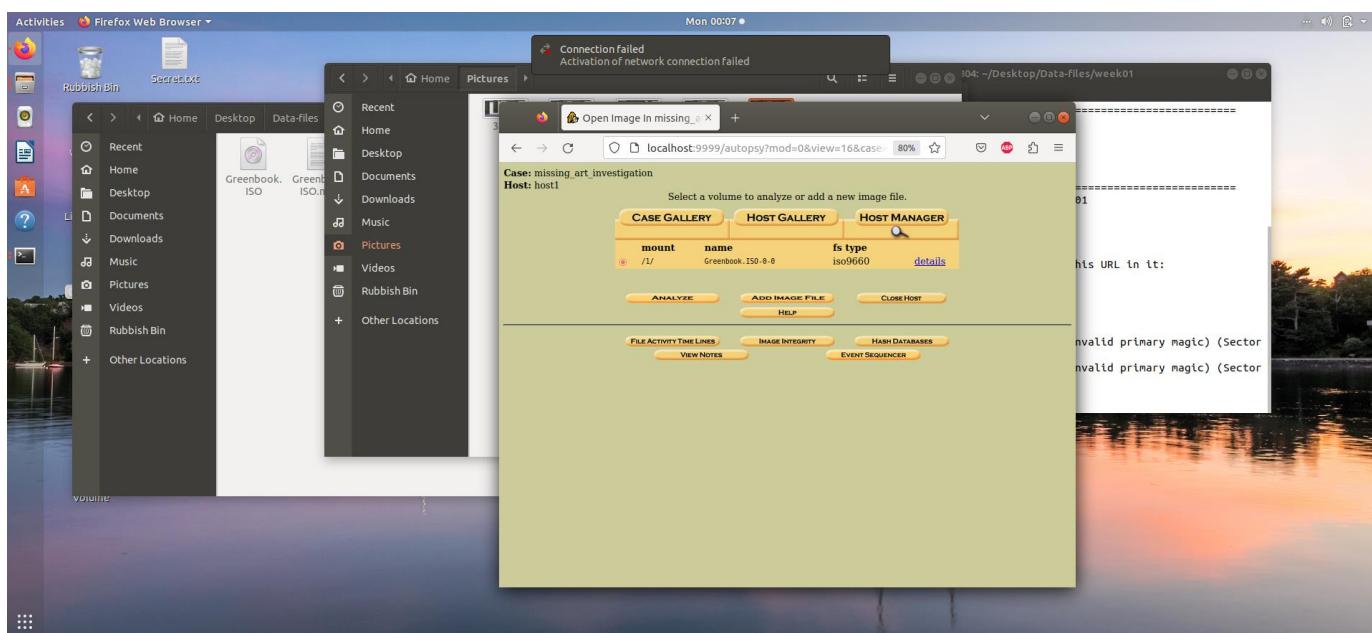
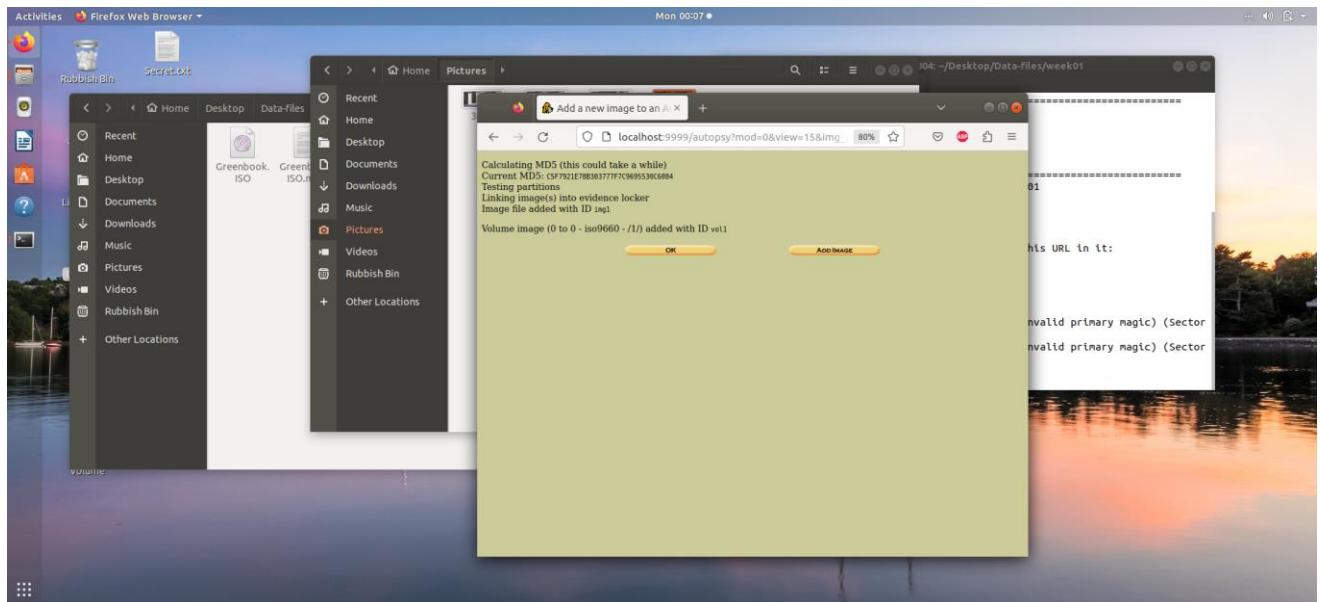
3. First, I entered the case details and opened a new case file for that



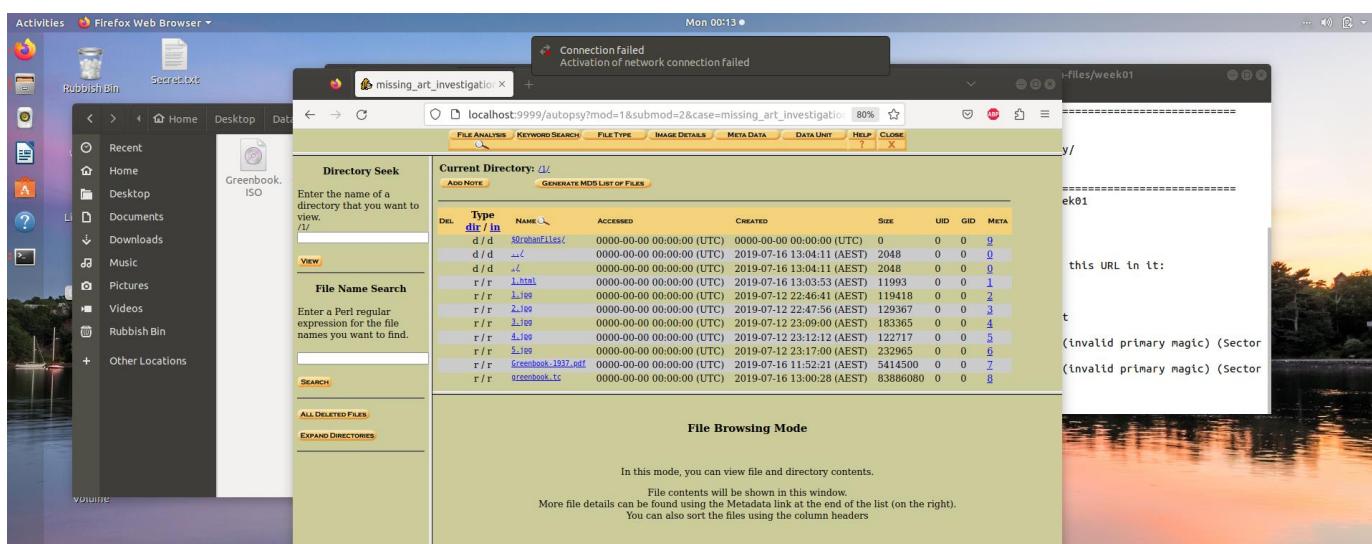


4. To verify the integrity of the file, I gave the md5hash value of the image to verify when the image is being verified by Autopsy.





