

SIT282 Computer Crime and Digital Forensics
ASSIGNMENT 3

Report Title: Forensic Analysis of Suspected Drug Manufacturing Operation

Table of Contents

1. *Digital Forensic Procedure*
 - *File download procedure*
 - *Precautions applied*
 - *Method to ensure integrity*
2. *Decrypting NTLM hash values*
3. *Process to open downloaded file*
4. *Contents of extracted files*
5. *Tools for further investigation*
6. *Investigation progress with screenshots*
7. *Digital forensic report*
 - *Recommendations*
 - *Summary of steps*
 - *Brief description of recovered items*
 - *Interpretation of recovered items*
 - *Suggestions for further investigation*
8. *Evidence forms*

Investigator Name: Nirosh Ravindran

DIGITAL FORENSIC PROCEDURE

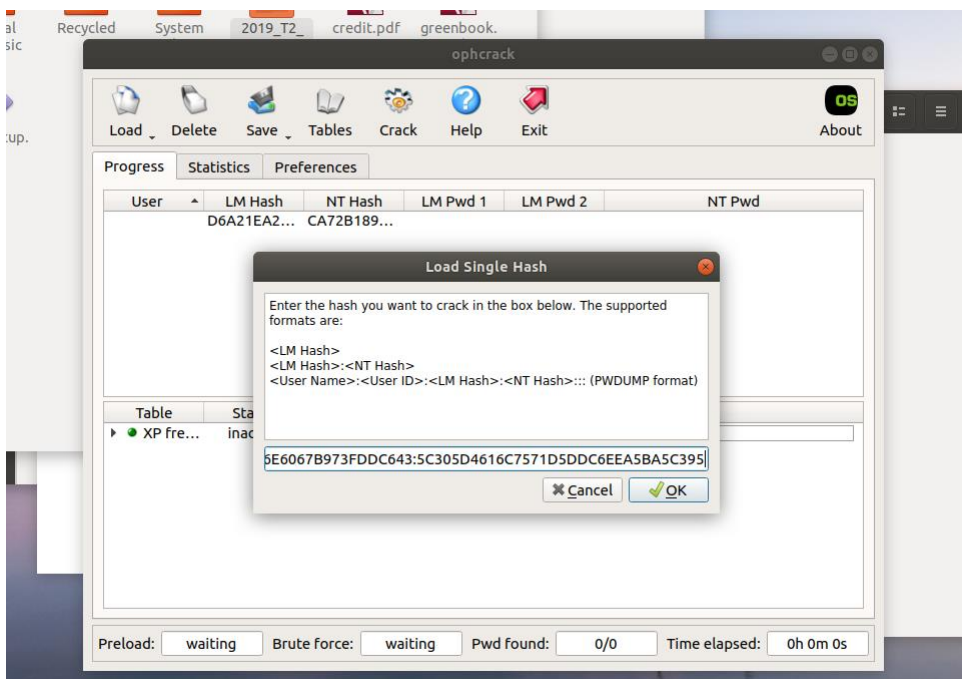
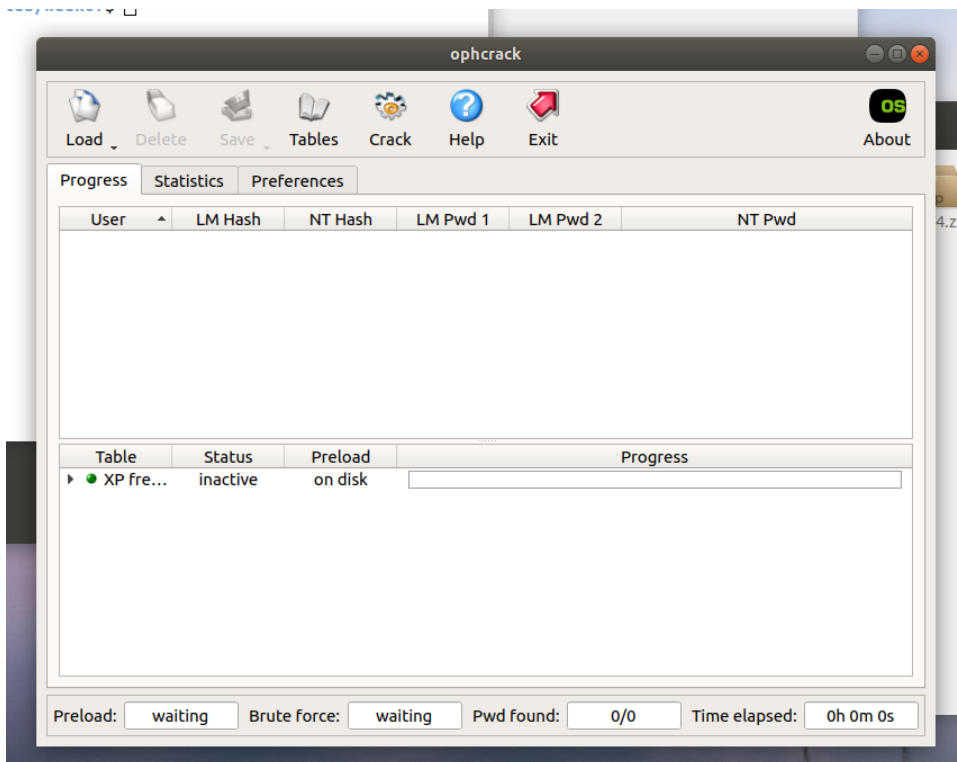
1. Explain how you downloaded the file, what precautions you took, and how you ensured its integrity.

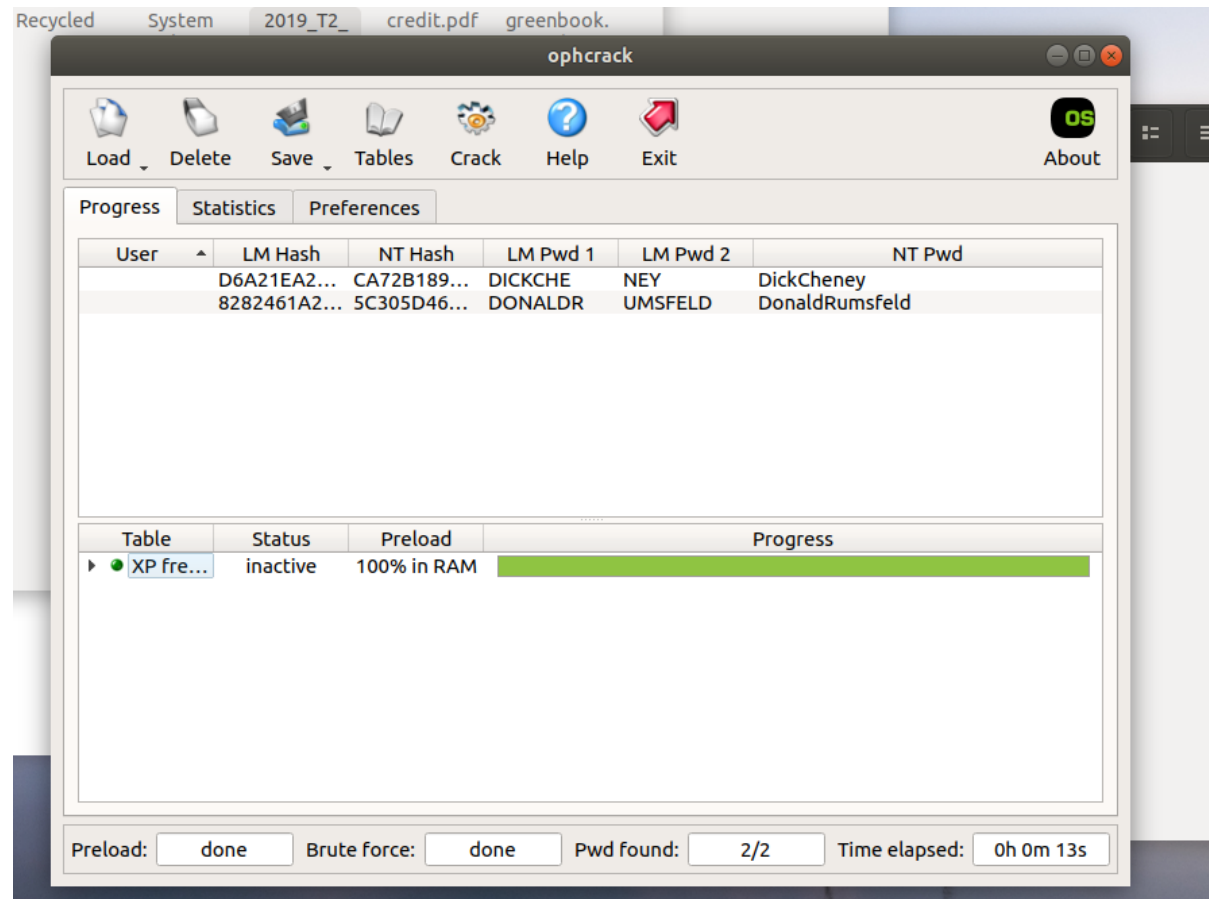
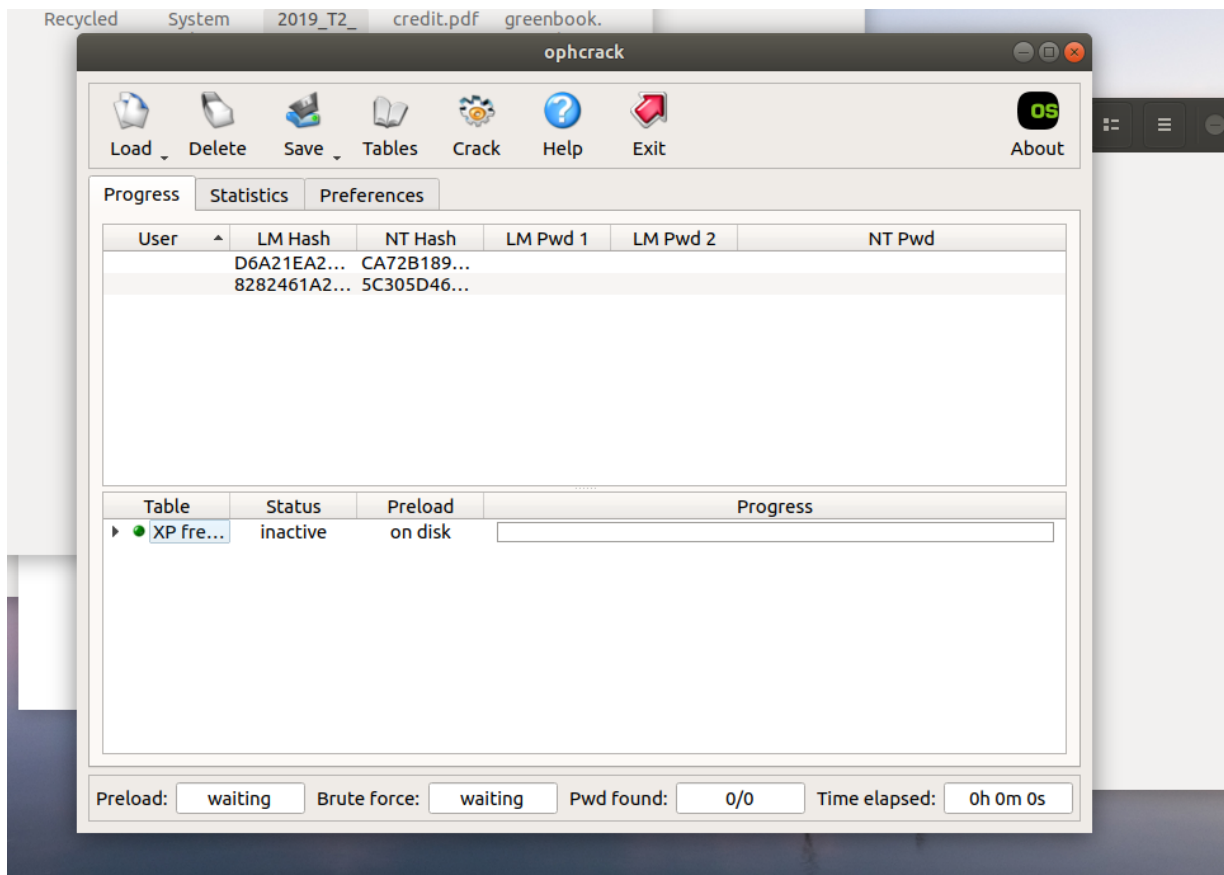
File Download Procedure	I downloaded the zip file from the link http://www.deakin.edu.au/~zoidberg/2019A02.zip
Precautions Applied	<p>I made sure my antivirus software was up-to-date and was active during the download process.</p> <p>I ensured the download took place over a secure network connection.</p> <p>Used a dedicated, isolated lab environment to prevent potential contamination and any security risks to my main system.</p>
Method used to ensure Integrity	I verified the md5 hash value of the executable file within the ZIP archive to be 9ec1c8f62429182349f3979c39aed8fb, ensuring the file was not tampered with during the download.

```
user@Ubuntu1804:~/Desktop/Data-files/ass 2$ md5deep 2019A02.zip
9ec1c8f62429182349f3979c39aed8fb /home/user/Desktop/Data-files/ass 2/2019A02.zip
user@Ubuntu1804:~/Desktop/Data-files/ass 2$ █
```

