SIT282 Computer Crime and Digital Forensics

Roma St Drug Manufacturing Case - Criminal Investigation Report

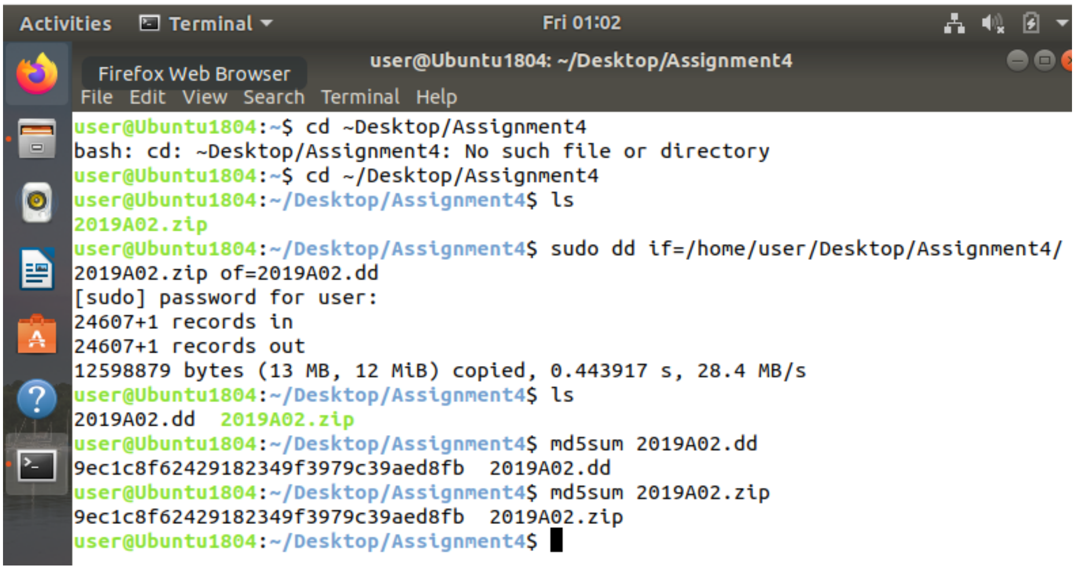
Investigator: Sangheetha Velayutham

Table of Contents:

DIGITAL FORENSIC PROCEDURE

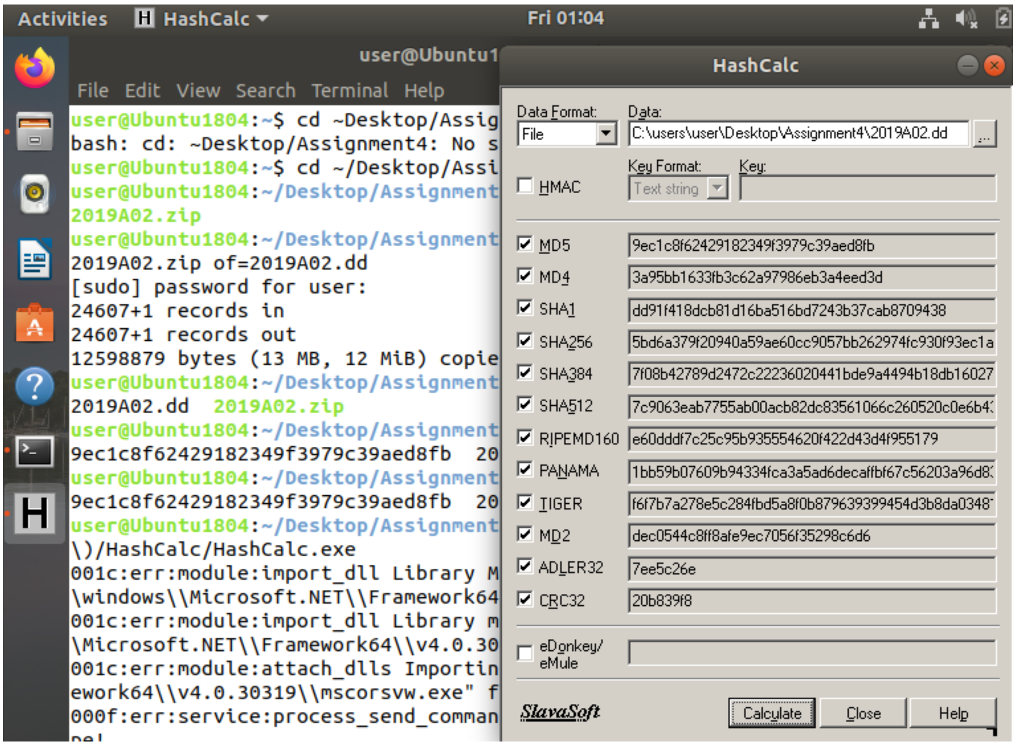
1. Explain how you downloaded the file, what precautions you took, and how you ensured its integrity.

