

# Assignment Submission Coversheet

Faculty of Science, Engineering and Built Environment



<b>Student ID:</b>	218478549
<b>Student Name:</b>	Justin Bland
<b>Campus:</b>	<input type="checkbox"/> Burwood <input type="checkbox"/> Waterfront <input type="checkbox"/> Waurin Ponds <input type="checkbox"/> Warrnambool <input checked="" type="checkbox"/> Cloud

<b>Assignment Title:</b>	Assessment Task 1		
<b>Due Date:</b>	11/August/2019	<b>Assessment Item:</b>	1
<b>Course Code/Name:</b>	S334 / Bachelor of Cyber Security		
<b>Unit Code/Name:</b>	SIT282 / Computer Crime and Digital Forensics	<b>Unit Chair / Campus Coordinator:</b>	
<b>Practical Group: (if applicable)</b>			

If this assignment has been completed by a group or team:

1. Each student in the group must complete and sign a separate coversheet
2. The assignment will be returned to the student in the group nominated below

<b>Assignment to be returned to:</b> (Student name and Student ID number)	
--	--

## PLAGIARISM AND COLLUSION

Plagiarism occurs when a student passes off as the student's own work, or copies without acknowledgement as to its authorship, the work of another person. Collusion occurs when a student obtains the agreement of another person for a fraudulent purpose with the intent of obtaining an advantage in submitting an assignment or other work. Work submitted may be reproduced and/or communicated for the purpose of detecting plagiarism and collusion.

## DECLARATION

I certify that the attached work is entirely my own (or where submitted to meet the requirements of an approved group assignment, is the work of the group), except where work quoted or paraphrased is acknowledged in the text. I also certify that it has not been previously submitted for assessment in this or any other unit or course unless permissions for this has been granted by the Unit Chair of this unit. I agree that Deakin University may make and retain copies of this work for the purposes of marking and review, and may submit this work to an external plagiarism-detection service who may retain a copy for future plagiarism detection but will not release it or use it for any other purpose.

<b>Signed:</b>	Justin Bland	<b>Date:</b>	12/01/2021
----------------	--------------	--------------	------------

An assignment will not be accepted for assessment if the declaration appearing above has not been signed by the author. If submitting electronically, print your full name in place of a signature.

<b>COMMENTS</b>			
<b>Mark Awarded:</b>		<b>Assessor's Signature:</b>	
		<b>Date:</b>	

A thick dark blue vertical bar runs down the left side of the page. A medium blue arrow points to the right, overlapping the bar, with the date '8/8/2019' written inside it in white.

8/8/2019

# Forensic Investigation Report

Joachim's Art Gallery

Several thin, curved lines in dark blue and light grey originate from the bottom left corner and sweep upwards and to the right, creating a dynamic, abstract design.

Report Prepared by: Justin Bland

Table of Contents

1. DIGITAL FORENSIC PROCEDURE ..... 4

1.1 Digital Evidence Form ..... 4

1.2 Description of Forensic Workstation and Image Download Procedure ..... 5

1.3 At Least Two SHA-based Hash Function Values of the ISO Image ..... 5

1.4 Explanation of the need for Multiple Hash Values to Verify Validity of Image File ..... 5

1.5 Explanation of Procedure used Before Accessing Image File in VM ..... 6

2. DESCRIPTION OF BINARY DETAILS ..... 7

2.1 Properties of the Undeleted Files Found on the ISO Image ..... 7

2.2 Description of Programs to be used to Perform Investigation..... 7

OUTCOMES OF DIGITAL FORENSIC INVESTIGATION ..... 7

Description and Justification of Key Words Used to Search ISO Image ..... 7

Document Procedure Including Appropriate Commands and Screenshots..... 8

Details of Search Result and Conclusions ..... 11

LEGAL IMPLICATIONS ..... 12

Possible Legislation Breaches ..... 12

Justification as to whether this Case is Best Pursued as a Corporate or Criminal Investigation..... 12