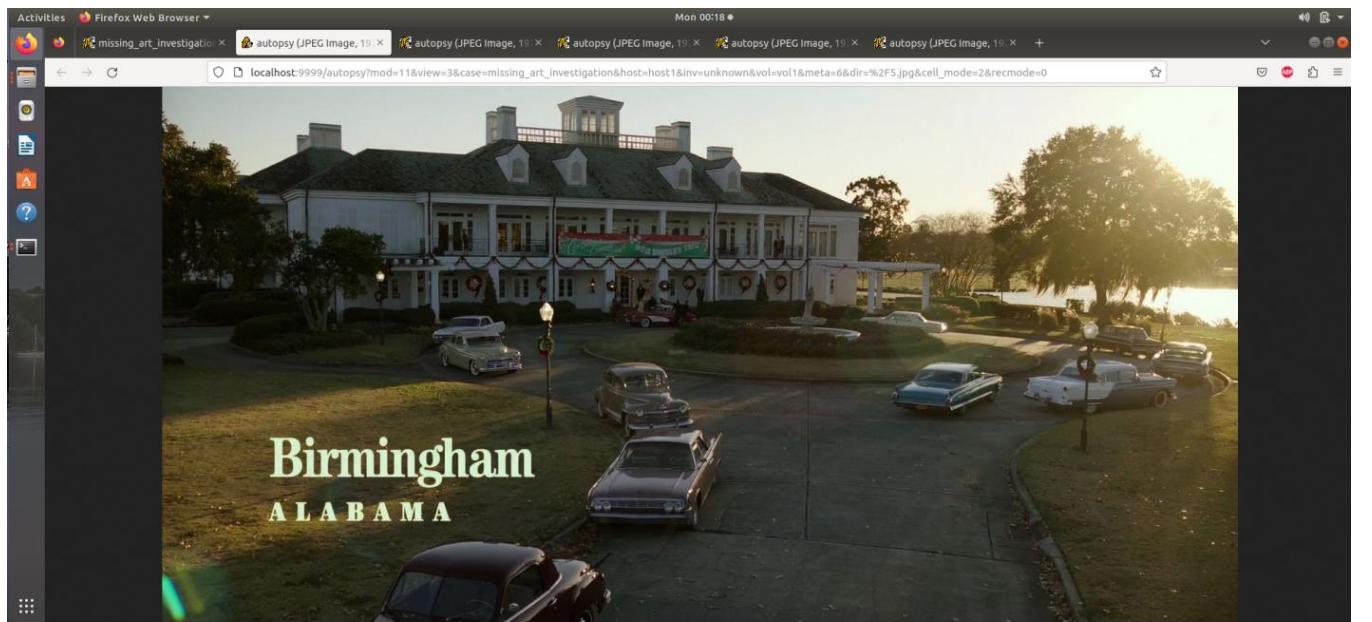
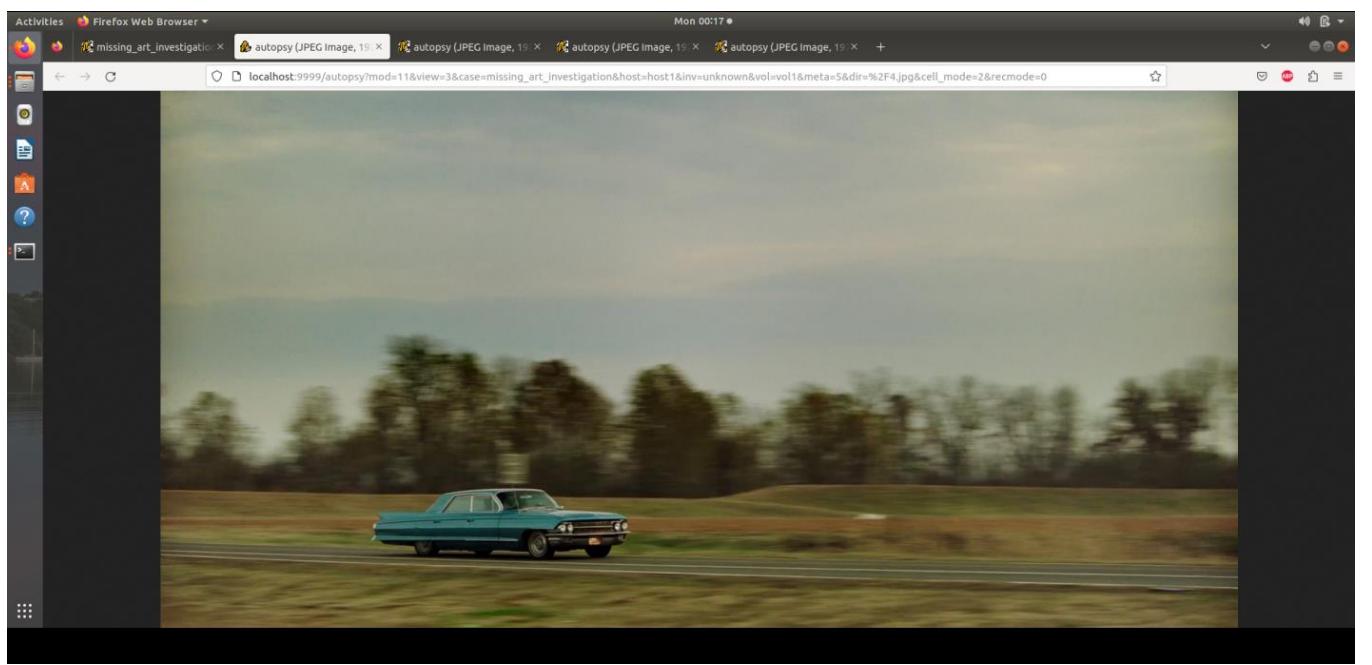
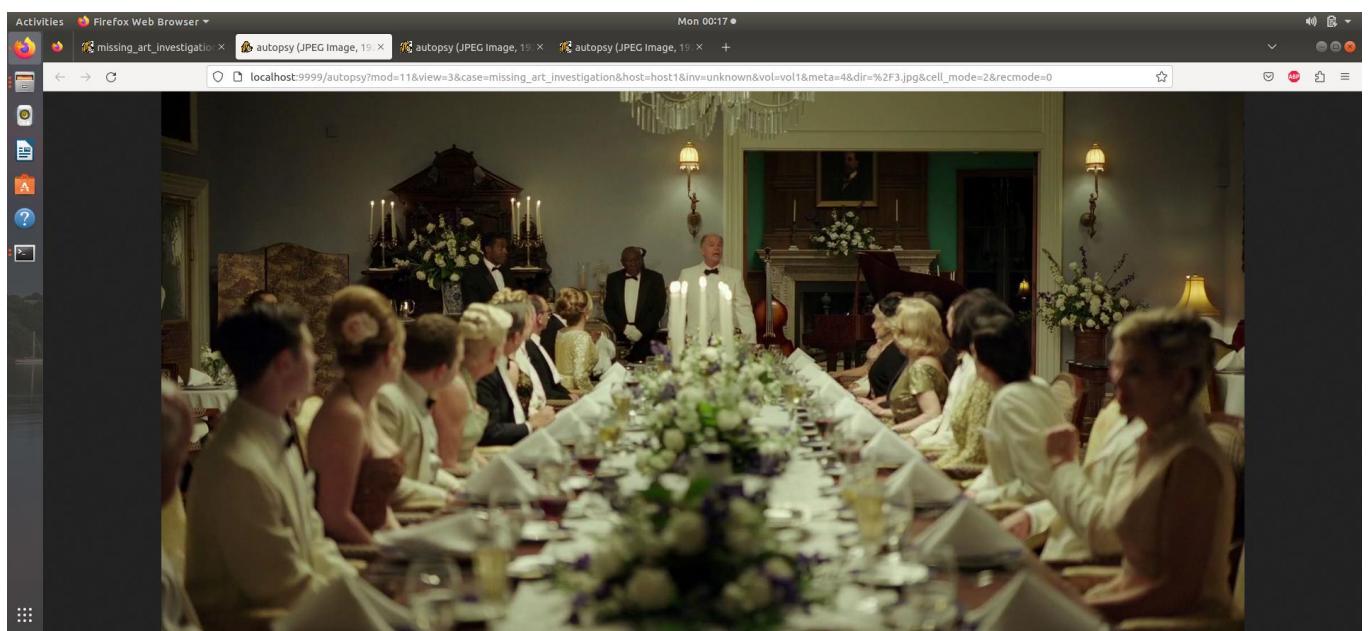
5. Now the case is ready to be analysed



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

A screenshot of a Firefox browser window. The title bar says "Activities" and "Firefox Web Browser". The address bar shows the URL "localhost:9999/autopsy?mod=11&view=3&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1&meta=2&dir=%2F1.jpg&cell_mode=2&reemode=0". The main content area is a movie still from "The Artist" (2011). It depicts George Valence (Jean Dujardin) singing into a vintage microphone. He is wearing a light-colored suit and a black bow tie. In the background, a band is performing on stage, including a drummer, a saxophone player, and another singer. The stage backdrop features stylized faces. The overall atmosphere is that of a 1920s-30s jazz club.

A close-up portrait of a Black man with short hair, looking directly at the camera. He is wearing a black turtleneck and a gold chain necklace with a large, ornate pendant. The background is blurred, suggesting an indoor setting with warm lighting.



7. Then I went through the general file systems

General File System Details

Mon 00:50 •

Activities Firefox Web Browser missing_art_investigation +

localhost:9999/autopsy?mod=1&submod=7&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

General File System Details

==== PRIMARY VOLUME DESCRIPTOR 1 ====
FILE SYSTEM INFORMATION
File System Type: ISO9660
Volume Name: ISO Label
Volume Set Size: 1
Volume Set Sequence: 1
Publisher:
Data Preparer:
Recording Application: MKISOF5 ISO9660/HFS/UDF FILESYSTEM BUILDER & CDRECORD CD/DVD/BluRay CREATOR (C) 1993 E.YOUNGDALE (C) 1997 J.PEARSON/J.SCHILLING
Copyright:

METADATA INFORMATION
Path Table Location: 22-22
Inode Range: 0 - 9
Root Directory Block: 28

CONTENT INFORMATION
Sector Size: 2048
Block Size: 2048
Total Sector Range: 0 - 44177
Total Block Range: 0 - 44177

==== SUPPLEMENTARY VOLUME DESCRIPTOR 1 ====
FILE SYSTEM INFORMATION
File System Type: ISO9660
Volume Name:
Volume Set Size: 1
Volume Set Sequence: 1
Publisher:
Data Preparer:
Recording Application:
Copyright:

General File System Details

Mon 00:50 •

Activities Firefox Web Browser missing_art_investigation +

localhost:9999/autopsy?mod=1&submod=7&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

General File System Details

==== PRIMARY VOLUME DESCRIPTOR 1 ====
FILE SYSTEM INFORMATION
File System Type: ISO9660
Volume Name:
Volume Set Size: 1
Volume Set Sequence: 1
Publisher:
Data Preparer:
Recording Application:
Copyright:

METADATA INFORMATION
Path Table Location: 22-22
Inode Range: 0 - 9
Root Directory Block: 28

CONTENT INFORMATION
Sector Size: 2048
Block Size: 2048
Total Sector Range: 0 - 44177
Total Block Range: 0 - 44177

==== SUPPLEMENTARY VOLUME DESCRIPTOR 1 ====
FILE SYSTEM INFORMATION
File System Type: ISO9660
Volume Name:
Volume Set Size: 1
Volume Set Sequence: 1
Publisher:
Data Preparer:
Recording Application:
Copyright:

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

Activities Firefox Web Browser missing_art_investigation +

localhost:9999/autopsy?mod=1&submod=2&case=missing_art_investigation&host=host1&inv=unknown&vol=vol1

FILE ANALYSIS KEYWORD SEARCH FILE TYPE IMAGE DETAILS META DATA DATA UNIT HELP CLOSE

All Deleted Files

Mon 00:51 •

Enter the name of a directory that you want to view.
/L

Type
dir / in

NAME ACCESSED CREATED SIZE UID GID META

None

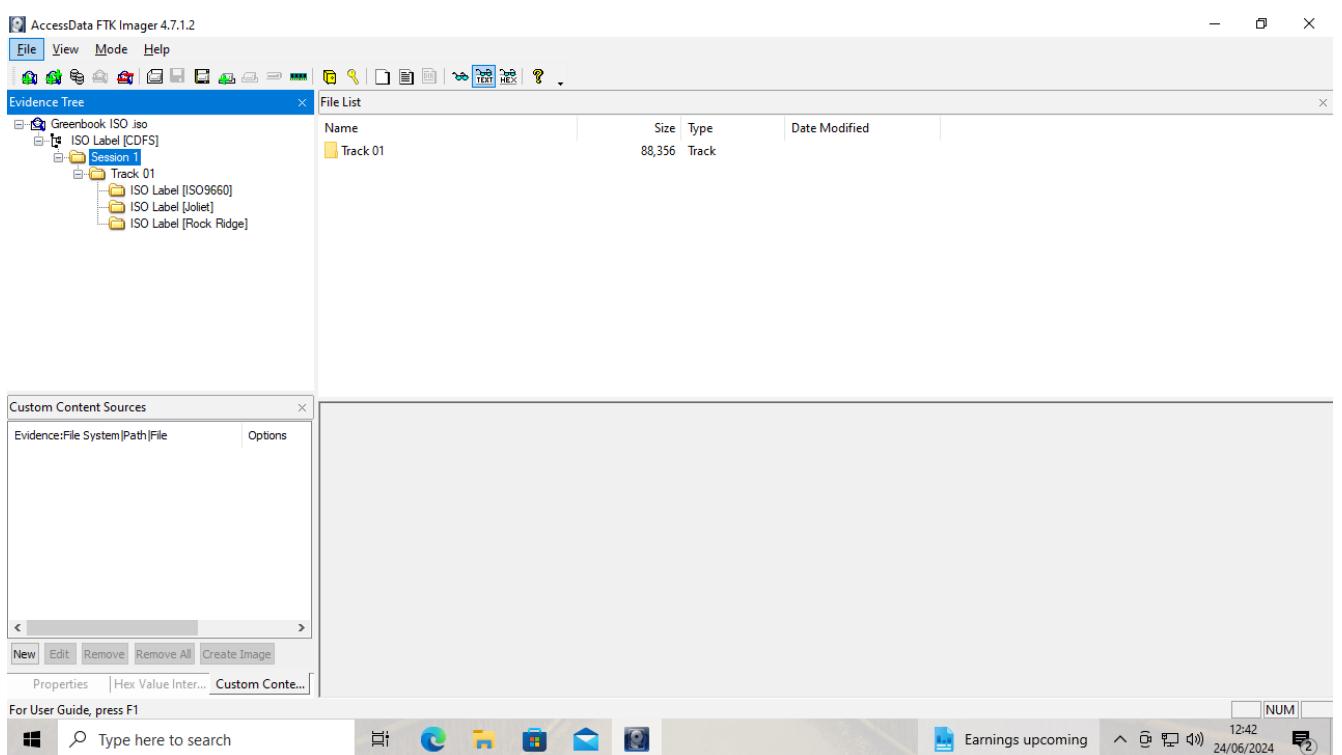
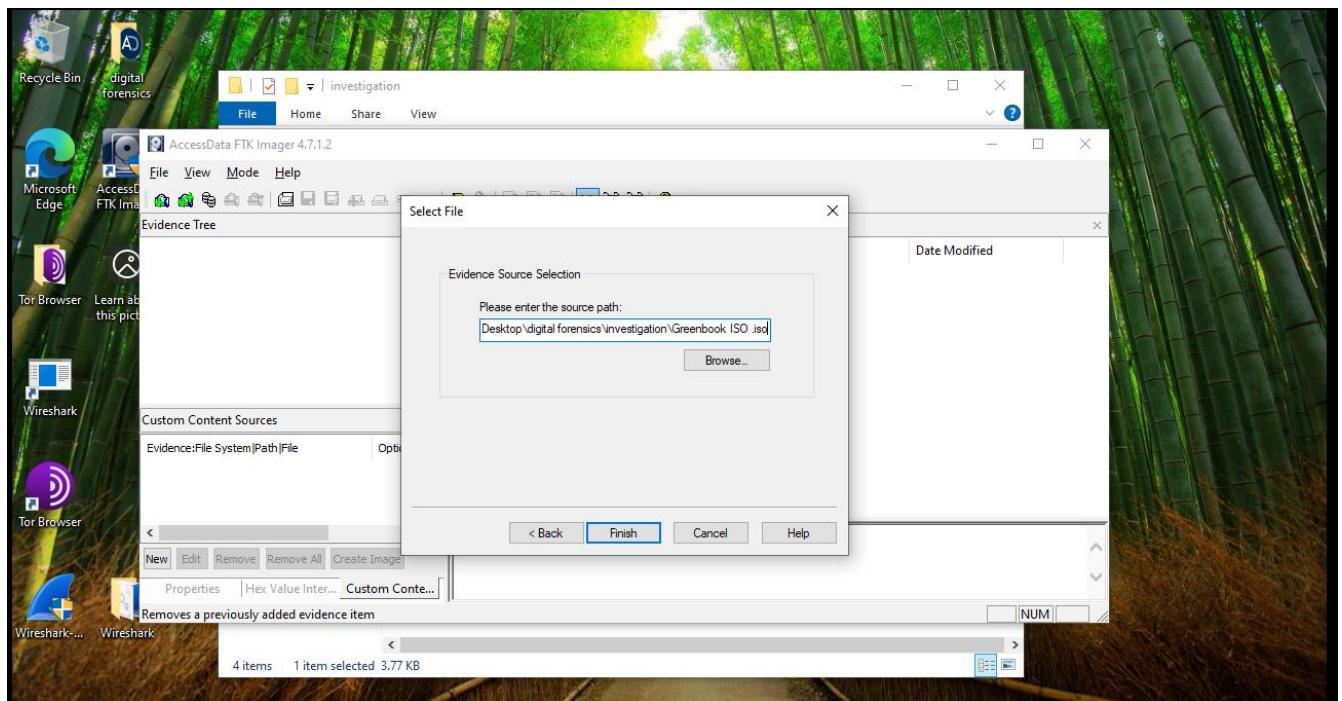
File Name Search
Enter a Perl regular expression for the file names you want to find.
SEARCH

