

Joachim's Art Gallery Incident: Report Case



Assignment

SIT282: Computer Crime and Digital Forensics Tri 2
Assignment 1 – Digital Forensics Report 2021

Created by: Connor Gent

Table of Contents

1. DIGITAL FORENSIC PROCEDURE	3
1.1. Evidence Form.....	3
1.2. Workstation and Image Download Procedure	4
1.3. SHA-based Hash Values of ISO Image.....	4
1.4 Intel on multiple hash values to verify Image File.....	6
1.5 Steps undertaken before Accessing Image File.....	6
2. DETAILS OF BINARY DETAILS.....	7
2.1. The properties of discovered files on the ISO Image	8
2.2. Details of programs used to during Investigation.....	8
3. FORENSIC DETAILS.....	9
3.1. Key Words Used to Search ISO Image.....	9
3.2. Document Procedure Including Commands and Screenshots.....	10
3.3. Written intel on the Search Conclusions.....	22
4. IMPLICATIONS	23
4.1. Violation and Justification Against: Cybercrime Act 2001 & Crimes Act 1958	23
4.2. Reasonings whether pursued as Corporate or Criminal Investigation.....	23
REFERENCING	24

1. DIGITAL FORENSIC PROCEDURE

1.1. Evidence Form:

DEAKIN SIT282 COMPUTER CRIME AND FORENSIC. EVIDENCE FORM.			
Case No:	Joachim's Art 08192024	Unit Number:	02
Investigator:	Connor Gent		
Nature of Case:	Suspected burglary of valuable piece of art. Mr Donald Price is suspected of the crime.		
Location where evidence was obtained:	Joachim's Art Gallery		
Item # ID	Description of evidence	Vendor Name	Model No/Serial No.
ID:0.6	CD-ROM was discovered at the Joachim's Art Gallery during investigation of the location and the work computer.	AccessData	9
Evidence Recovered by:	Connor C Gent	Date & Time:	23/08/21 10:30am
Evidence Placed in Locker:	Michael Jordan	Date & Time	23/08/21 11:20 p.m.
Evidence Processed by	Description of Evidence		Date & Time
Jackson Merritt	Mr Prince assigned Work PC	Mr Princes Work files	
	Security Footage from		
NOTES	Investigator has managed to make a forensic image of CD_ROM		

1.2. Description of Forensic Workstation and Image Download Procedure

This investigation I opted to use a host machine in conjunction with a virtual machine. The system details and additional information on the two machines have been mentioned below.

Virtual Machine Information:

Product: VMware Workstation 15 pro

Hard Disk: 50GB

Memory: 2GB

Version: 15.0.4 build-1299004

Virutal Machine Operation System

Ubuntu 18.04.2

Host Machine Information

Processor Intel(R) Core(TM) i7-1165G7 @ 2.80GHz 2.80 GHz
Installed RAM 8.00 GB (7.65 GB usable)
Device ID 5FBF6555-A506-4FD1-AAE5-7990690C0D8C
Product ID 00325-96744-43641-AAOEM
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Host Operating System

Windows 10 Pro

The virtual machine is going to be created on top of the Windows 10 host operating system. For this task I was provided with two URLs that are downloadable. One is for the raw format of the CD-ROM the other is the MD5 hash value. I downloaded the CD-ROM ISO image to my working directory and then got started from there. I have attached the links below.

CD-ROM ISO image:

URL - <https://www.dropbox.com/s/ov5ksmt7afurqw/2019Greenbook.ISO?dl=0>

MD5 Hash:

URL - <https://www.dropbox.com/s/gu7wjpkvymhr1u0/2019Greenbook.ISO.md5?dl=0>

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

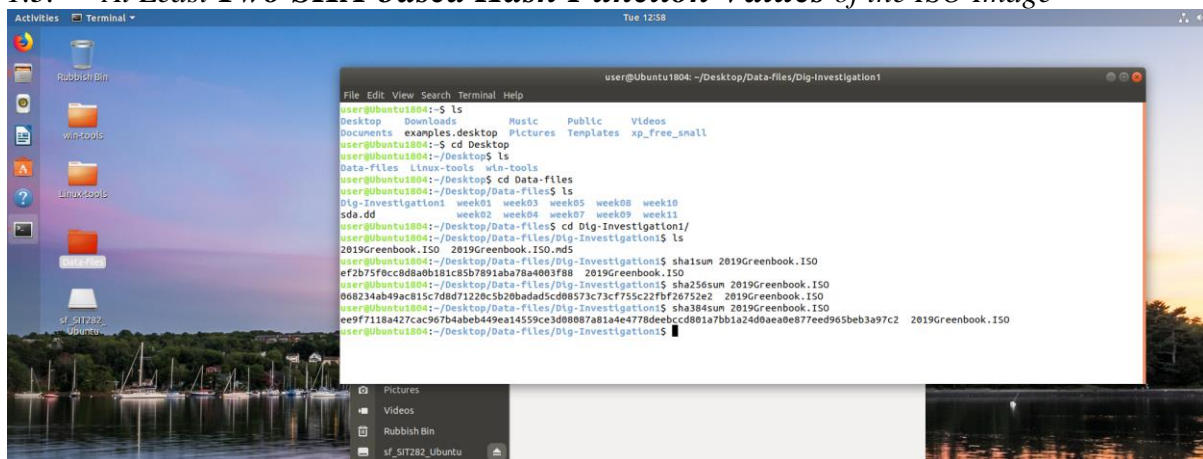
A screenshot of a Linux desktop environment with a terminal window open. The terminal shows the user navigating to the Desktop directory, then to a subdirectory named 'Data-files', and finally to 'Dig-Investigation1'. The user lists the contents of the directory, which includes '2019Greenbook.ISO' and '2019Greenbook.ISO.md5'. The user then runs the 'sha1sum' command on the ISO file, and the terminal displays the resulting SHA1 hash value: 'ef2b75f6cc8da0b181c85b7891aba78a4003f88 2019Greenbook.ISO'. The user then runs the 'sha256sum' command on the ISO file, and the terminal displays the resulting SHA256 hash value: '066234ab49ac815c7dd71228c5b20bad45cd08973c7755c22f0f26752e2 2019Greenbook.ISO'. The user then runs the 'sha384sum' command on the ISO file, and the terminal displays the resulting SHA384 hash value: 'ee9f7118a427cac967b4abeb449ea14559ce3d08087a81a4e4778deebcc8d81a7bb1a24d0aae0e877eed965eb3a97c2 2019Greenbook.ISO'. The user then runs the 'sha512sum' command on the ISO file, and the terminal displays the resulting SHA512 hash value: 'ee9f7118a427cac967b4abeb449ea14559ce3d08087a81a4e4778deebcc8d81a7bb1a24d0aae0e877eed965eb3a97c2 2019Greenbook.ISO'. The terminal window is titled 'user@Ubuntu1804: ~/Desktop/Data-files/Dig-Investigation1'.

Fig 1.0

<i>SHA-Hash Values</i>	<i>Discovered values</i>
'SHA-1'	ef2b75f0cc8d8a0b181c85b7891aba78a4003f88
'SHA-256'	068234ab49ac815c7d8d71220c5b20badad5cd08573c73cf755c22fbf26752e2
'SHA-384'	ee9f7118a427cac967b4abeb449ea14559ce3d08087a81a4e4778deebccd801a7 b b1a24d0aea0e877eed965beb3a97c2

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

In the world of forensics, Digital evidence can unfortunately be damaged, manipulated and even permanently damaged in some instances. This tends to occur during data transfer/examinations. Hash values are the described as digital fingerprints for files. When contents of a file are processed through the 'cryptographic algorithm' hash values are produced to correlate with the contents of the file. Hash values are needed and used to check the integrity of evidence disks (Disk image created for analysis), images discovered are expected to be a perfect copy of the disk. If contents are modified in any way the value of the hash will change drastically. Moreover, using multiple hash values ensures that clones/copies of the original image are identical (No change).

1.5 Explanation of Procedure used Before Accessing Image File in VM

The following numbered method below explains the set up procedure/stages of the investigation:

1. First step was the creation of a folder titled Dig-investigation1. I used this folder as the destination point of the downloaded image folder. (Direct download into file).
2. Then it was analysing and checking the hash values of the ISO image with the hash value provided through the assignment overview. I did this to determine if there were any differences in the values
3. I made the decision to create another folder to help me in this investigation, it was duplicate of the first folder but titled 'Dig-investigation1 (Copy)'. I then copied and pasted the exact same image file contents into it. This file was the default file of the investigation to minimise errors or destruction to the original file.
4. The main purpose of making a copy was to determine if their were any changes to the image file when copied over to a new file. There were no changes when tested. Hex Tested though the command '**md5sum**'2019Greenbook.ISO

```

user@Ubuntu1804: ~/Desktop/Data-files/Dlg-Investigation1 (Copy)
File Edit View Search Terminal Help
user@Ubuntu1804:~$ ls
Desktop  Downloads  Music  Public  Videos
Documents  examples.desktop  Pictures  Templates  xp_free_small
user@Ubuntu1804:~$ cd Desktop
user@Ubuntu1804:~/Desktop$ ls
Data-files  Linux-tools  win-tools
user@Ubuntu1804:~/Desktop$ cd Data-files/
user@Ubuntu1804:~/Desktop/Data-files$ ls
Dlg-Investigation1  week01  week04  week08  week11
Dlg-Investigation1 (Copy)  week02  week05  week09
sda.dd  week03  week07  week10
user@Ubuntu1804:~/Desktop/Data-files$ Dlg-Investigation1
Dlg-Investigation1
user@Ubuntu1804:~/Desktop/Data-files$ Dlg-Investigation1 (Copy)
bash: syntax error near unexpected token 'Copy'
user@Ubuntu1804:~/Desktop/Data-files$ cd 'Dlg-Investigation 1 (Copy)'
bash: cd: Dlg-Investigation 1 (Copy): No such file or directory
user@Ubuntu1804:~/Desktop/Data-files$ cd 'Dlg-Investigation1 (Copy)'
user@Ubuntu1804:~/Desktop/Data-files/Dlg-Investigation1 (Copy)$ ls -ls
total 88356
-rw-rw-r-- 1 user user 98476544 Aug 24 12:53 2019Greenbook.ISO
user@Ubuntu1804:~/Desktop/Data-files/Dlg-Investigation1 (Copy)$ chmod 444 2019Greenbook.ISO
user@Ubuntu1804:~/Desktop/Data-files/Dlg-Investigation1 (Copy)$ ls -ls
total 88356
-r--r--r-- 1 user user 98476544 Aug 24 12:53 2019Greenbook.ISO
user@Ubuntu1804:~/Desktop/Data-files/Dlg-Investigation1 (Copy)$ md5sum 2019Greenbook.ISO
c5f7921e78b3037777c9695530c084 2019Greenbook.ISO
user@Ubuntu1804:~/Desktop/Data-files/Dlg-Investigation1 (Copy)$