References ..... 13

Appendices ..... 13

## 1. DIGITAL FORENSIC PROCEDURE

## 1.1 Digital Evidence Form

<p align="center"><b>&lt;Place name of Investigative Unit here&gt;</b></p> <p align="center"><i>This form is to be used for only one piece of evidence.</i></p> <p align="center"><i>Fill out a separate form for each piece of evidence.</i></p>			
Case No:	Price_02082019	Unit Number:	Price_20
Investigator:	Justin Bland		
Nature of Case:	Theft of Property		
Location where evidence was obtained:	Accused Workplace		
Item # ID	Description of evidence	Vendor Name	Model No/Serial No.
	CD-ROM	Unknown	Unknown
Evidence Recovered by:	Justin Bland	Date & Time:	01/08/2019 @10:00
Evidence Placed in Locker:		Date & Time:	01/08/2019 @10:30
Evidence Processed by	Description of Evidence	Date & Time	
		Page __ of __ <	

### 1.2 Description of Forensic Workstation and Image Download Procedure

The forensics workstation consists of a physical system that is running Microsoft® Windows 10 Professional, then a Hypervisor (Virtual Box) runs various operating systems designed for the forensics tasks needed, in order to download the image file to the work directory of the virtual machine to perform the forensics analysis, the image was downloaded from the supplied Dropbox folder to a shared folder between the host operating system on the physical machine and the guest operating system in the hypervisor.

Physical System	
CPU	Intel Xeon E3-1231V3 Quad Core H/T @ 3.4GHz
RAM	Kingston 32GB DDR 3 Memory
Mainboard	Gigabyte Z97 Soc Force
Graphics	ATI Radeon RX570
Operating System	Windows 10 Pro x64
Storage	480GB Crucial SSD
Virtual System	
Operating System	Ubuntu 18.04

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

SHA256

068234ab49ac815c7d8d71220c5b20badad5cd08573c73cf755c22fbf26752e2

SHA512

e8814c02915b11c8d9e03a42daa6b3f7365707f2d6fb7ff2ba1107151214e21919cedd3037113c  
1acac67da1e1739fe7f00a8d192c5f4ecb4dbdcc9d4a3c7d35

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

Digital Evidence like physical evidence requires a means of identification in order to show that it has not been modified or altered, using multiple hash values to verify the validity of if an image file, is good proactive measure to ensure that the evidence has not been modified or altered.