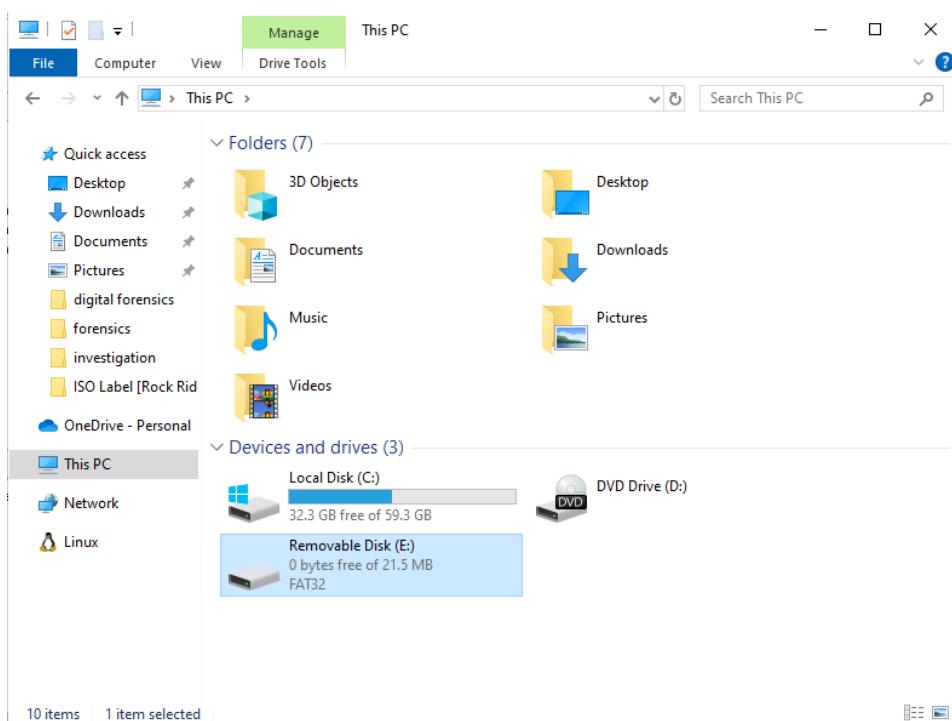
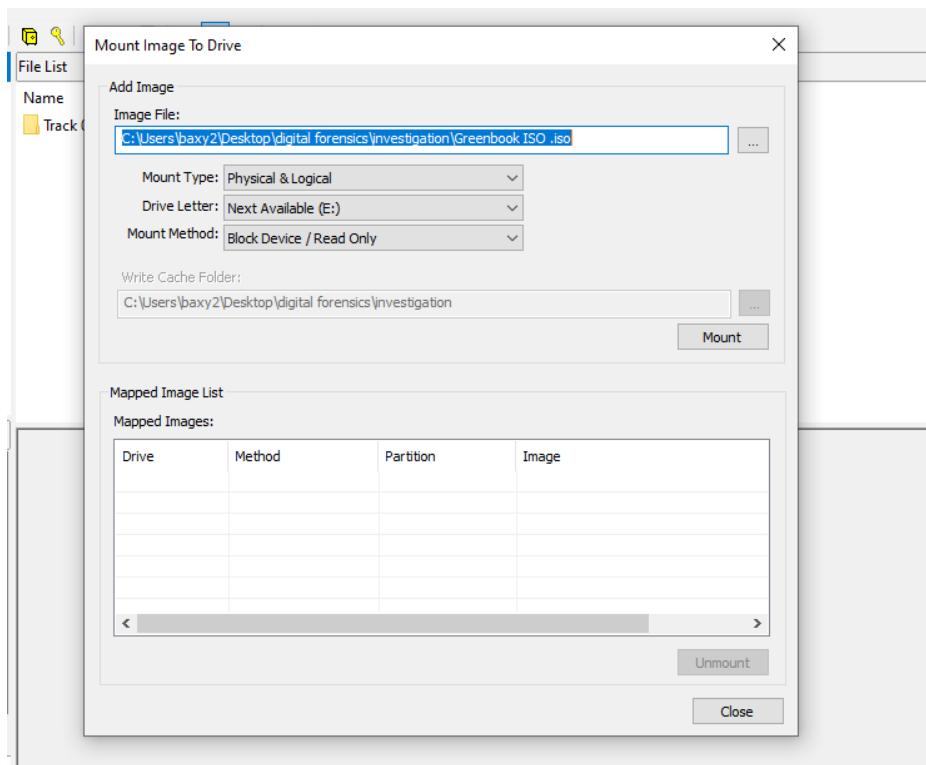
ALL DELETED FILES EXPAND DIRECTORIES

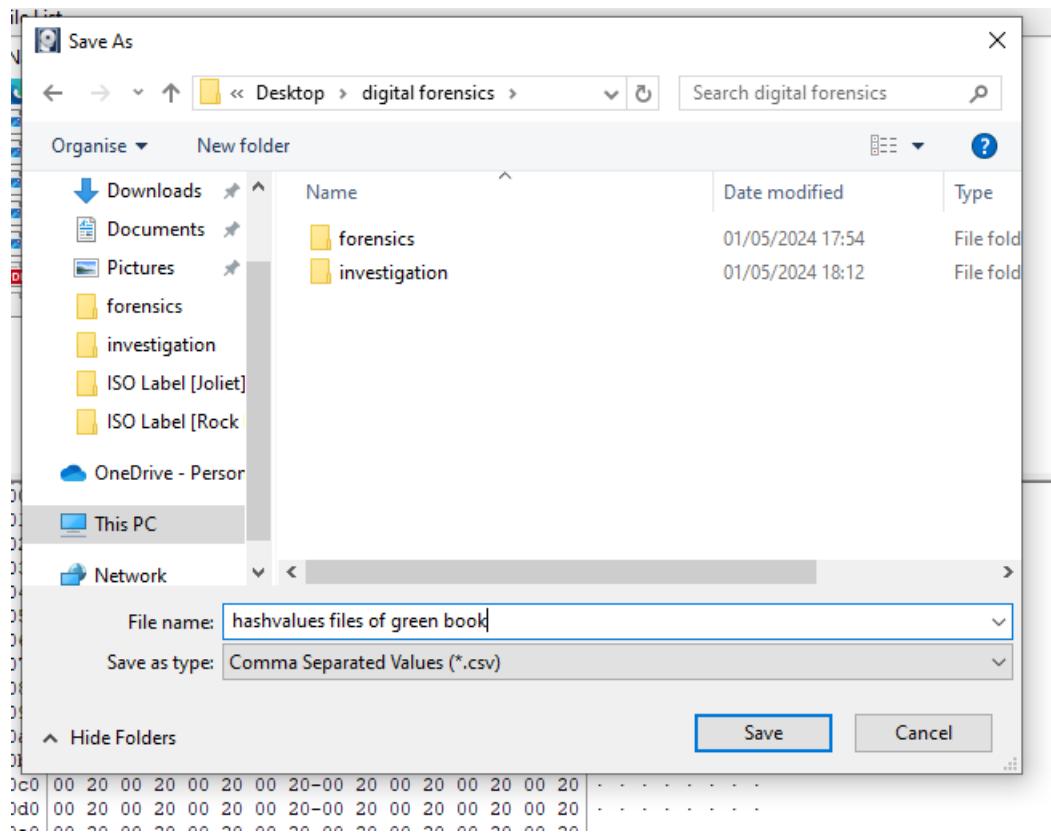
File Browsing Mode

In this mode, you can view file and directory contents.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers.

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.







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

MD5	SHA1	FileNames
2a9d47cd337565ecbc4556b85d675b2		2088912a1ce7ea54d2fd4540d0ba1fd7d748b1c47
1831b1f5e0e5a22a1f9d5cab2099fb1b		133b871f9fbfe164ac4c3ef66f722c67627606eb
aefef080a292374a866de59a9bd55712f		d95551b859539e961e55db75d57505b1084ae3d
d3060c3925e2f21274c5d04ce465ef08		51e50e8e53dfa51c59a33637dd9f43f3a1b243c1
30c58285a32ac6ff2232fe09cf8a11dd		2f41da33c4a1716808faaa9a8f42a4843bf757f7
853bd591239b0225bbcce59ffd7da1bc6		0dbf190c43472e9703fc507e08be6447f3f5c8b4
39e0cc888b3d96fb07c411b4d52da1fa		51876d6af0f5134bc873b801bc06647159fdb2c8
1bcfb60df2629a35dabc4bcbfb1b2071		294e93d0348743c8ebfecc8173193e2d2f94a679
2a9d47cd337565ecbc4556b85d675b2		2088912a1ce54d2fd4540d0ba1fd748b1c47
1831b1f5e0e5a22a1f9d5cab2099fb1b		133b871f9fbfe164ac4c3ef66f722c67627606eb
aefef080a292374a866de59a9bd55712f		d95551b859539e961e55db75d57505b1084ae3d
d3060c3925e2f21274c5d04ce465ef08		51e50e8e53dfa51c59a33637dd9f43f3a1b243c1
30c58285a32ac6ff2232fe09cf8a11dd		2f41da33c4a1716808faaa9a8f42a4843bf757f7
853bd591239b0225bbcce59ffd7da1bc6		0dbf190c43472e9703fc507e08be6447f3f5c8b4
39e0cc888b3d96fb07c411b4d52da1fa		51876d6af0f5134bc873b801bc06647159fdb2c8
1bcfb60df2629a35dabc4bcbfb1b2071		294e93d0348743c8ebfecc8173193e2d2f94a679
2a9d47cd337565ecbc4556b85d675b2		2088912a1ce54d2fd4540d0ba1fd748b1c47
1831b1f5e0e5a22a1f9d5cab2099fb1b		133b871f9fbfe164ac4c3ef66f722c67627606eb
aefef080a292374a866de59a9bd55712f		d95551b859539e961e55db75d57505b1084ae3d
d3060c3925e2f21274c5d04ce465ef08		51e50e8e53dfa51c59a33637dd9f43f3a1b243c1
30c58285a32ac6ff2232fe09cf8a11dd		2f41da33c4a1716808faaa9a8f42a4843bf757f7
853bd591239b0225bbcce59ffd7da1bc6		0dbf190c43472e9703fc507e08be6447f3f5c8b4
1bcfb60df2629a35dabc4bcbfb1b2071		294e93d0348743c8ebfecc8173193e2d2f94a679
39e0cc888b3d96fb07c411b4d52da1fa		51876d6af0f5134bc873b801bc06647159fdb2c8

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.