```

Fig 1.1

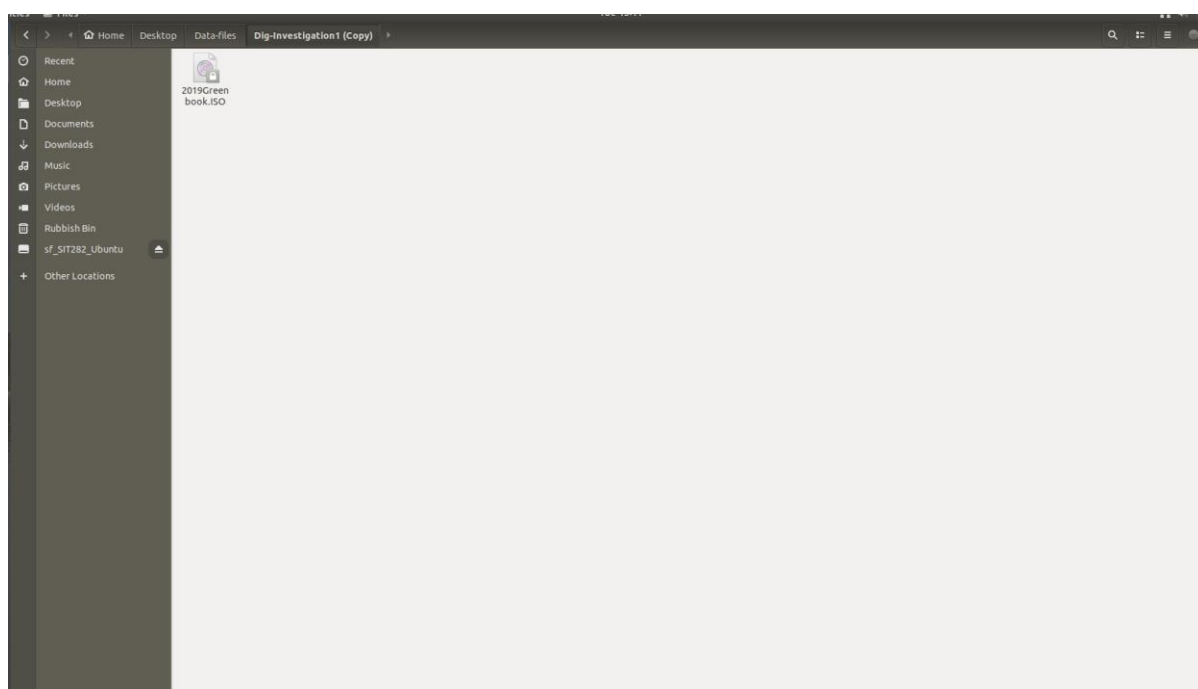


Fig 1.2

5. I decided to change the permission of the file in the new file to read only mode. This decision was made due to when it's a read only file people/other investigators cannot make unauthorised changes to the file, and the data won't be altered or changed inside of the file. **CHMOD 444 2019Greenbook.ISO** was the command used to change the permission.
6. Again, the hash value was checked to determine changes to the hex values
7. No changes to the hex value after the change of permission were discovered. Meaning it was identical.

2. DESCRIPTION OF BINARY DETAILS

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

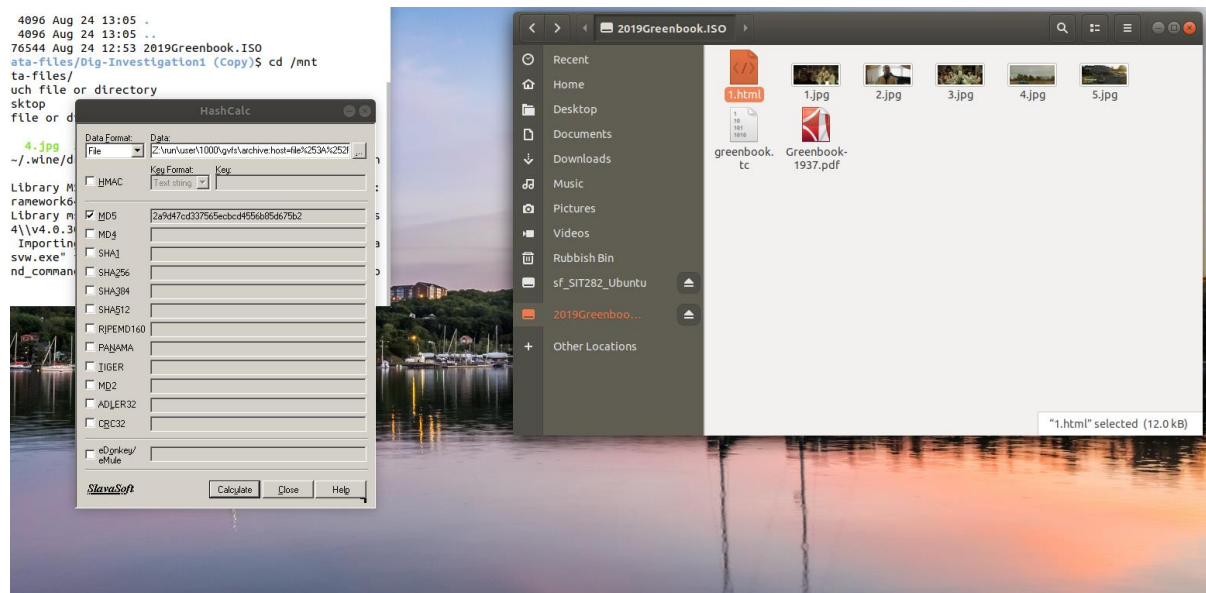


Fig 1.3

File Name	Physical Size	MD5 Hash
1.html	12.0 kb	2a9d47cd337565ecbcd4556b85d675b2
1.jpg	119.4 kb	1831b1f5e0e5a22a1f9d5cbab2099f1b
2.jpg	129.4 kb	ae9ef080a292374a866d659abd55712f
3.jpg	183.4 kb	d3060c3925e2f21274c5d04ce465ef08
4.jpg	122.7 kb	30c58285a32ac6ff2232fe09cf8a11dd
5.jpg	233.0 kb	853bd591239b0225bbce59fdd7da1bc6
greenbook.tc	83.9 MB	39e0cc888b3d96fb07c411b4d52da1fa
Greenbook1937.pdf	5.4 MB	1bcbf60d6f2629a35dabcb4bcf1b2071

2.2. Description of Programs to be used to Perform Investigation

Autopsy:

I would use Autopsy for further detailed analysis of the image file. It's an open-source program that and it runs on Unix systems (Can also be run on window-based systems as well). Its able to analyse major file systems, it's extremely fast and able to display the results from the forensics search of the volume meaning it's easier to flag pertinent sections of data.

HxD:

HxD is often used in digital investigation as it enables an investigator the opportunity to open any file to inspect the contents within. It's an hex editor/disk editor and even at times a memory editor that allows for editing of raw contents of disk drives. HxD can also be used to display and edit the memory used by running processes. Some of the main features of HxD include Data inspection, searching and replacing several data types, and calculating checksums and hashes.

Veracrypt:

VeraCrypt is an open-source software that can create virtual encrypted disks. It has the ability to encrypt this disk that's within a file and then mount it as if it was real. This is something I will have to do throughout this investigation and is why this software is a primary choice. Moreover, it has the ability to improve and enhance the security of the algorithms used when systems and partitions are encrypted. (Ellis, 2021)

HashCalc:

I used the software HashCalc to calculate the files checksum values and HMACS. It was extremely easy to use and offered and supported a choice of 12 well known documented hash and checksum algorithm. I was able to use the drag and drop support to determine the properties of the undeleted files found on the ISO image. (Refer to figure 1.3 in regards to the drag and drop element)

3.OUTCOMES OF DIGITAL FORENSIC INVESTIGATION

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

Digital forensic investigators often use Keyword searching during their work. It's a powerful searching tool used to identify evidence that is grouped in a large data set. It enables investigators the opportunity to establish a defined search by identifying a word/combination of words in digital words. After analysing the evidence provided in the case description, the suspect and the overall nature I came to the conclusion that the key words that will be used in my search are:

Keyword – Donald Prince:

Given this is the suspects name (identified in the case) it has to be considered a key word in this investigation. Hence why I decided to use the name as a key word in my forensic investigation of the ISO image.

Keyword – Joachim:

'Joachim' was the first keyword that I will centre my search around. This is crucial key word to the investigation. It's deemed crucial as it's the title of the art gallery mentioned in the case description. This is where the suspect worked, where the art belonged and where it was stolen/Disappeared. All this relevant as establishes the belief that this key word will be available in majority of the discovered files and holds the key to finding more relevant evidence.

Keyword – Two boats:

'Two boats' is deemed a keyword and was used in my investigation as it ties into the evidence of the crime committed. Two boats were the elements within the stolen/disappeared art created via water colours. This led me to believe perhaps this key word would provide a link to more information and would be available in the recovered files being analysed in this case. Therefore I chose to use this key word.

3.2. Document Procedure Including Appropriate Commands and Screenshots

The following listed steps (In numerical order) in conjunction with screenshots shows this investigation from start to finish:

1. As mentioned in section 1.5 the first step of this investigation was to download the ISO image (<https://www.dropbox.com/s/ov5ksmt7afurqw/2019Greenbook.ISO?dl=0>) as well as the MD-5 hash value (<https://www.dropbox.com/s/gu7wjpkvymhr1u0/2019Greenbook.ISO.md5?dl=0>). Links have been provided here.
2. After these links were provided, I began tests to compare the MD-5 hash values of the original ISO image downloaded in step 1 as well as the MD-5 hash values provided through the 2nd link. (Command **md5sum '2019Greenbook.ISO'**) **used for the comparison.**
3. Through the comparing (Conducted via Linux terminal) and the values produced I was able to determine that the values are the same, this meant that the downloaded image was real and a direct copy of the original.
4. My next decision was to change the file permission to read only mode. This was done through the command: **chmod 444 '2019Greenbook.ISO'**. This was done to remove issues such as professional curiosity and so that no unauthorized changes can be made to the ISO. Doing this does not affect the data contained inside.