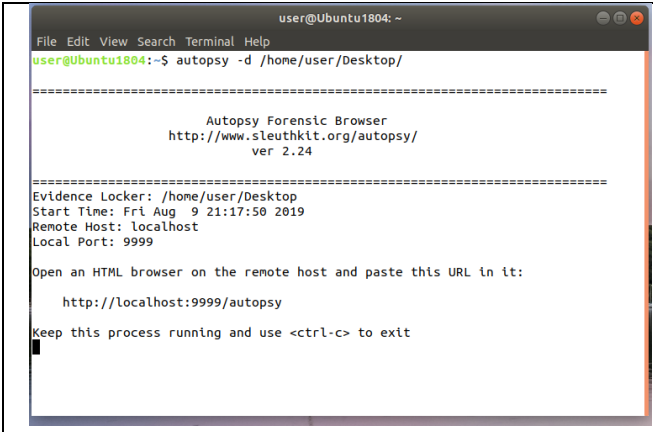
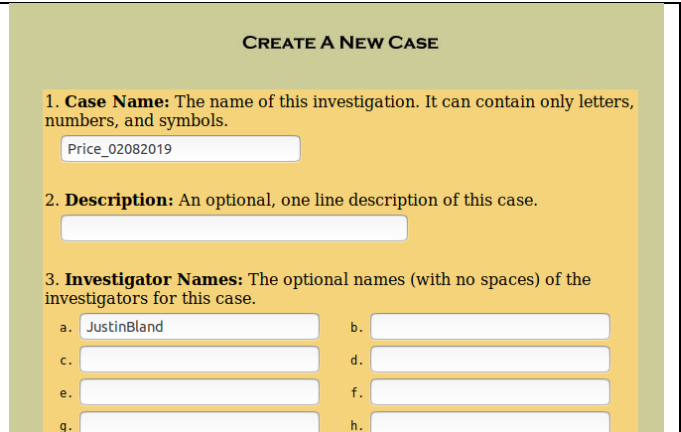
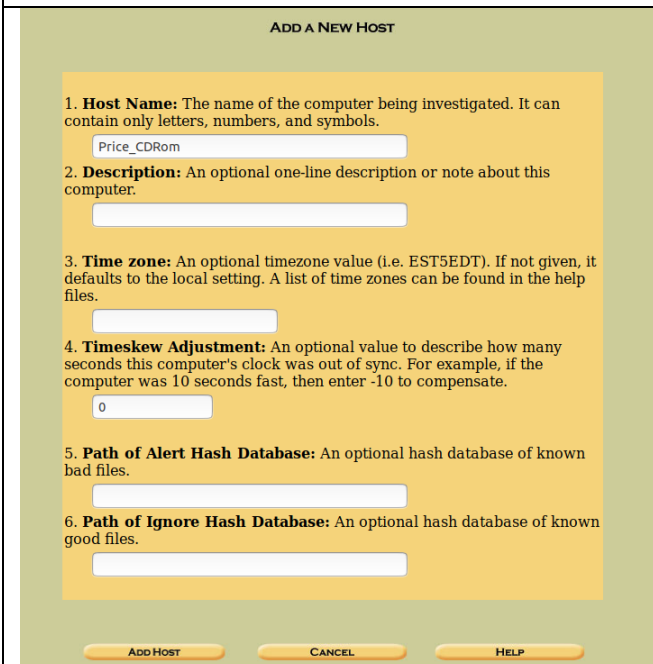
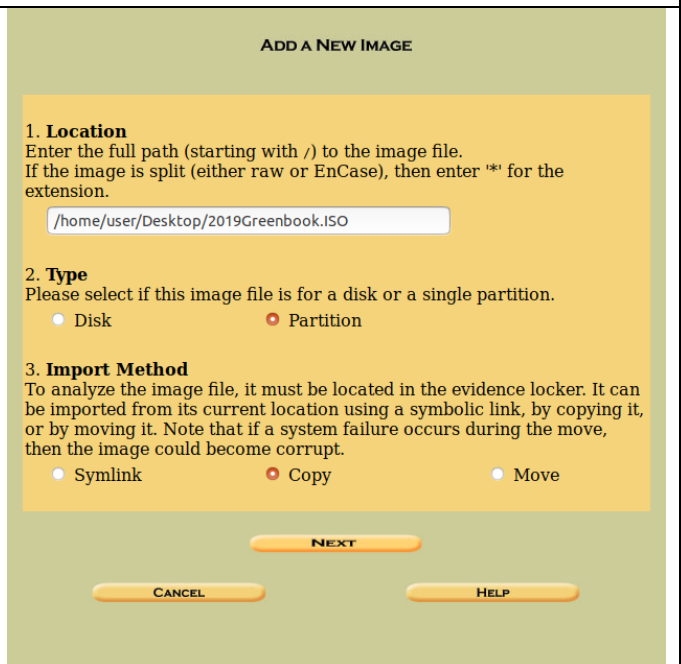
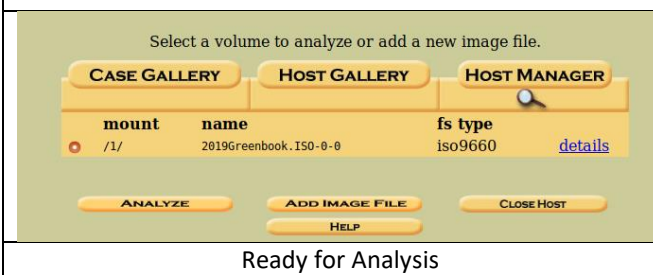
In particular to avoid issues due to those identified by an article published in 2004, *Xiaoyun Wang and Hongbo Yu of Shandong University* in China (Wang, 2005), where two different data sets of 128 bytes each, once hashed using MD5 produced the exact same hash value, although this hash collision is unlikely to occur in a real world setting, it could bring the validity of evidence in to question.