File Download Procedure	The zip file was initially downloaded in the host windows OS. The zip file was then transferred into the VM via directory sharing. The zip file was saved in the shared folder which linked the host machine and the VM. Then the zip file was transferred to a directory on the Desktop called Assignment4.
Precautions Applied	Zip file was received from a trusted source (Sandra). BitDefender antivirus program is installed in host windows OS and it would scan for any infected files contained in the zip file. The option called (hide extensions for known file types) is unchecked.
Method used to ensure Integrity	A copy of the zip file was made using the dd tool to preserve tampering of the original file when investigating. Then the zip file (copy) is thoroughly checked to make sure none of the data is tampered with. This is done via hashcalc and MD5 command on the terminal. The hash value of the original and the copy is compared to verify that the copy is not altered.



Activities
Terminal
Fri 01:02
Firefox Web Browser
user@Ubuntu1804: ~/Desktop/Assignment4
File Edit View Search Terminal Help

```
user@Ubuntu1804:~$ cd ~Desktop/Assignment4
bash: cd: ~Desktop/Assignment4: No such file or directory
user@Ubuntu1804:~$ cd ~/Desktop/Assignment4
user@Ubuntu1804:~/Desktop/Assignment4$ ls
2019A02.zip
user@Ubuntu1804:~/Desktop/Assignment4$ sudo dd if=/home/user/Desktop/Assignment4/
2019A02.zip of=2019A02.dd
[sudo] password for user:
24607+1 records in
24607+1 records out
12598879 bytes (13 MB, 12 MiB) copied, 0.443917 s, 28.4 MB/s
user@Ubuntu1804:~/Desktop/Assignment4$ ls
2019A02.dd  2019A02.zip
user@Ubuntu1804:~/Desktop/Assignment4$ md5sum 2019A02.dd
9ec1c8f62429182349f3979c39aed8fb  2019A02.dd
user@Ubuntu1804:~/Desktop/Assignment4$ md5sum 2019A02.zip
9ec1c8f62429182349f3979c39aed8fb  2019A02.zip
user@Ubuntu1804:~/Desktop/Assignment4$ 
```



```
user@Ubuntu1804:~$ cd ~Desktop/Assig
bash: cd: ~Desktop/Assignment4: No s
user@Ubuntu1804:~$ cd ~/Desktop/Assi
user@Ubuntu1804:~/Desktop/Assignment
2019A02.zip
user@Ubuntu1804:~/Desktop/Assignment
2019A02.zip of=2019A02.dd
[sudo] password for user:
24607+1 records in
24607+1 records out
12598879 bytes (13 MB, 12 MiB) copie
user@Ubuntu1804:~/Desktop/Assignment
2019A02.dd  2019A02.zip
user@Ubuntu1804:~/Desktop/Assignment
9ec1c8f62429182349f3979c39aed8fb  20
user@Ubuntu1804:~/Desktop/Assignment
9ec1c8f62429182349f3979c39aed8fb  20
user@Ubuntu1804:~/Desktop/Assignment
\)/HashCalc/HashCalc.exe
001c:err:module:import_dll Library M
\windows\\Microsoft.NET\\Framework64
001c:err:module:import_dll Library m
\Microsoft.NET\\Framework64\\v4.0.30
001c:err:module:attach_dlls Importin
ework64\\v4.0.30319\\mscorsvw.exe" f
000f:err:service:process_send_comman
ne!
```