The screenshot shows the AccessData FTK Imager interface. The top menu bar includes File, View, Mode, Help, and various tool icons. The Evidence Tree pane on the left shows a hierarchical structure of files from an ISO image named 'Greenbook ISO.iso'. The File List pane on the right displays detailed information for each file, including Name, Size, Type, and Date Modified. The bottom half of the screen features a large hex editor window titled 'Custom Content Sources' with tabs for Evidence, File System, Path, and File. It shows binary data in hex, ASCII, and Unicode formats. A status bar at the bottom provides file details like 'Sel start = 260, len = 6; log sec = 31' and a date/time stamp '24/06/2024 14:58'.

Evidence Tree

File List

Name	Size	Type	Date Modified
1.HTML	12	Regular File	16/07/2019 03:03:53
1.JPG	117	Regular File	12/07/2019 12:46:41
2.JPG	127	Regular File	12/07/2019 12:47:56
3.JPG	180	Regular File	12/07/2019 13:09:00
4.JPG	120	Regular File	12/07/2019 13:12:12
5.JPG	228	Regular File	12/07/2019 13:17:00
GREENBOOK.TC	81,920	Regular File	16/07/2019 03:00:28
GREENBOOK_1937.PDF	5,288	Regular File	16/07/2019 01:52:21

Custom Content Sources

Evidence:File System|Path|File Options

Hex View

Properties | Hex Value Inter... | Custom Conte... | Sel start = 260, len = 6; log sec = 31

Listed: 8 Selected: 1 Greenbook ISO.iso/ISO Label [CDFS]/Session 1/Track 01/ISO Label [ISO9660]/1.HTML

32°C Mostly sunny

14:58

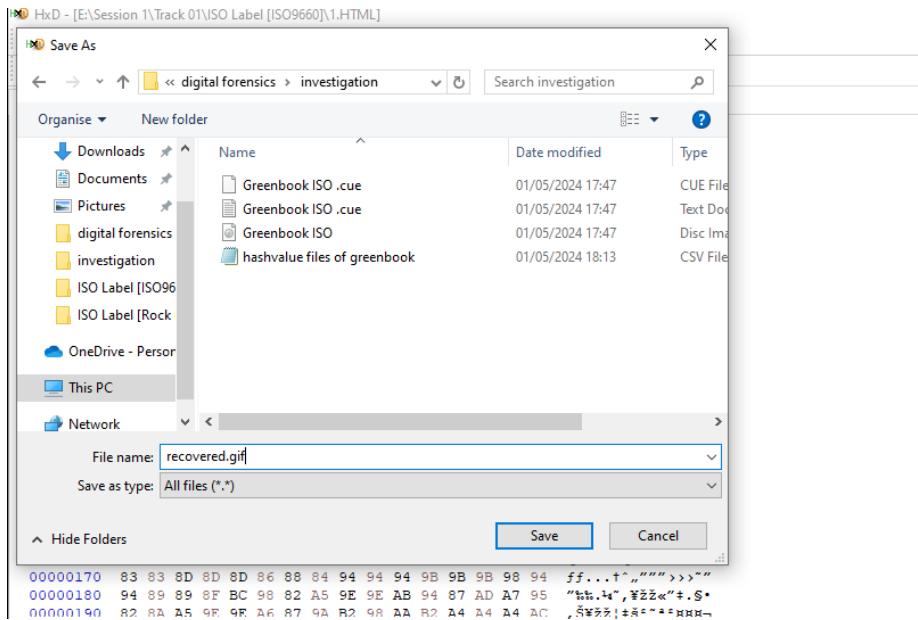
24/06/2024

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.

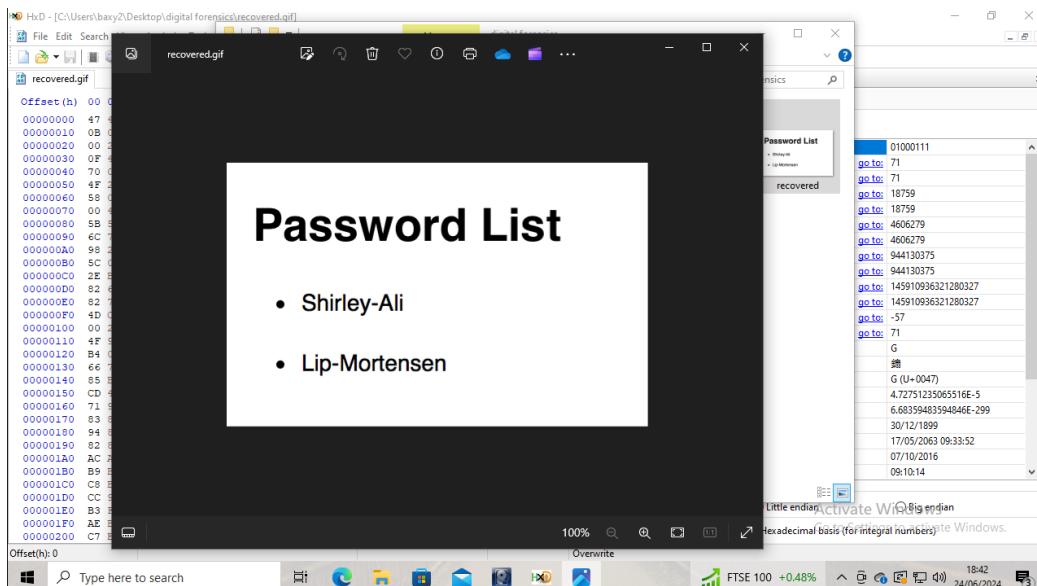
The screenshot shows the HxD Hex Editor interface with the following details:

- Title Bar:** HxD - [E:\Session 1\Track01\ISO Label [ISO9660].1.HTML]
- Menu Bar:** File, Edit, Search, View, Analysis, Tools, Window, Help
- Toolbar:** Includes icons for Open, Save, Find, Replace, Copy, Paste, and various analysis tools.
- Address Bar:** Offset(h): 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
- Text View:** Decoded text pane showing the ISO Label content.
- Special Editors:** Data inspector pane with a table of memory dump details.

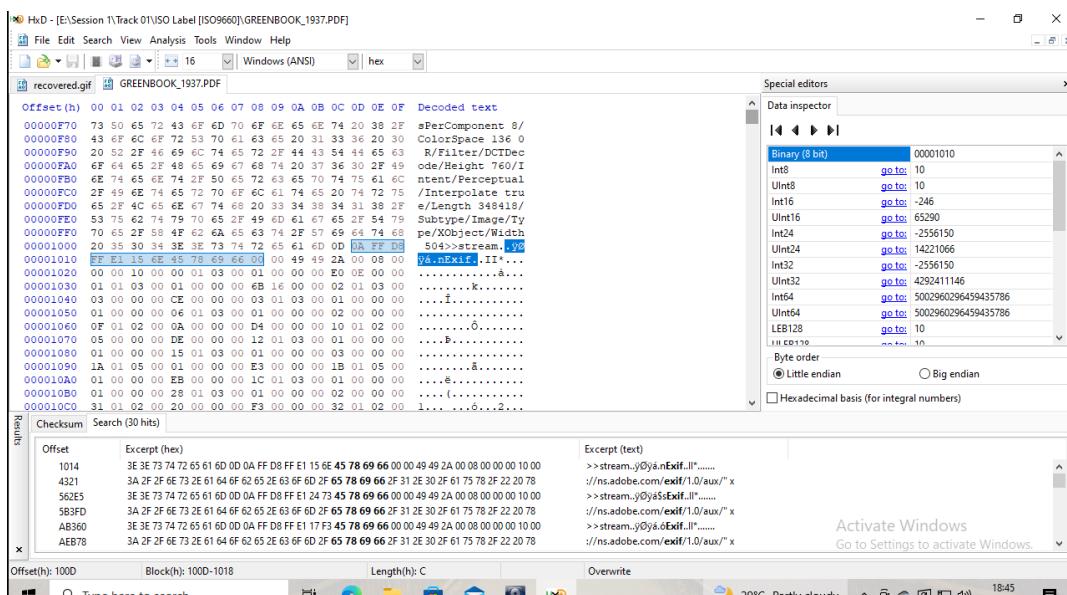
Binary (8 bit)	01000111
Int8	go to: 71
UInt8	go to: 71
Int16	go to: 18759
UInt16	go to: 18759
Int24	go to: 4606279
UInt24	go to: 4606279
Int32	go to: 944130375
UInt32	go to: 944130375
Int64	go to: 145910936321280327
UInt64	go to: 145910936321280327
LEB128	go to: -57
ULEB128	go to: 71
AnsiChar / char8_t	G
WideChar / char16_t	鑄
UTF-8 code point	G (U+0047)
Single (float32)	4.72751235065516E-5
Double (float64)	6.68359483594846E-299
OLETIME	30/12/1899
FILETIME	17/05/2063 09:33:52
DOS date	07/10/2016
DOS time	09:10:14



