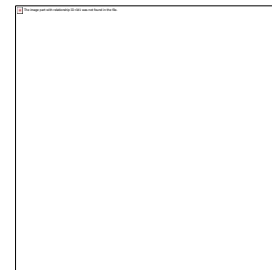


Assignment Submission Coversheet

Faculty of Science, Engineering and Built Environment



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

Assignment Title:	Assessment Task 2		
Due Date:	22 nd September 2019	Assessment Item:	2
Course Code/Name:	S334 / Bachelor of Cyber Security		
Unit Code/Name:	SIT282 / Computer Crime and Digital Forensics	Unit Chair / Campus Coordinator:	
Practical Group: (if applicable)			

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

Assignment to be returned to: (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.

Signed:	Justin Bland	Date:	22/09/2019
----------------	--------------	--------------	------------

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.

COMMENTS			
Mark Awarded:		Assessor's Signature:	
		Date:	



JUSTIN MICHAEL WILLIAM BLAND
Digital Forensic Procedure and Report

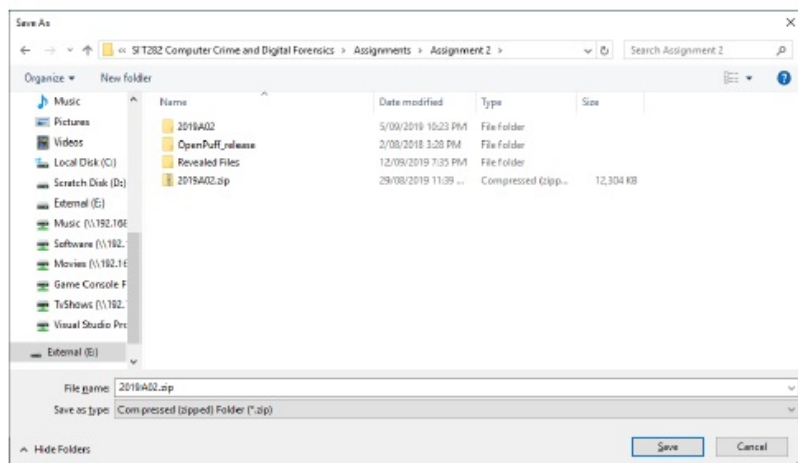
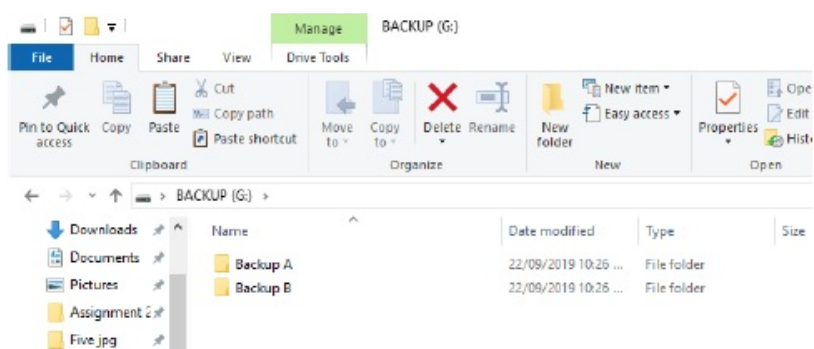
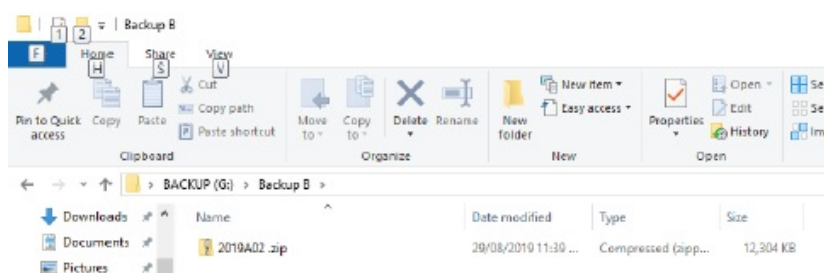
Table of Contents