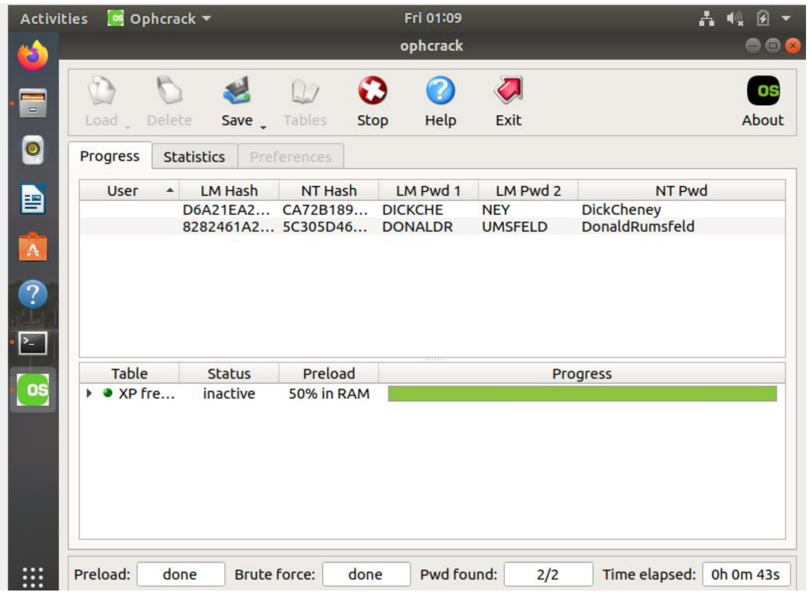
Data Format: File
Data: C:\users\user\Desktop\Assignment4\2019A02.dd

□ HMAC   Key Format: Text string   Key:

☑ MD5	9ec1c8f62429182349f3979c39aed8fb
☑ MD4	3a95bb1633fb3c62a97986eb3a4eed3d
☑ SHA1	dd91f418dcb81d16ba516bd7243b37cab8709438
☑ SHA256	5bd6a379f20940a59ae60cc9057bb262974fc930f93ec1a
☑ SHA384	7f08b42789d2472c22236020441bde9a4494b18db16027
☑ SHA512	7c9063eab7755ab00acb82dc83561066c260520c0e6b4
☑ RIPEMD160	e60dddf7c25c95b935554620f422d43d4f955179
☑ PANAMA	1bb59b07609b94334fca3a5ad6decaffbf67c56203a96d8
☑ TIGER	f6f7b7a278e5c284fbd5a8f0b879639399454d3b8da0348
☑ MD2	dec0544c8ff8afe9ec7056f35298c6d6
☑ ADLER32	7ee5c26e
☑ CRC32	20b839f8
□ eDonkey/ eMule	

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

First I launched the OphCrack application. Then I pressed load -> single hash. Pasted one of the NTLM hash in the box and pressed ok. Repeated the steps for the second NTLM hash. Then pressed crack and obtained the below passwords. (NTLM hashes:
D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A08176773
and
8282461A2BDAF626E6067B973FDDC643:5C305D4616C7571D5DDC6EEA5BA5C395)



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
	D6A21EA2...	CA72B189...	DICKCHE	NEY	DickCheney
	8282461A2...	5C305D46...	DONALDR	UMSFELD	DonaldRumsfeld

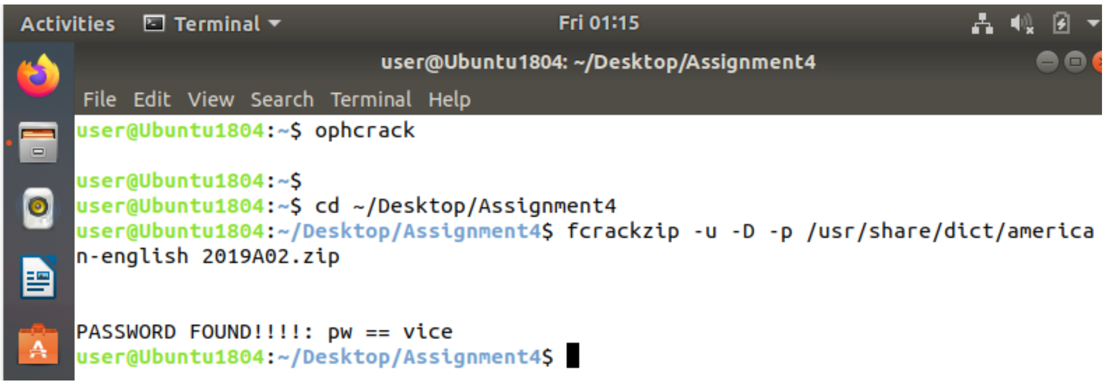
Table	Status	Preload	Progress
XP fre...	inactive	50% in RAM	🟩

Preload: done Brute force: done Pwd found: 2/2 Time elapsed: 0h 0m 43s

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) First I tried to open the zip file using the passwords I obtained via ophcrack (DickCheney and DonaldRumsfeld). However, it returned an error message. 2) So, I then used the frackzip zip file password cracker tool to see if I could obtain a password via dictionary mode. 3) I obtained the password ‘vice’. 4) I entered the password to open the image files and it was successful. 5) Finally I extracted the contents of the zip file to another directory called Extract.