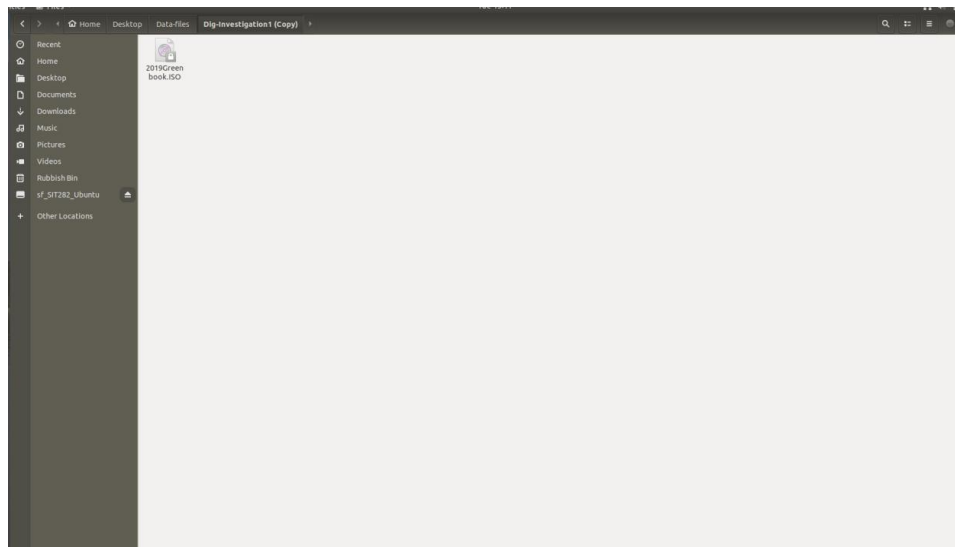


Fig – 1.4

5. To conduct a further investigation on the ISO I used the Autopsy forensic tool. I had prior experience using it and was already installed on the Ubuntu. To access the program the command **“sudo autopsy”** a link then appeared **<https://localhost:9999/autopsy>** which was copied and pasted in order to be used to access and open Autopsy in the fire fox web browser. This is an application that is often used to inspect files. This was an important program in my investigation.

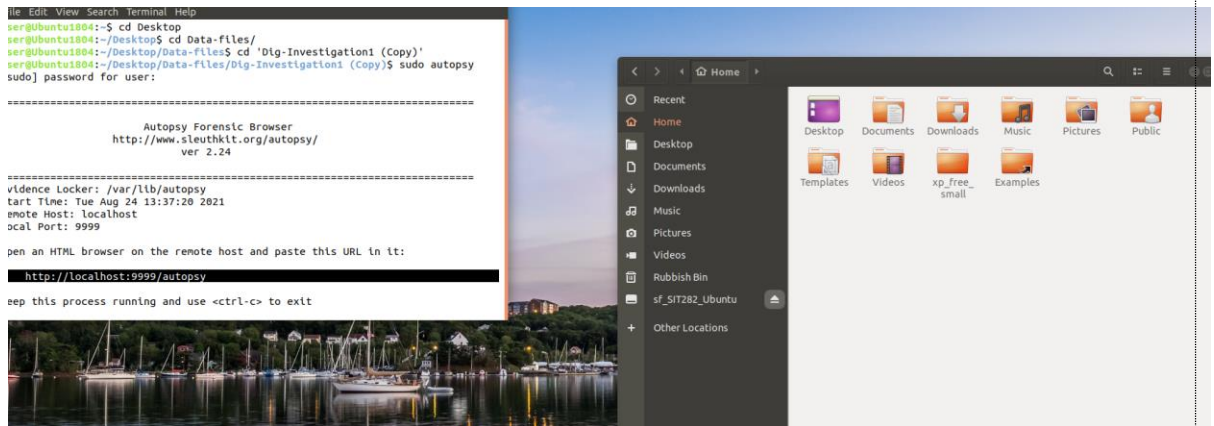


Fig – 1.5

6. The next step once on autopsy was to click on the option **New Case**. As you can see autopsy offers 3 options on it's home page



Fig 1.6

7. After clicking new case I was given the option to add Case details to which I filled out appropriately to the investigation. I gave a case **name**, **description**, and the **investigating officers name (My Name)**.

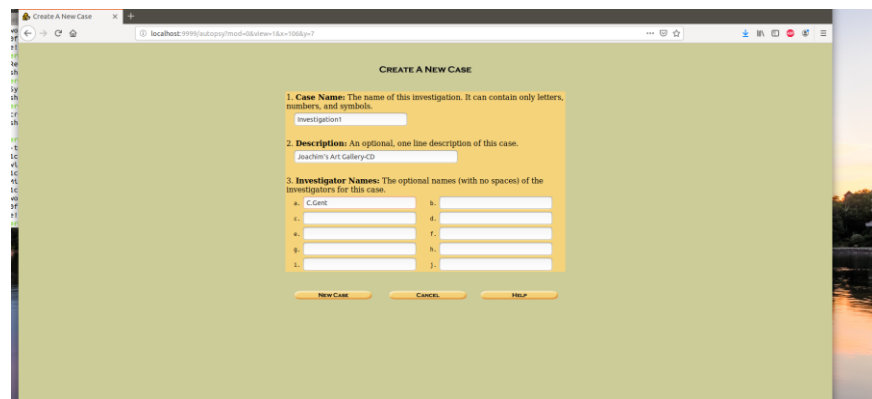


Fig 1.7

8. I continued through **adding a host and filling in spaces with the appropriate information**: Entering the details for the host name and the description of the host. E.g. the host computer details.