2. Describe how you decrypt two given NTLM hash values by using OphCrack, including screen shots.

- First, I loaded the NTLM hashed into the OphCrack tool.
- Then, I used the rainbow table in that came default with the OphCrack tool.
- Finally, I initiated the decryption process and waited for the hashes to be cracked.
- the first hash value
D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A0817677
3 was decrypted into **DickCheney**
- the second hash value
8282461A2BDAF626E6067B973FDDC643:5C305D4616C7571D5DDC6EEA5BA5
C395 was decrypted into **DonaldRumsfeld**

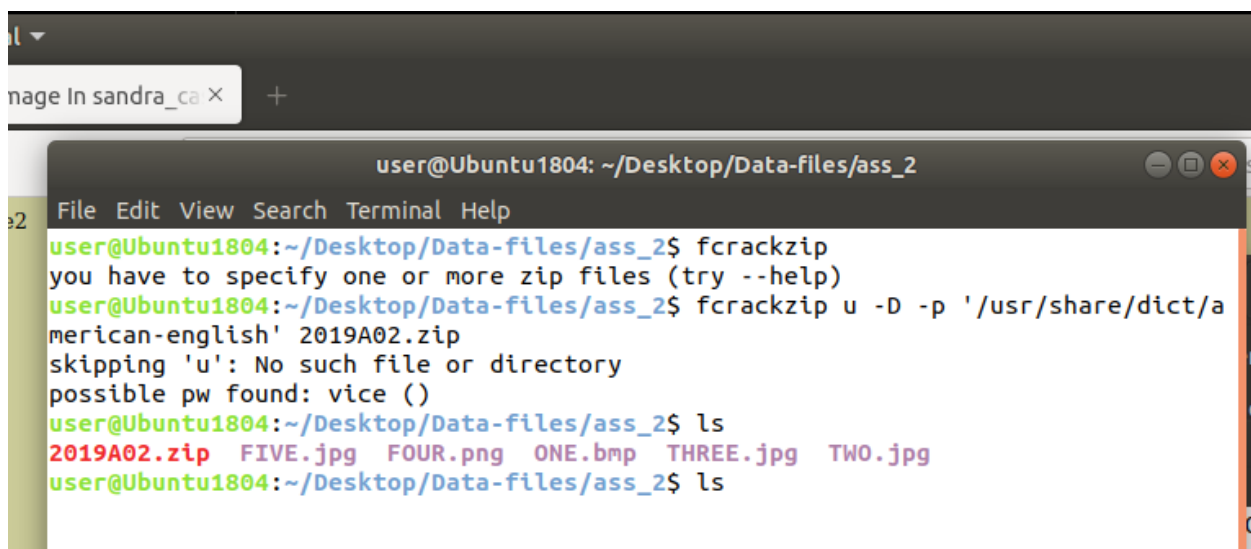




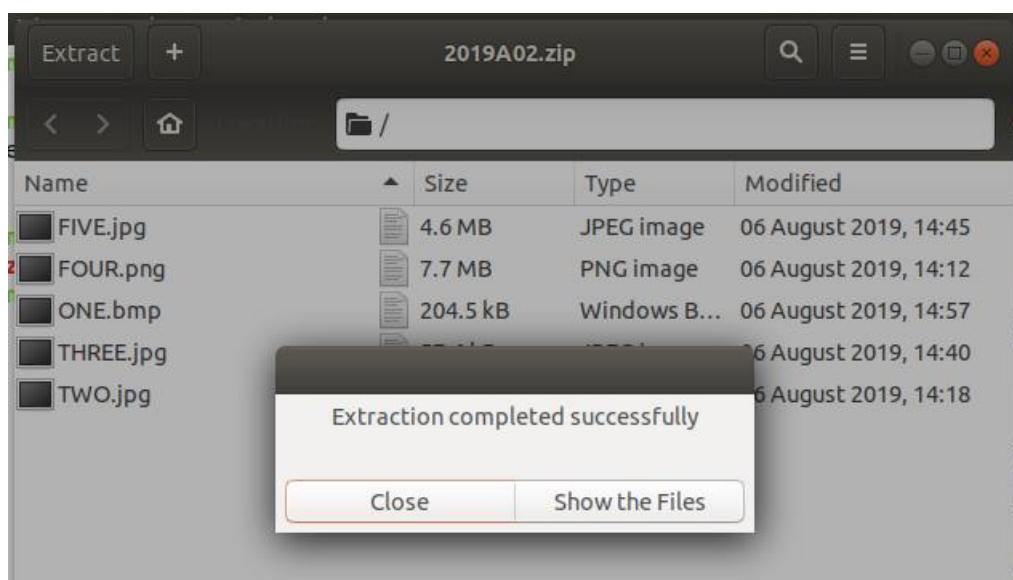
3. Describe the process that you apply to open the downloaded file. Describe whether there is a relationship between this process and the information obtained in Step 2.

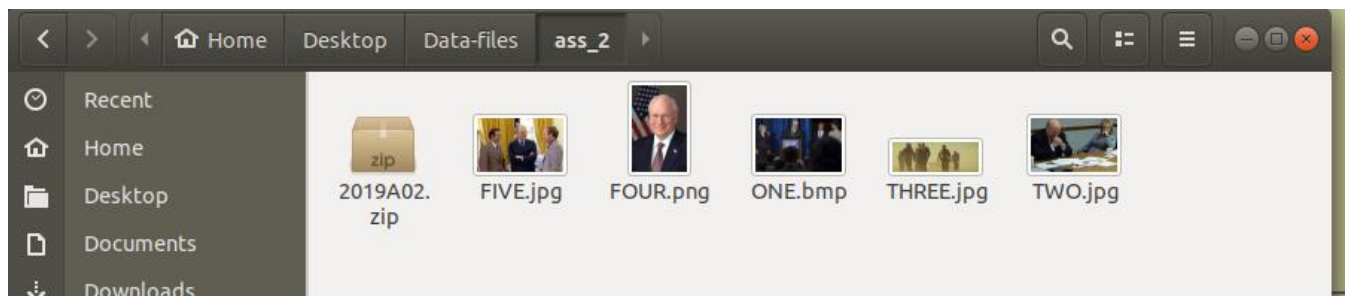
Steps performed to open the file were:	<ol style="list-style-type: none">1. I extracted the contents of the zip file using fcrackzip tool.2. For that, I first, brute forced the ZIP file using the word list american-english.3. Then the password was found using brute forcing. It was vice4. Then, I opened the ZIP file, it asked for a password since it was password protected. I typed the password vice.5. Finally, the files inside the ZIP file got extracted and was in a viewable format.
--	--

There is a relationship between the decrypted NTLM hashes and how to open the downloaded file because of the thorough technique used in the investigation. Even though the passwords derived from the NTLM hashes weren't used to unlock the ZIP file, recording this process is essential since it demonstrates a comprehensive investigation of all potential entry points and there are possibilities of these passwords being used later. In the end, brute forcing was required to open the ZIP file, highlighting the importance of adaptability and a variety of techniques in digital forensic investigations.