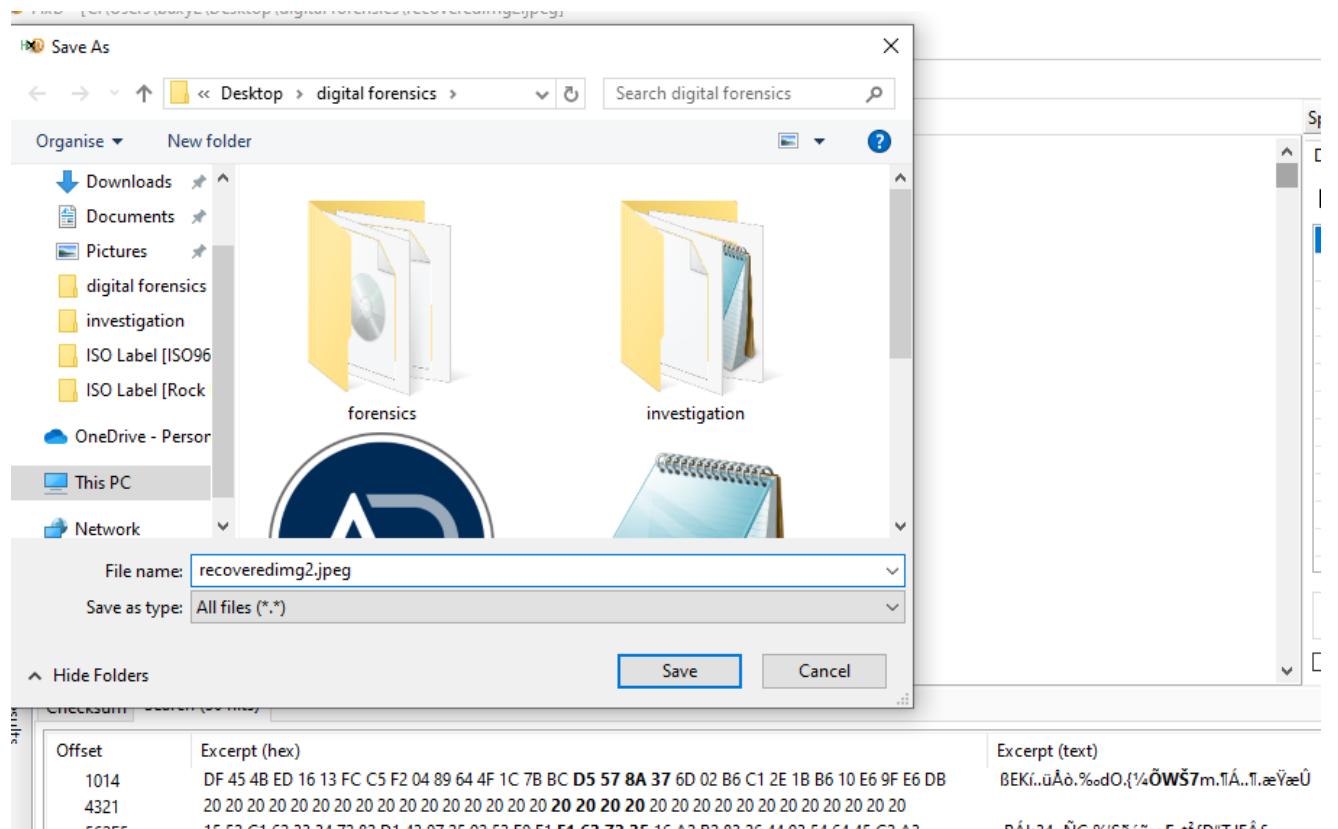
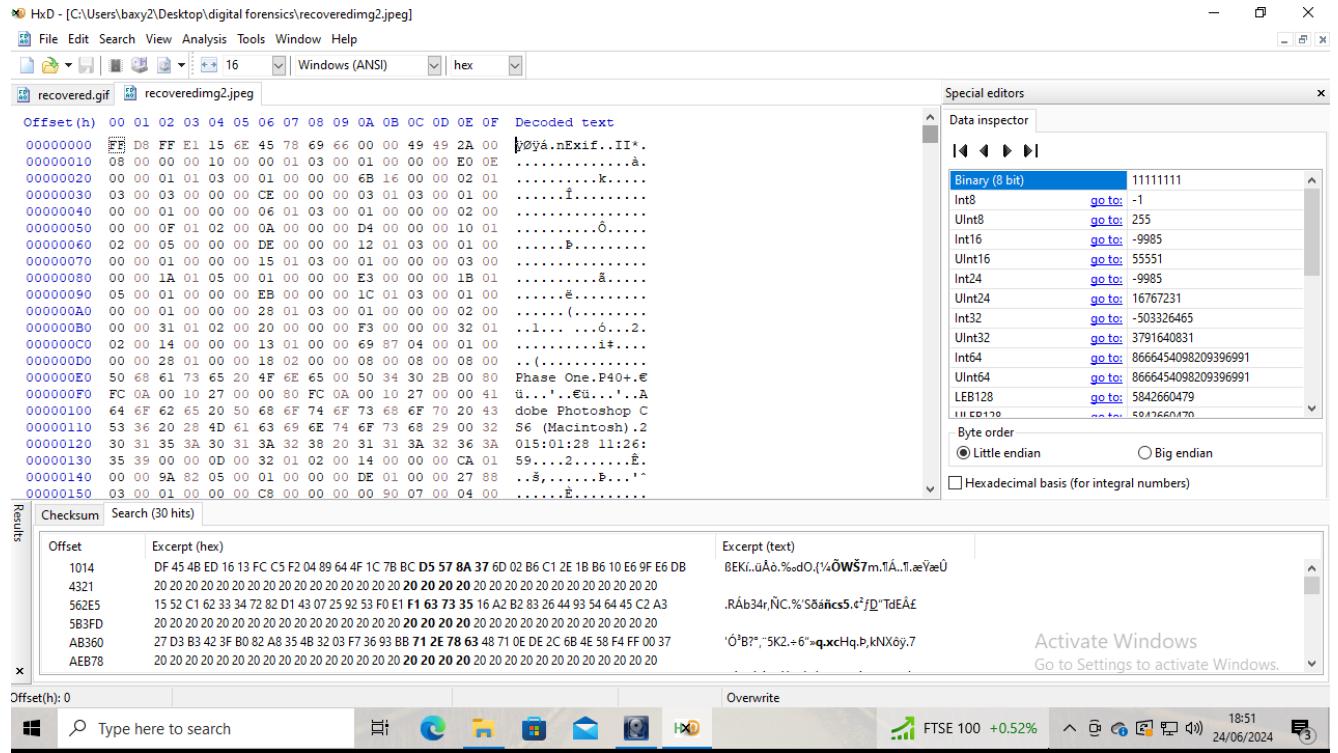
The recovered gif file contained a list of passwords. So, I investigated into other files much further to find out why these passwords are given.



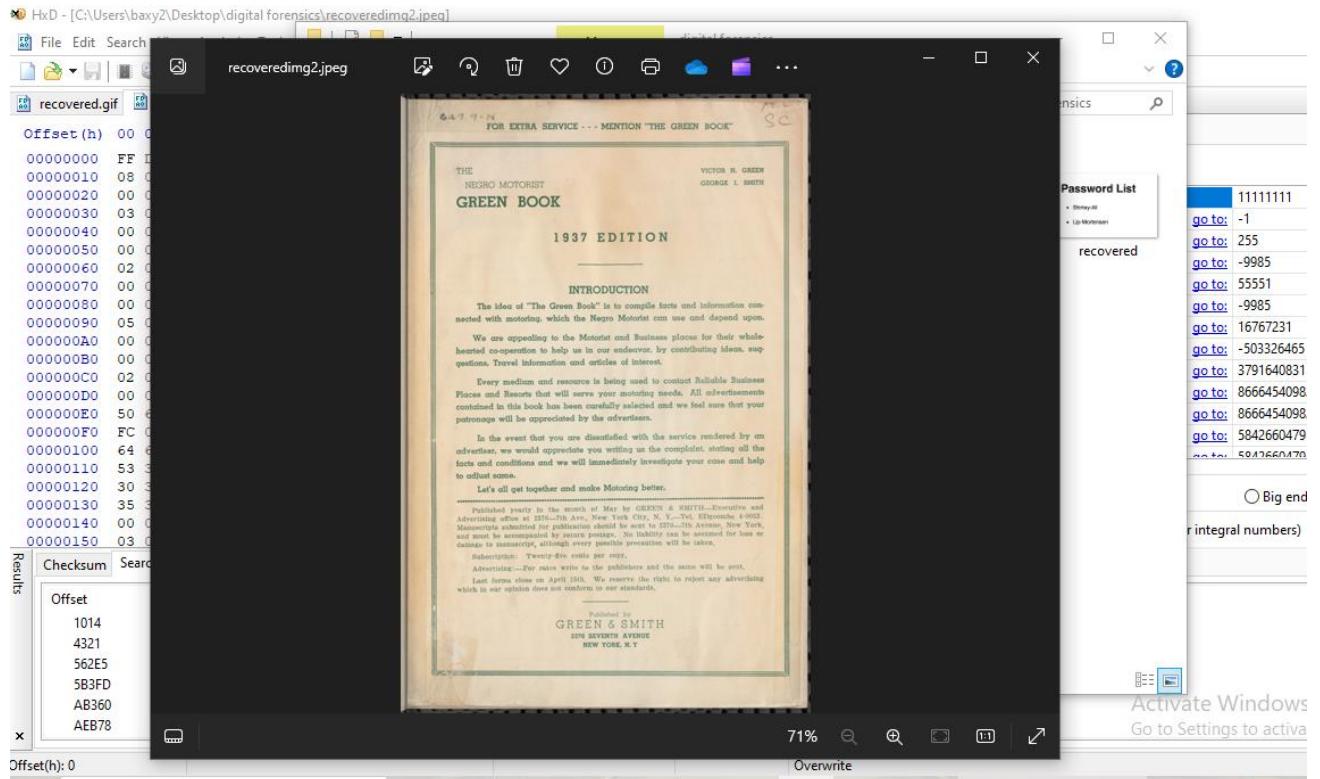
Then there was a PDF file, Greenbook.pdf, I opened it with the hex editor



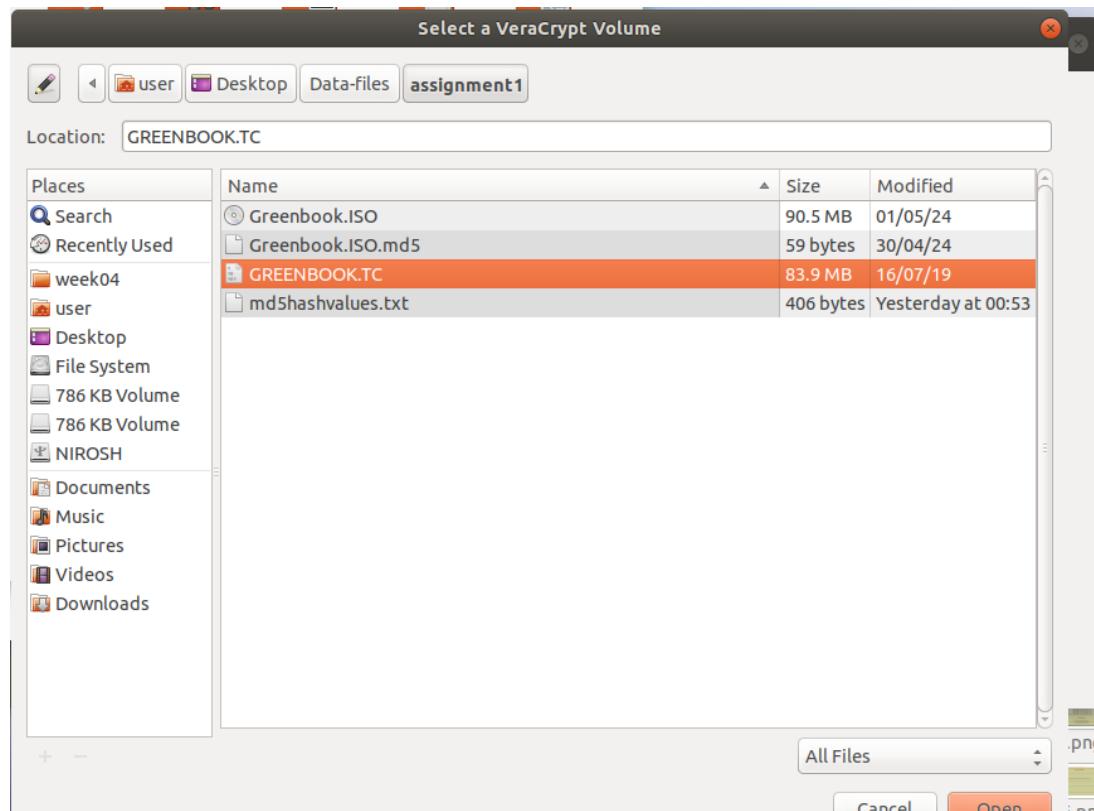
I found that there is an exif file hidden in this as well. So, to recover the exif file, I deleted the hex values above the 0A FF D8 to make the header a Exif file header. Then I saved the file as recovered2.jpeg.