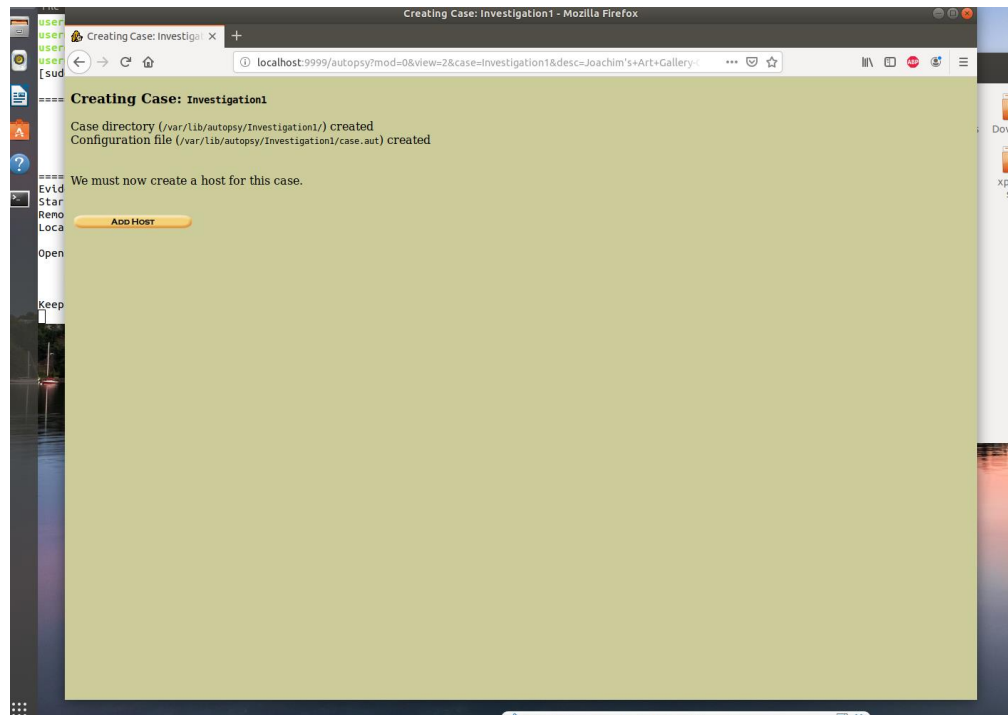


Fig 1.8

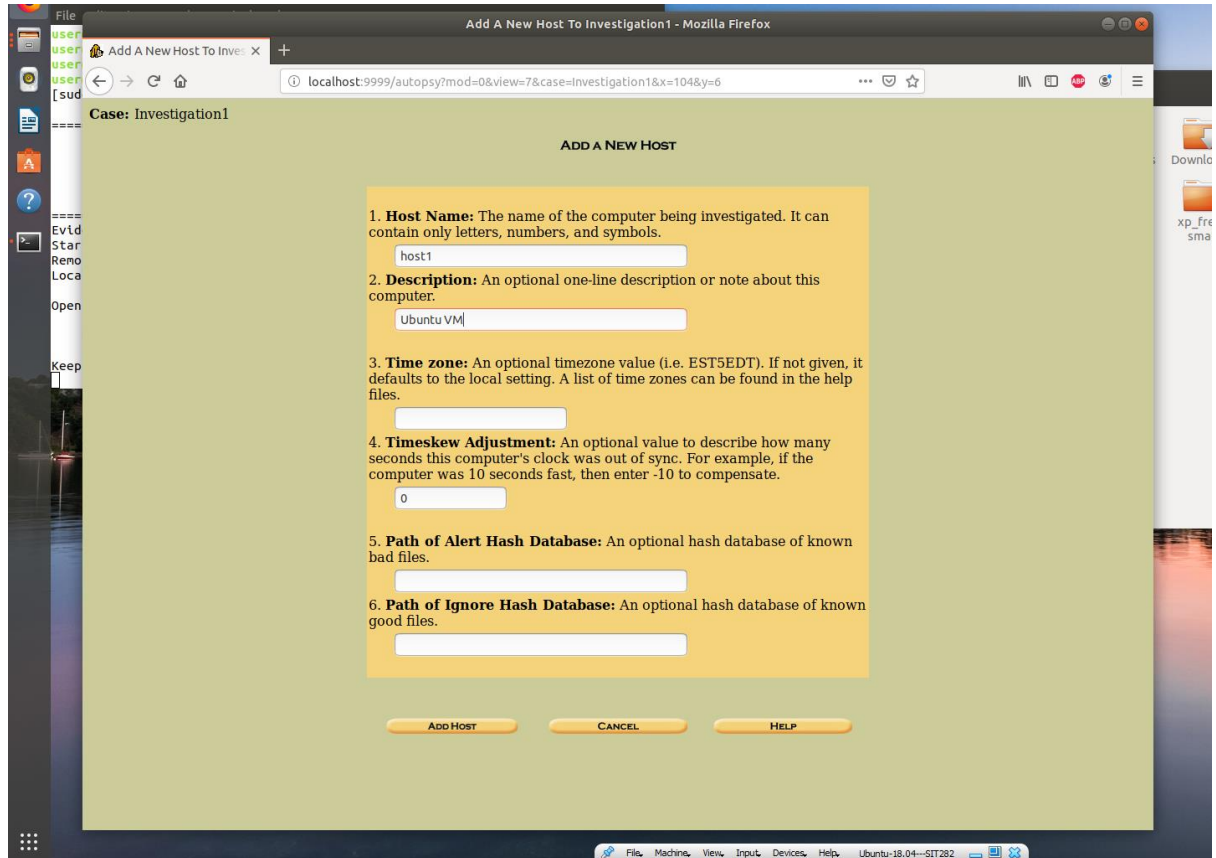


Fig 1.9

9. After the host was successfully created/added, adding the image was next:

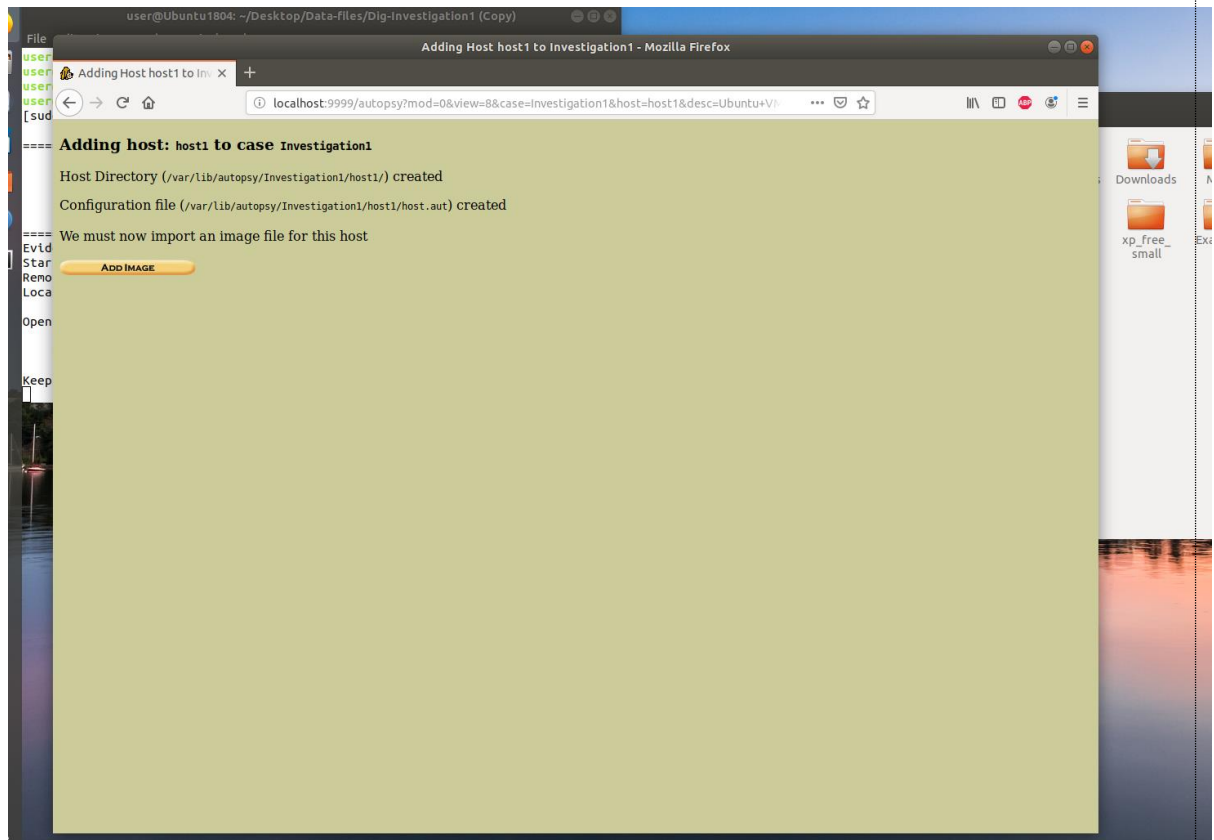


Fig 2.0

10. Selecting the correct location of the image to analyse was a crucial next step. I chose Symlink. This was the image file can be imported from its current location to the evidence locker without the risks associated with moving or copying the image file. (Selection details below).
1. Enter the full path to the image file: (**Type in the details the full path had to be specified**)
 2. Select: **Partition** instead of disk
 3. Import Method: **Symlink**

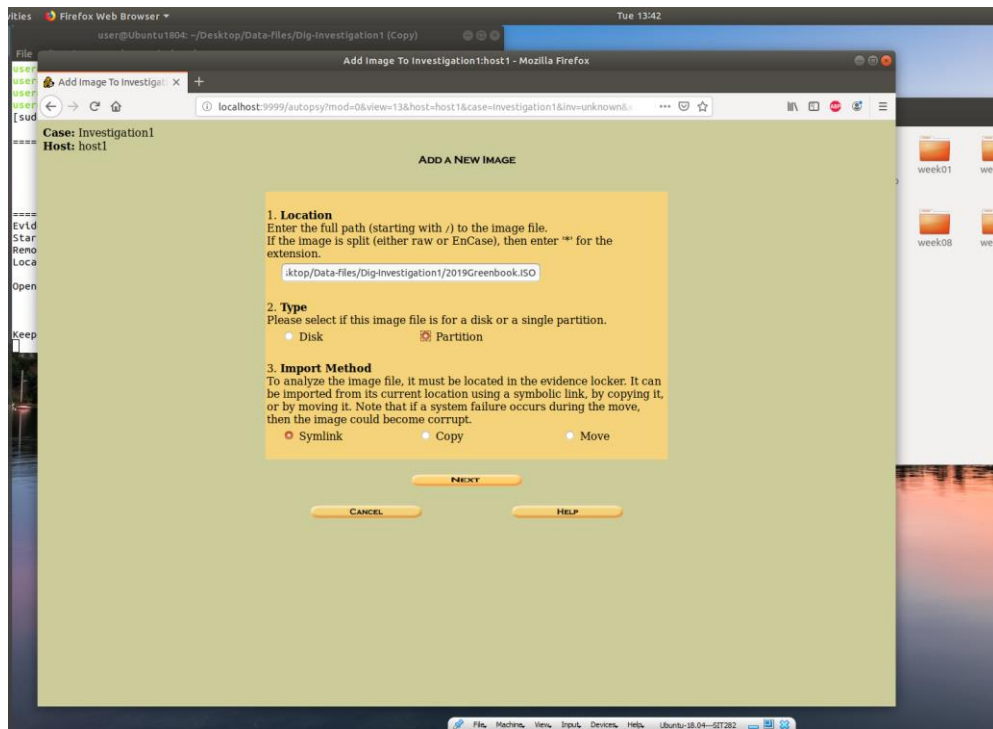


Fig 2.1

11. Once this was created and added correctly Autopsy allowed me the option to analysis the file (File Analysis): This was allowed after the creation of the case, host information was added with appropriate directories and the acquired image had been added. I was able to inspect and examine the directories and files within the image. Whilst also being able to see through the Autopsy fields when the items were written, accessed, changed. and created.