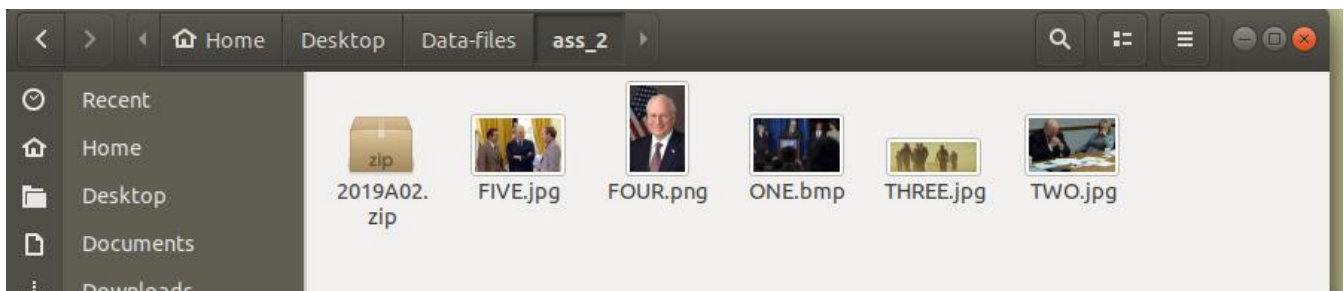
```
user@Ubuntu1804: ~/Desktop/Data-files/ass_2
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ fcrackzip
you have to specify one or more zip files (try --help)
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ fcrackzip u -D -p '/usr/share/dict/a
merican-english' 2019A02.zip
skipping 'u': No such file or directory
possible pw found: vice ()
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ ls
2019A02.zip FIVE.jpg FOUR.png ONE.bmp THREE.jpg TWO.jpg
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ ls
```





4. Describe the actual content of the encrypted file that you identified in Step 3. If there are multiple files, list their file names, types and MD5 hash values. Describe the visual contents in each file.

Content description	<p>The actual files that were extracted from the downloaded ZIP files were image files. There were totally 5 image files extracted.</p> <p>In the ONE.bmp file it was a group of people on a stage. Looks like white house's speech giving stage. Then I observed that it was from the movie called Vice.</p> <p>In the TWO.jpg file there were two people sitting near a table being anxious about something while looking down at a file on the table. This was also a scene from the movie Vice.</p> <p>In the THREE.jpg file I saw a group of people walking on a sandy place. This was also a scene from the movie called Vice.</p> <p>In the FOUR.png file, I saw an elderly person face.</p> <p>In the FIVE.jpg, there were a group of three people discussing something.</p>
---------------------	---

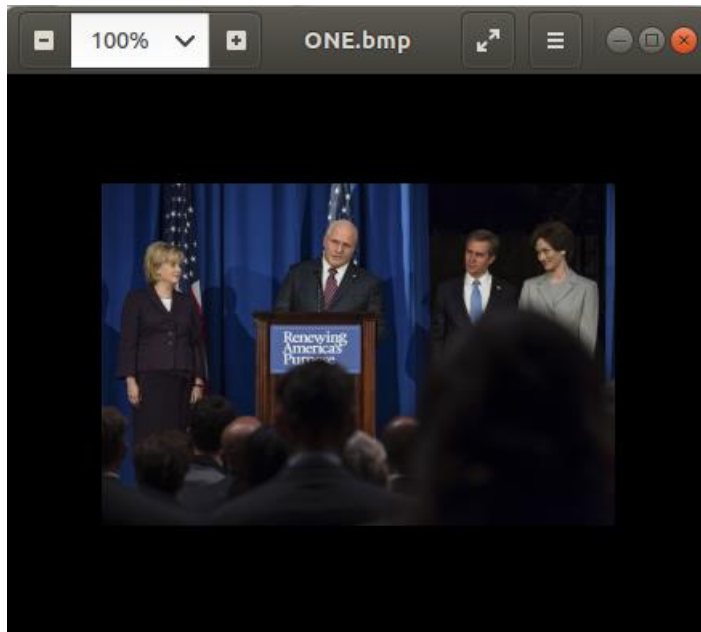


```

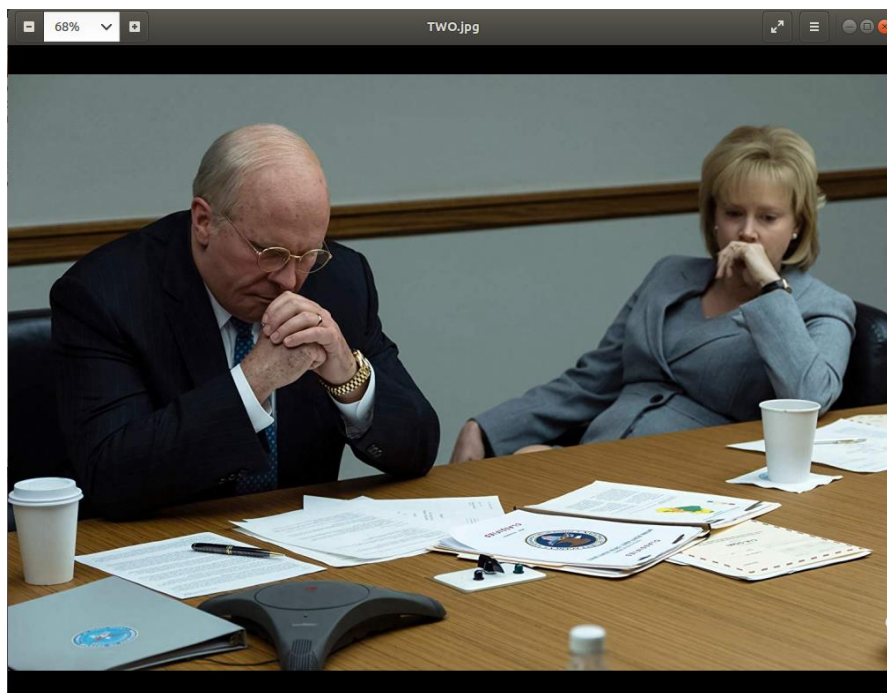
user@Ubuntu1804: ~/Desktop/Data-files/ass_2
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ md5deep ONE.bmp
ab873ec4d5c826db5d337f5f287006d5 /home/user/Desktop/Data-files/ass_2/ONE.bmp
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ md5deep TWO.jpg
4da131832b963f03f990d4c545b2d533 /home/user/Desktop/Data-files/ass_2/TWO.jpg
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ md5deep THREE.jpg
004b451689688f2d9bb83fb3fc5607aa /home/user/Desktop/Data-files/ass_2/THREE.jpg
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ md5deep FOUR.png
ac88ed263a80632167102c93a966f655 /home/user/Desktop/Data-files/ass_2/FOUR.png
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ md5deep FIVE.jpg
815025ac61891bf35ea4f38d7c543db0 /home/user/Desktop/Data-files/ass_2/FIVE.jpg
user@Ubuntu1804:~/Desktop/Data-files/ass_2$

```

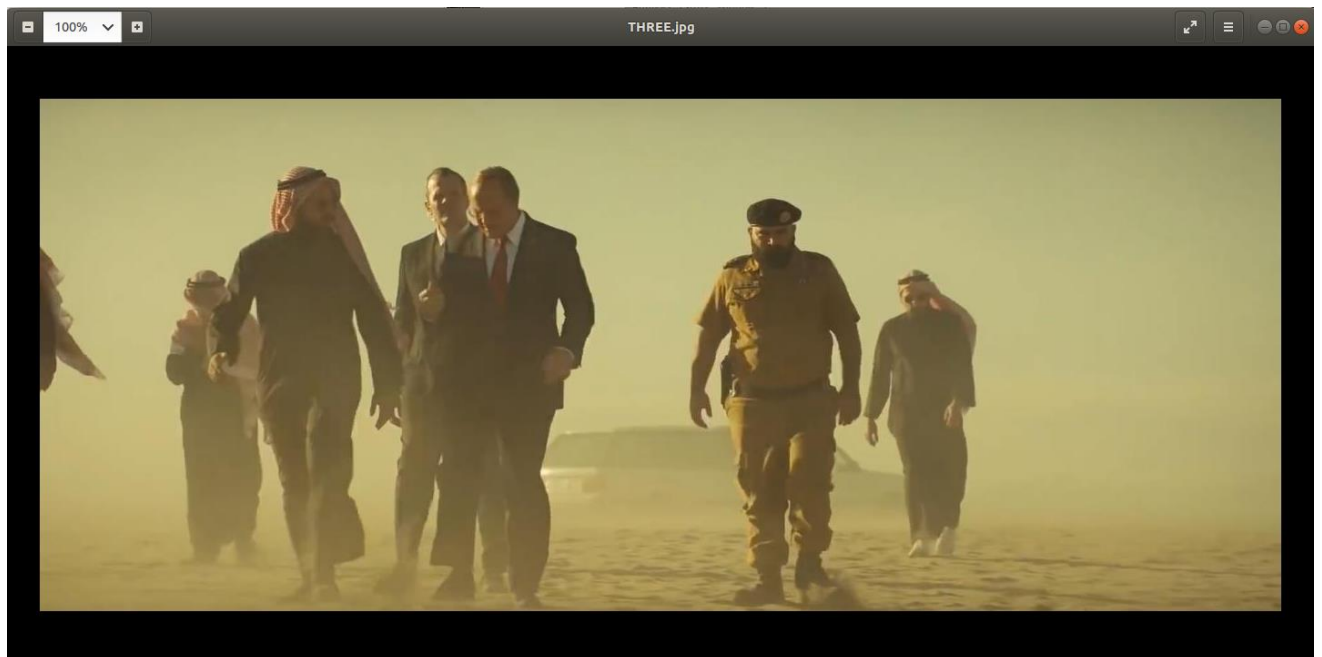
<i>File Name</i>	<i>File Type</i>	<i>MD5 Hash Value</i>
<i>ONE</i>	<i>.bmp</i>	<i>ab873ec4d5c826db5d337f5f287006d5</i>



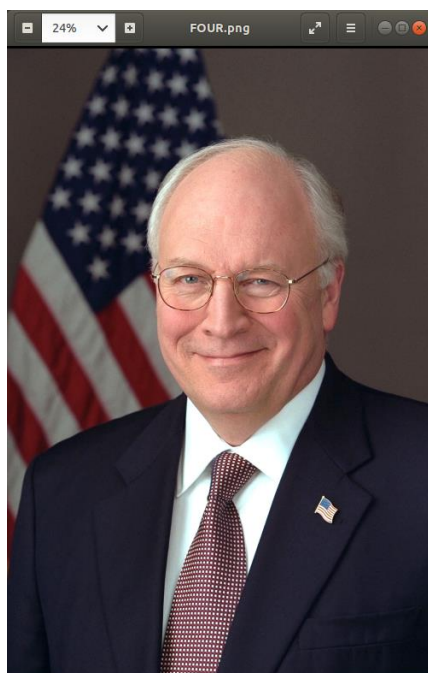
<i>File Name</i>	<i>File Type</i>	<i>MD5 Hash Value</i>
<i>TWO</i>	<i>.jpg</i>	<i>4da131832b963f03f990d4c545b2d533</i>



