***SIT282 Computer Crime and Digital Forensics***

**ASSIGNMENT 3 – Investigation Report || James Papas 217265358**

Contents

[**DIGITAL FORENSIC PROCEDURE 1**](#)

[Question 1: 1](#)

Question 2: 2

[Question 3: 3](#)

[Question 4: 4](#)

[Question 5: 4](#)

[Question 6: 5](#)

[Question 7: Two Page Report 11](#)

[**Recommendations: 11**](#)

[**Steps Performed: 11**](#)

[**Recovered Content: 12**](#)

[**Interpretation of Content: 12**](#)

[**Investigative Suggestions: 12**](#)

# **DIGITAL FORENSIC PROCEDURE**

## **Question 1:**

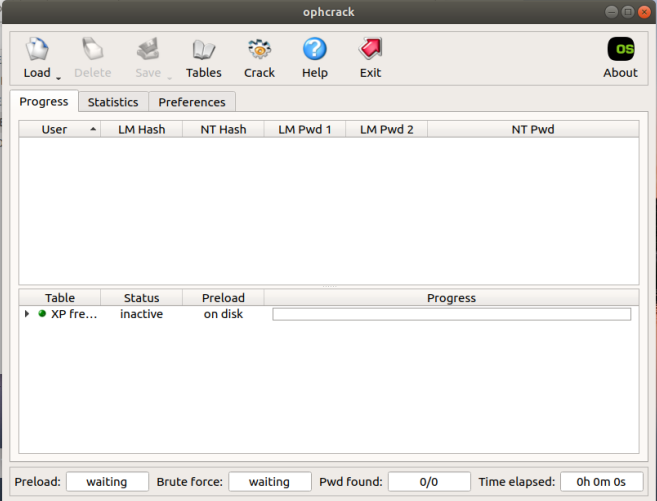
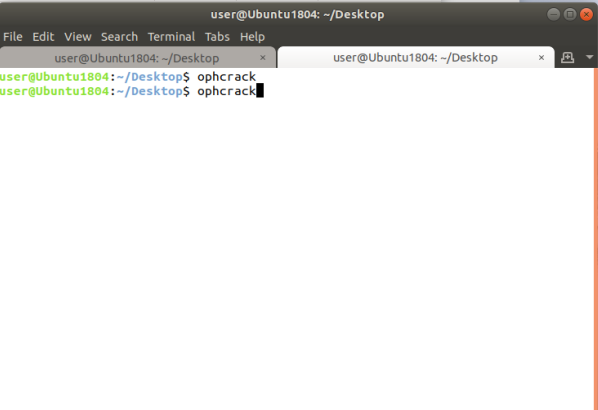
Explain how you downloaded the file, what precautions you took, and how you ensured its integrity.

| File Download Procedure | I went to the secure URL and downloaded the file onto my PC running Windows 10. I would then make a copy of the zip file and save it in two different directories so I can test the 1:1 copy of the evidence supplied. I then transferred the copied zip file through the shared folder for the zip file to appear in Ubuntu for analysis. This completed the download sequence. |
| --- | --- |
| Precautions Applied | I determined the resources I need to investigate the case, tested MD5 hash file integrity, obtained and copied evidence and identified and mitigated risks. |
| Method used to ensure Integrity | The first thing I did was check if the MD5 Hash Sandra sent, matches the zip I downloaded from the email. Both the MD5 Hashes were matching: “9ec1c8f62429182349f3979c39aed8fb 2019A02.zip”. I also ensured not to accidentally taint the original evidence. Investigating on the original evidence file could compromise the integrity of the data. I mitigated this by creating a copy of the zip file sent by Sandra. As such, the Original evidence was secured in my secure directory whereas the copied data was analysed using ubuntu. |

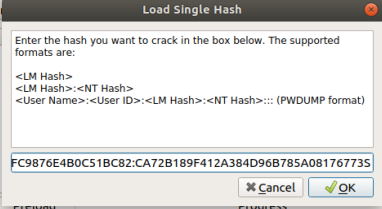
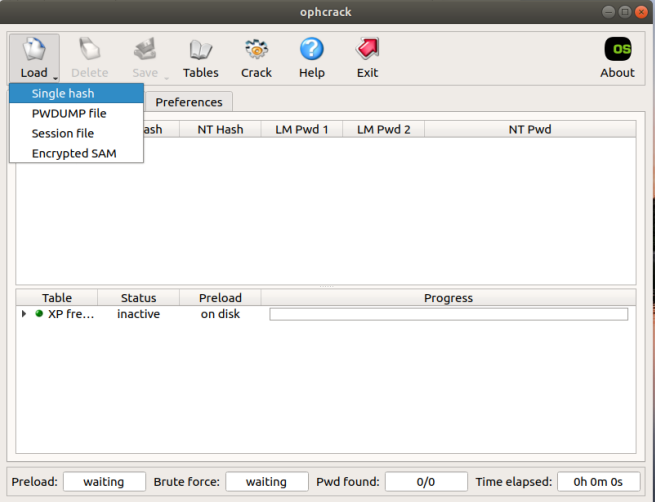
## **Question 2:**