DIGITAL FORENSIC PROCEDURE	4
1. Explain how you downloaded the file, what precautions you took, and how you ensured its integrity.....	4
2. Describe how you decrypt two given NTLM hash values by using OphCrack.	5
3. Describe the process that you apply to open the downloaded file.	5
4. Describe the actual content of the encrypted file that you identified.....	6
5. What tools will you now use to proceed your investigation and why?	6
6. Describe how your investigation proceeded at this point.	7
File: ONE.bmp	7
File: TWO.jpg	8
File: THREE.jpg	9
File: FOUR.png	10
File: Five.jpg	11
DIGITAL FORENSIC REPORT	12
Recommendations.....	12
Summary of steps that were performed.....	12
Brief description/summary of what was recovered.....	12
Interpretation of what was recovered in relation to the case	12
Appropriate suggestions on how a further investigation should proceed.....	12
Evidence Form	13

DIGITAL FORENSIC PROCEDURE

1. Explain how you downloaded the file, what precautions you took, and how you ensured its integrity.

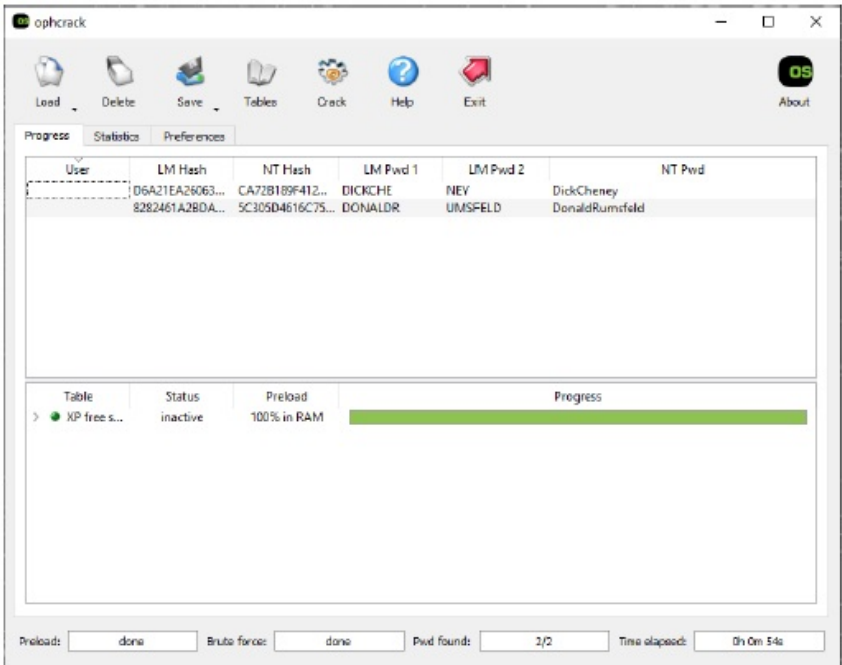
File Download Procedure	The file was downloaded from the secure email server, then the MD5 Hash was verified against the MD5 Hash in the secure email to ensure the file was correct.
Precautions Applied	The file was immediately backed up to two separate folders with one being an external flash drive, then a working directory was created on an Ubuntu virtual machine where the file was moved to for forensic analysis
Method used to ensure Integrity	All copies, working and backup copies had their MD5 Hash verified against the hash that is on record for this file

Downloading the file from the Secure ServerShowing Backup LocationShowing File in Backup Location

2. Describe how you decrypt two given NTLM hash values by using OphCrack.

The two given NTLM hash values were loaded into OphCrack as single hash values and checked against the Rainbow Table “XP Free Small”, using this table the software was able to decrypt both passwords.