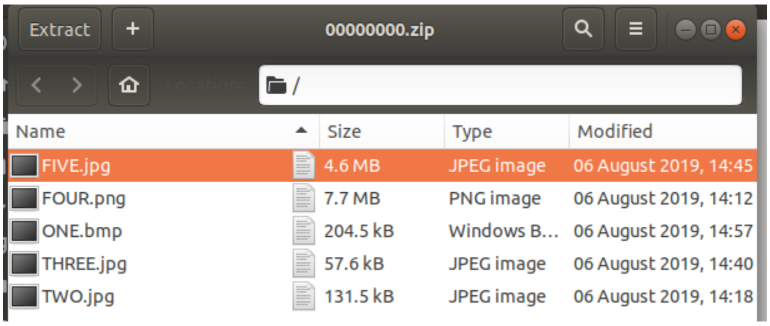
There is no relationship between this process and the NTLM passwords I obtained from ophcrack.



```
user@Ubuntu1804:~$ ophcrack

user@Ubuntu1804:~$
user@Ubuntu1804:~$ cd ~/Desktop/Assignment4
user@Ubuntu1804:~/Desktop/Assignment4$ fcrackzip -u -D -p /usr/share/dict/america
n-english 2019A02.zip


PASSWORD FOUND!!!!: pw == vice
user@Ubuntu1804:~/Desktop/Assignment4$ █
```

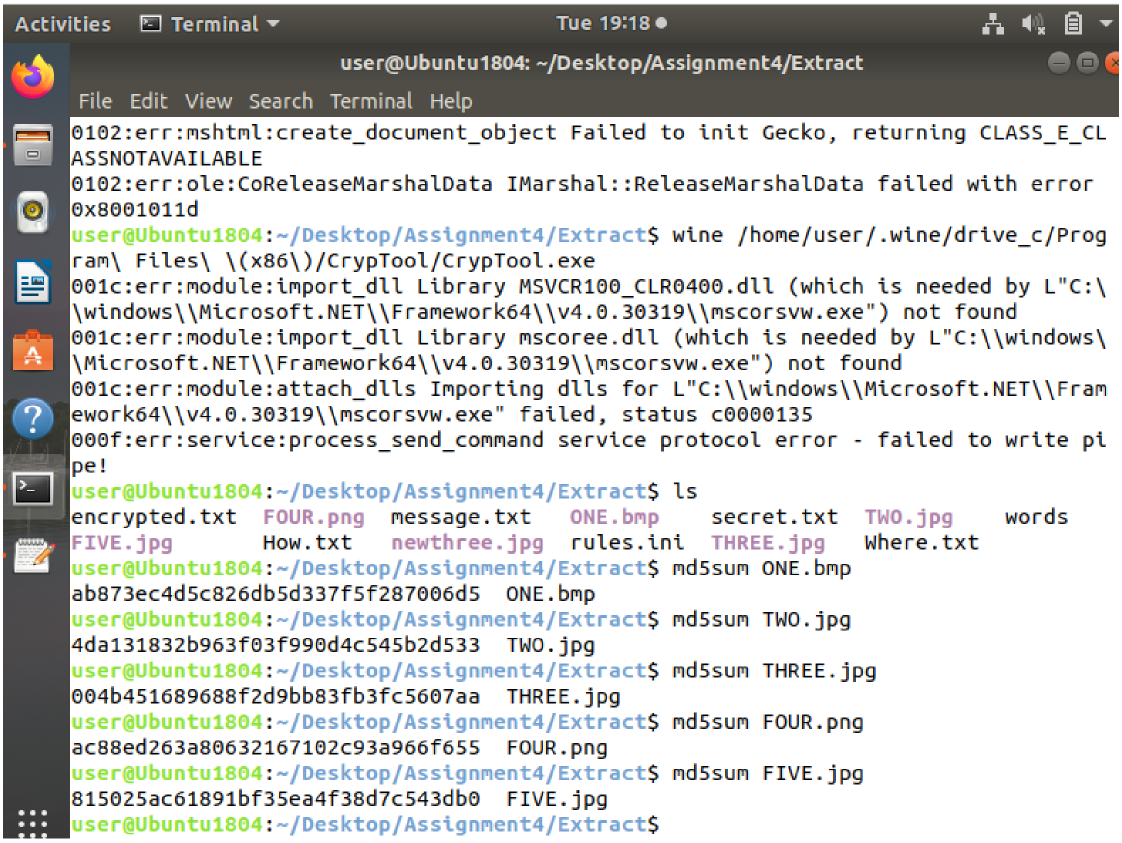
4. Describe the actual content of the encrypted file that you identified in Step 3. If there are multiple files, list their file names, types and MD5 hash values. Describe the visual contents in each file.