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

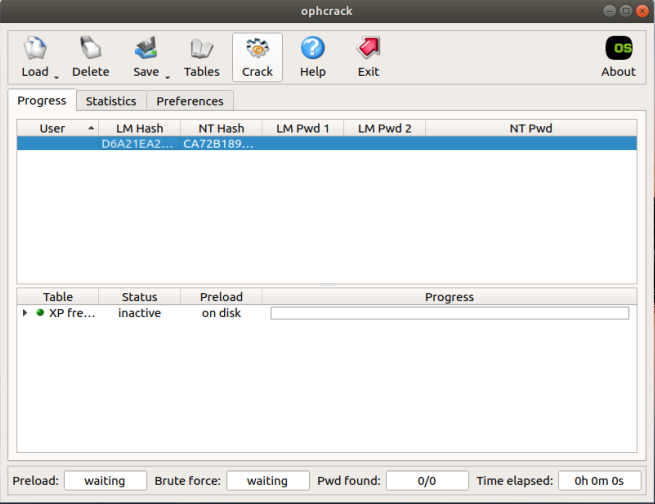
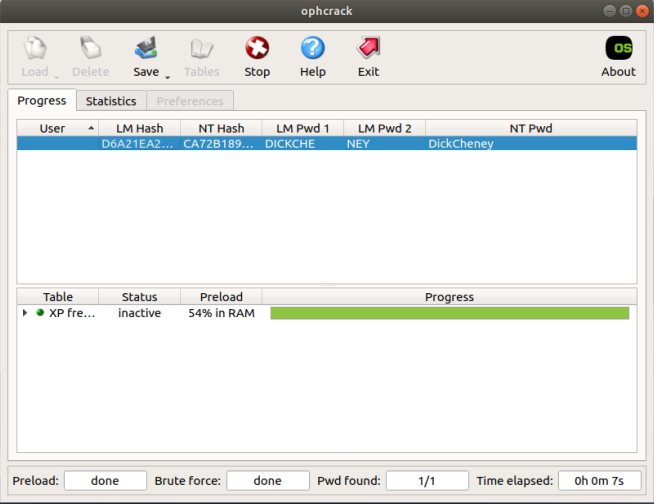
1. In order to decrypt both NTLM hashes received from Sandra, I would first ensure that I have my Ubuntu (Linux) system running with terminal open.
2. I then would proceed to open the OphCrack by simply using the following command “ophcrack” in the terminal then click enter:



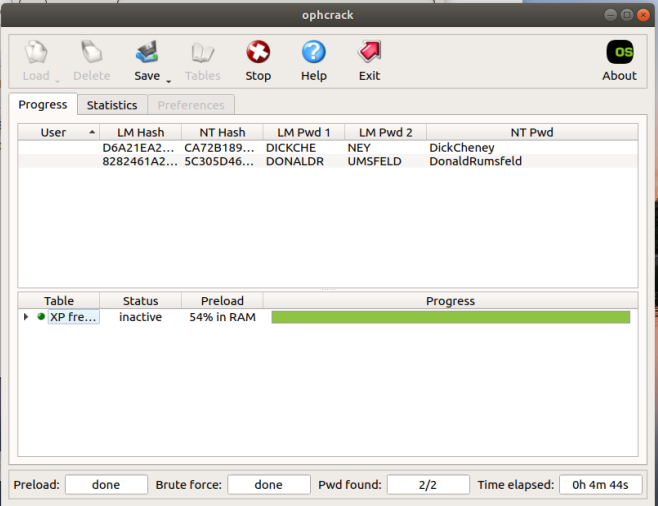
1. I would then take NTLM hash 1: “D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A08176773” and simply click load, select single hash, and then paste the hash into the text box screen, then click ok:



1. I then would click and highlight the NTLM hash in OphCrack, and click crack , and wait for brute force to complete crack.