Using multiple hash values ensures that should it be possible for a hash collision to occur, there are safe guards in place to ensure the validity of the data, in my experience I have never seen a hash collision in “the wild”, a hash collision may occur with one hash value but is extremely unlikely with two or more separate hash values with differing hashing methods.

1.5 Explanation of Procedure used Before Accessing Image File in VM

In order to access the image file inside the virtual machine, it needed to be imported into the forensics software, in this case that was Autopsy 2.24 the achieve this the following steps were performed.

- Start Autopsy and specify working directory
- Open HTML browser and specify autopsy URL “http://localhost:9999/autopsy”
- Create a “New Case”, a “Host”
- Add the Image “2019GreenBook.ISO”
- Specify the Image Details and Mount Point
- The Image is now Ready to be Analysed

	
Starting Autopsy	Creating the Case
	
Adding a Host	Adding the Disk Image
	
Ready for Analysis	

## 2. DESCRIPTION OF BINARY DETAILS

### 2.1 Properties of the Undeleted Files Found on the ISO Image

<u>File Name</u>	<u>Physical Size</u>	<u>MD5 Hash</u>
1.html	11993	2a9d47cd337565ecbcd4556b85d675b2
1.jpg	119418	1831b1f5e0e5a22a1f9d5cbab2099f1b
2.jpg	129367	ae9ef080a292374a866d659abd55712f
3.jpg	183365	d3060c3925e2f21274c5d04ce465ef08
4.jpg	122717	30c58285a32ac6ff2232fe09cf8a11dd
5.jpg	232965	853bd591239b0225bbce59fdd7da1bc6
Greenbook-1937.pdf	5414500	1bcbf60d6f2629a35dabcb4bcf1b2071
greenbook.tc	83886080	39e0cc888b3d96fb07c411b4d52da1fa

### 2.2 Description of Programs to be used to Perform Investigation

In order to analyse the data in the disk image associated with this investigation, the following programs will be used.

Autopsy 2.24	To perform the initial analysis of the data
HashCalc	To create the SHA based hash of the disk image
JpHide and StegBreak	To Check the image files for any Steganographic data
HxD	View files in Raw format

## 3. OUTCOMES OF DIGITAL FORENSIC INVESTIGATION

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

### 3.2 Document Procedure Including Appropriate Commands and Screenshots

Initially the investigation started by analysing the disk image in Autopsy using the “File Analysis” tools built into autopsy. This showed a small selection of files including 1 html file, 5 images, a pdf and a .tc file that at this point I am unsure what this file is. At this point I also created a MD5 list of all files

Current Directory: /1/									
ADD NOTE		GENERATE MDS LIST OF FILES							
DEL	Type	NAME	ACCESSED	CREATED	SIZE	UID	GID	META	
dir / in									
d / d		\$orphansFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	0	0
d / d		لجند	0000-00-00 00:00:00 (UTC)	2019-07-16 13:04:11 (AEST)	2048	0	0	0	0
d / d		لجند	0000-00-00 00:00:00 (UTC)	2019-07-16 13:04:11 (AEST)	2048	0	0	0	0
r / r		1.html	0000-00-00 00:00:00 (UTC)	2019-07-16 13:03:53 (AEST)	11993	0	0	0	1
r / r		1.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 22:46:41 (AEST)	119418	0	0	0	2
r / r		2.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 22:47:56 (AEST)	129367	0	0	0	3
r / r		3.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:09:00 (AEST)	183365	0	0	0	4
r / r		4.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:12:12 (AEST)	122717	0	0	0	5
r / r		5.jpg	0000-00-00 00:00:00 (UTC)	2019-07-12 23:17:00 (AEST)	232965	0	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	0	7
r / r		greenbook.tc	0000-00-00 00:00:00 (UTC)	2019-07-16 13:00:28 (AEST)	83886080	0	0	0	8

#### File and Directory Listing

MD5 Values for files in /1/ (2019Greenbook.ISO-0-0)