Content description	There were 5 image files found in the zip file where 3 of them were Jpeg, 1 of them was a PNG image and the other 1 was a windows bitmap image. All five images were stills of the cast members from the movie Vice.	
File Name	*File Type*	*MD5 Hash Value*
ONE.bmp	Windows Bitmap	ab873ec4d5c826db5d337f5f287006d5
TWO.jpg	Jpeg Image	4da131832b963f03f990d4c545b2d533
THREE.jpg	Jpeg Image	004b451689688f2d9bb83fb3fc5607aa
FOUR.png	PNG Image	ac88ed263a80632167102c93a966f655
FIVE.jpg	Jpeg Image	815025ac61891bf35ea4f38d7c543db0



Name	Size	Type	Modified
FIVE.jpg	4.6 MB	JPEG image	06 August 2019, 14:45
FOUR.png	7.7 MB	PNG image	06 August 2019, 14:12
ONE.bmp	204.5 kB	Windows B…	06 August 2019, 14:57
THREE.jpg	57.6 kB	JPEG image	06 August 2019, 14:40
TWO.jpg	131.5 kB	JPEG image	06 August 2019, 14:18

MD5 hash values of the files.


Activities
Terminal
Tue 19:18
user@Ubuntu1804: ~/Desktop/Assignment4/Extract
File Edit View Search Terminal Help

```
0102:err:mshtml:create_document_object Failed to init Gecko, returning CLASS_E_CL
ASSNOTAVAILABLE
0102:err:ole:CoReleaseMarshalData IMarshal::ReleaseMarshalData failed with error
0x8001011d
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ wine /home/user/.wine/drive_c/Prog
ram\ Files\ \(x86\)/CrypTool/CrypTool.exe
001c:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:\
\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001c:err:module:import_dll Library mscoree.dll (which is needed by L"C:\\windows\
\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001c:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fram
ework64\\v4.0.30319\\mscorsvw.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write pi
pe!
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ ls
encrypted.txt  FOUR.png   message.txt   ONE.bmp    secret.txt  TWO.jpg    words
FIVE.jpg       How.txt    newthree.jpg  rules.ini  THREE.jpg   Where.txt
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ md5sum ONE.bmp
ab873ec4d5c826db5d337f5f287006d5  ONE.bmp
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ md5sum TWO.jpg
4da131832b963f03f990d4c545b2d533  TWO.jpg
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ md5sum THREE.jpg
004b451689688f2d9bb83fb3fc5607aa  THREE.jpg
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ md5sum FOUR.png
ac88ed263a80632167102c93a966f655  FOUR.png
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ md5sum FIVE.jpg
815025ac61891bf35ea4f38d7c543db0  FIVE.jpg
user@Ubuntu1804:~/Desktop/Assignment4/Extract$
```