D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A08176773 = DickCheney
8282461A2BDAF626E6067B973FDDC643:5C305D4616C7571D5DDC6EEA5BA5C395 = DonaldRumsfeld



3. Describe the process that you apply to open the downloaded file.

<p>Steps performed to open the file were:</p>	<p>In order to open the file “2019A02.zip” the password protection on the file needed to be cracked. To do this I used a program called “fcrackzip” to preform a dictionary attack on the file in order to obtain the password. This attack revealed the password is “vice”. After the password was obtained I was able to extract the .zip file.</p> <div><pre>user@Ubuntu1804: ~/Desktop/Assignment 2 File Edit View Search Terminal Help user@Ubuntu1804:~/Desktop/Assignment 2\$ fcrackzip -u -D -p '/usr/share/dict/american-english' 2019A02.zip PASSWORD FOUND!!!!: pw == vice user@Ubuntu1804:~/Desktop/Assignment 2\$</pre></div>
---	---

4. Describe the actual content of the encrypted file that you identified.

Content description		Assorted Images
File Name	File Type	MD5 Hash Value
ONE.bmp	Bitmap Image	ab873ec4d5c826db5d337f5f287006d5
	This image contains four people (2 men and 2 women) addressing a crowd of people from a podium with two US Flags and a blue back drop in the background	
TWO.jpg	JPEG Image	4da131832b963f03f990d4c545b2d533
	This image contains two people (a man and a women) sitting at a large desk/conference table with what appears to be US Government "Classified" documents In front of them on the desk	
THREE.jpg	JPEG Image	004b451689688f2d9bb83fb3fc5607aa
	This image contains six people (all men) walking in a desert with a 4x4 in the background	
FOUR.png	PNG Image	ac88ed263a80632167102c93a966f655
	This image contains a man in a suit standing in front of a US Flag	
FIVE.jpg	JPEG Image	815025ac61891bf35ea4f38d7c543db0
	This image contains the men in suits standing in front of a desk, with a window with bright yellow curtains, and a US Seal style flag (possibly the White House Seal)	

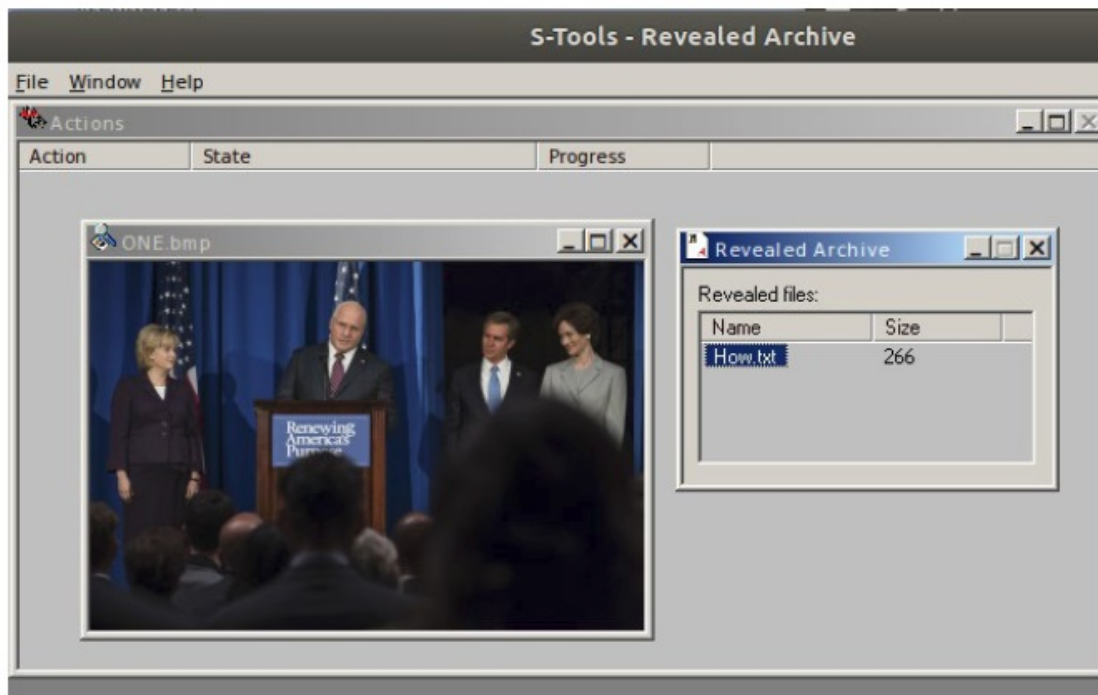
5. What tools will you now use to proceed your investigation and why?