<i>File Name</i>	<i>File Type</i>	<i>MD5 Hash Value</i>
<i>THREE</i>	<i>.jpg</i>	<i>004b451689688f2d9bb83fb3fc5607aa</i>



<i>File Name</i>	<i>File Type</i>	<i>MD5 Hash Value</i>
<i>FOUR</i>	<i>.png</i>	<i>ac88ed263a80632167102c93a966f655</i>



<i>File Name</i>	<i>File Type</i>	<i>MD5 Hash Value</i>
<i>FIVE</i>	<i>.jpg</i>	<i>815025ac61891bf35ea4f38d7c543db0</i>



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

<i>Tool</i>	<i>Reason</i>
<i>S-Tools</i>	<i>S-Tools is a steganographic analysis tool designed specifically for BMP files. Because BMP files are uncompressed and have a consistent data structure, they are useful for data concealment and are frequently used in steganography. In this instance, ONE.bmp was analyzed using S-Tools in order to find and extract any hidden information that might be present in the picture and be important for the inquiry.</i>
<i>jpseek</i>	<i>JPG picture steganographic content analysis is the specialty of jpseek. Because JPG files are so widely used, there is less reason to suspect them when it comes to data concealing. TWO.jpg was examined using jpseek to make sure that no hidden information was missed, as it is necessary to carefully check all JPG images for hidden messages or data.</i>
<i>Foremost</i>	<i>With the help of its own data structures, headers, and footers, the data recovery utility Foremost is able to extract files. It works especially well for extracting files that might have been buried or erased. Foremost was utilized on THREE.jpg in this experiment to retrieve any possibly embedded or obscured data that conventional viewing techniques could overlook. This guarantees the discovery of all relevant evidence.</i>
<i>OpenPuff</i>	<i>OpenPuff is a flexible steganography application that works with a variety of file formats, including PNG files, and enables data extraction and concealing. Because of their lossless compression, which maintains the concealed data without sacrificing image quality, PNG files are utilized in steganography. Because it is capable of efficiently locating hidden data that could be essential to the inquiry, OpenPuff was selected to examine FOUR.png for any hidden information.</i>
<i>CrypTool</i>	<i>A powerful tool for cryptography analysis, CrypTool can perform a wide range of encryption and decryption operations. Although its main purpose is not steganography, it is capable of deciphering encrypted data buried in files. In this instance, CrypTool was used to examine FIVE.jpg in order to locate and unlock any encrypted data that may have been contained. This allowed investigators to completely access any information that might have been hidden in the picture.</i>
<i>HxD</i>	<i>HxD's ability to perform detailed examination and manipulation of the FIVE.jpg's binary data provides a deeper level of analysis. It helps in identifying and extracting hidden data, verifying the integrity of the file, and uncovering any embedded content that other tools might miss.</i>

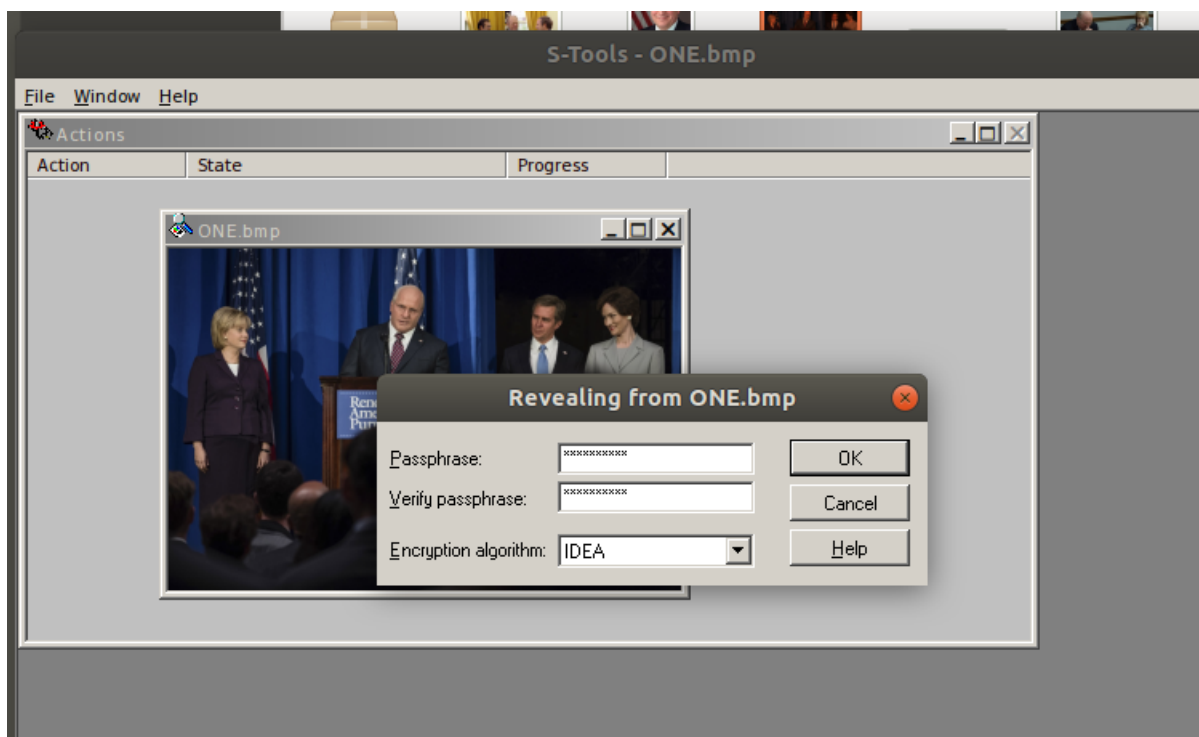
6. Describe how your investigation proceeded at this point, including screen shots.

1. For the first image file, ONE.bmp, I used the S-Tools to reveal any hidden files inside it.

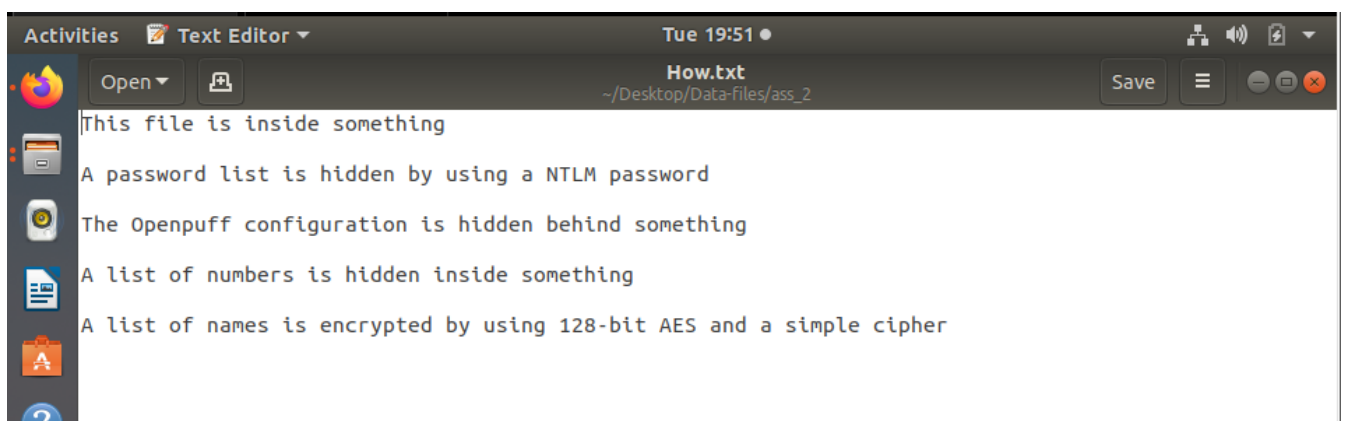
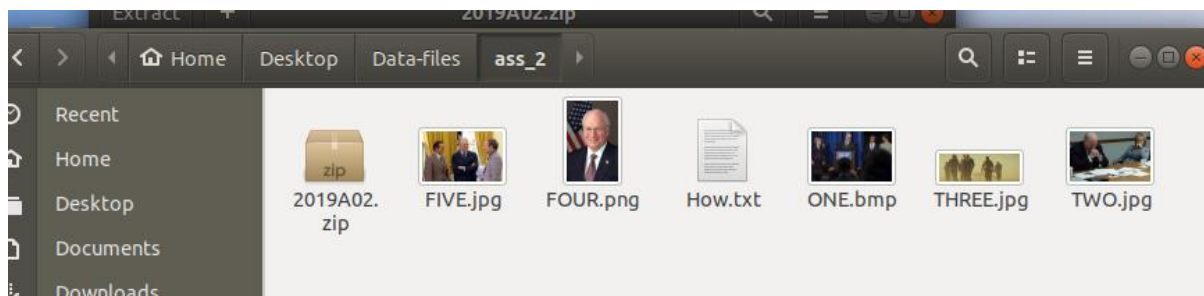
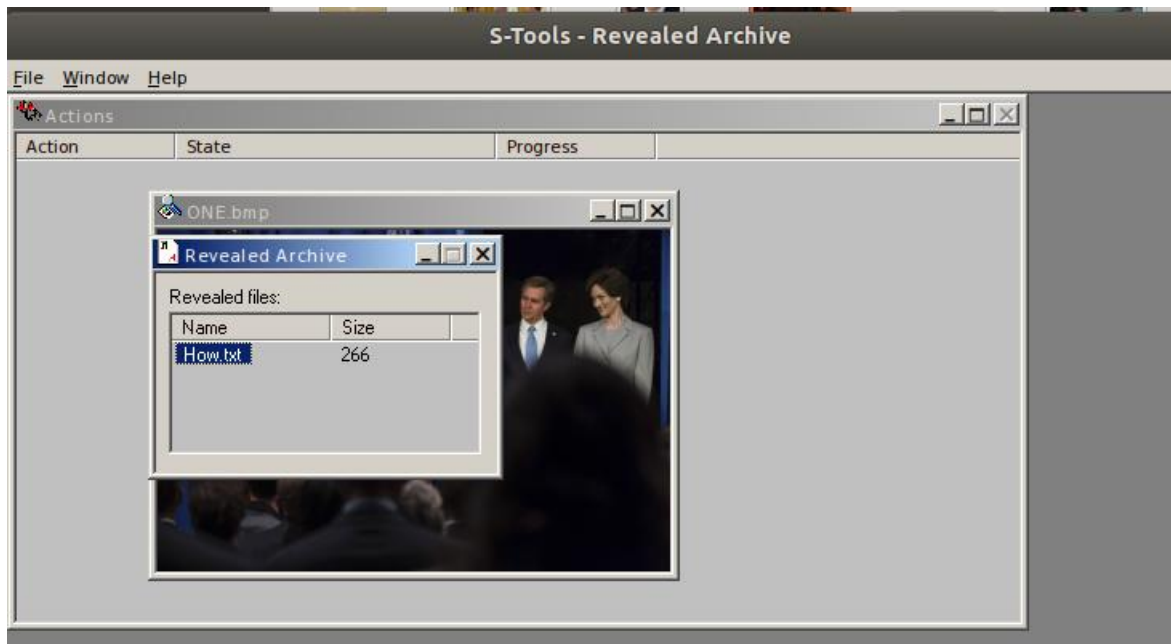
For that I first opened the tool using the command `wine ~/Desktop/win-tools/jphide\ and Stegbreak/S-tools/S-Tools.exe`. then drag and dropped the ONE.bmp file inside it



Then I right clicked the image file and selected the reveal option. It prompted for a password, since I have extracted two passwords using the NTLM hashes, I used the first password, **DickCheney** on this to reveal the hidden file.