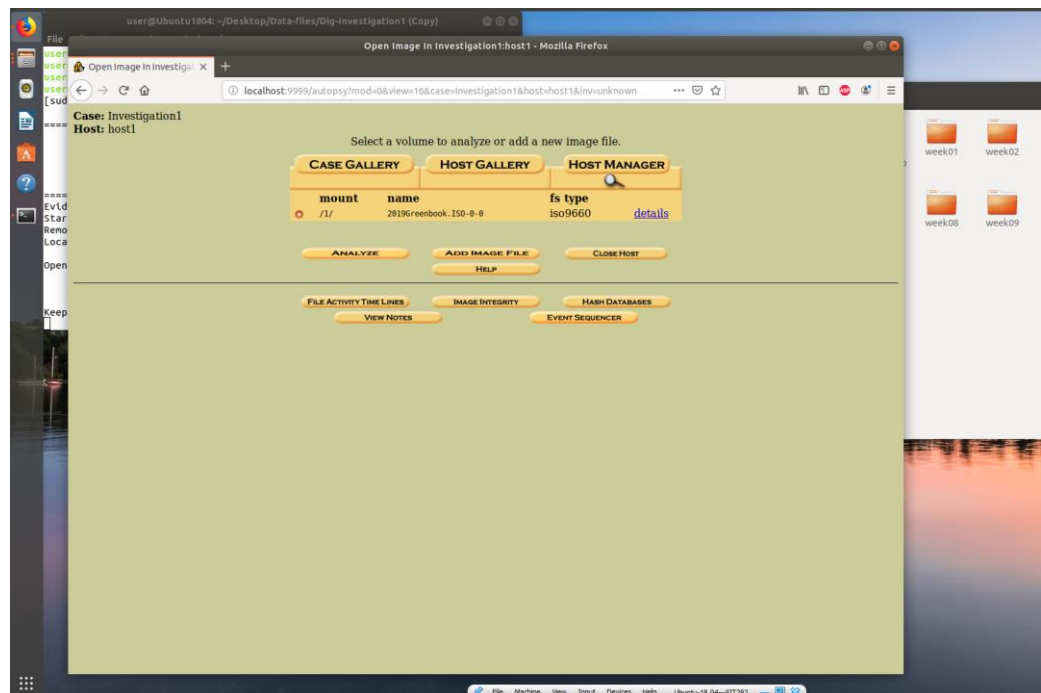


Fig 2.2

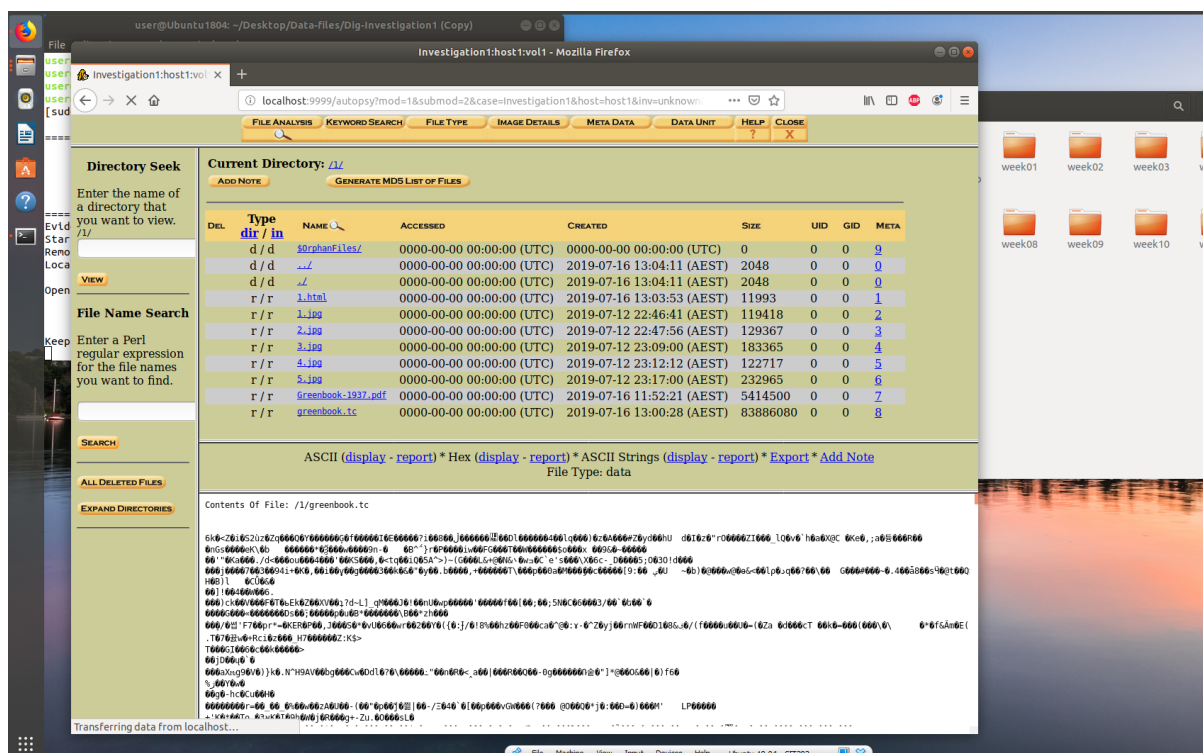


Fig 2.3(Inspection of greenbook.TC)

12. After a thorough examination of the files hex values, I came across the 1.HTMl file which established suspicion. I inspected the 1.HTMl file and came across a gif format file header. Due to these finding I decided to export the file where more analysis can be conducted via HxD.

	d/d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	9
	d/d	ل	0000-00-00 00:00:00 (UTC)	2019-07-16 13:04:11 (AEST)	2048	0	0	0
	d/d	ل	0000-00-00 00:00:00 (UTC)	2019-07-16 13:04:11 (AEST)	2048	0	0	0
Search	r/r	1.html	0000-00-00 00:00:00 (UTC)	2019-07-16 13:03:53 (AEST)	11993	0	0	1
	r/r	1.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 22:46:41 (AEST)	119418	0	0	2
	r/r	2.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 22:47:56 (AEST)	129367	0	0	3
	r/r	3.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:09:00 (AEST)	183365	0	0	4
	r/r	4.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:12:12 (AEST)	122717	0	0	5
	r/r	5.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:17:00 (AEST)	232965	0	0	6
	r/r	greenbook-1937.pdf	0000-00-00 00:00:00 (UTC)	2019-07-16 11:52:21 (AEST)	5414500	0	0	7
	r/r	greenbook.TC	0000-00-00 00:00:00 (UTC)	2019-07-16 13:00:28 (AEST)	83886080	0	0	8

ES	RIES	Hex Contents Of File: /1/1.html
		<pre> 00000000: 3C68 7460 6C3E 0A8A 2020 8A3C 626F 6479 <html>...<body 00000010: 3E0A 2020 3C69 6067 2073 7263 3022 312E >...
 00000040: 2020 3C69 6067 2073 7263 3022 322E 6A70
 00000070: 3C69 6067 2073 7263 3022 332E 6A70 6722
...<i 000000A0: 6067 2073 7263 3022 342E 6A70 6722 2073 mg src="4.jpg" s 000000B0: 7479 6C65 3022 7769 6474 683A 3230 3070 tyle="width:200p 000000C0: 783B 223E 203C 6272 3E0A 2020 3C69 6067 x;">
...
...<img s 00000100: 7263 3022 4749 4638 3961 0602 4401 F700 rce="gif02.png" 00000110: 0000 0000 0000 0014 1414 1B1B 1B2E 0000 00000120: 002E 0000 002E 2424 242C 2C2C 3232 323C\$\$.222< 00000130: 3C3C 1F2E 0F41 0000 4F00 0050 0000 5C00 <<...A..O..P.. 00000140: 0067 0000 7000 0079 0000 552E 0079 2000 .g..p..y..U..Y.. 00000150: 7548 0066 4F20 0000 4100 004F 0000 5000 uH..fO...A..O..P. 00000160: 005C 0028 5000 2E4F 0000 6000 0070 0000 .\..X..O..f..p.. </pre>

Fig 2.4 (Inspection of Hex contents of 1.HTMl file)

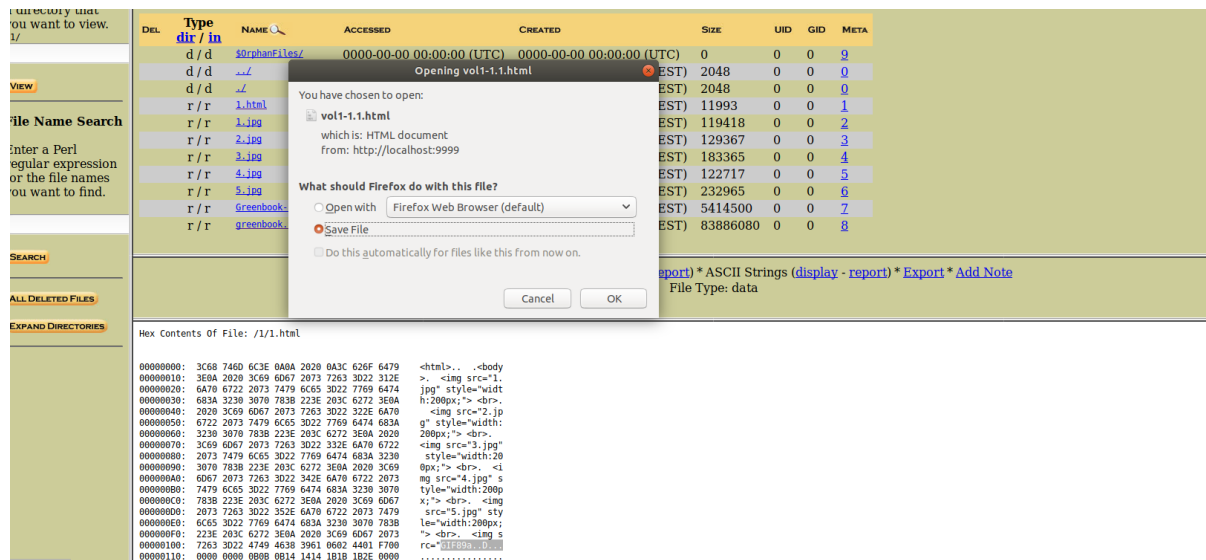


Fig 2.5

13. I researched more on the Gif89 header hex values e.g., starting values and ending values. And found the hex value starts with 47 49 46 38. The ending values are 00 3B. I copied those image contents onto a new HxD document and ensured the starting and ending values were correct. I then saved the file type as gif.

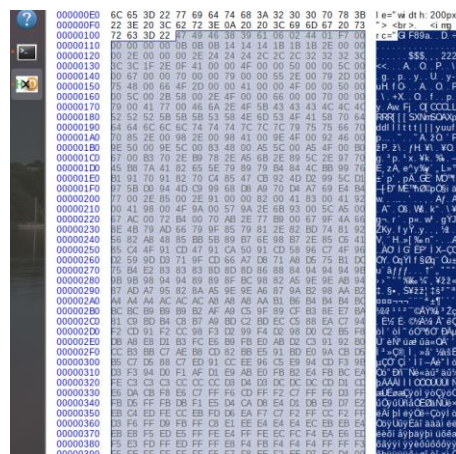


Fig 2.6

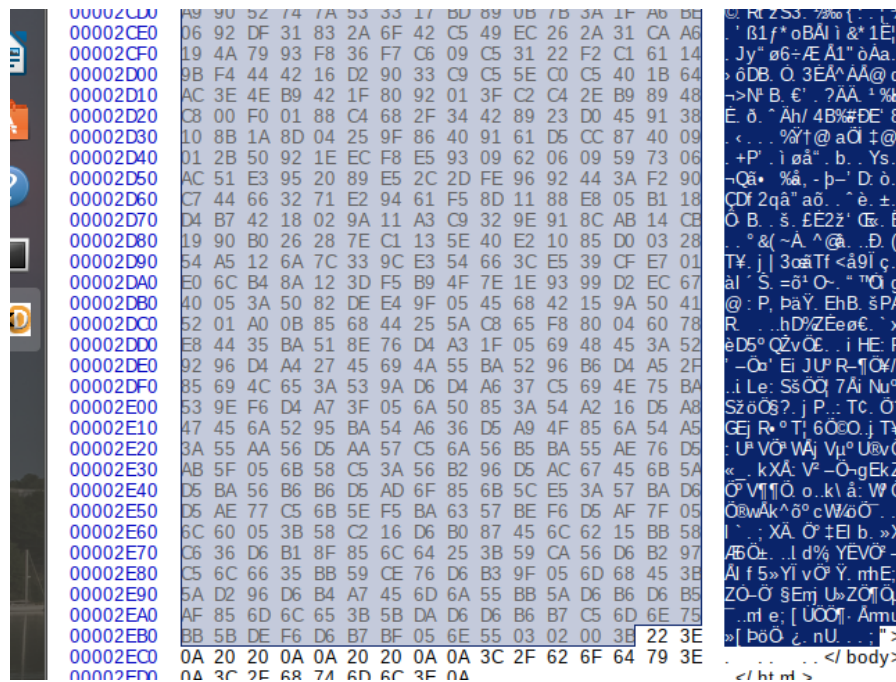
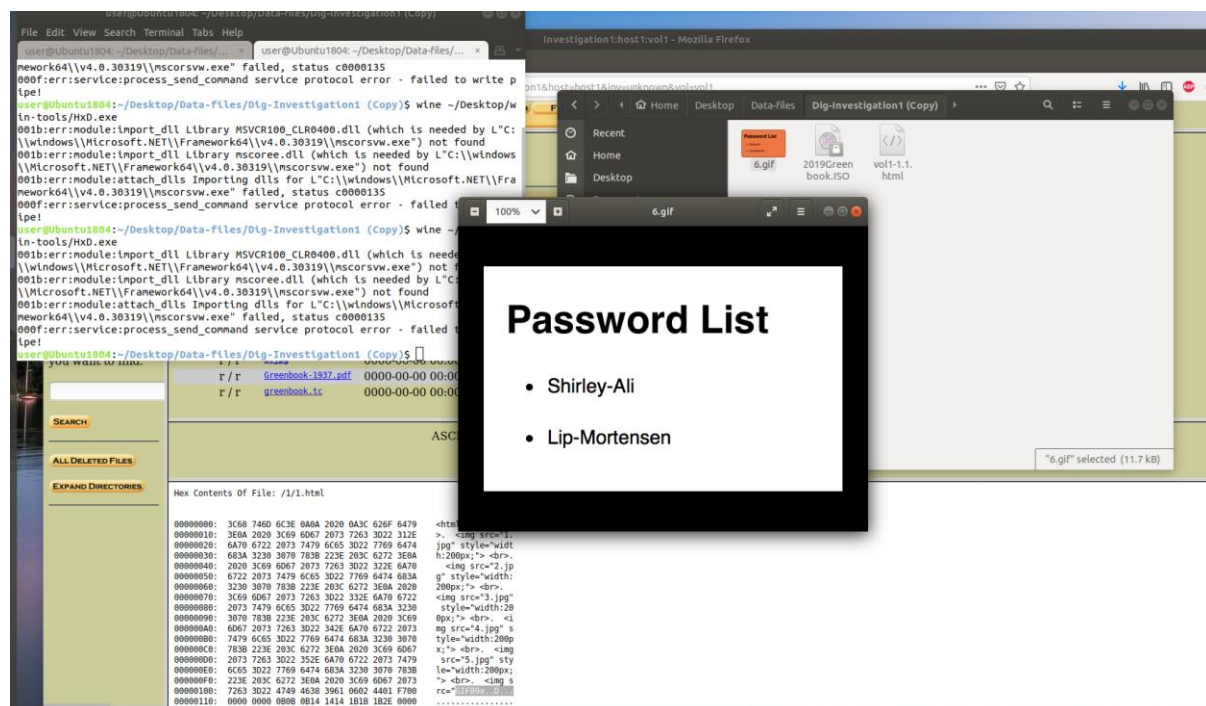