Tool	Reason
OphCrack	OphCrack will be used to decode NTLM hash values
StegDetect	StegDetect will be used initially in an attempt to identify any Steganographic inclusions in the image files from the password protected .zip file
OpenPuff	OpenPuff will be used to retrieve any Steganographic Inclusions
HxD	HxD will be used to inspect the files for manipulation at a manual HEX level
BinWalk	BinWalk will be used to examine the files for "extra" included data
FCrackZip	FCrackZip will be used to perform a dictionary attack in an attempt to crack the .zip file


6. Describe how your investigation proceeded at this point.

File: ONE.bmp

Initially during the analysis of the file ONE.bmp StegDetect and BinWalk did not detect any Steganographic inclusions, however after viewing the file in HxD it appeared there was something hidden in the file. Being a .bmp file I decided to try using S-Tools on the file, I was successfully able to retrieve the file "How.txt" from the file using the password "DickCheney" and "IDEA" Encryption algorithm.



S-Tools Revealed Archive – Showing the file in the Image

Open ▾  **How.txt**
~/Desktop/Assignment 2/Revealed Files

This file is inside something

A password list is hidden by using a NTLM password|

The Openpuff configuration is hidden behind something

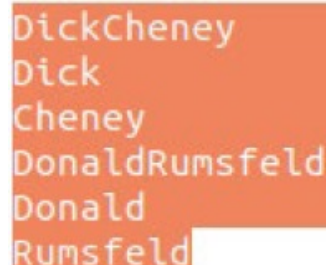
A list of numbers is hidden inside something

A list of names is encrypted by using 128-bit AES and a simple cipher

The Contents of How.txt

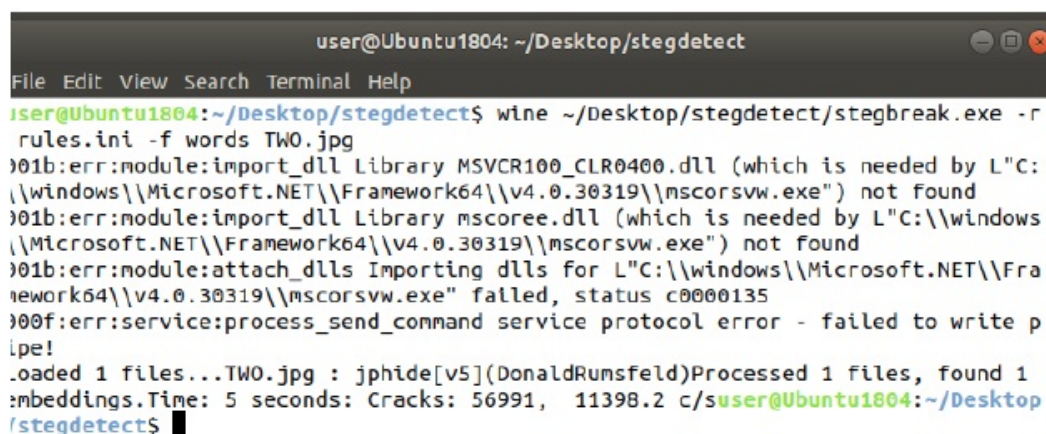
File: TWO.jpg

During the analysis of TWO.jpg “BinWalk” did not detect any steganographic inclusions, however I added the two decrypted NTLM hashed passwords found on the evidence computer into the detection words file for “StegDetect” in various forms, after adding these detection words “StegDetect” detected there was one inclusion using the password “DonaldRumsfeld”, using JP-Seek and this password I was able to extract a text file that contained a list of what appears to be six passwords.