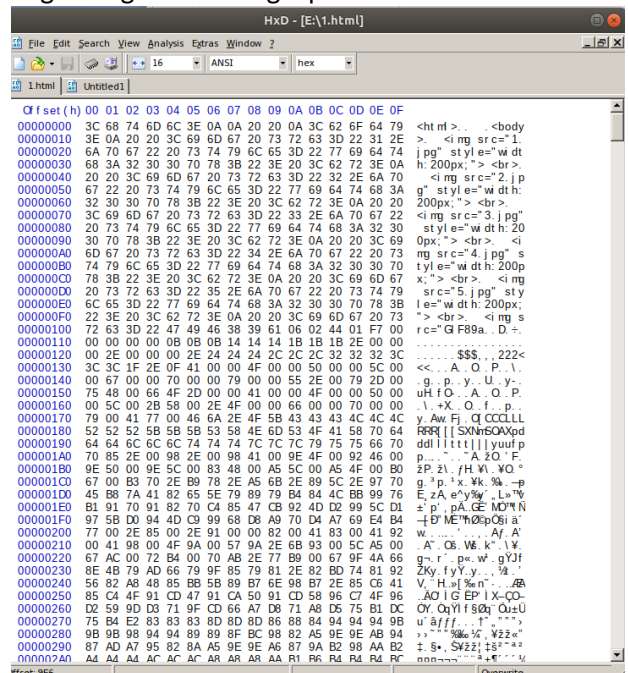
```

2a9d47cd337565ecbcd4556b85d675b2 - 1.html
1831b1f5e0e5a22a1f9d5cbab2099f1b - 1.jpg
ae9ef080a292374a866d659abd55712f - 2.jpg
d3060c3925e2f21274c5d04ce465ef08 - 3.jpg
30c58285a32ac6ff2232fe09cf8a11dd - 4.jpg
853bd591239b0225bbce59fdd7da1bc6 - 5.jpg
1bcbf60d6f2629a35dabcb4bcf1b2071 - Greenbook-1937.pdf
39e0cc888b3d96fb07c411b4d52da1fa - greenbook.tc

```

#### MD5 List of Files

After this initial analysis of the disk image, my next step was to analyse the file “1.html” after a basic inspection of this file it seemed that there was something not right with it, the file should be a .html file however most of the content of the file is not consistent with a html file, the content that is not consistent appears to be a .gif file embedded into a html tag. I then proceeded to remove all of the html specific content leaving only the .gif content, then I saved this content as a .gif file and the result was a .gif image containing a password list.



## Password List

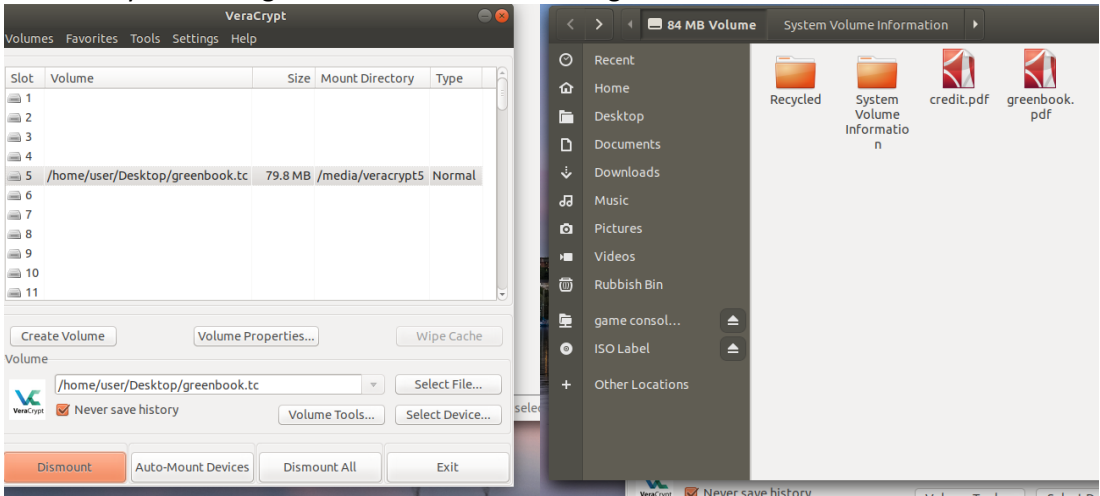
- Shirley-Ali
- Lip-Mortensen



The next step was to check the 5 images for any steganographic inclusions, using various tools each image was checked, the results are listed below.