Fig 2.7

I was then able to open the image after the changing of its hex values. The contents of the image can be seen in Figure 2.8. They placed a crucial part in my coming steps/findings.



14. Once this acquiring this information I turned my focus onto the 'greenbook.tc' file. After analysing this file in Autopsy, it was noted as an encrypted file. I determined this also thorough using Truecrypt. To decrypt this file to allow me to open the file after exporting from Autopsy I used Veracrypt. (Command: **'veracrypt'** in Ubuntu terminal). I was then allowed access to the file in conjunction with the ability to mount onto volume 4. When mounting I was asked to enter a password, which was password number one

from the gif “Shirley-Ali” this disabled the protection protocols of the file and enable access to the contents of the file. (Seen in figure 2.8), during this process I deselected TrueCrypt mode to minimise the chances of error.

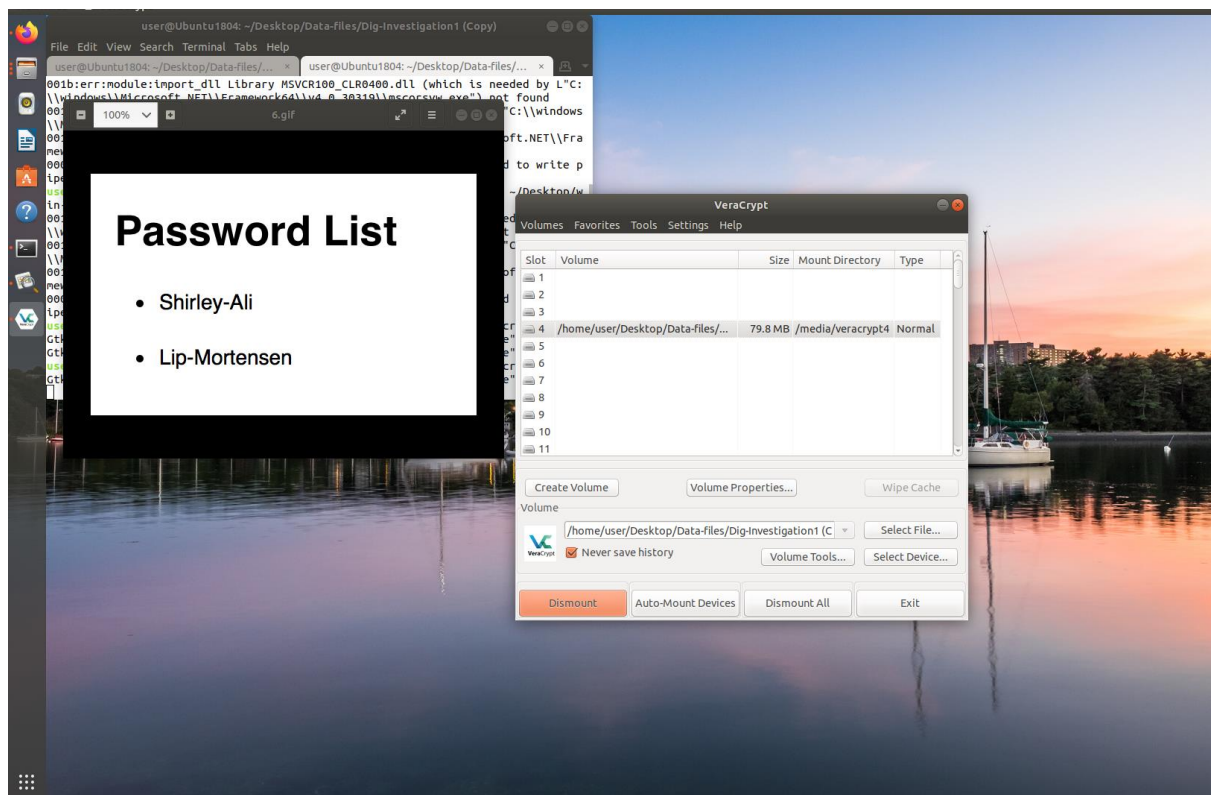


Figure 2.9

Once I had access to the mounted volume, I discovered four files which were recovered (Refer to figure 3).

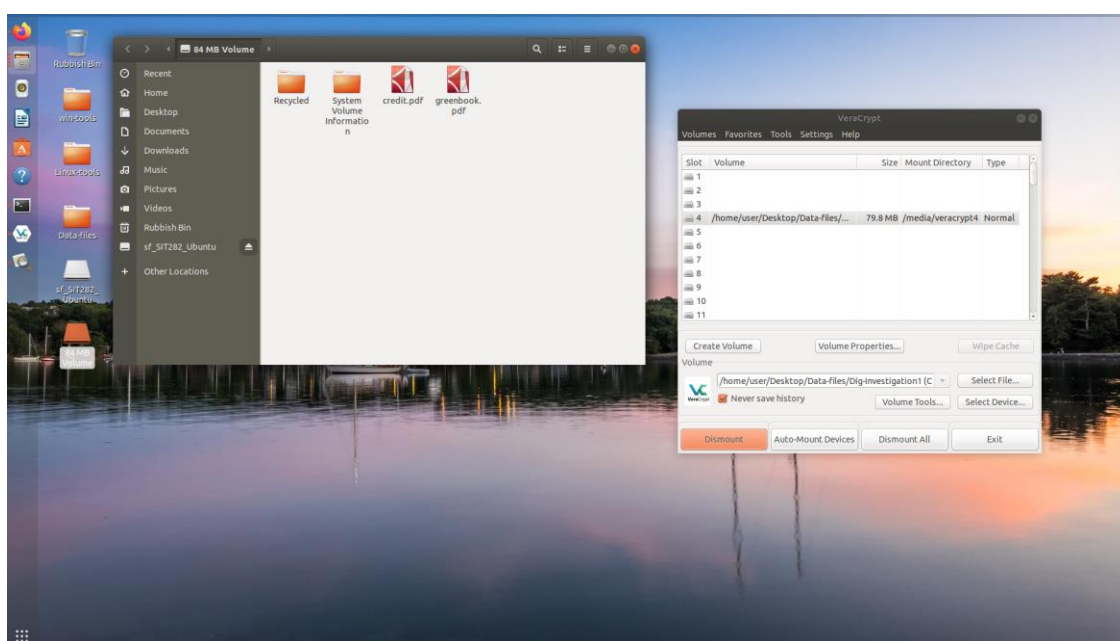


Figure 3.0

Inspecting the recycled folder of the mounted volume, I came across the water-coloured picture of two boats which Mr Prince was a suspect of stealing/leading to its disappearance. This was a big moment in the investigation as it meant we were making progress.