DickCheney
Dick
Cheney
DonaldRumsfeld
Donald
Rumsfeld

Inclusion of Deciphered NTLM Hash into Words List



```
user@Ubuntu1804: ~/Desktop/stegdetect
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/stegdetect$ wine ~/Desktop/stegdetect/stegbreak.exe -r
rules.ini -f words TWO.jpg
01b:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:
:\windows\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe") not found
01b:err:module:import_dll Library mscorlib.dll (which is needed by L"C:\windows
\Microsoft.NET\Framework64\v4.0.30319\mscorlib.exe") not found
01b:err:module:attach_dlls Importing dlls for L"C:\windows\Microsoft.NET\Fra
mework64\v4.0.30319\mscorlib.exe" failed, status c0000135
00f:err:service:process_send_command service protocol error - failed to write p
ipe!
Loaded 1 files...TWO.jpg : jphide[v5](DonaldRumsfeld)Processed 1 files, found 1
:embeddings.Time: 5 seconds: Cracks: 56991, 11398.2 c/suser@Ubuntu1804:~/Desktop
/stegdetect$
```

“StegDetect” detection of hidden file



Unitary
Executive
ChristianBale
AmyAdams
AlisonPil
LilyRabe

Contents of Hidden File

File: THREE.jpg

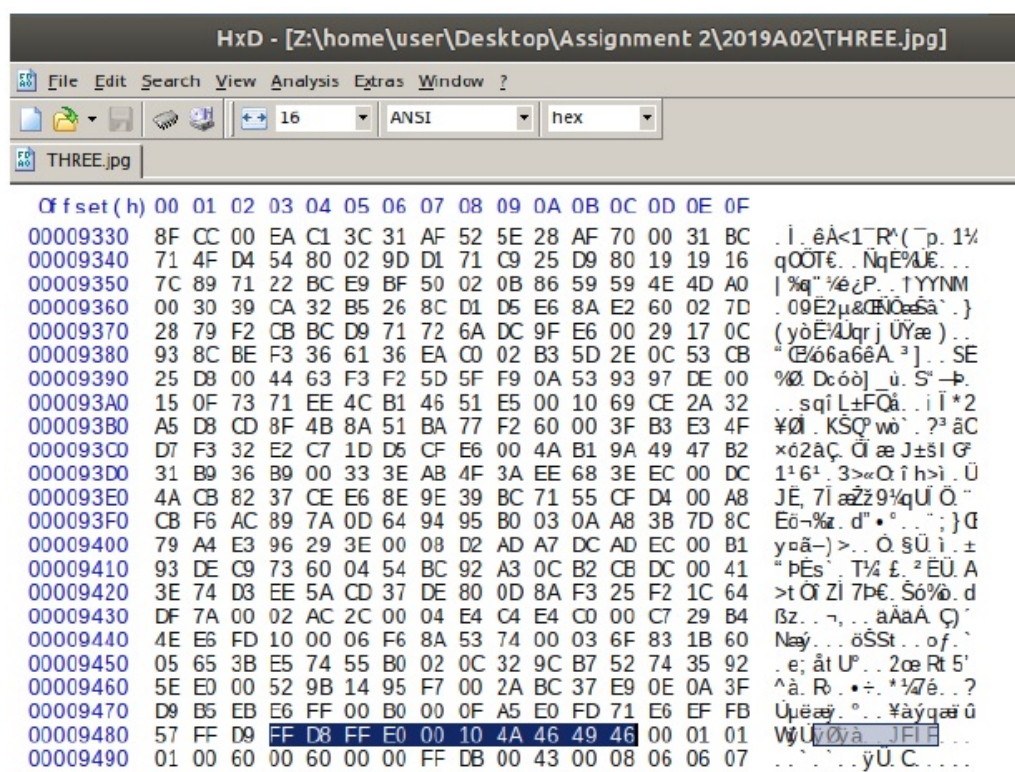
During the analysis of file "THREE.jpg" after StegDetect indicated there were no steganographic inclusions and the files header and footer seemed intact, I ran the file through "BinWalk" which indicated that there were 4 .jpg files in this file. After verifying this I found four separate header and footer inclusions for a .jpg file. I then proceeded to separate the files by copying the raw data from each file into a new file.