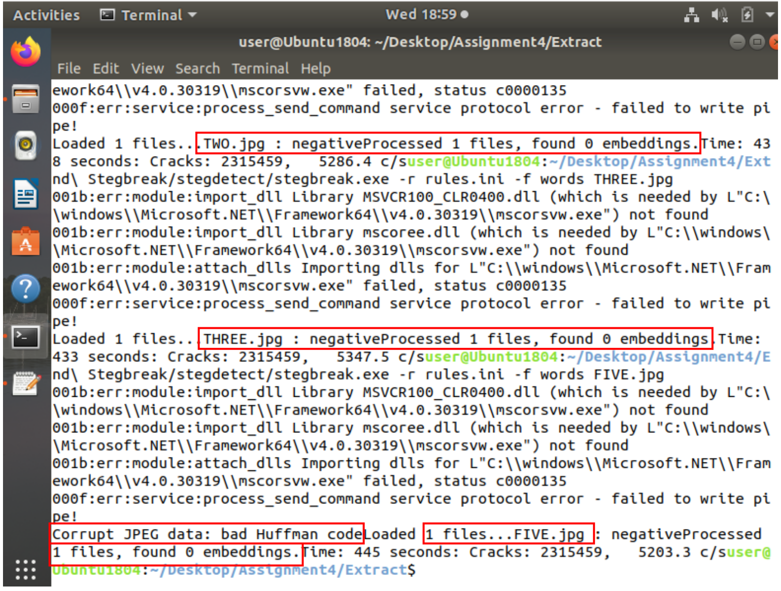
5. What tools will you now use to proceed your investigation and why?

Tool	*Reason*
Stegbreak	This tool is used to detect stenographic content in JPEG images.
S-Tools	This tool is used to hide and reveal contents in a graphic file.
JPseek	This tool is used to recover Steganography Images and reveal the hidden contents.

HxD Tool (Hex Editor)	This tool is used to compare image files, to recover corrupted files by using the right header, to overwrite the wrong header with the correct ones. This tool is also used to extract encrypted message, to reveal hidden images in the image file itself.
Openpuff	This tool is used to perform multimedia steganography. Also it can detect hidden files within the files.
Cyptool	This tool is used to encrypt a message or decrypt an encrypted message using many different encryptions.
Image viewer	This tool was used to view all the jpg, bmp and png images that were found in the files.
Text Editor	To view text files
RapidTables online ASCII Text to Hex Code Converter	To convert ASCII text into Hex numbers.

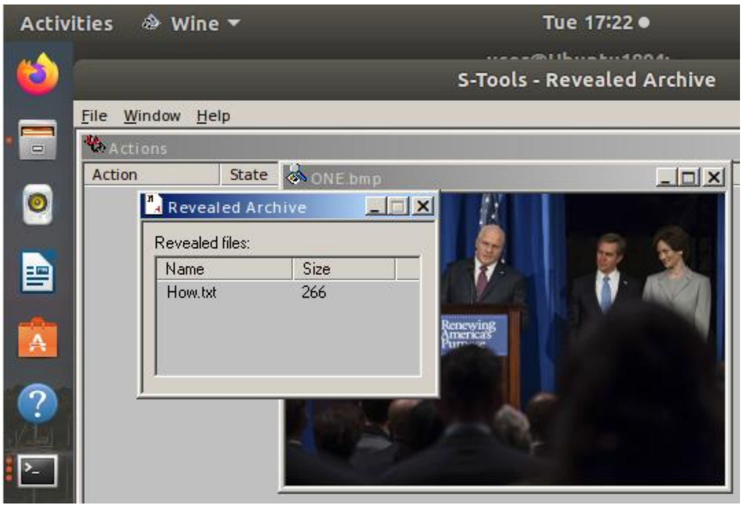
6. Describe how your investigation proceeded at this point, including screen shots.

First I transferred the rules.ini file and the words file from week09 directory to Extract directory where all the images were in. Then I used, Stegbreak tool to check if the 3 Jpeg images (TWO.jpg, THREE.jpg and FIVE.jpg) had any stenographic content in them. But all the jpeg images returned as no embedding found. Command example: wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/stegdetect/stegbreak.exe -r rules.ini -f words TWO.jpg