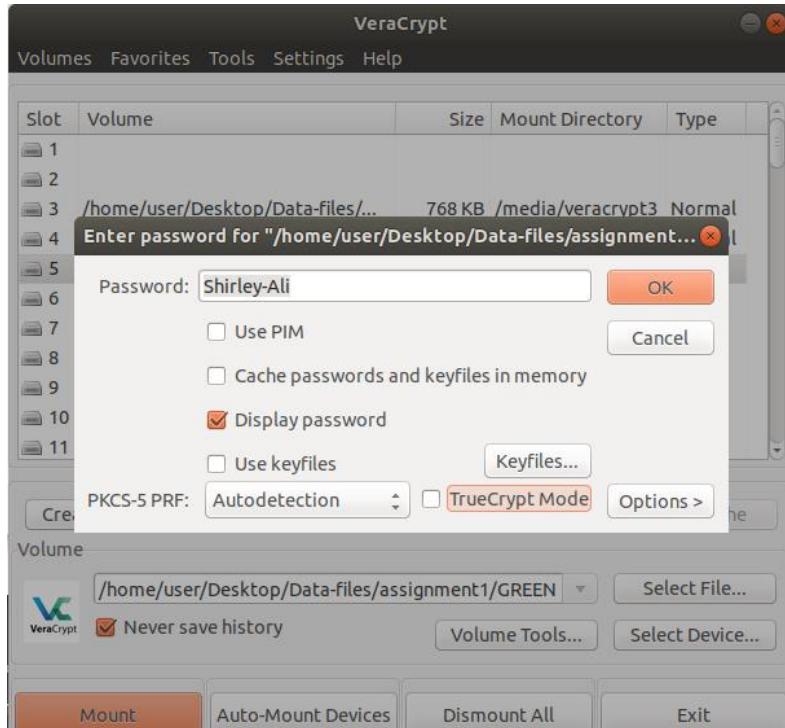
The recovered image shows about an introduction page to a book called GREEN BOOK



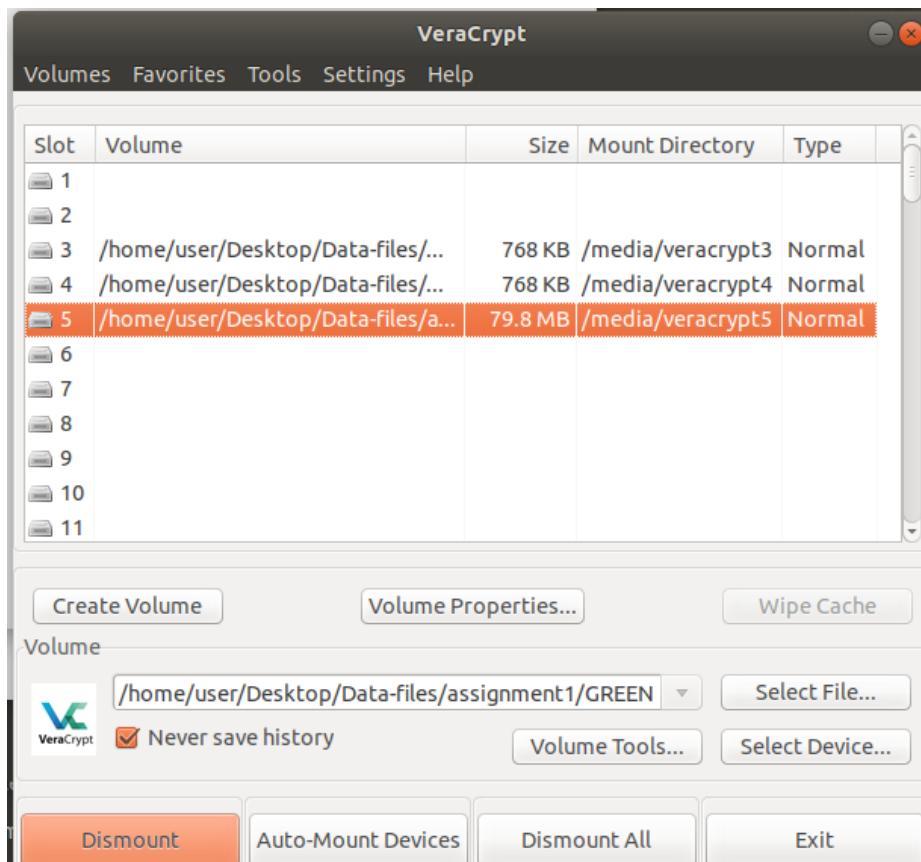
Now let's move on to GREENBOOK.tc file. This is a TrueCrypt file and it is encrypted. So, inorder to decrypt it, I'm using VeraCrypt to do that.



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.



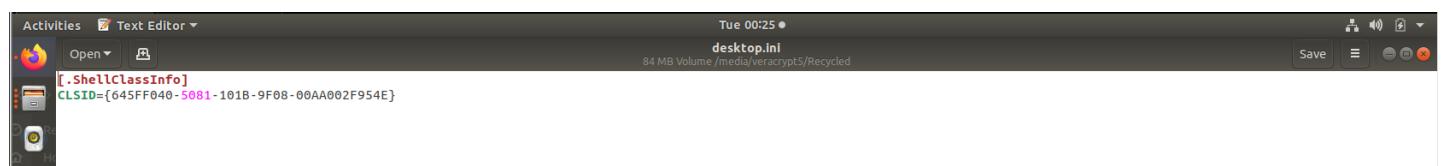
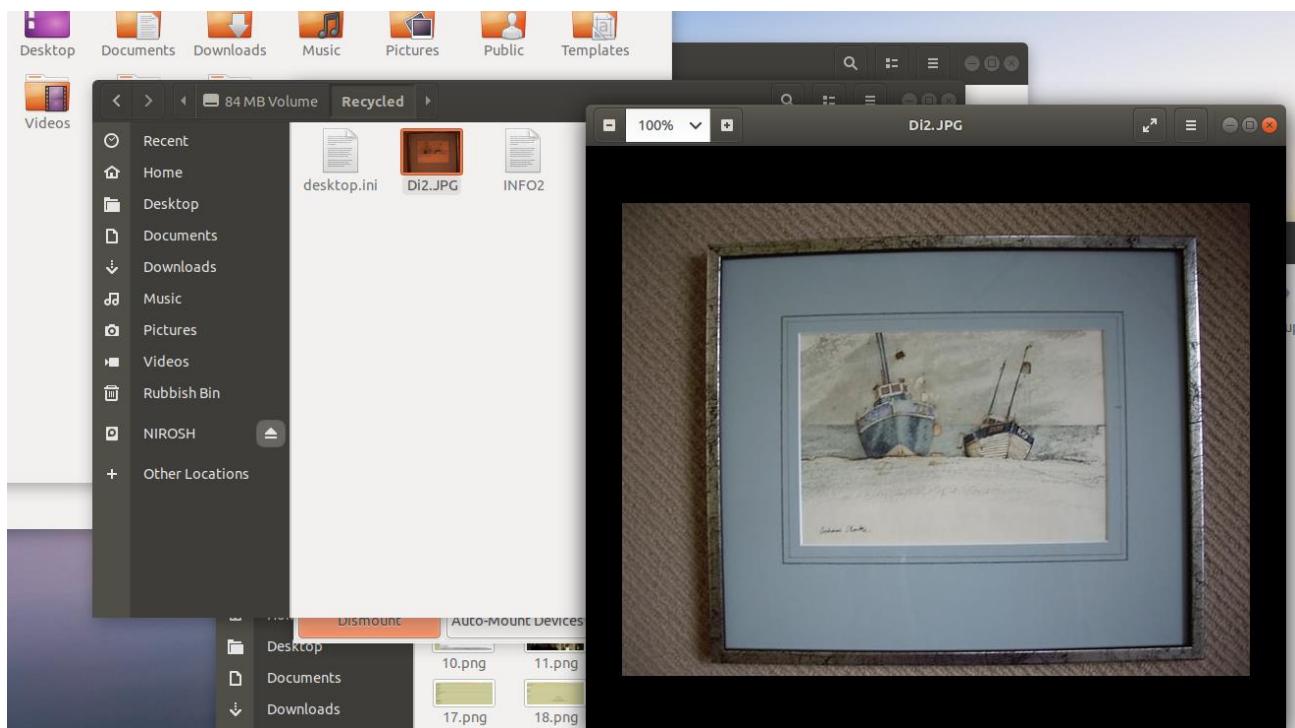
Then the password was correct and it got mounted and the decrypted files were recovered



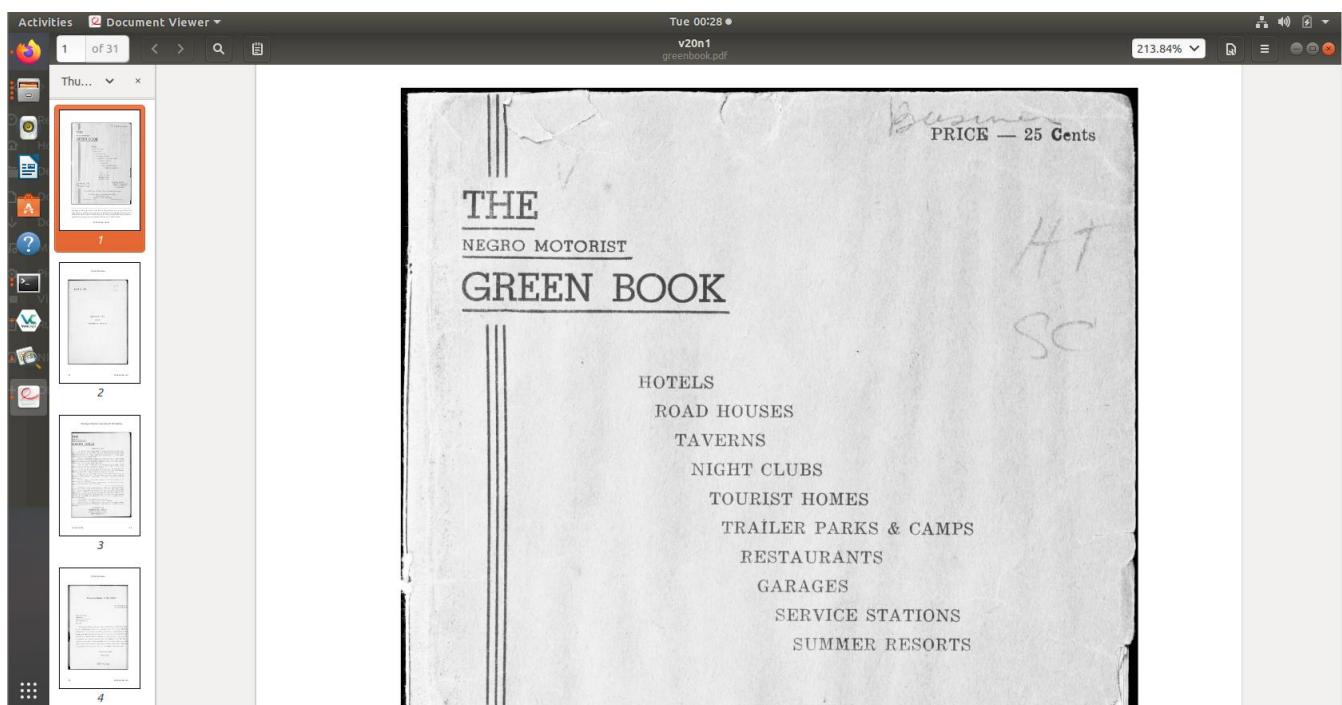
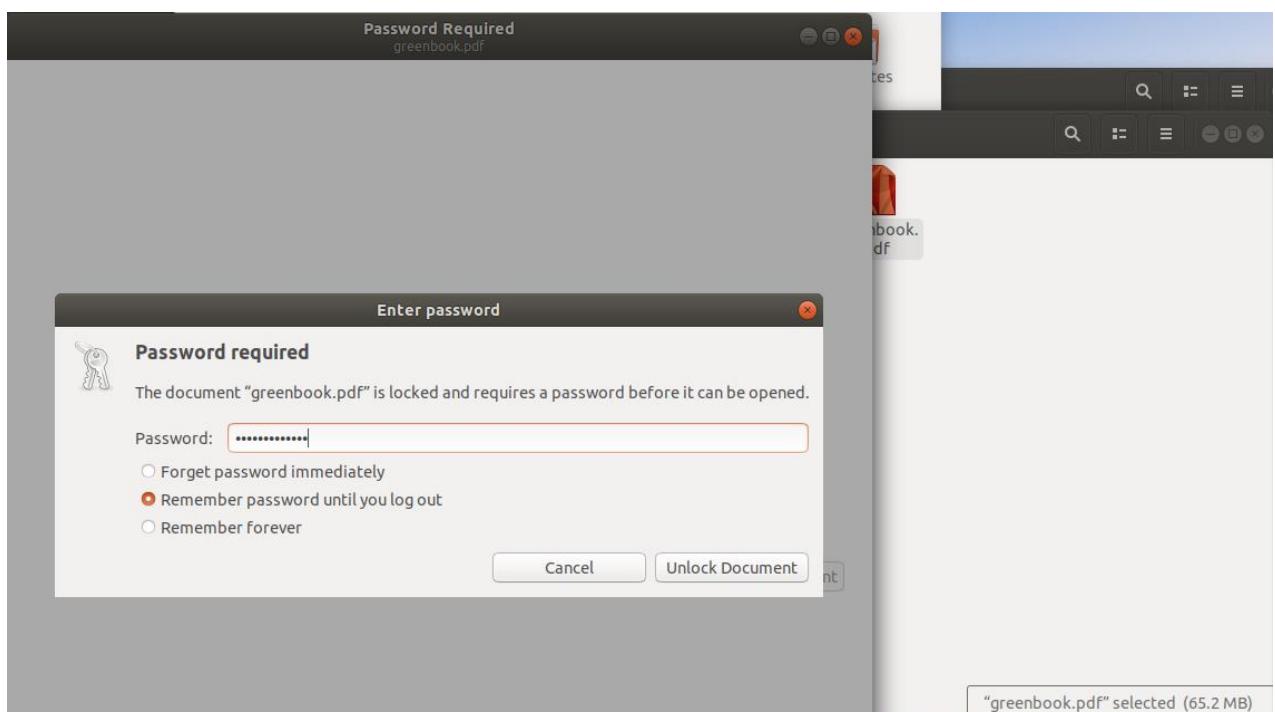