- 1.jpg No Steganographic Results Found
- 2.jpg No Steganographic Results Found
- 3.jpg No Steganographic Results Found
- 4.jpg No Steganographic Results Found
- 5.jpg No Steganographic Results Found

After these steps were taken, I moved onto investigating the greenbook.tc file, this file appears to be an encrypted folder, using VeraCrypt I mounted and decrypted the folder using password “Shirley-Ali” found in the hidden .gif image, at this point I made an image of the folder to preform analysis on using Ubuntu’s built in disk manager.



I imported the image into autopsy for analysis and this folder contains what appears to be a corrupt .pdf, a password enabled .pdf a photo of the alleged stolen artwork and a few other files that haven’t been identified, along with six deleted files

r / r	C:/ MGP0248.JPG	2009-05-01 01:27:44 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 13:01:00 (AEST)	41215	0	0	6
r / r	C:/Recycled/ esktop.ini	2019-07-16 13:01:10 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 13:01:09 (AEST)	65	0	0	2041253
r / r	C:/Recycled/D11.JPG	2009-05-01 01:27:44 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 13:01:00 (AEST)	41215	0	0	2041256
d / d	C:/System Volume Information/ restore{68280360-D973-42C3-B19D-7B50A81F4C94}/ P21	2019-07-16 13:01:10 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 13:01:09 (AEST)	1024	0	0	2041317
r / r	C:/System Volume Information/ restore{68280360-D973-42C3-B19D-7B50A81F4C94}/ P21/change.log	2019-07-16 13:01:10 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 13:01:09 (AEST)	568	0	0	2041349
r / r	C:/ MGP0248.JPG	2009-05-01 01:27:44 (AEST)	2019-07-16 00:00:00 (AEST)	2019-07-16 14:21:34 (AEST)	41215	0	0	12

The files of interest here are the three .jpg files, after examining them I feel that the two MGP0248\*\*\* files are part of the same file, however I have not been able to re assemble them at this time.

After unlocking and inspecting the password protected .pdf file “Greenbook.pdf” (password was Lip-Mortensen) I found an inserted page that is not part of the original document this page appears to be an email from Andrea to Donald regarding an offer of \$20,000 for the artwork “Two Boats”.


Dear Donald,

Thanks for your letter. I am pleased to offer you \$20,000 for 'two boats'. If you agree, let me know and I will give you my cred phone me on 02-23174593.