After entering the password, a text file was revealed, How.txt. I opened it using the text editor and found some clues on how to find the rest of the hidden files and evidences.



2. Since I have now found the hidden file in the ONE.bmp, I'll now move on to the TWO.jpg file. The How.txt file says that a password list is hidden using the NTLM hash password. Using this clue, I started to analyse the TWO.jpg.

For that I used the tool jpseek to recover the hidden password list inside it. In order to do that, I typed in the command **wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/jpseek.exe TWO.jpg recovered.txt**.

When prompted for the passphrase, I entered the second NTLM password **DonaldRumsfeld**.

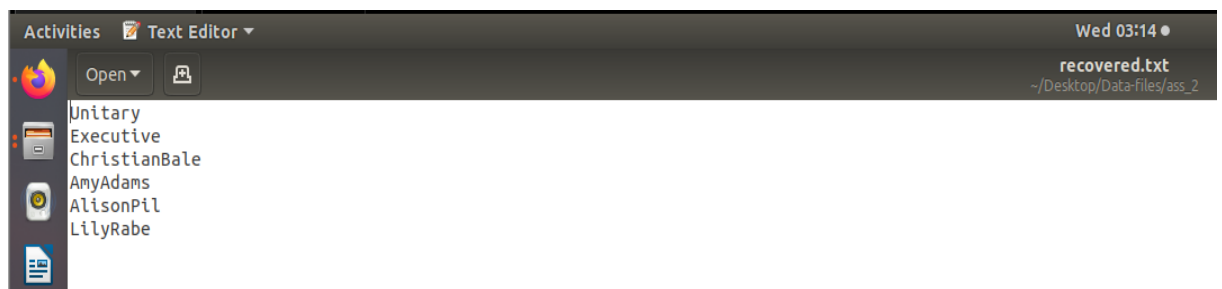


```
user@Ubuntu1804: ~/Desktop/Data-files/ass_2
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ wine ~/Desktop/win-tools/jphide\ and\
\ Stegbreak/jpseek.exe TWO.jpg recovered.txt

Welcome to jpseek Rev 0.51
(c) 1998 Allan Latham <alatham@flexsys-group.com>
This program is freeware.
No charge is made for its use.
Use at your own risk. No liability accepted whatever happens.
Contains cryptogaphy which may be subject to local laws.

Passphrase:
user@Ubuntu1804:~/Desktop/Data-files/ass_2$
```

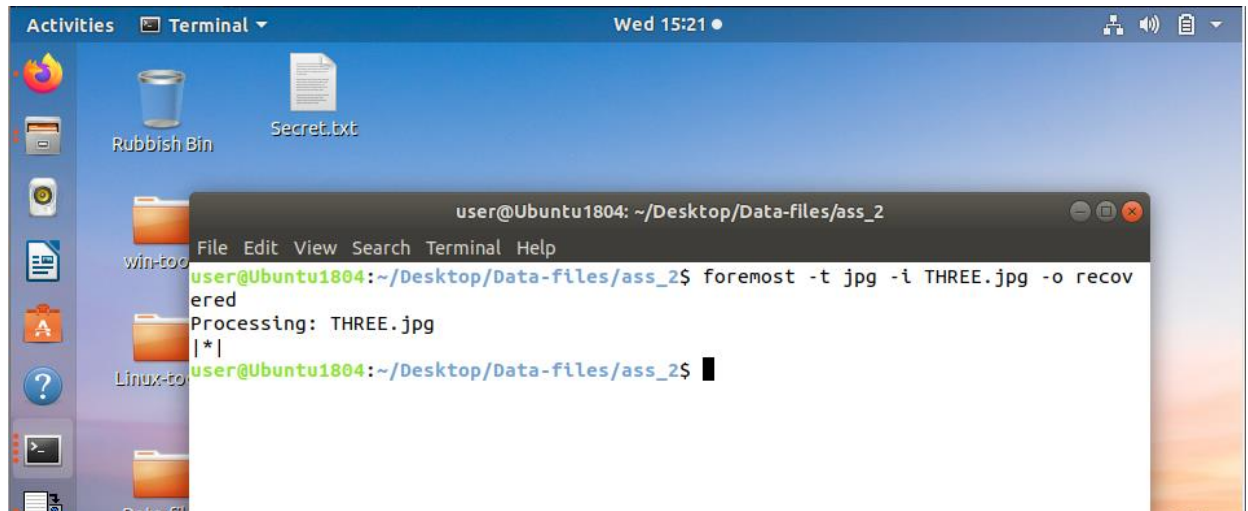
A text file was extracted, recovered.txt. it contained a list of passwords, as mentioned in the How.txt file.



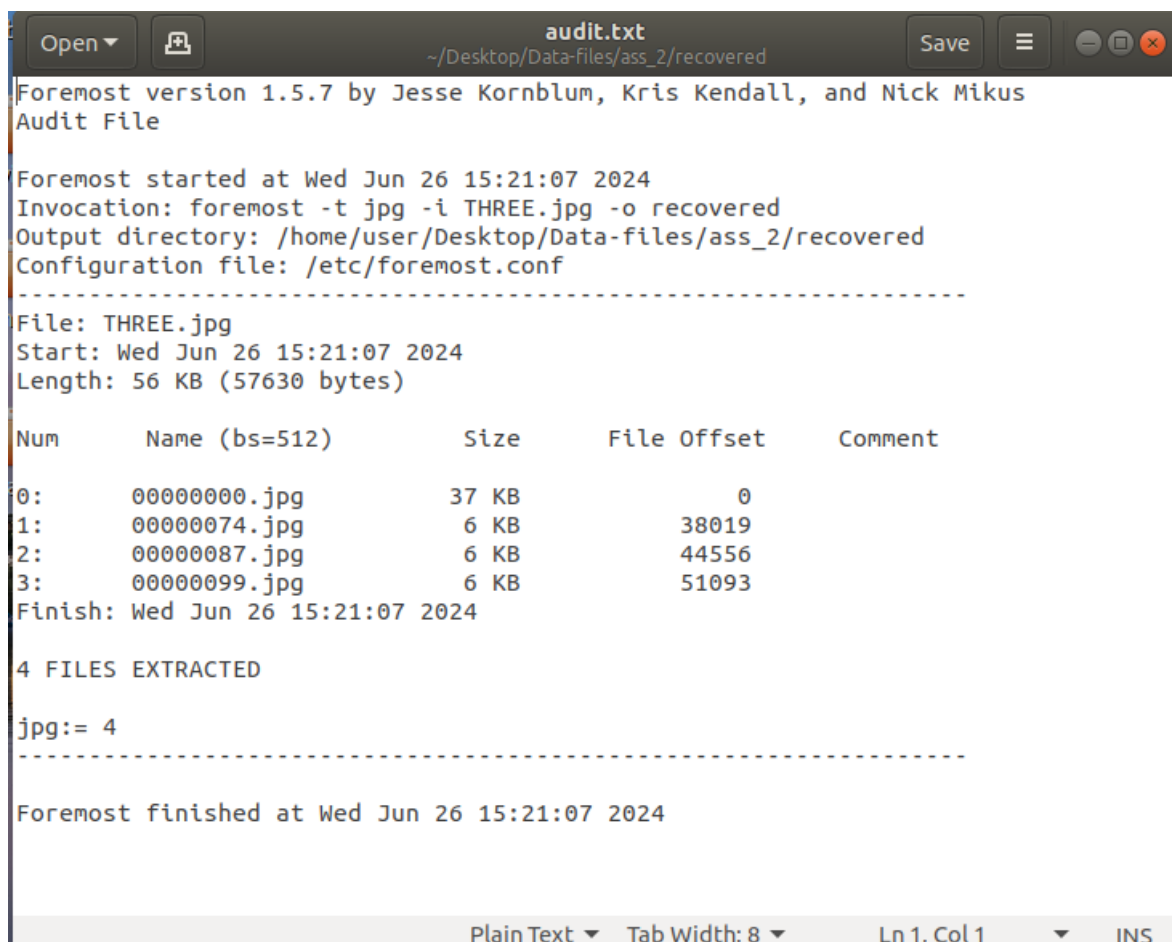
```
Activities Text Editor
Open
Unitary
Executive
ChristianBale
AmyAdams
AlisonPil
LilyRabe
Wed 03:14
recovered.txt
~/Desktop/Data-files/ass_2
```