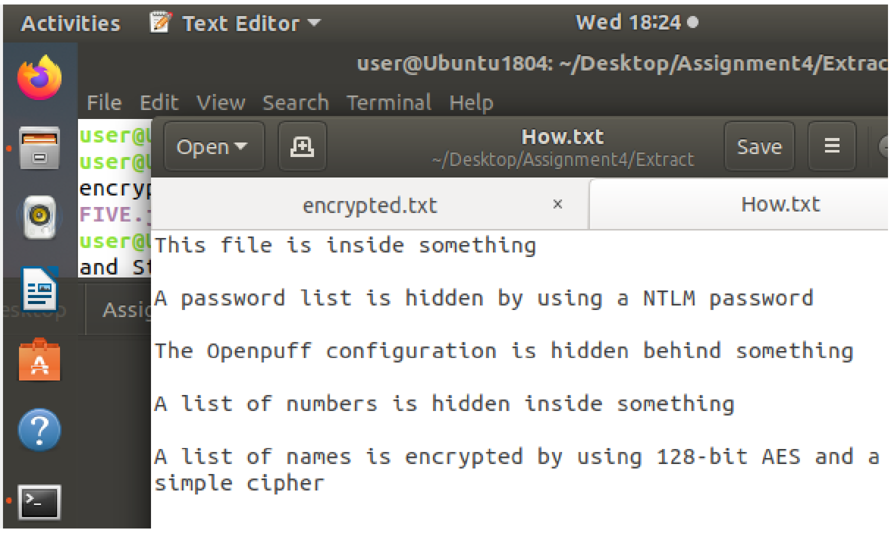
```
ework64\\v4.0.30319\\mscorsvw.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write pi
pe!
Loaded 1 files...TWO.jpg : negativeProcessed 1 files, found 0 embeddings.Time: 43
8 seconds: Cracks: 2315459,   5286.4 c/suser@Ubuntu1804:~/Desktop/Assignment4/Ext
nd\ Stegbreak/stegdetect/stegbreak.exe -r rules.ini -f words THREE.jpg
001b:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:\
\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001b:err:module:import_dll Library mscoree.dll (which is needed by L"C:\\windows\
\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001b:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fram
ework64\\v4.0.30319\\mscorsvw.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write pi
pe!
Loaded 1 files...THREE.jpg : negativeProcessed 1 files, found 0 embeddings.Time:
433 seconds: Cracks: 2315459,   5347.5 c/suser@Ubuntu1804:~/Desktop/Assignment4/E
nd\ Stegbreak/stegdetect/stegbreak.exe -r rules.ini -f words FIVE.jpg
001b:err:module:import_dll Library MSVCR100_CLR0400.dll (which is needed by L"C:\
\windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001b:err:module:import_dll Library mscoree.dll (which is needed by L"C:\\windows\
\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe") not found
001b:err:module:attach_dlls Importing dlls for L"C:\\windows\\Microsoft.NET\\Fram
ework64\\v4.0.30319\\mscorsvw.exe" failed, status c0000135
000f:err:service:process_send_command service protocol error - failed to write pi
pe!
Corrupt JPEG data: bad Huffman codeLoaded 1 files...FIVE.jpg : negativeProcessed
1 files, found 0 embeddings.Time: 445 seconds: Cracks: 2315459,   5203.3 c/suser@
Ubuntu1804:~/Desktop/Assignment4/Extract$
```

Then, I used S-Tools to check if the ONE.bmp image had any contents hidden in it. Command: wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/S-tool/S-Tools.exe was used to launch the S-tools application. After dragging the image onto the tool and pressing reveal it prompted for a password. I entered the NTLM password that I received from Ophcrack (DickCheney) and it revealed a text file called How.txt. I extracted that file into the extract directory. That How.txt file contained a list of instructions which let us know that there are several important information hidden in the other images.