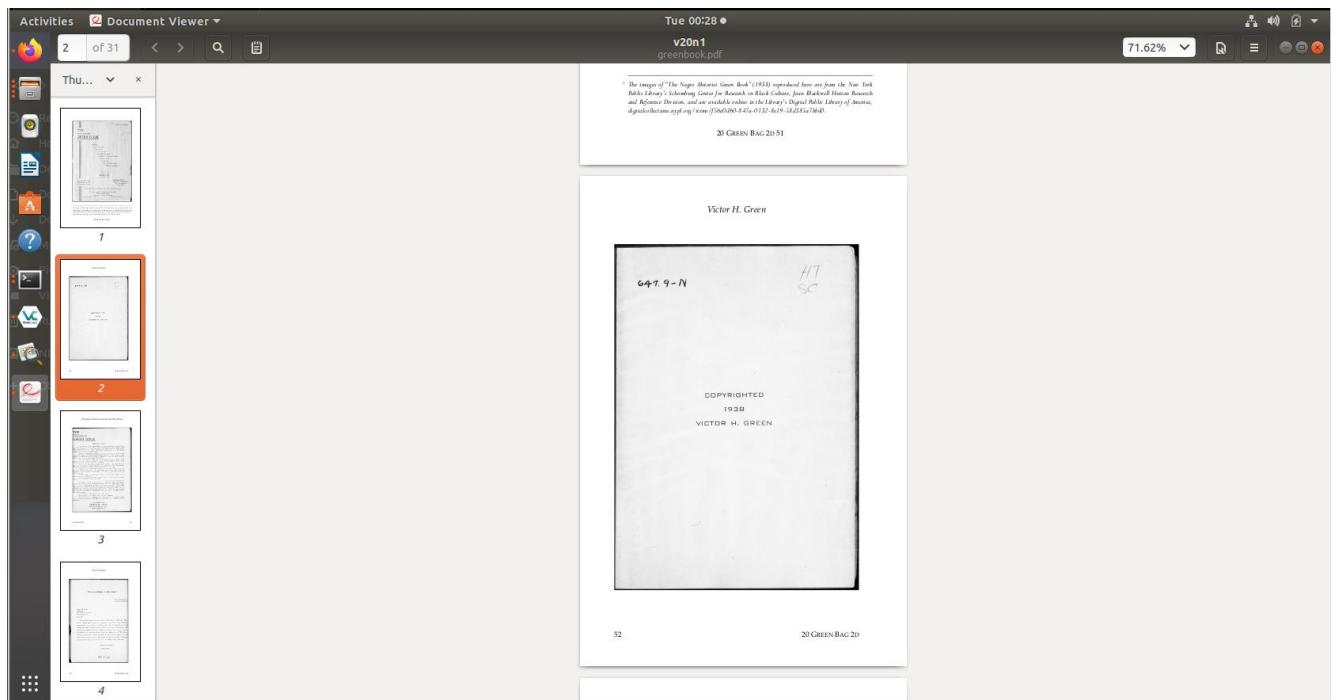
Then I went through the file, there in the Recycled folder I got the deleted items. Finally, there were 2 other pdfs, greenbook.pdf and credit.pdf.

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

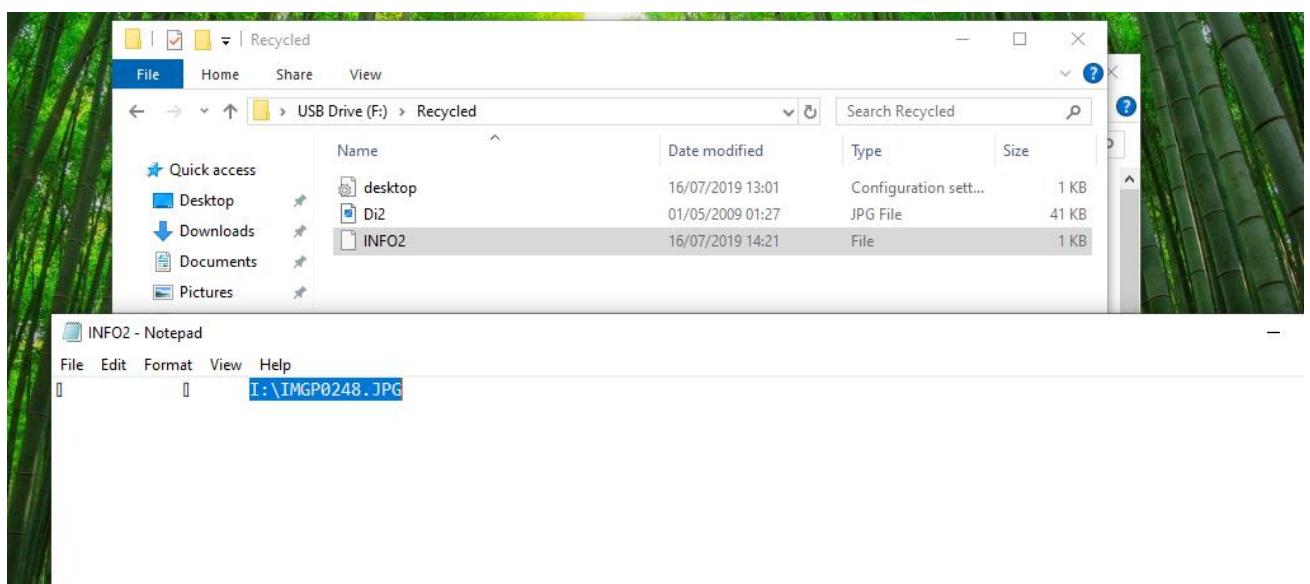


Now I tried access the Greenbook.pdf. Once I tried to do it, it asked for the password. I used the second password that was in the password list that I recovered earlier. The password was Lip-Mortensen. Then the pdf was about the Green Book.

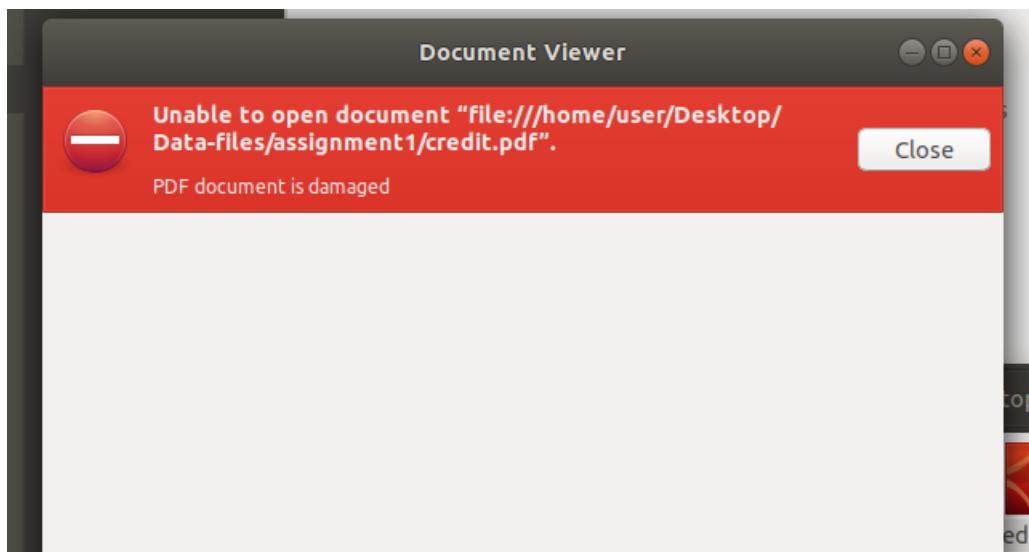




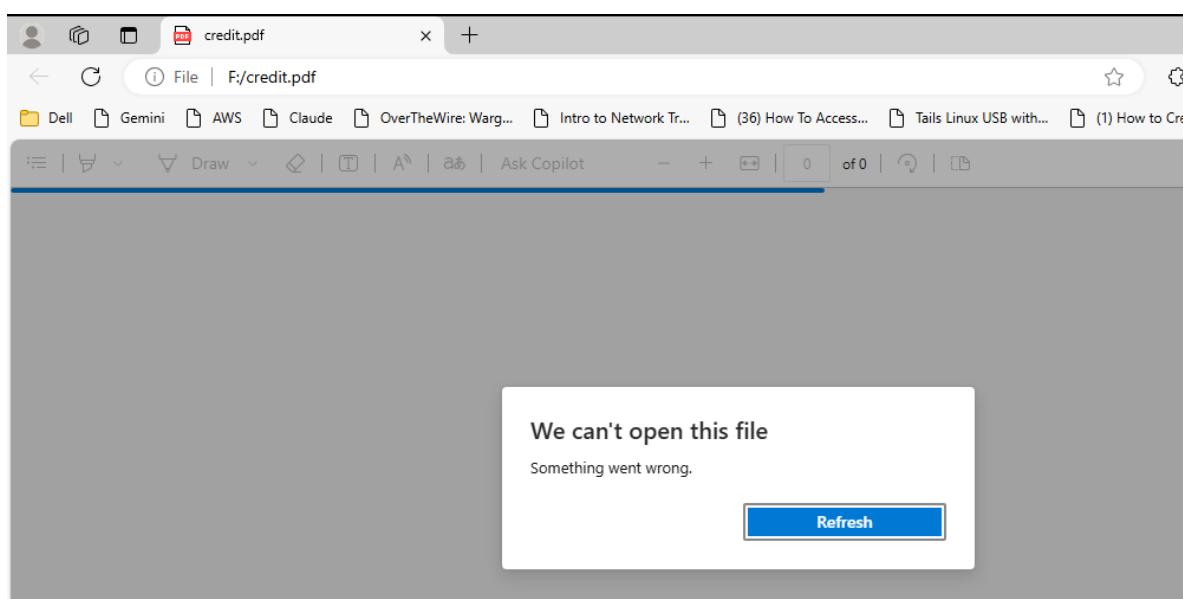
The INFO2 file contained a name of a jpeg file.



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.