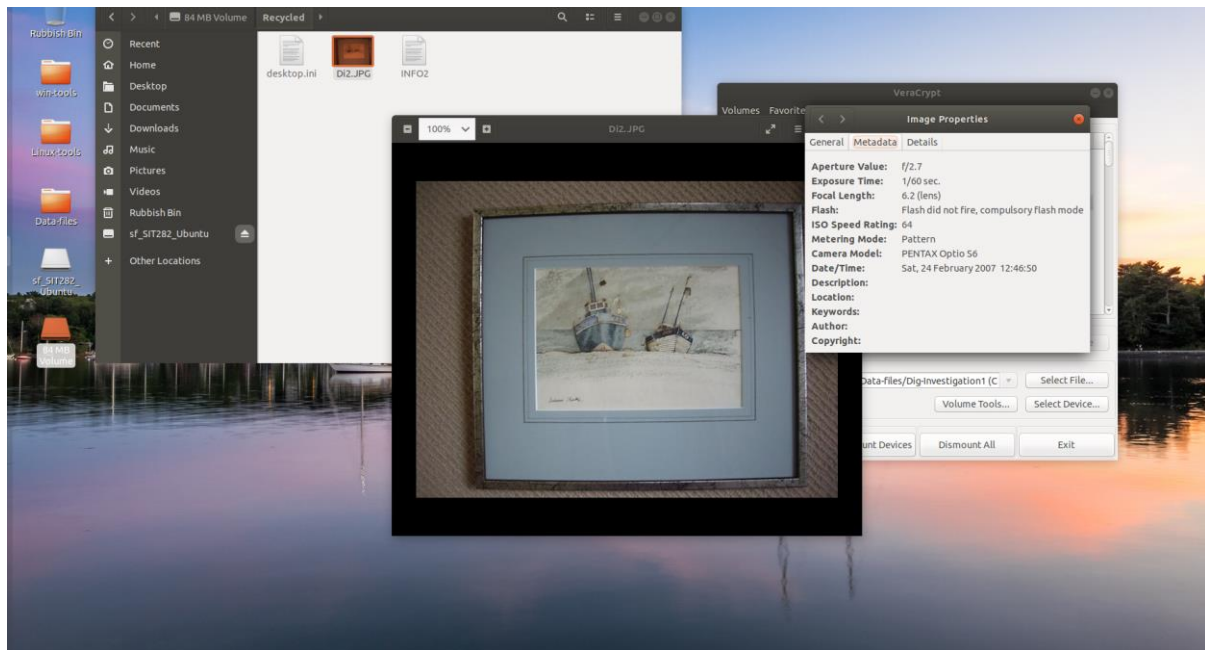
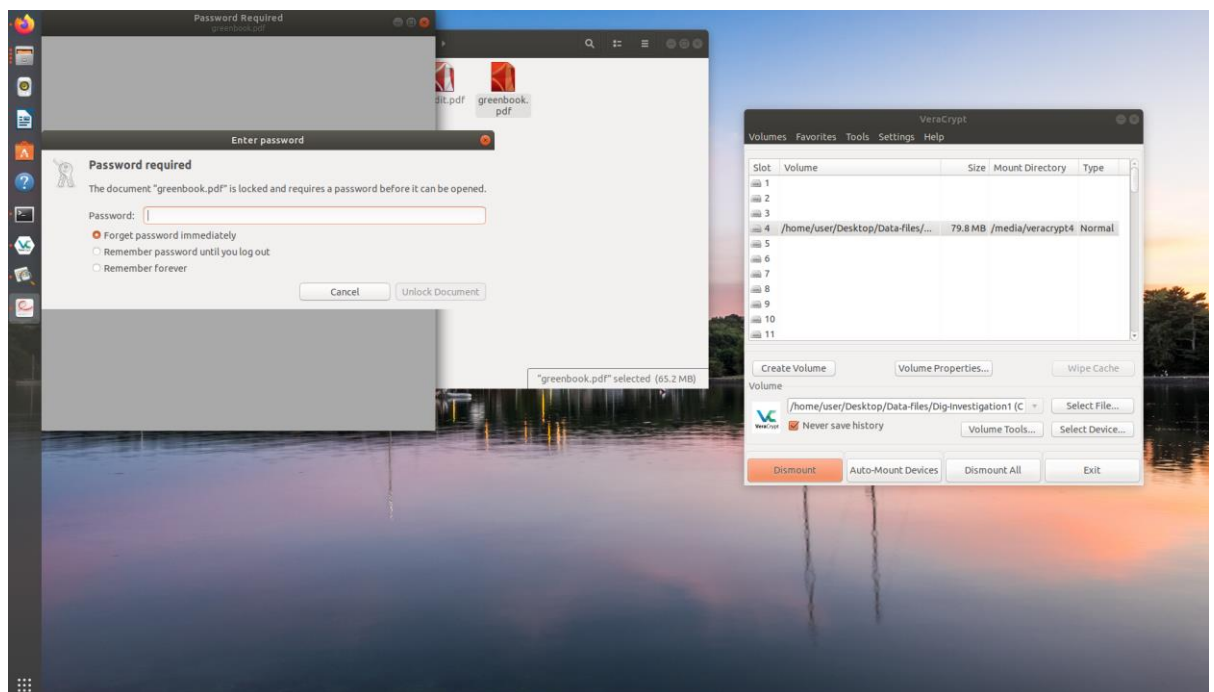


Figure 3.1

15. After this big discovery I wanted to move my focus onto the other files especially greenbook.pdf. However, it was password protected again. Although the 2nd password on the password list (Lip-Mortensen) unlocked the file and granted me access to the content inside.



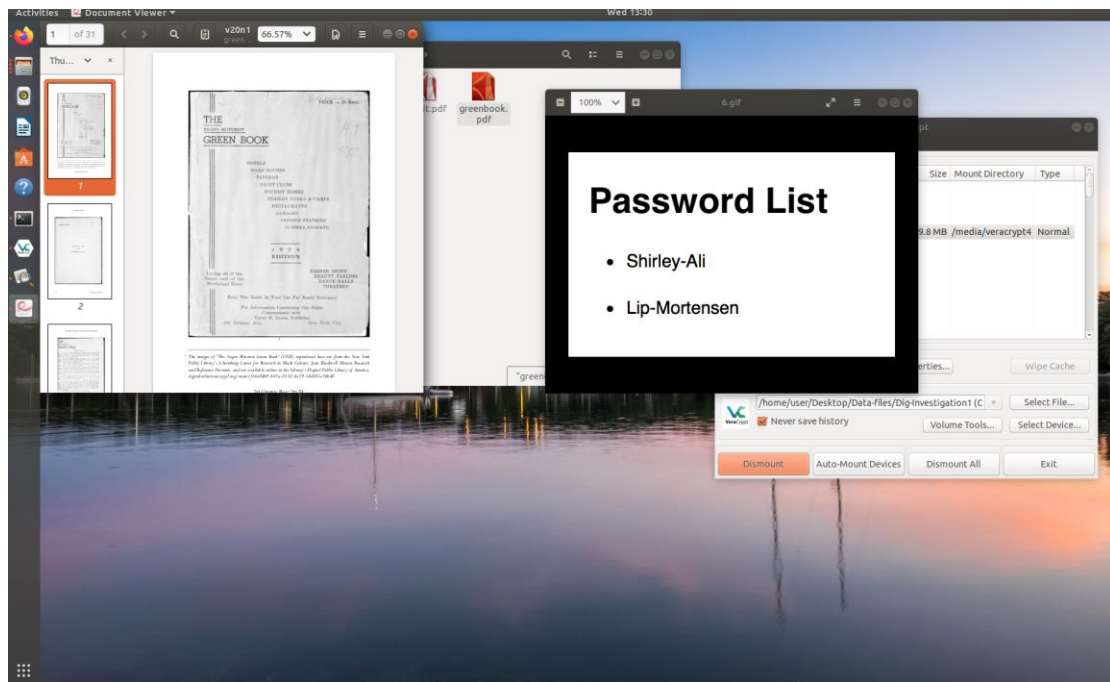


Figure 3.3

The **greenbook.pdf** file after searching presented me with a email copy of a deal struck between Donald (Referring to Mr Prince) and Andrea (page 25 of file). The email contains a financial offer of \$20,000 for the missing art and a sample sent by Donald Prince to indicate his seriousness to struck a deal.

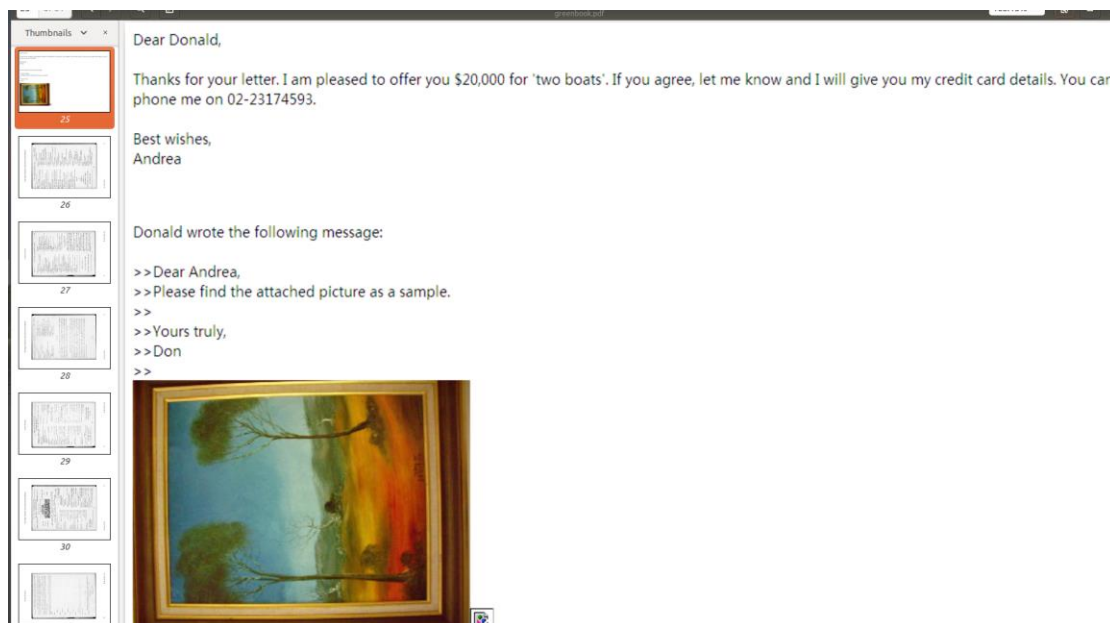


Figure 3.4

16. Moving on from this discover I attempted to inspect the contents within **credit.pdf** file. However, I came across an issue when trying to open. The file was damaged and therefore could not be opened

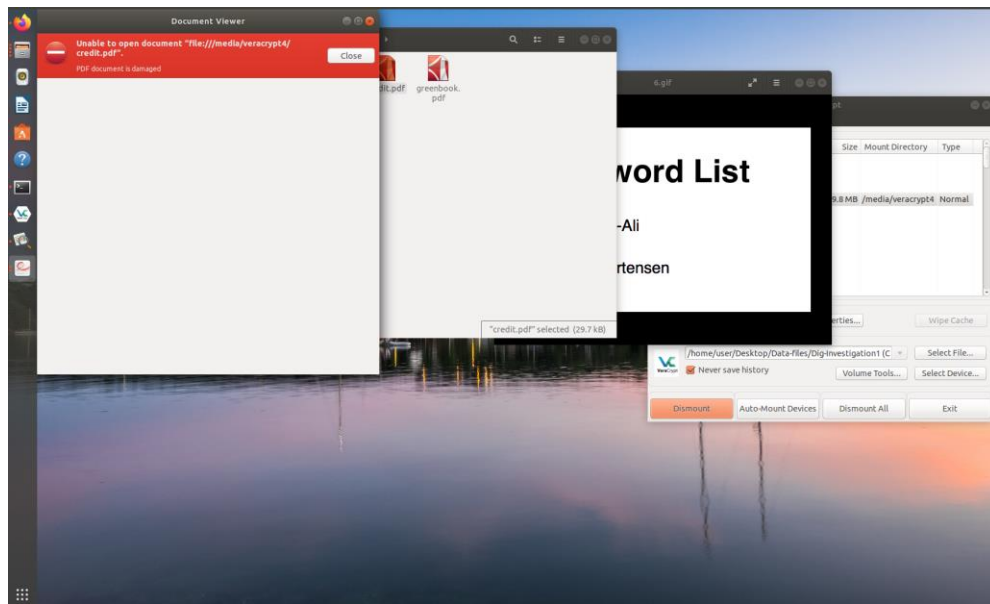


Figure 3.5

The decision was made to examine the file through the program HxD again to gain more intel. When examining in HxD it became apparent that this can't be a pdf due to exif string within the second line. (Refer to Figure 3.6) It was a jpg image not a pdf.