This successfully separated all four images, the first image was the original carrier image and then the three other .jpg inclusions were identical, an "OpenPuff" configuration containing three different passwords for extracting an image from another carrier image, the passwords included in this file are three of the six passwords hidden in the TWO.jpg, it might be reasonable to assume the other three passwords could be a second "OpenPuff" configuration set.

```
user@Ubuntu1804:~/Desktop/Assignment 2/2019A02$ binwalk -e THREE.jpg
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.02
38019	0x9483	JPEG image data, JFIF standard 1.01
44556	0xAE0C	JPEG image data, JFIF standard 1.01
51093	0xC795	JPEG image data, JFIF standard 1.01

"BinWalk" analysis of THREE.jpg



Verification of multiple .jpg files in carrier file

OpenPuff Configuration

Password A: "AmyAdams"
Password B: "AlisonPil"
Password C: "LilyRabe"

Retrieved Data from carrier file

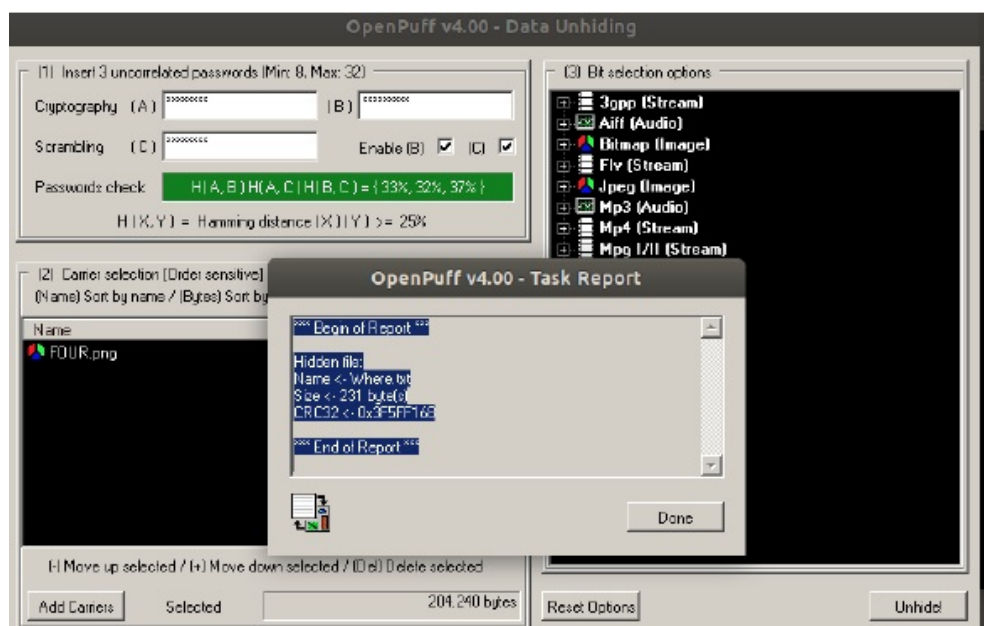
File: FOUR.png

The analysis of this file was pretty straight forward, “BinWalk” detected there was an inclusion in the carrier file, as the last file contained an “OpenPuff” configuration I decided to try that configuration on this file in an attempt to recover the inclusion.

This was successful and I was able to retrieve a text file (Where.txt) with what appears to be a list of 15 Australian mobile phone numbers