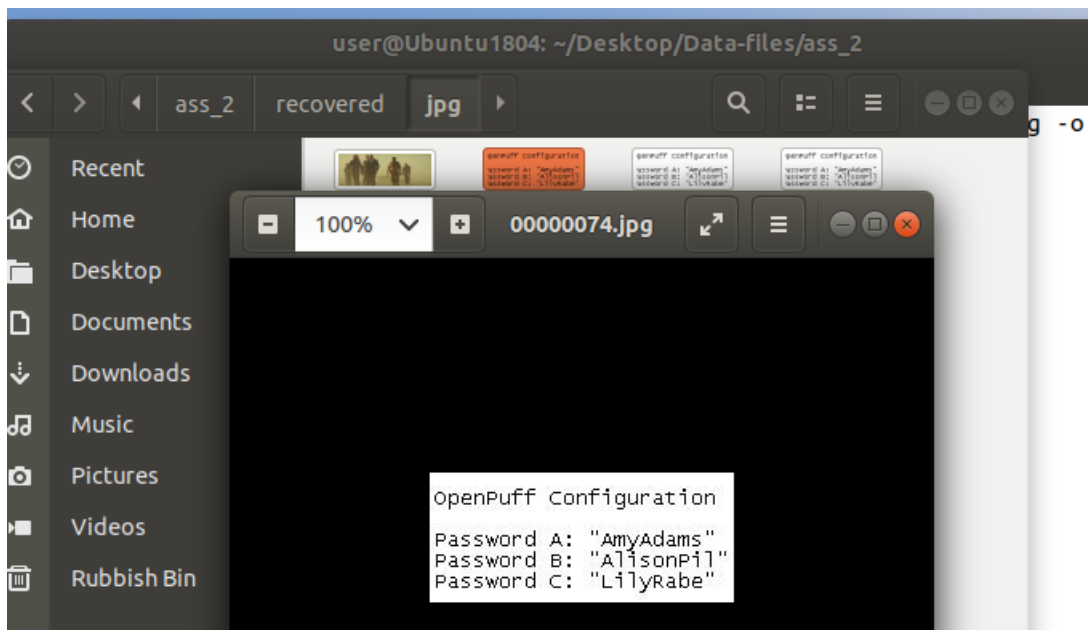
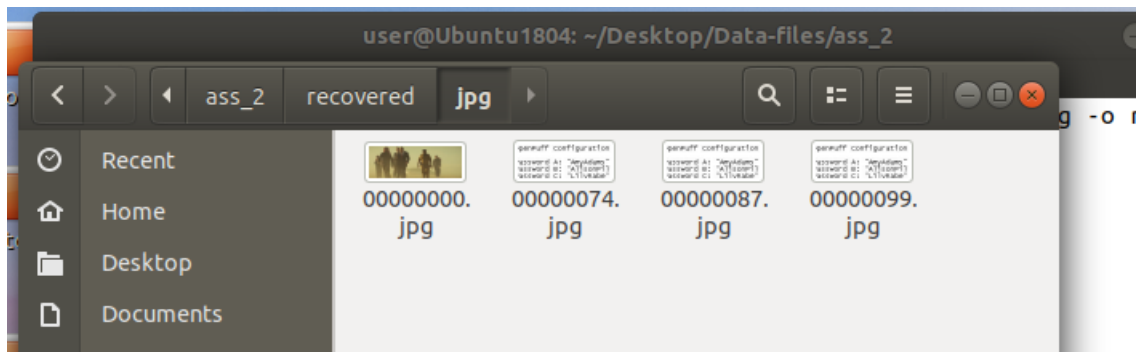

3. According to the *How.txt*, now we should find the OpenPuff configuration. For that let's analyse the *THREE.jpg*. it was said that the OpenPuff file configuration has been hidden. So, I decided to use the tool called *Foremost* on *THREE.jpg* to recover any hidden OpenPuff configuration files.

I used the command `foremost -t jpg -i THREE.jpg -o recovered`.



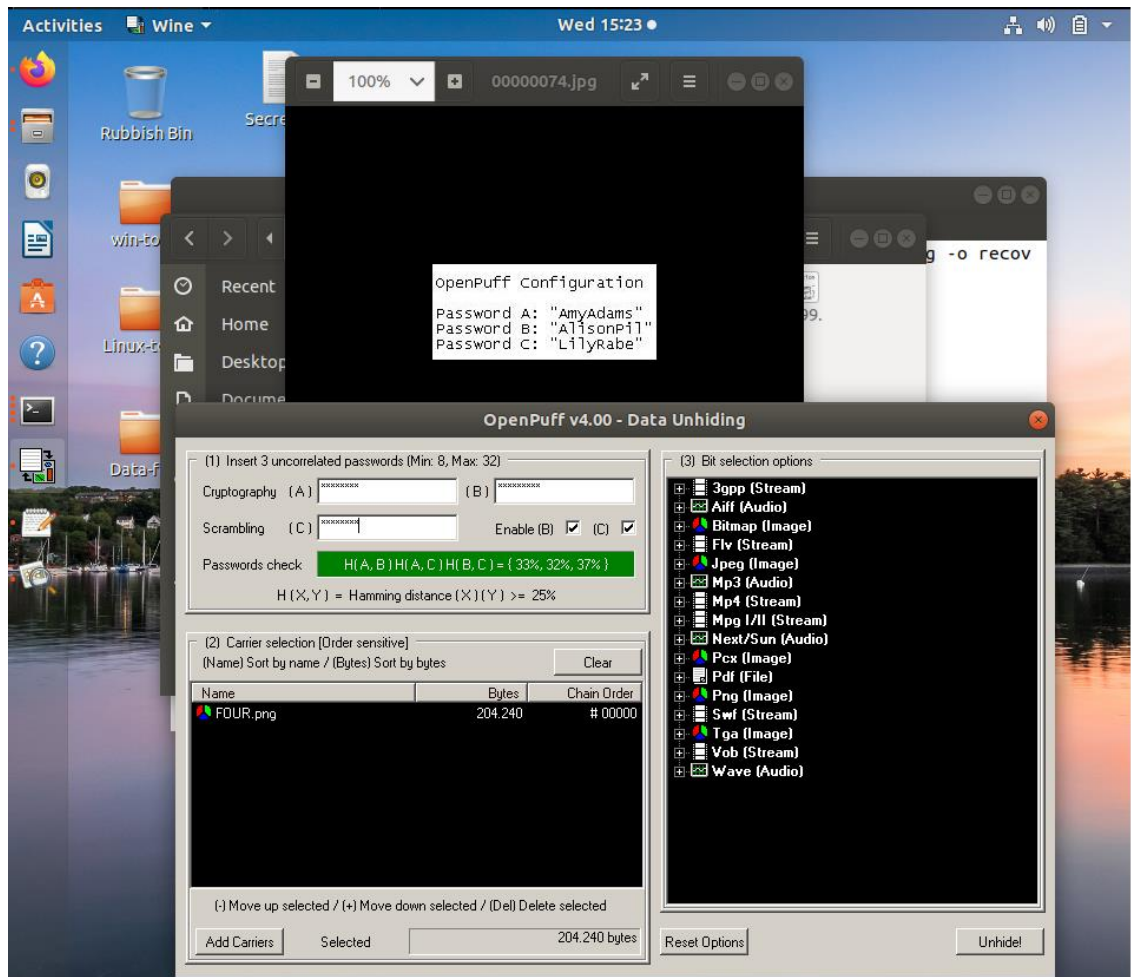
*There were four text files extracted in the folder *recover*. Three of them contained the same OpenPuff file configuration and the fourth one contained an *audit.txt* file.*