1. Brute force now completed and 1 password decrypted: “DickCheney”, clicked stop and loaded next Hash.
2. I repeated steps 1 – 4 using 2nd NTLM hash: “8282461A2BDAF626E6067B973FDDC643:5C305D4616C7571D5DDC6EEA5BA5C395”
3. 2nd NTLM hash password decrypted: “DonaldRumsfeld”



## **Question 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: | 1. I ensured to move the copied zip file to the Ubuntu desktop, in order to analyse the evidence. 2. I then opened a terminal in Ubuntu, and navigated to the Desktop directory using the following command in terminal: “cd ~/Desktop/” 3. I then executed the following command: “user@Ubuntu1804:~/Desktop$ fcrackzip -u -D -p /usr/share/dict/american-english 2019A02.zip 4. This command executed a dictionary attack revealing the password as “vice”. 5. I then tried accessing all files in the zip and the password worked correctly, allowing me access to view and extract to a decrypted folder.   The relationship between both the NTLM decrypted hashes and the zip folder password shows that there are similar content relating back to American “vice” President Dick Cheney. Additionally, I used 2 different attacks to reveal different passwords. Ophcrack used a brute force approach, whereas fcrackzip used a dictionary attack. Both were similar in the sense that they required attacks to decrypt secure files and information. |
| --- | --- |

## **Question 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 | There appears to be 5 image files, 3 JPEGs, 1 Bitmap and 1 PNG. In ONE.bmp vice president Dick Cheney appears to be speaking in a press conference at a ‘Renewing Americas Pumage’ rally. In TWO.JPG, Dick Cheney appears to be looking down at paperwork critical thinking. In THREE.jpg what appears to be Dick Cheney or Donald Rumsfeld, is in discussion with middle eastern militia or law enforcement. In FOUR.png, displays Dick Cheney’s presidential profile image in politics. And FIVE.jpg, shows US Congressman, Donald Rumsfeld having a friendly conversation with President Ford (Left) and Dick Cheney (Right). All images appear to be made last modified on the 6th August 2019. |
| --- | --- |

| File Name | File Type | MD5 Hash Value |
| --- | --- | --- |
| ONE | .bmp (Bitmap image) | ab873ec4d5c826db5d337f5f287006d5 |
| TWO | .jpg (JPEG Image) | 4da131832b963f03f990d4c545b2d533 |
| THREE | .jpg (JPEG Image) | 004b451689688f2d9bb83fb3fc5607aa |
| FOUR | .png (PNG Image) | ac88ed263a80632167102c93a966f655 |
| FIVE | .jpg (JPEG Image) | 815025ac61891bf35ea4f38d7c543db0 |

## **Question 5:**

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

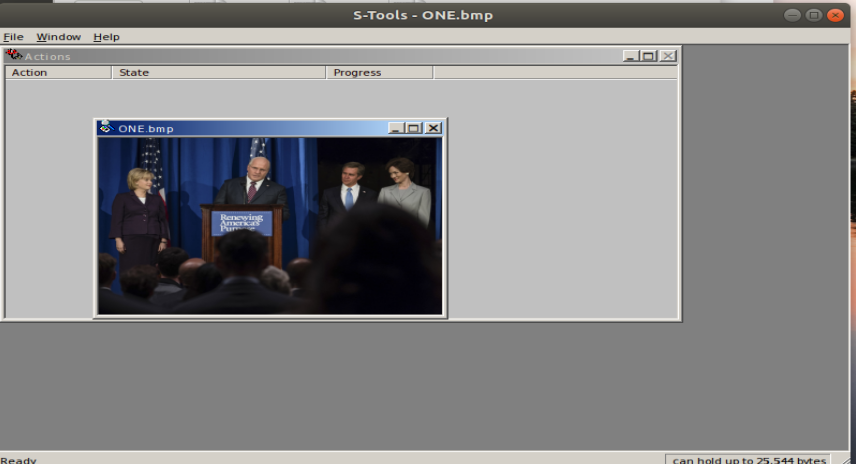
| Tool | Reason |
| --- | --- |
| HashCalc | To ensure the integrity of each file, I will use Hash Calc to find the MD5sum of each file and match that with the md5 hash in terminal. This ensures integrity in evidence files and can find any inconsistencies in files. |
| HxD | This tool would be required in order to ensure that the file headers are matching with the correct footers. |
| StegDetect | By using stegdetect I would be able to search each of the 3 JPEG images to find hidden data. This included Two.jpg, THREE.jpg and FIVE.jpg. I would copy the words and rules.ini files to the evidence directory in order to perform the file crack. No cracks were revealed.  Code used: “wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/stegdetect/stegbreak.exe -r rules.ini -f words TWO.jpg” |
| S-Tools | I will use this tool to examine the .bmp file and with the recovered NTLM passwords obtained with ophcrack. |
| Jpseek | This tool allows the opportunity to find any hidden text files within JPG images. I will investigate this tool using the NTLM password recovered. |
| CrypTool | This tool will allow the effective use for deciphering AES encryption aswell as decoding Base64 ciphers. This toiol also works well with deciphering Caesar ciphers. |