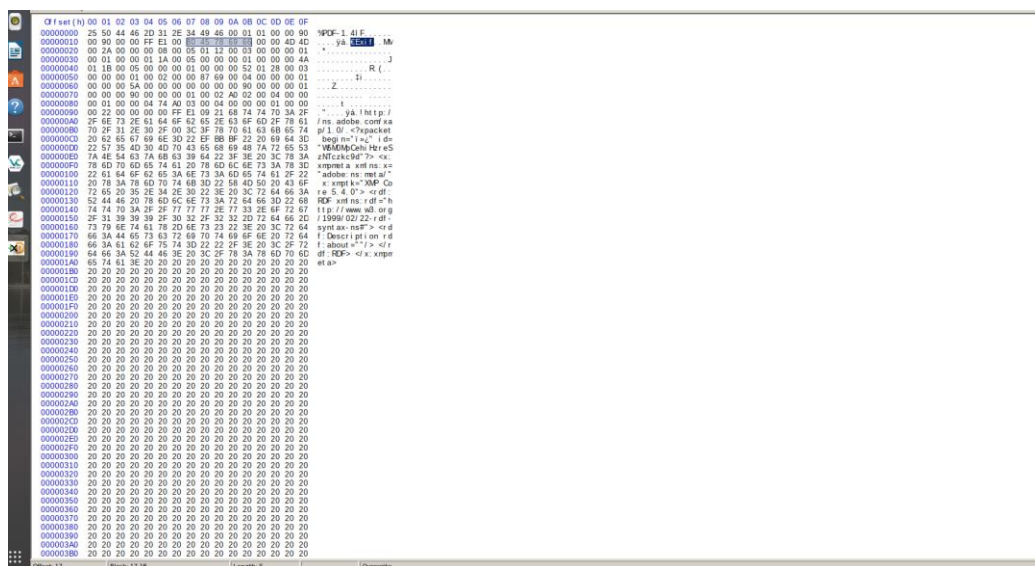
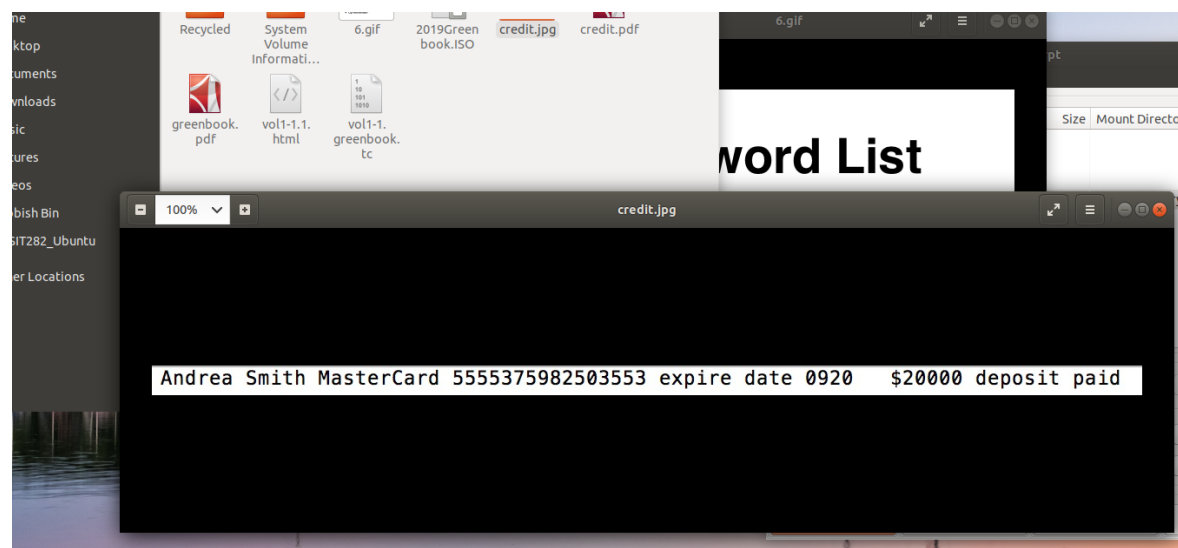


Figure 3.6

The plan after this discover was to restore the header done via replacement of the contents. Research was conducted to find the correct hex values assigned to a jpg image.



17. I was granted access to the image after the restoration of the header and the following results were found. It confirmed the transaction between the 2 individuals had taken place, total amount and credit card details used to make the transaction. This was the final step in forensic investigation stage.



3.3. *Details of Search Result and Conclusions*

As the lead digital investigator in this case, I can conclude the digital investigation a success. All the boxes were ticked in regards to the task at hand. We discovered the following that is regarded as crucial evidence in relation to this case:

- The image of the watercolour of two boats was discovered in Mr Price's files. It was alleged that Mr Donald Prince was responsible for the disappearance of this image.
- Through close inspection of the greenbook.pdf file a secret transaction of art was planned between Mr Prince and Andrea Smith, the secret transmission was communicated via email and the pair had been communicating prior to the disappearance. The email indicated Andrea Smith had made a financial offer of \$20,000 to Mr Prince to purchase the piece of art
- Evidence obtained through the reconstruction of the damaged file 'Credit.pdf'. indicated that transaction had gone through. This assumption is made through the containments of that image. It contained Anrea Smith's name, credit card details and total amount paid to Mr Prince which gives a strong indication that this piece of art is not missing it has in fact been sold privately to Mrs Smith for a financial sum which has been deposited into Mr Princes individual account.

Overall, this evidence indicates that Mr Prince has abused his employment powers at Joachim's art gallery to commit the act of employee theft and has privately/secretly without the business's consent/known sold the gallery's property to achieve a personal financial gain. He is a prime suspect in this case and the evidence achieve by investigating his work PC's CD-ROM drive proves him to be responsible for the art's disappearance from Joachim's Art Gallery.

4. **LEGAL IMPLICATIONS**

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

Cyber Act 2001:

Under Division 477 (Serious Computer Offences) It is focuses around the unauthorized Access, modification, or impairment with intent to commit a serious commonwealth, (Government, 2001) state or territory offence.

Under the act a person is guilty of an offence if the person:

- A) The person causes any unauthorised modification of data held in a computer and*
- B) The person knows the modification is unauthorized.*

Division 478.2 Unauthorised impairment held on a computer disk etc.

1. A person is guilty of an offence if;

- (A) The person causes any unauthorised impairment of the reliability, security or operation of data held on*
 - (i) A Computer disk or*
 - (ii) A Credit card or*
 - (iii) Another device used to store data by electronic means and*
- (B) The person intends to cause the impairment' and*
- (C) The person knows that the impairment is unauthorised (Government, 2001)*

This applies to Mr. Donald Prince as stated in the case brief, he was suspected for the disappearance of art work in his place of employment. He then wiped the hard drive of his office PC's CD-ROM drive. The case brief indicates that it was his office computers drive that was wiped not his personal computer, therefore the device did not belong to him making him unauthorized to modify the data held within the computers CD-ROM drive. He was not permitted by high up employees at the workplace to do such actions.

Donald Prince also knew that he was a suspected of this case due to the company suspending him, therefore whipping the hard disk of the work PC he was intending to cause impairment. He also knew that this impairment was unauthorised doing this action was an attempt to find evidence stored on the disk to get away with the crimes committed. Under Section 478.2 (Government, 2001) he has committed a violation of the Cybercrime Act 2001 and his actions are considered a serious computer offence. His penalty for his computer crimes would be at least 2 years imprisonment if found guilty by the CJS. He is also committing the crime of theft through the action of stealing art from the gallery. The art belonged to the company not him and is not his to sell.

Crimes Act 1958:

Section 254: Destruction of Evidence (Acts, 2008)

(1) A person who –

(a) Knows that a document or other thing of any kind is, or is responsibly likely to be, required in evidence in legal proceedings –

(b) Either –

(i) Destroys or conceals it or renders it illegible, undecipherable, or incapable of identification: or

(ii) Expressly, tacitly or impliedly authorises or permits another person to destroy or conceal it or render it illegible, undecipherable or incapable of identification and that other person does so: and

C Acts as described in paragraph (B) with the intention of preventing it from being used in a legal processing.

Mr Donald Prince can be charged with the crime of destruction of crime which is justifiable through section 254 of Crimes Act 1958 (Acts, 2008). He knew that there was evidence within his works PC drive and that it would be used to tie him into the disappearance of the Artwork. He attempted to destroy this evidence by whipping the hard disk before investigators were deployed to clear him of the crimes committed. This definition of the crime makes it justifiable for law enforcement to charge Mr Prince with this offence. He potentially could be charged with Handling of stolen goods as he sold the artwork for his own financial benefit. According to section 74 of the crimes act 1958(Acts, 2008) Mr Prince's actions fall under the crime of 'theft' due to stealing an object that did not belong to him but belong to his place of work this means he is liable to level 5 imprisonment.

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

Criminal Investigation:

This case is best suited to be pursued as a criminal investigation. This is due to criminal investigation have a broader definition in comparison to corporate investigation. The process of this case and the findings fall under the definition of a criminal investigation therefore this case I believe would be best suited to be a criminal investigation. Due to Mr Prince being individually responsible for the disappearance in conjunction with the private sale of the artwork to Anrea Smith \$20,000. All this evidence indicates it has to be a criminal investigation as corporate investigations are ineligible to proceed/take action as this crime was committed outside of the corporate environment. Therefore, the case is best suited to be treated as a criminal investigation.

References:

ACTIVE. (2016). JPG Signature Format Retrieved from <https://www.file-recovery.com/jpg-signature-format.htm>

Acts, V. C. (2008). CRIMES ACT1958. Retrieved from http://classic.austlii.edu.au/au/legis/vic/consol_act/ca195882/s74.html

Ellis, W. (2021). VeraCrypt Review. Retrieved from <https://privacyaustralia.net/veracrypt-review/>

Government, A. (2001). Cybercrime Act 2001. Retrieved from <https://www.legislation.gov.au/Details/C2004A00937>

Deakin University Lecture/Practical class notes Weeks 1, 2, 3 and 4