```
user@Ubuntu1804:~/Desktop/Assignment 2/2019A02$ binwalk -e FOUR.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 2041 x 3000, 8-bit/color RGB, non-interlaced
62	0x3E	Zlib compressed data, compressed

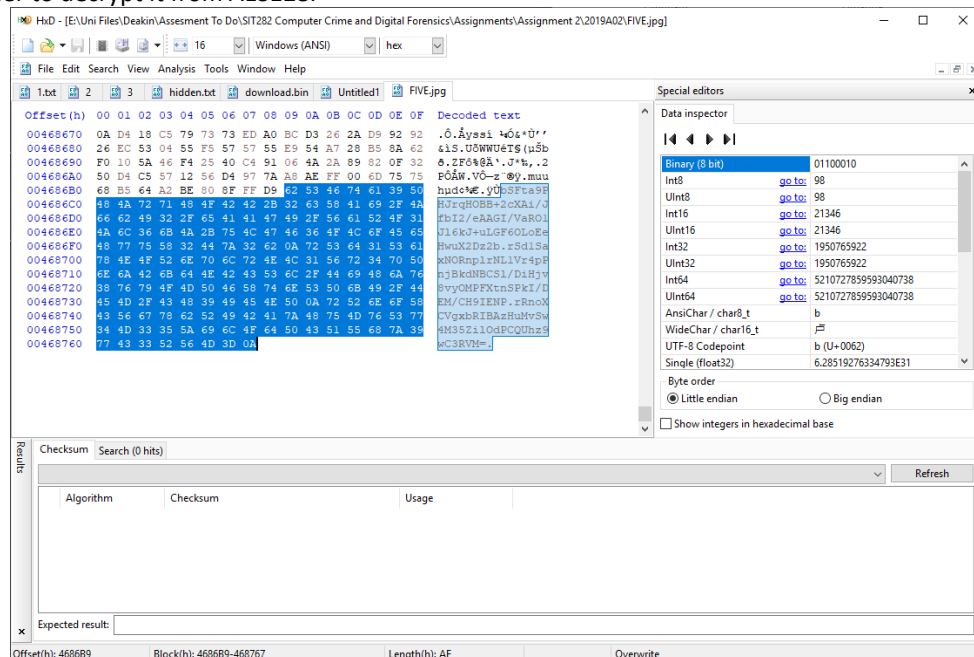
“BinWalk analysis of the file FOUR.png“OpenPuff” File Extraction

```
1. 0409267531
2. 0412563993
3. 0500287456
4. 0416327897
5. 0400286482
6. 0486375296
7. 0500374092
8. 0483956280
9. 0484974488
10. 0429846759
11. 0500329674
12. 0492695873
13. 0402389756
14. 0423940785
15. 0478822256
```