## **Question 6:**

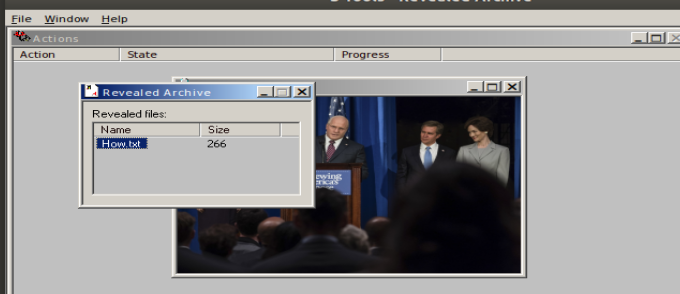
Describe how your investigation proceeded at this point, including screen shots.

Note. Clearly identify the steps that were performed, and evidence found supported by screen shots.

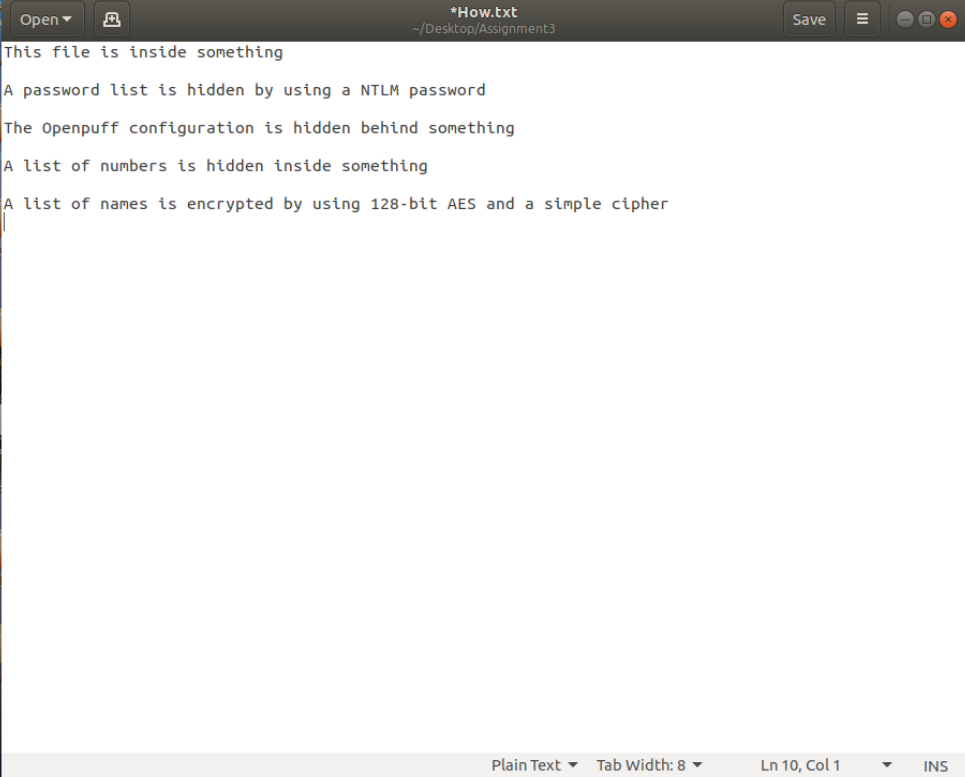
1. I firstly opened the S-Tool window using the following command in terminal: “wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/S-tool/S-Tools.exe”. This tool allowed me to examine if any .txt files were hidden in any images.



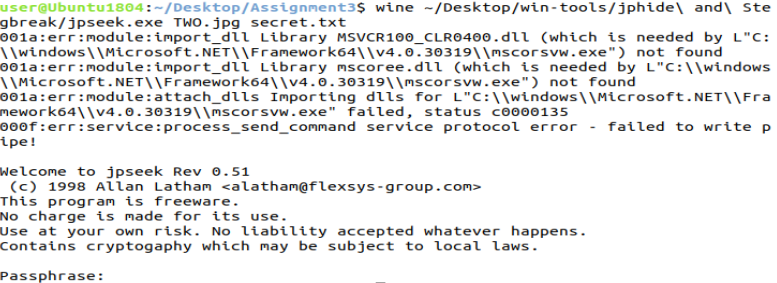
1. Whilst I was examining the image ONE.bmp, I tried using NTLM Hash password “DickCheney” to reveal the secret How.txt file.