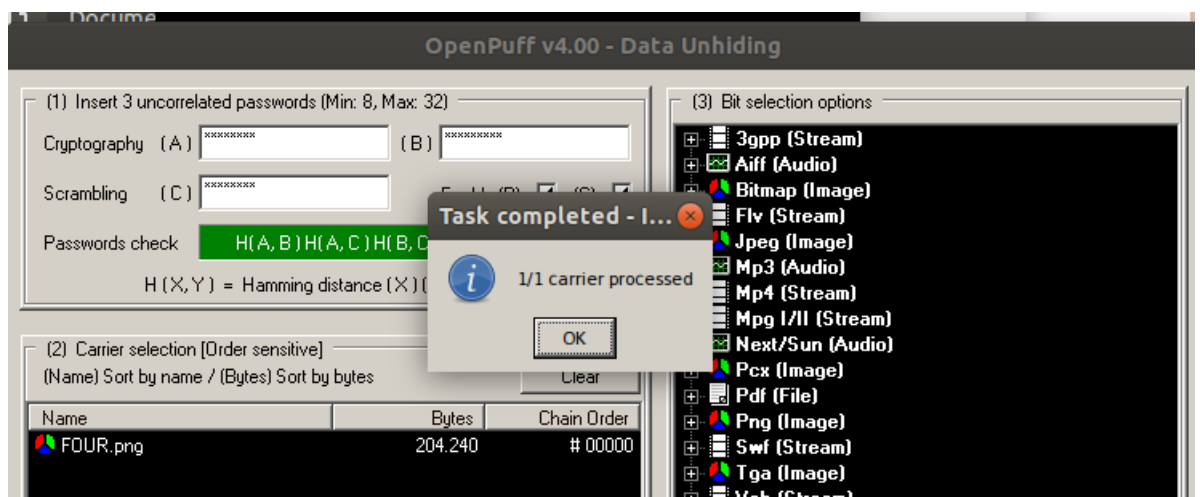


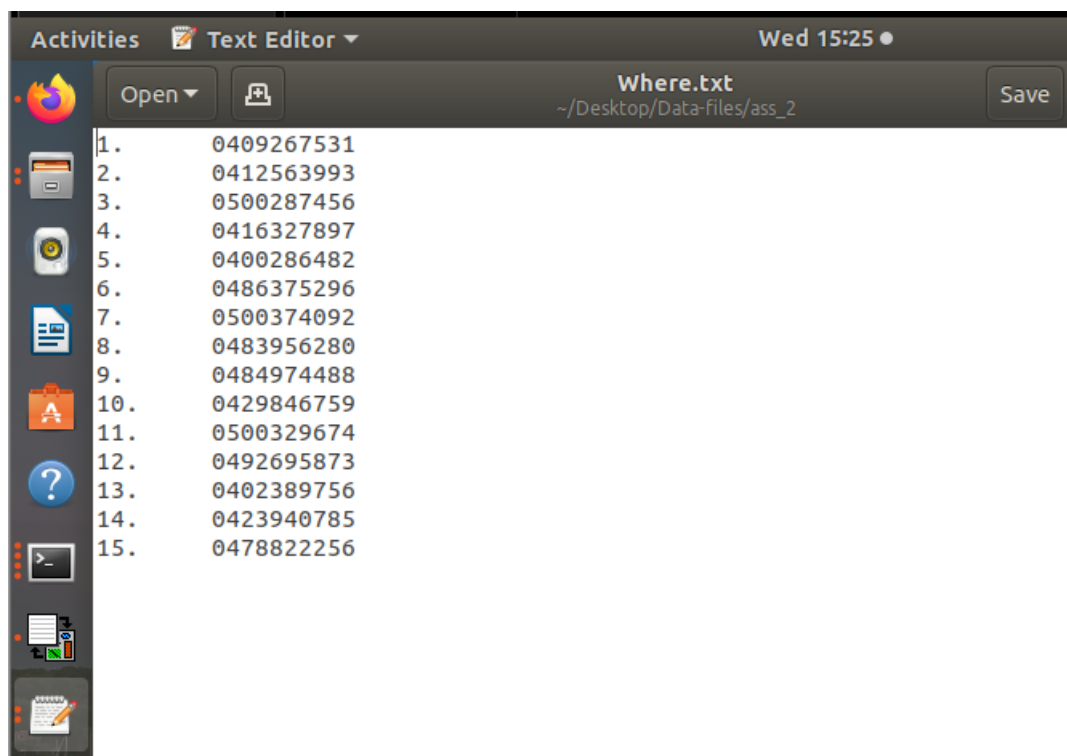
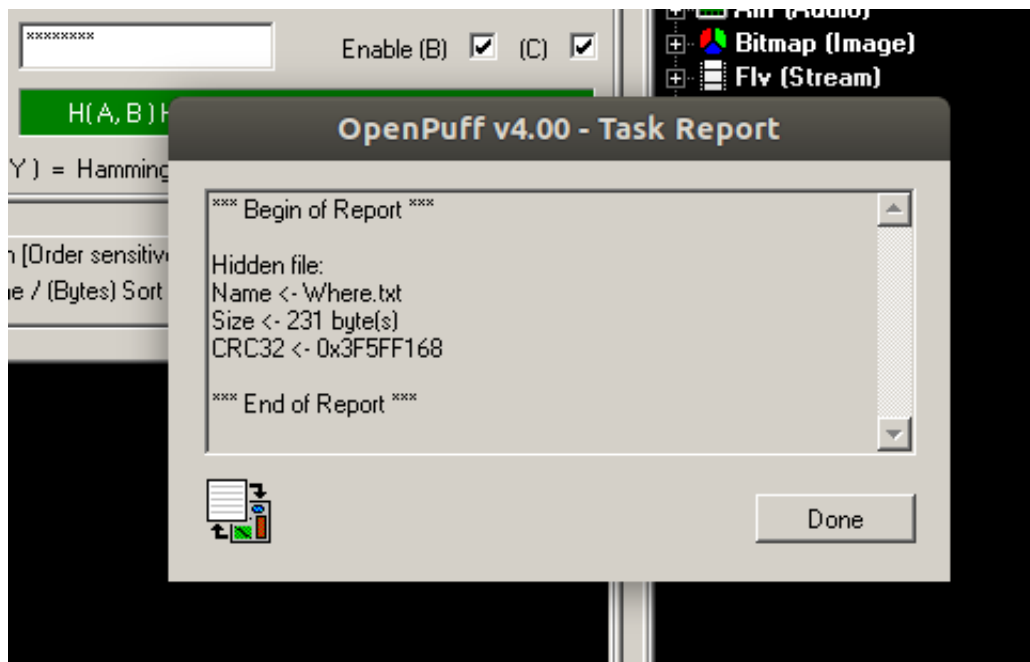
4. Now moving on to the *FOUR.png* file. Since we have now got the *OpenPuff* configurations, we can use that to extract the hidden list of numbers from the *FOUR.png* file as mentioned in the *How.txt* file.

For that I opened the *OpenPuff* tool, entered the *OpenPuff* configuration that I got in the previous step. Then added the carrier as *FOUR.png*. now I clicked the *Unhide* button.



After unhiding, a text file, *Where.txt* got extracted containing a list of numbers. As I suspect, these could be the phone numbers of the members involved in the drug warehouse



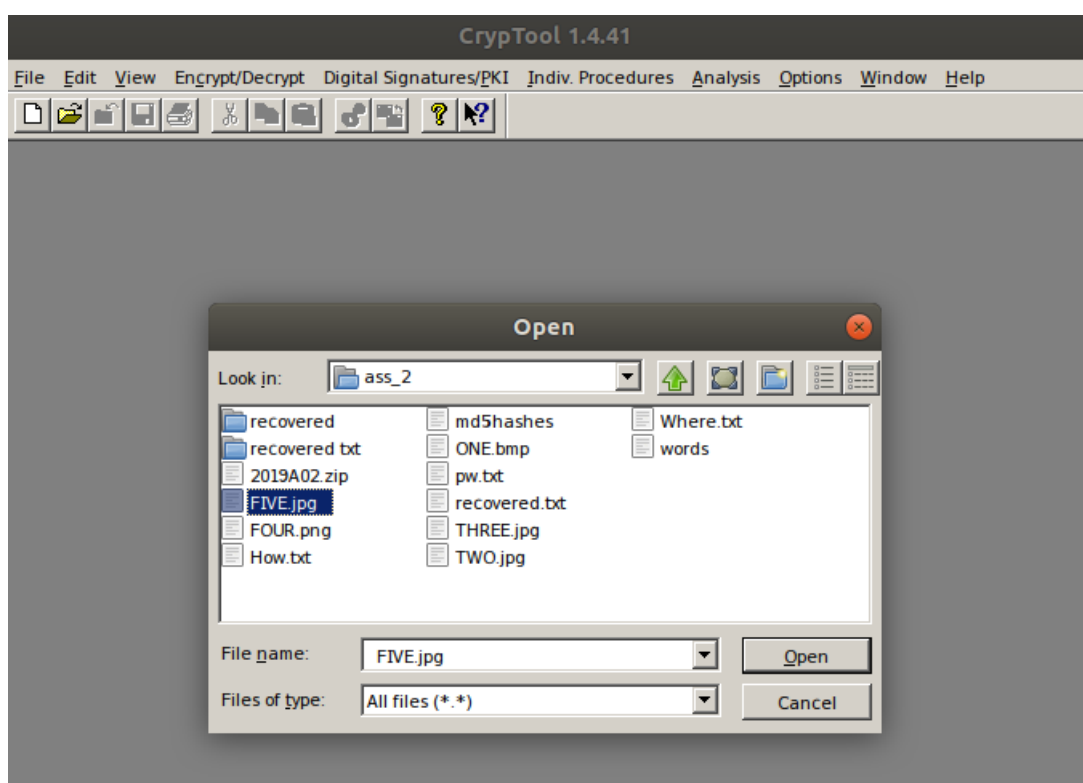


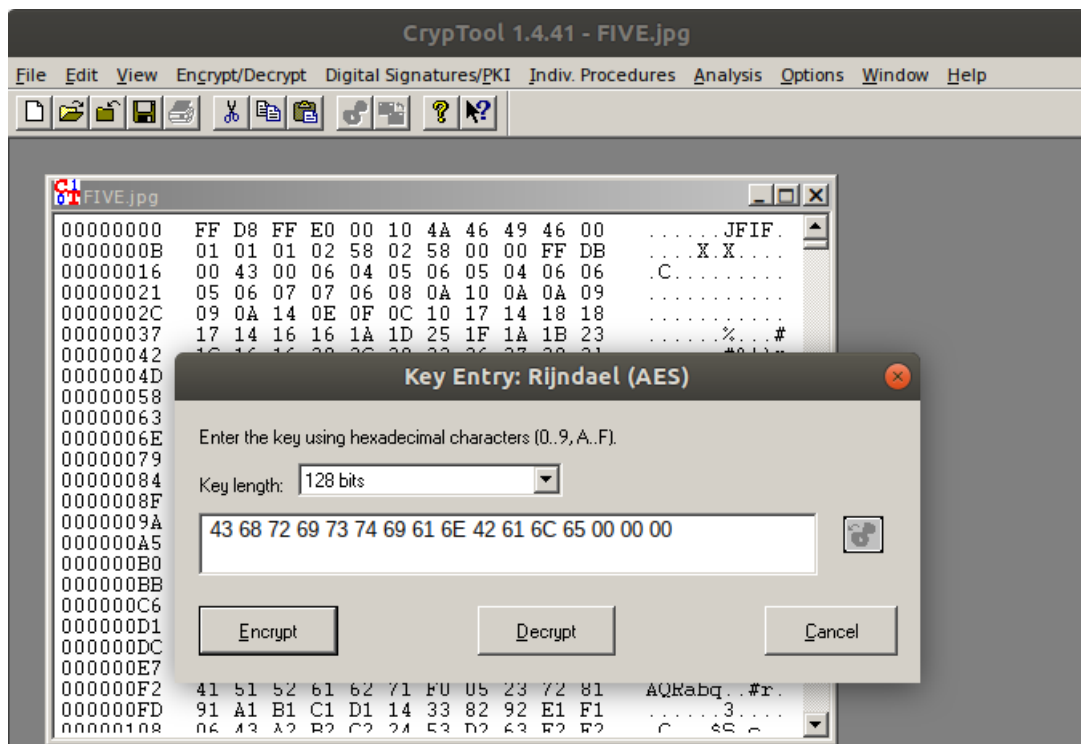
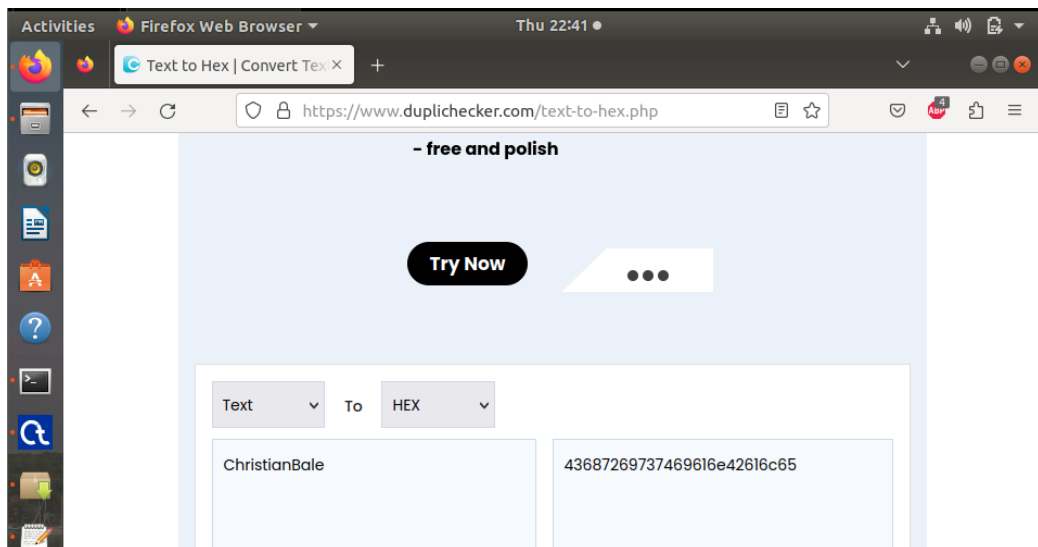
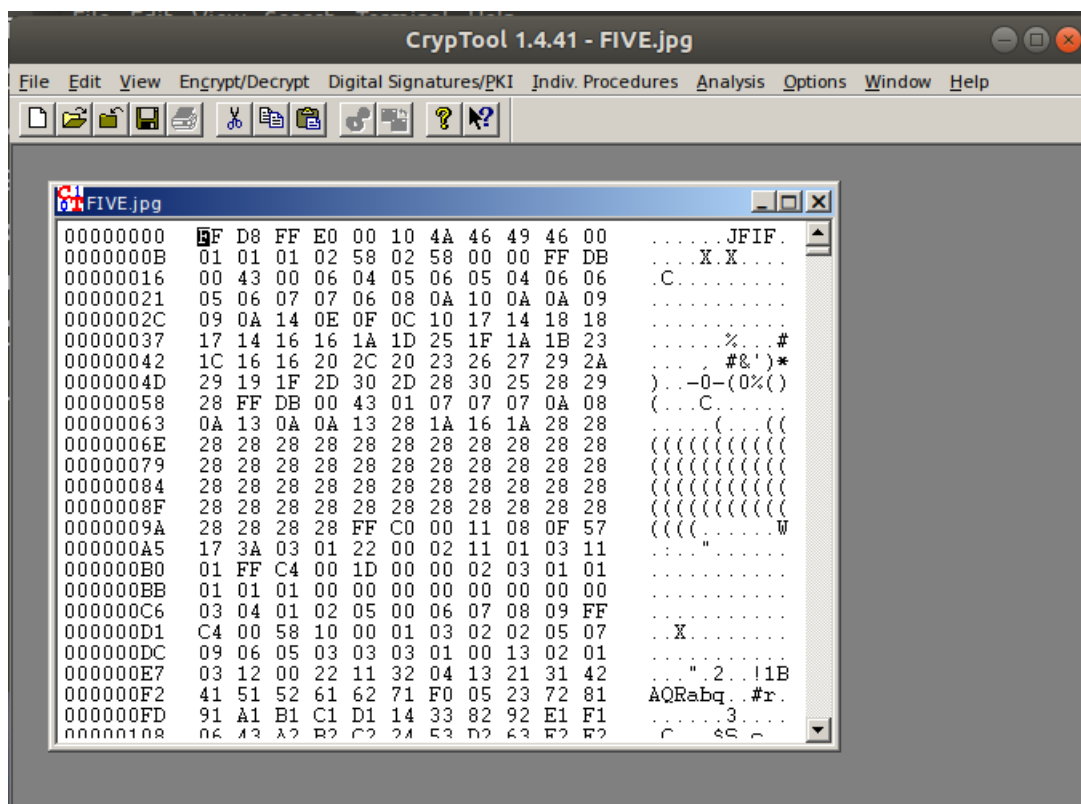
5. Now according to the How.txt, the last clue states that a list of names are hidden, so in order to find that, I'll have to now analyse the FIVE.jpg.