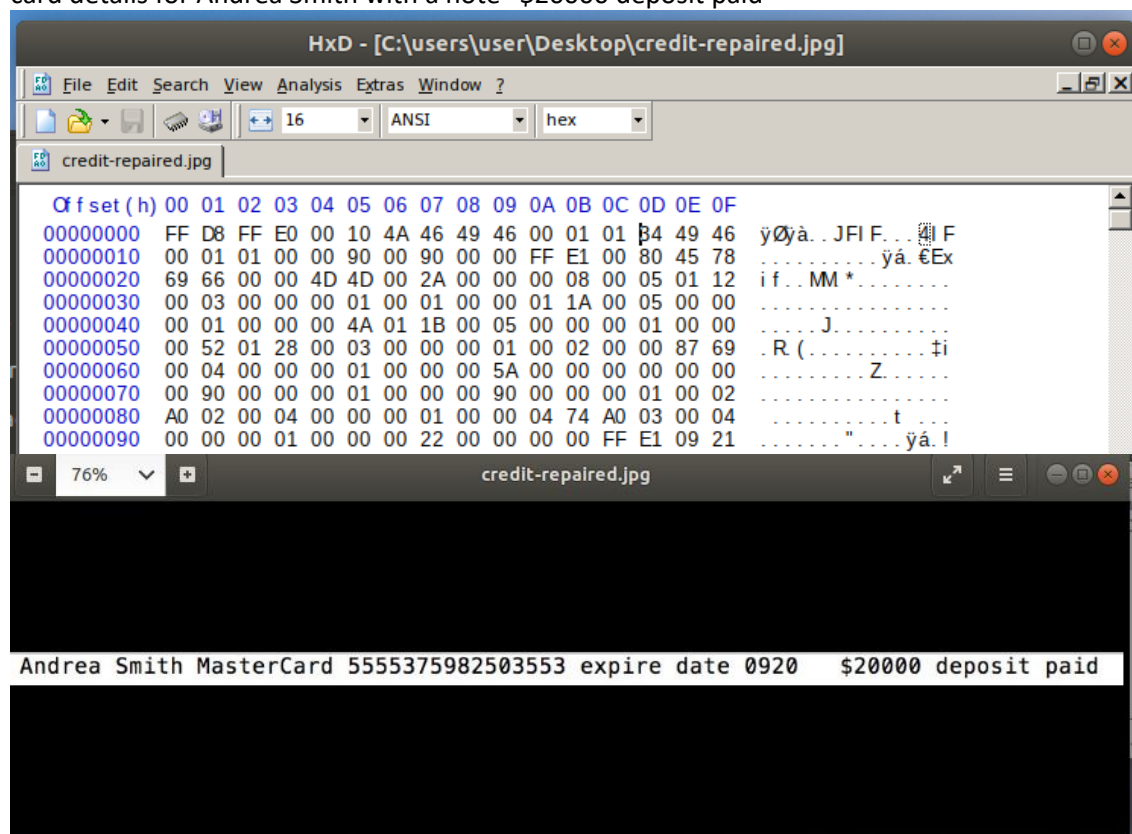
Best wishes,  
Andrea

Donald wrote the following message:

>>Dear Andrea,  
>>Please find the attached picture as a sample.  
>>  
>>Yours truly,  
>>Don  
>>



The next step was to investigate the corrupt credit.pdf file, after inspection of the file in HxD it appeared that the file was actually a .jpg image with a .pdf file extension and file header, after correcting the header and file extension to the correct format I found what appears to be credit card details for Andrea Smith with a note “\$20000 deposit paid”



After the analysis of the disk image, the next step was to check the image for any additional or

hidden partitions, while being a CD disk image it is unlikely to contain any of these sorts of partitions, however it is always good practice to check. This was done by mounting a copy of this disk image directly to the Linux virtual system and using built in partition manager in the operating system, this showed only one 90MB partition in CD Rom format ISO9660.



### 3.3 Details of Search Result and Conclusions

During this investigation there were several files found or recovered that show evidence of the theft of "Two Boats", these include

- A Photo of the artwork in question
- An Email pertaining to the sale of the artwork
- Credit Card details for payment

#### 4. LEGAL IMPLICATIONS

##### 4.1 Possible Legislation Breaches

Mr. Price allegedly wiped the hard drive of his work computer, perhaps in an attempt to hide incriminating evidence of his alleged involvement in the disappearance of the artwork involved, by doing this Mr. Price may have breached *Section 477.2 of the Cybercrime Act 2001*, this section refers to *Unauthorized Modification of Data to Cause Impairment*, which carries a prison term of up to 10 years if found guilty.

A lesser offence for this action could be *Section 478.2 of the Cybercrime Act 2001* which refers to *Unauthorised impairment of data held on a computer disk etc.* which if found guilty carries an imprisonment term of up to 2 years if found guilty.

Mr Price has also allegedly stolen artwork from his employer as evident by the evidence found during the forensic investigation supporting the charge. By doing this Mr. Price may have breached *Section 72 of the Crimes Act 1958 (VIC) Theft*, there are also provisions under *Section 73 of the Crimes Act 1958 (VIC)* for theft from an employer.

##### 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 at least on the part of the stolen artwork as there is clear evidence of Mr. Price's involvement and due to the value of the artwork "Two Boats" being around \$20,000 at least on the black market.

## References

Wang, X. & Y. H., 2005. *How to Break MD5 and Other Hash Functions*, Jinan 250100: Shandong University.

## Appendices