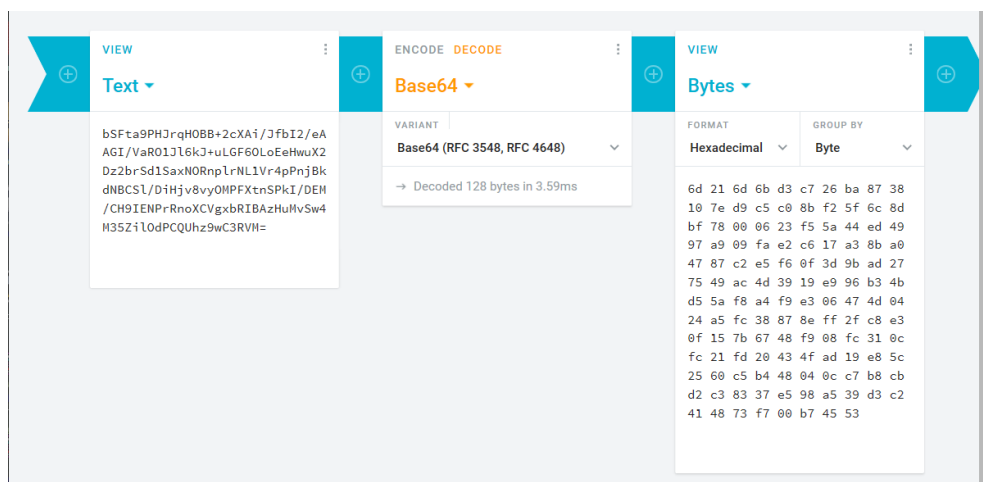
Contents of Where.txt

File: Five.jpg

The analysis of this file in HxD showed there was hidden content at the end of the file after the end of the jpg file footer "FF D9". this data appears to be encrypted; the first step was to decode the data from base64 in order to decrypt it from AES128.



Showing the Hidden Data



Decoding the Base 64 Data

DIGITAL FORENSIC REPORT

Recommendations

I would recommend another investigator to follow my procedures listed in the Digital Forensic Procedure document to verify my findings and to ensure that nothing has been missed or overlooked, the information found in the images FOUR.png and FIVE.jpg should be forwarded on to Team member Moti for further (Police) investigation.

Summary of steps that were performed

- Downloaded the file from the Secure Server
- Made Backup Copies
- Decrypted the two NTLM Hash Values
- Performed Dictionary Attack on .ZIP file and obtained password
- Analysed Contents of .Zip file (Five image files)
 - Retrieved hidden file from ONE.bmp using a NTLM password using S-Tools
 - Retrieved hidden file from TWO.jpg using a NTLM password using StegDetect
 - Retrieved 3 Hidden files from THREE.jpg by extracting the binary data that was included at the end of the carrier binary file.
 - Retrieved hidden file from FOUR.png by using OpenPuff and configuration found in THREE.jpg
 - Retrieved hidden encrypted file from FIVE.jpg (Still haven't Decrypted it)

Brief description/summary of what was recovered

2019A02.zip

This file contained five image files, ONE.bmp, TWO.jpg, THREE.jpg, FOUR.png and FIVE.jpg

ONE.bmp

This file contained a text file "How.txt" which contained a brief summary of what each file contained

TWO.jpg

This file contained a text file which contained six passwords

THREE.jpg

This file contained three identical .jpg image files, all of which were an OpenPuff configuration file

FOUR.png

This file contained a text file "Where.txt" which contained fifteen phone numbers

FIVE.jpg

Interpretation of what was recovered in relation to the case

The majority of the data that was recovered in one way or another was related to extracting the data hidden in the files FOUR.png and FIVE.jpg, which appears to be contact details for fifteen people. Given where the data was recovered from (an alleged drug manufacturing location) it is reasonable to assume that the contact information recovered in these files is linked to the manufacturing operation.

Appropriate suggestions on how a further investigation should proceed

From a Digital Forensic point of view, the investigation should proceed by verifying the results of the data found, then pass the results along to Team member Moti for further investigation (Police).

Evidence Form

<p align="center"><Place name of Investigative Unit here> This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.</p>			
Case No:	RMADRG100519	Unit Number:	001
Investigator:	Sandra / Justin Bland		
Nature of Case:	Criminal Activity (Drug Related)		
Location where evidence was obtained:	CD Located At Crime Scene		
Item # ID	Description of evidence	Vendor Name	Model No/Serial No.
01	Compact Disc (CD)	N/A	N/A
Evidence Recovered by:	Moti	Date & Time:	10/05/2019: 03:17
Evidence Placed in Locker:	Sandra	Date & Time	10/05/2019: 10:00
Evidence Processed by	Description of Evidence	Date & Time	
Justin Bland	CD Image Containing Password Protected. Zip Archive	26/09/2019: 12:00	
		Page 1 of 1	