To do that, I used a tool called CrypTool to decrypt and extract any hidden information in the FIVE.jpg image file. I entered the command `wine /home/user/.wine/drive_c/Program\ Files\ |(x86\)/CrypTool.exe`

For that I first loaded the FIVE.jpg in the CrypTool and decrypted it using the AES encryption and then tried to decode it using Base64 decoding. But unfortunately, it didn't work. For the AES decryption key, I converted the name ChristianBale that was found from the list of passwords found earlier into hex value using an online tool duplichecker.com.

```
user@Ubuntu1804: ~/Desktop/Data-files/ass_2
File Edit View Search Terminal Help
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ wine ~/wine/drive_c/Program\ Files\
|(x86\)/CrypTool/CrypTool.exe
wine: cannot find '/home/user/wine/drive_c/Program Files (x86)CrypTool/CrypTool.
exe'
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ wine ~/home/user/.wine/drive_c/Progr
am\ Files\ |(x86\)/CrypTool/CrypTool.exe
wine: cannot find '/home/user/home/user/.wine/drive_c/Program Files (x86)CrypToo
l/CrypTool.exe'
user@Ubuntu1804:~/Desktop/Data-files/ass_2$ wine /home/user/.wine/drive_c/Progra
m\ Files\ |(x86\)/CrypTool/CrypTool.exe
001b: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
001b:err:module:import_dll Library mscoree.dll (which is needed by L"C:\\windows
\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorlib.exe") not found
001b:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fra
mework64\\v4.0.30319\\mscorlib.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write p
ipe!
```

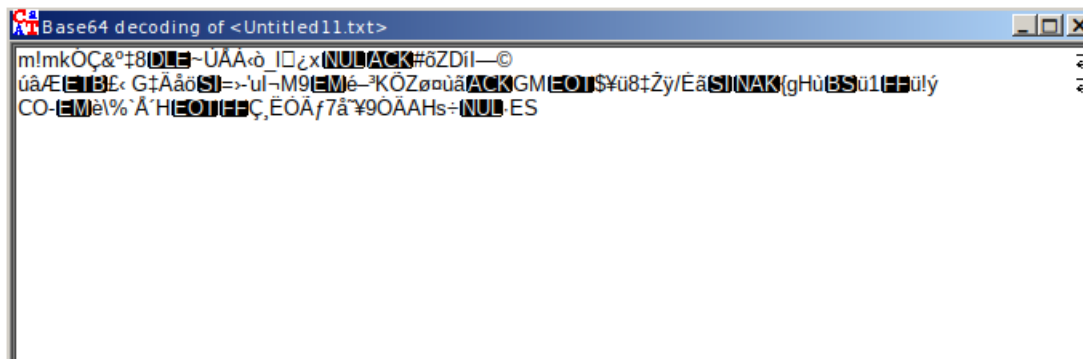




So, to resolve it, I used the Hxd hex editor to analyse the FIVE.jpg. In that I separated the last part of the hex values, because they were a bit odd than others. That was without any jumbled words or symbols. So, I cut and pasted it as a new hex document.

Then I saved it as a new text file loaded it in the CrypTool again and was able to observe encrypted words.

Now I first applied the Base64 decoding in it.



Then, I decrypted it using the AES decryption, the key I used was the hex value that I converted from ChristianBale. Then I was able to see some words but still a bit jumbled



Now to decrypt this, I used the Caesar cipher decryption, with some random keys. Finally, I was able to get a decrypted set of words that were mentioned in the How.txt. these words look like the names of the gang members that involved in the drug manufacturing.



So, this is the end of my investigation procedure.

DIGITAL FORENSIC REPORT

7. Write a two-page report for Sandra listing your findings and recommendations. Make appropriate suggestions on how a further investigation should proceed. Construct and complete a single-item evidence form as part of your report.

Findings and Recommendations

Case summary:

Five picture files were discovered after downloading and extracting a password-protected ZIP file that was discovered during the examination of a possible drug manufacturing activity. With the use of several steganographic technologies, every image was examined for hidden content. These are the investigation's conclusions and suggestions.

Summary of steps:

1. *Downloaded the ZIP file and verified its integrity using the MD5 hash.*
2. *Decrypted NTLM hash values to attempt accessing encrypted content.*
3. *Brute-forced the zip file to extract the image files.*
4. *Analysed each image file using appropriate steganographic tools:*
 - *ONE.bmp: analysed with S-Tools*
 - *TWO.jpg: analysed with jpseek*
 - *THREE.jpg: analysed with Foremost*
 - *FOUR.png: analysed with OpenPuff*
 - *FIVE.jpg: analysed with Cryptool and HxD.*
5. *Description of recovered items:*
 - *ONE.bmp: contained a hidden text file, How.txt providing clues for further analysis.*
 - *TWO.jpg: contained a password list hidden using NTLM hash password.*
 - *THREE.jpg: contained OpenPuff configuration files essential for further analysis.*
 - *FOUR.png: contained a text file, where.txt with a list of numbers, suspected to be phone number*
 - *FIVE.jpg: contained a list of names, decrypted using CrypTool and HxD, likely belonging to gang members involved in the drug operation.*
6. *Recommendations for further investigation:*
 1. *Further analysis of recovered data:*
 - *Verify the authenticity and relevance of the phone number and name recovered.*
 - *Cross-reference the names and numbers with existing criminal databases.*
 2. *Malware analysis:*
 - *Upload the executable file to virustotal to check for known malware signatures.*
 - *Conduct a detailed analysis of the executable to understand its function and potential threats.*

3. *Extended steganographic analysis:*
 - *Use additional steganographic tools to ensure no hidden content is missed.*
 - *Perform a deeper analysis on the extracted images for any overlooked data.*
4. *Collaboration with law enforcement:*
 - *Share findings with law enforcement agencies for a coordinated effort in dismantling the drug operation.*
 - *Utilize law enforcement resources for tracking and apprehending suspects based on the recovered data.*

Evidence Form (Figure 1-11 of the text)

The hazardous materials team <i>This form is to be used for only one piece of evidence.</i> <i>Fill out a separate form for each piece of evidence.</i>			
Case No:	Case_2024_00002	Unit Number:	Unit_0002
Investigator:	Nirosh Ravindran		
Nature of Case:	Suspected Drug Manufacturing		
Location where evidence was obtained:	warehouse behind Roma St station in Brisbane		
Item # ID	Description of evidence	Vendor Name	Model No/Serial No.
ID_0002_0001	CD drives	Unknown	Unknown
Evidence Recovered by:	Moti	Date & Time:	10/03 @ 3.17 am
Evidence Placed in Locker:	Moti	Date & Time	10/03 @ 4.00 am
Evidence Processed by	Description of Evidence	Date & Time	
Nirosh Ravindran	Downloaded a password protected zip file, 2019A02.zip from a secure link	10/03 @ 7.00 am	
	Decrypted the passwords from the NTLM hashes given	10/03 @ 7.15 am	
	Extracted the contents in them which were 5 image files	10/03 @ 8.00 am	
	Started investigating them	10/03 @ 8.15 am	
	Finished the investigation	10/03 @ 6.19 pm	
	Sent the Digital Forensic report to Sandra	10/03 @ 8.00 pm	
		Page _1_ of _1_	

-end of template -