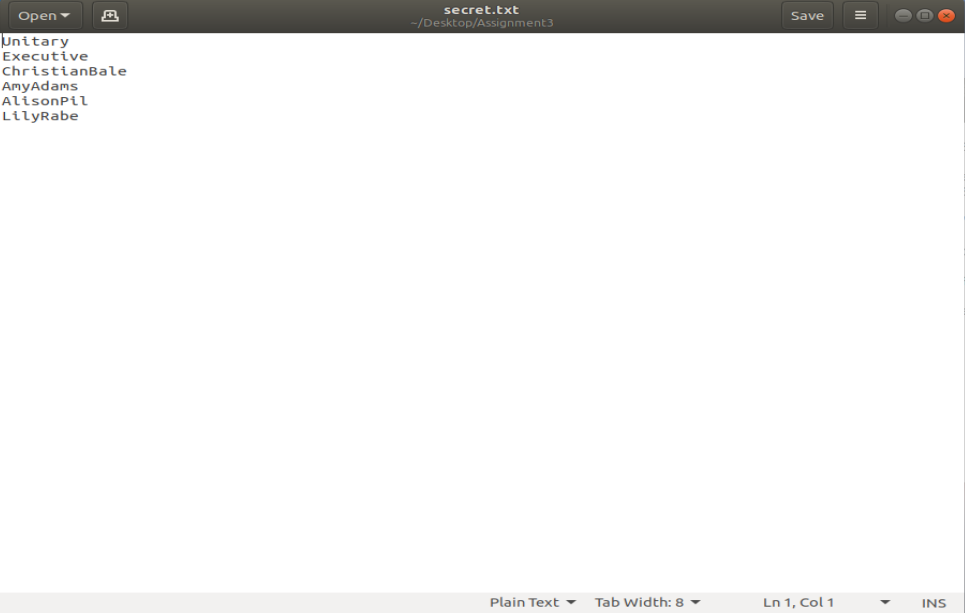


1. I then opened the hidden How.txt file, and hints generated.

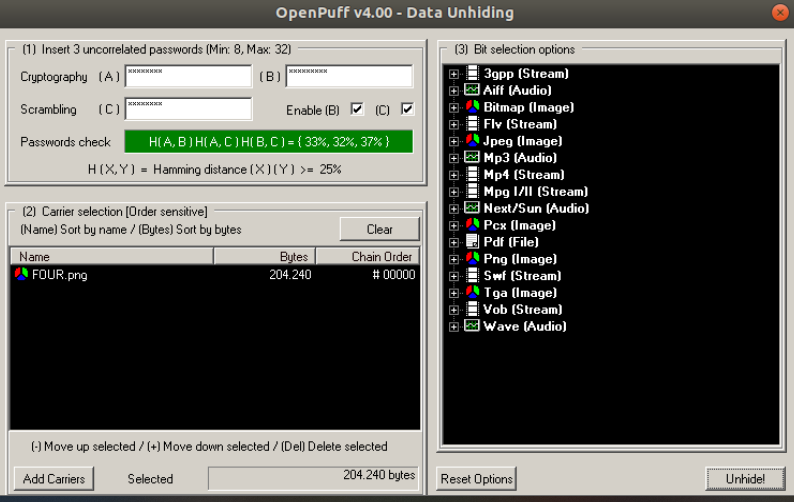


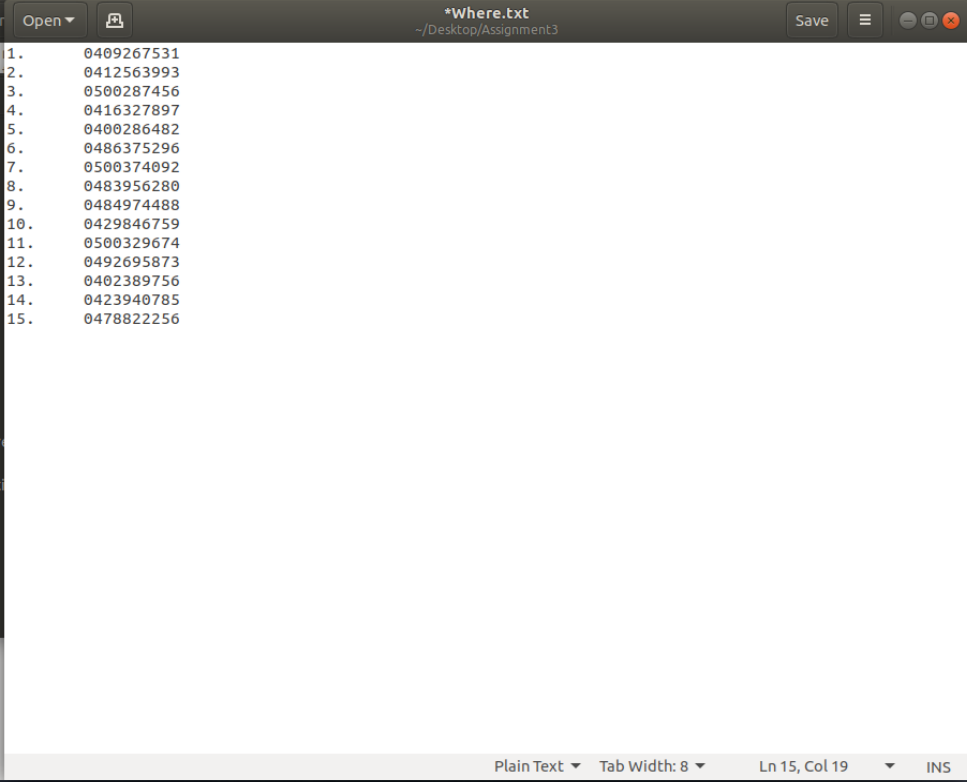
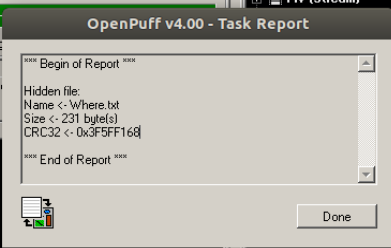
1. I then performed jpseek to recover list of passwords for TWO.jpg, used password from NTLM Password “DonaldRumsfeld”. No other images worked with password. Re-opened secret.txt to reveal passwords.



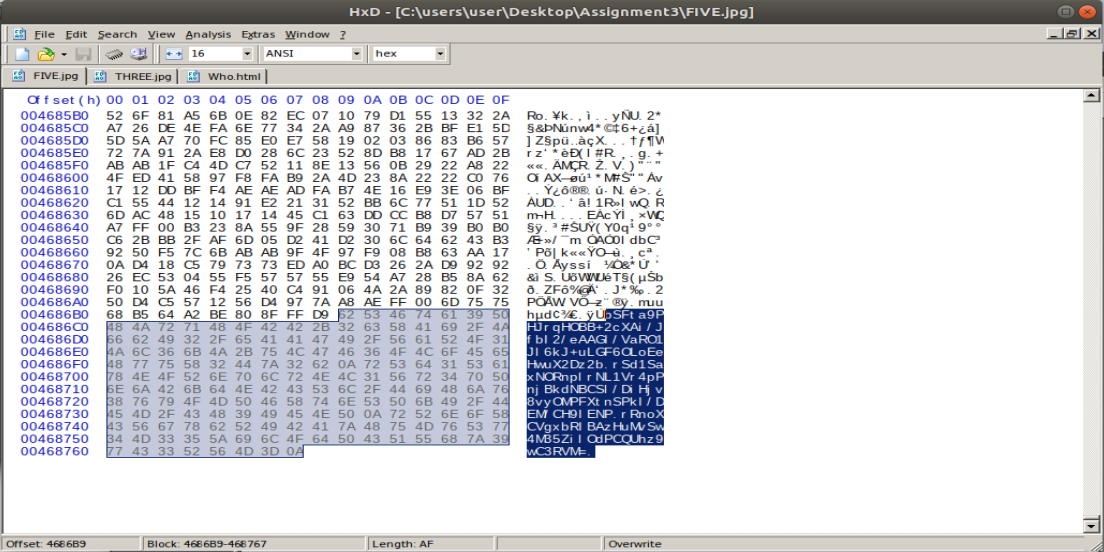


1. I Then opened up an OpenPuff window using the following command: “wine ~/Desktop/win-tools/OpenPuff/OpenPuff.exe”
   * I then tried adding the 3 passwords from the list that share things in common, AmyAdams, AlisonPil and LilyRabe are all females. I used these 3 passwords on the FOUR.png file. Whereas the other passwords are not similar. Adding these passwords into OpenPuff allowed me to save a new document, Where.txt, showing a list of numbers.