Offset(h)	Decoded text
00 00 00 00	%PDF-1.4IF.....
00 00 00 10	00 90 00 FF E1 00 80 45 78 69 66 00 00 4D 4D ..yá.Exif..MM
00 00 00 20	00 2A 00 00 08 00 05 01 12 00 03 00 00 00 01 .*.....J
00 00 00 30	00 01 00 00 01 1A 00 05 00 00 01 00 00 00 4AR(..
00 00 00 40	01 1B 00 05 00 00 00 01 00 00 00 52 01 28 00 03+i.....
00 00 00 50	00 00 01 00 02 00 00 87 69 00 04 00 00 00 01Z.....
00 00 00 60	00 00 00 5A 00 00 00 00 00 00 90 00 00 00 00 01t
00 00 00 70	00 00 00 90 00 00 00 01 00 02 A0 02 00 04 00 00t
00 00 00 80	00 01 00 00 04 74 A0 03 00 04 00 00 00 01 00 00t
00 00 00 90	00 22 00 00 00 00 FF E1 09 21 68 74 74 70 3A 2F ."....yá.!http:/
00 00 00 A0	02 6E 73 2E 61 64 6F 62 65 2E 63 6F 6D 2F 78 61 /ns.adobe.com/xadef
00 00 00 B0	70 2F 31 2E 30 2F 00 3C 3F 78 70 61 63 6B 65 74 p/1.0.<?xpacket
00 00 00 C0	20 62 65 67 69 6E 3D 22 EF BB BF 22 20 69 64 3D begin="i>" id=
00 00 00 D0	22 57 35 4D 30 43 65 68 69 48 7A 72 65 53 "W5MOMpCeh1HzreS
00 00 00 E0	7A 4E 54 63 7A 6B 63 39 64 22 3F 3E 20 3C 78 3A zNTczkc9d"?> <x:
00 00 00 F0	78 6D 70 6D 65 74 61 20 78 6D 6C 6E 73 3A 78 3D xmpmeta xmlns:x=
00 00 01 00	22 61 64 6F 62 65 3A 6E 73 3A 6D 65 74 61 2F 22 "adobe:ns:meta/"
00 00 01 10	20 78 3A 78 6D 70 74 6B 3D 22 58 4D 50 20 43 6F x:xmptk="XMP Co
00 00 01 20	72 65 20 35 2E 34 2E 30 22 3E 20 3C 72 64 66 3A re 5.4.0"> <rdf:
00 00 01 30	52 44 46 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68 RDF xmlns:rdf="h
00 00 01 40	74 74 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67 ttp://www.w3.org
00 00 01 50	2F 31 39 39 39 2F 30 32 2F 32 32 2D 72 64 66 2D /1999/02/22-rdf-

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.

Offset(h)	Decoded text
00 00 00 00	%PDF-1.4IF.....
00 00 00 10	00 90 FF D8 FF E1 00 80 45 78 69 66 00 00 4D 4D ..yá.Exif..MM
00 00 00 20	00 2A 00 00 08 00 05 01 12 00 03 00 00 00 01 .*.....J
00 00 00 30	00 01 00 00 01 1A 00 05 00 00 00 01 00 00 00 4AR(..
00 00 00 40	01 1B 00 05 00 00 00 01 00 00 00 52 01 28 00 03+i.....
00 00 00 50	00 00 00 01 00 02 00 00 87 69 00 04 00 00 00 01Z.....
00 00 00 60	00 00 00 5A 00 00 00 00 00 00 90 00 00 00 00 01t
00 00 00 70	00 00 00 90 00 00 00 01 00 02 A0 02 00 04 00 00t
00 00 00 80	00 01 00 00 04 74 A0 03 00 04 00 00 00 01 00 00t
00 00 00 90	00 22 00 00 00 00 FF E1 09 21 68 74 74 70 3A 2F ."....yá.!http:/
00 00 00 A0	02 6E 73 2E 61 64 6F 62 65 2E 63 6F 6D 2F 78 61 /ns.adobe.com/xadef
00 00 00 B0	70 2F 31 2E 30 2F 00 3C 3F 78 70 61 63 6B 65 74 p/1.0.<?xpacket
00 00 00 C0	20 62 65 67 69 6E 3D 22 EF BB BF 22 20 69 64 3D begin="i>" id=
00 00 00 D0	22 57 35 4D 30 43 65 68 69 48 7A 72 65 53 "W5MOMpCeh1HzreS
00 00 00 E0	7A 4E 54 63 7A 6B 63 39 64 22 3F 3E 20 3C 78 3A zNTczkc9d"?> <x:
00 00 00 F0	78 6D 70 6D 65 74 61 20 78 6D 6C 6E 73 3A 78 3D xmpmeta xmlns:x=
00 00 01 00	22 61 64 6F 62 65 3A 6E 73 3A 6D 65 74 61 2F 22 "adobe:ns:meta/"
00 00 01 20	20 78 3A 78 6D 70 74 6B 3D 22 58 4D 50 20 43 6F x:xmptk="XMP Co
00 00 01 30	72 65 20 35 2E 34 2E 30 22 3E 20 3C 72 64 66 3A re 5.4.0"> <rdf:
00 00 01 40	52 44 46 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68 RDF xmlns:rdf="h
00 00 01 50	74 74 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67 ttp://www.w3.org
00 00 01 60	2F 31 39 39 39 2F 30 32 2F 32 32 2D 72 64 66 2D /1999/02/22-rdf-

HxD - [C:\Users\baxy2\Desktop\digital forensics\investigation\credit.pdf]

File Edit Search View Analysis Tools Window Help

Recovered files: recovered.gif, recoveredimg2.jpeg, GREENBOOK.TC, credit.html, credit.pdf

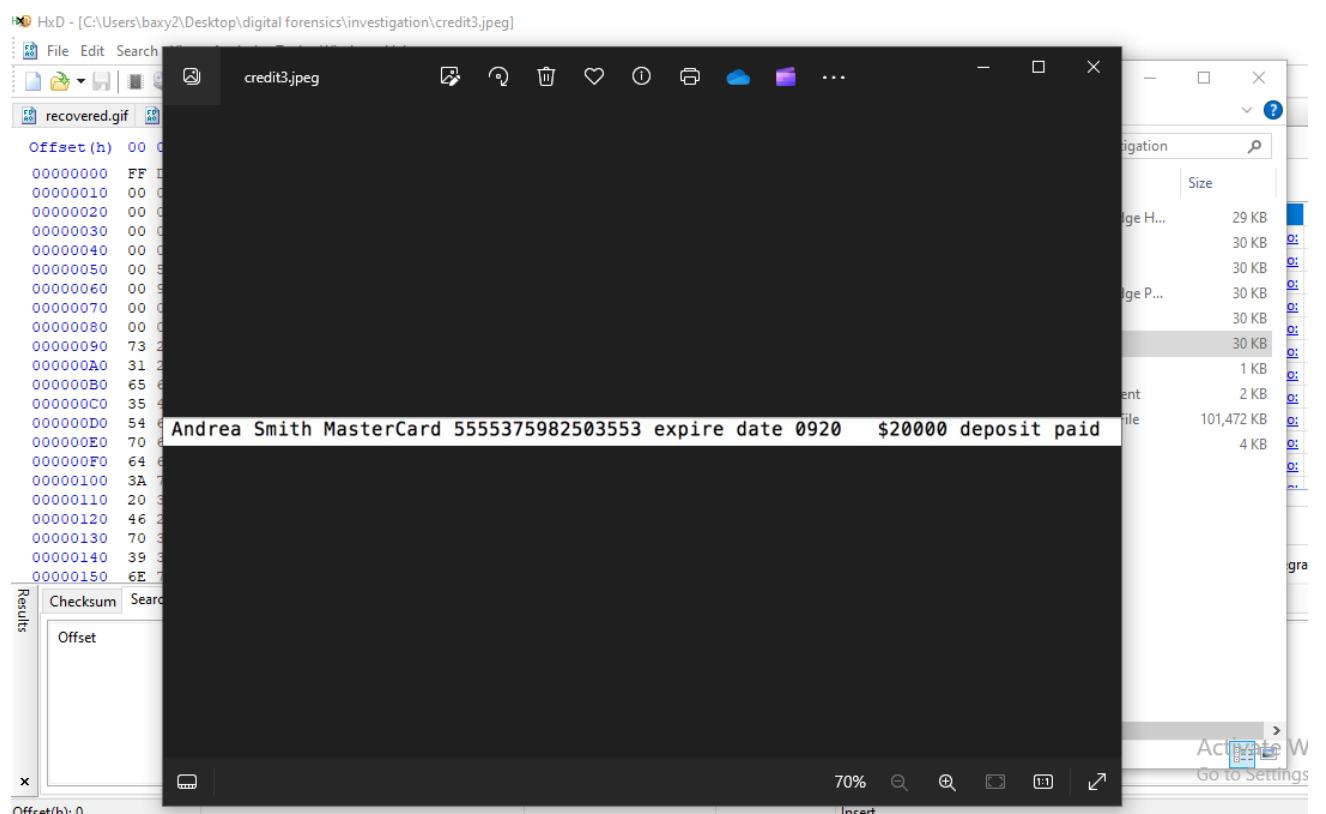
Offset(h)	Decoded text
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	ÿþá..Exif..MM.*
00000000 D8 FF E1 00 80 45 78 69 66 00 00 4D 4D 00 2A
00000010 00 00 08 00 05 01 12 00 03 00 00 00 01 00 01J..
00000020 00 00 01 1A 00 05 00 00 00 01 00 00 4A 01 1BR.
00000030 00 05 00 00 00 01 00 00 00 52 01 28 00 03 00 00#i.....
00000040 00 01 00 02 00 00 87 69 00 04 00 00 00 01 00 00Z.....
00000050 00 5A 00 00 00 00 00 00 00 90 00 00 00 01 00 00
00000060 00 90 00 00 00 01 00 02 A0 02 00 04 00 00 00 01
00000070 00 00 04 74 A0 03 00 04 00 00 00 01 00 00 00 22	...t
00000080 00 00 00 00 FF E1 09 21 68 74 74 70 3A 2F 2F 6Eýá.!http://n
00000090 73 2E 61 64 6F 62 65 2E 63 6F 6D 2F 78 61 70 2F	s.adobe.com/xap/
000000A0 31 2E 30 2F 00 3C 3F 78 70 61 63 6B 65 74 20 62	1.0/.<?xpacker b
000000B0 65 67 69 6E 3D 22 EF BB BF 22 20 69 64 3D 22 57	egin="i»; id="W
000000C0 35 4D 30 4D 70 43 65 68 69 48 7A 72 65 53 7A 4E	SMOMpCeHiHzreSzN
000000D0 54 63 7A 6B 63 39 64 22 3F 3E 20 3C 78 3A 78 6D	Tczkc9d"?> <x:xm
000000E0 70 6D 65 74 61 20 78 6D 6C 6E 73 3A 78 3D 22 61	pmeta xmlns:x="a
000000F0 64 6F 62 65 3A 6E 73 3A 6D 65 74 61 2F 22 20 78	dobe:ns:meta/" x
00000100 3A 78 6D 70 74 6B 3D 22 58 4D 50 20 43 6F 72 65	:xmptk="XMP Core
00000110 20 35 2E 34 2E 30 22 3E 20 3C 72 64 66 3A 52 44	5.4.0"> <rdf:RD
00000120 46 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68 74 74	F xmlns:rdf="ht
00000130 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67 2F 31	p://www.w3.org/1
00000140 39 39 39 2F 30 32 2F 32 32 2D 72 64 66 2D 73 79	999/02/22-rdf-sy
00000150 6E 74 61 78 2D 6E 73 23 22 3E 20 3C 72 64 66 3A	ntax-ns#"> <rdf:

Checksum Search (0 hits)

Results

Offset	Excerpt (hex)	Excerpt (text)
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	ÿþá..Exif..MM.*	ÿþá..Exif..MM.*

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>