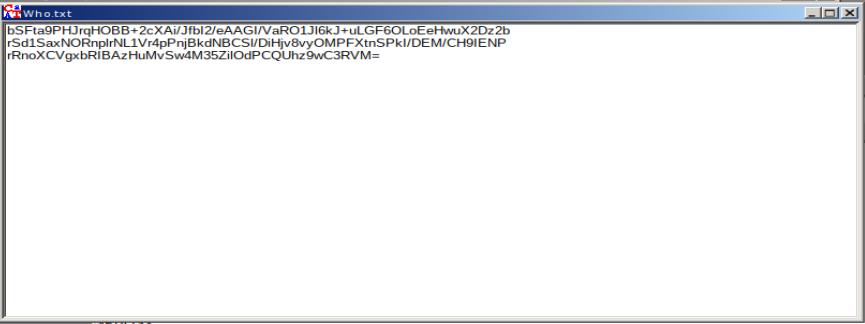


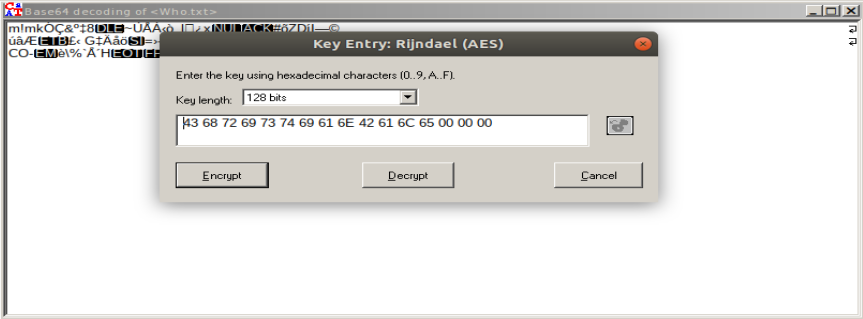
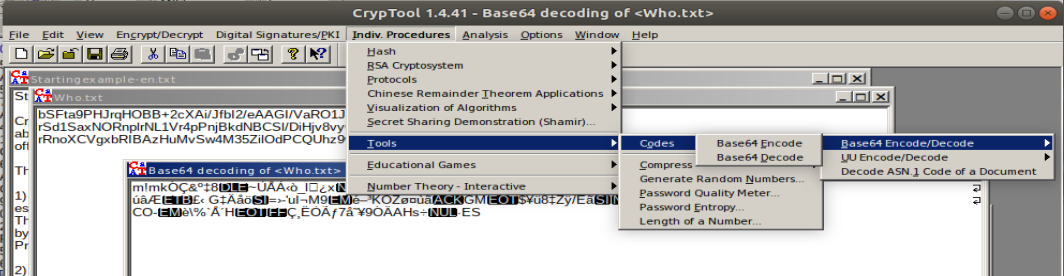
 

1. I then looked at the “FIVE.jpg” file in HxD to examine if there is any hidden content, and found a hidden cipher after the footer of the JFIF file format.



1. I used the cipher found in the FIVE.jpg file, and pasted it into Cryptool to show the following Base64 content:



1. Following this I converted the Base64 file using AES decryption with the password equipped from the secret.txt password list:“ChristianBale” (In Hex: 43687269737469616e42616c65). The hex was used to decrypt in 128 bits to reveal a list of ceasar ciphered names. 



1. I then used the the ceasar decryption tool to change the key entry to start at “K”. This revealed the full decryted list of 15 names. Now there a persons of interest and phone numbers linking people to crimes.  
   it

*DIGITAL FORENSIC REPORT*

## **Question 7: Two Page Report**

***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.***

*Note. The single evidence form provided below is included as part of the two page report.*

*Prepare your report for Sandra using the following headings as a guideline:*

* *Recommendation(s) – what needs to be done back at the lab (since you did this from your holiday destination)*
* *Summary of steps that were performed (can use bullet points for this)*
* *Brief description/summary of what was recovered*
* *Your interpretation of what was recovered in relation to the case*
* *Appropriate suggestions on how a further investigation should proceed*

# **Recommendations:**

It is recommended that as soon as the recovered evidence is sent back to Sandra, she should instantly lock the evidence in the evidence locker to avoid evidence tainting, damage and tampering. After locking the evidence in the locker, she should also complete the evidence custody form that had been already filled out. As the digital forensics was completed abroad, it is not possible to secure and protect evidence. As such, evidence needs to be sent back to Sandra.

# **Steps Performed:**

The following steps were performed systematically to ensure the accuracy of results. The steps will include the summary of what tasks were performed and the order of which they were performed.

* Created a copy of zip file so original evidence is not tampered or tainted.
* Verified MD5 Hash matches zip file.
* Bruteforced both NTLM Hashes using ophcrack, revealing passwords as ‘DichCheney’ and ‘DonaldRumsfeld’.
* Used terminal command to allow fcrackzip to crack the password of the zip file, revealing password as “vice”. I then extracted the copied files using ‘vice’ as password.
* Used ls -l command to find last created date of evidence files, revealing 6th August 2019.
* Used S-Tools with suspicious ‘ONE.bmp’ image file. Revealed How.txt file by inputting recovered NTLM hash password ‘DickCheney’.
* As per hints in How.txt, performed jpseek command with other NTLM password ‘DonaldRumsfeld’ on TWO.jpg file to reveal list of passwords called secret.txt.
* Opened OpenPuff tool with ‘FOUR.png’ in order to reveal hidden information in image. Used the three female passwords recovered in secret.txt to reveal a list of numbers within a Where.txt file.
* Examined ‘FIVE.jpg’ file in HxD, whereby an encryption cypher was hidden after the FFD9 JPG footer. Encryption cipher captured.
* Encryption cypher pasted into CrypTool. Cipher was then decrypted from base64 to AES, then decoded with base 64. This revealed a list of 15 Caesar ciphered names.
* Caesar cipher was decrypted with starting value of ‘k’. List of decrypted names revealed.
* Investigation Complete.

# **Recovered Content:**

Using fcrackzip, the zip file revealed the password as ‘vice’, which allowed the extraction of the files within. What appeared on the surface included 3 JPG, 1 BMP and 1 PNG file. Each file was examined thoroughly and revealed further hidden files. Given the 2 NTLM hashes, the 2 passwords recovered from ophcrack included ‘DickCheney’ and ‘DonaldRumsfeld’. Within the 1 BMP file, there appeared to be a hidden How.txt file, revealed by S-tools. Within the 1 PNG file, there appeared to be a Where.txt file, revealed by OpenPuff. Within one of the JPG files (TWO.jpg), there is a secret.txt file using the recovered NTLM password obtained from the brute force hash attack with ophcrack. Within one of the JPG files (FIVE.jpg), there appeared to be a hidden base64 cipher after the JPG footer. The cipher was decrypted using AES and Base64 decode/decryption, then decrypted using Caesar cipher decryption, revealing a decoded list of 15 names. In total the contents recovered include 3 JPG files, 1 BMP file, 1 PNG file, 3 TXT files and 1 decrypted list of names.

# **Interpretation of Content:**

From the recovered content, there appears to be some sort of direct link with American politicians Dick Cheney and Donald Rumsfeld, as all 5 images within the zip contain photography regarding the two. In addition to the photography, there appears to be a list of 15 names and phone numbers that directly link suspected individuals and their locations. The numbers are in both Australian and American format. As such, there may be illegal activity between both countries, and ultimately could be a global enterprise. The passwords obtained are primarily actors and actresses from the Hollywood movie ‘Vice’ about the same American politicians.

# **Investigative Suggestions:**

Back at the forensic lab it is suggested that investigators use the tools to further examine the evidence acquired. The investigators should to recreate the steps performed abroad in order to replicate the same evidence. Once the evidence is created from their copies, the investigators should cross references the list of 15 names and the list of 15 phone numbers. With this information they may be able to find prime suspects who may have worked for the drug manufacturing plant. An option to find further information for the case may include listening in on the Australian phone calls in order to determine any illegal activity to incriminate the suspects.

*Evidence Form (Figure 1-11 of the text)*

| Australian Federal Police  This form is to be used for only one piece of evidence.  Fill out a separate form for each piece of evidence. | | | |
| --- | --- | --- | --- |
| Case No: | 217265358 | Unit Number: | SIT282 |
| Investigator: | James Papas | | |
| Nature of Case: | Drug Manufacturing Lab discovered. | | |
| Location where evidence was obtained: | Roma Street Station, Brisbane, QLD, 4000 | | |
| Item #  ID | Description of evidence | Vendor Name | Model No/Serial No. |
| 01 | Lists of 15 names and 15 phone numbers identifying potential suspects associated with illegal drug manufacturing. | James Papas | 394162 |
| Evidence Recovered by: | James Papas | Date & Time: | 10/10/2020 |
| Evidence Placed in Locker: |  | Date & Time |  |
| Evidence Processed by | Description of Evidence | | Date & Time |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  | Page \_\_ of \_\_< |