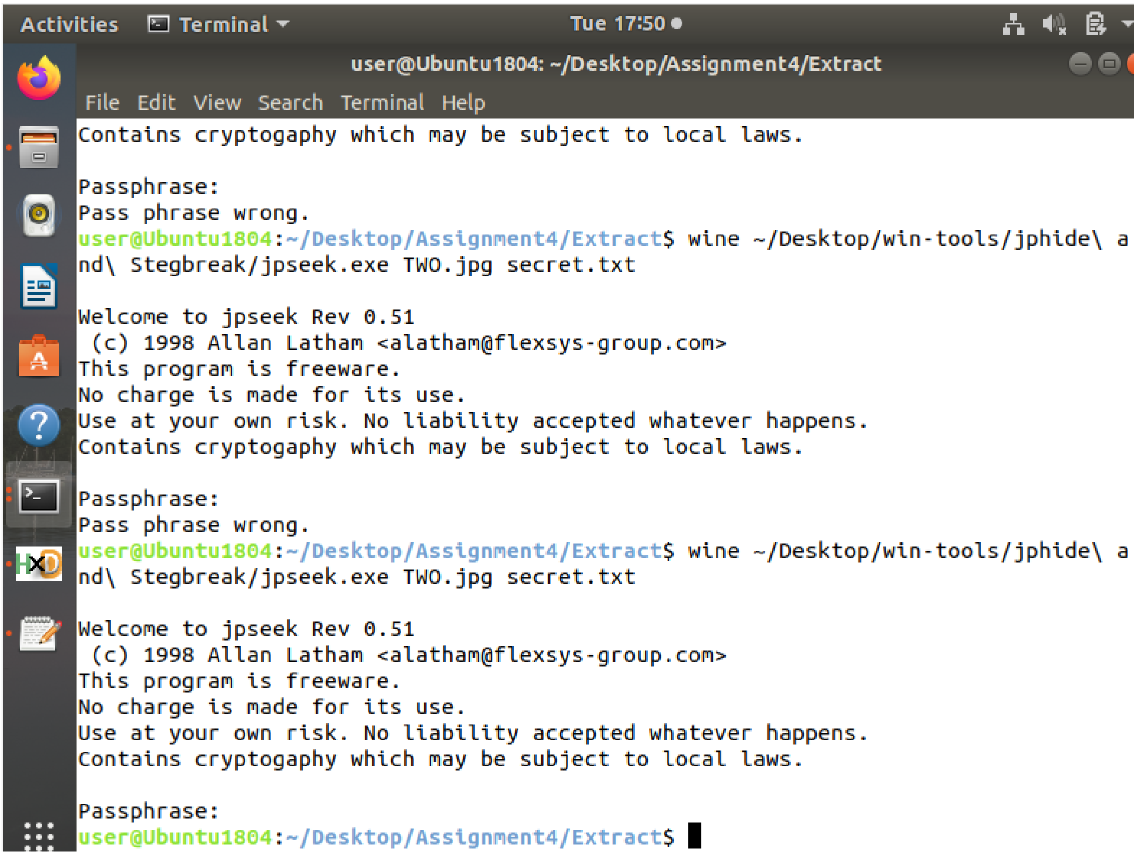
Revealed files:

Name	Size
How.txt	266

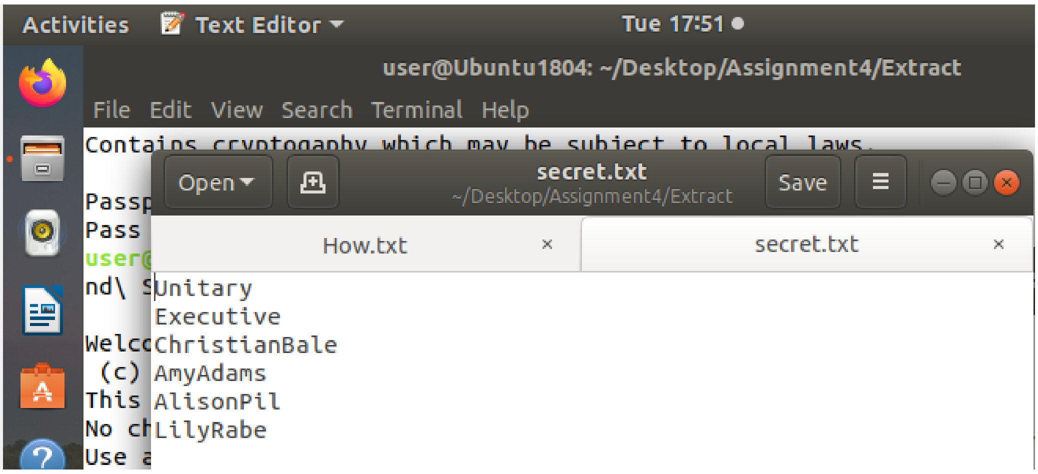

Activities
Text Editor
Wed 18:24
user@Ubuntu1804: ~/Desktop/Assignment4/Extrac
File Edit View Search Terminal Help
Open
How.txt
~/Desktop/Assignment4/Extract
Save
encrypted.txt
How.txt

```
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
```

Following the instructions, I used the JPseek tool to recover any hidden contents from Jpeg images. Since the 2nd instruction mentioned a password 'list' I entered the output to be a text file. Command: wine ~/Desktop/win-tools/jphide\ and\ Stegbreak/jpseek.exe TWO.jpg secret.txt. This also prompted for a password so based on 2nd instruction, I used the other NTLM password that I obtained from ophcrack (DonaldRumsfeld). I tried for THREE.jpg and FIVE.jpg but it said wrong passphrase and did not return anything. When I tried with TWO.jpg, it worked. The secret.txt was found in the Extract directory and it had a password list.

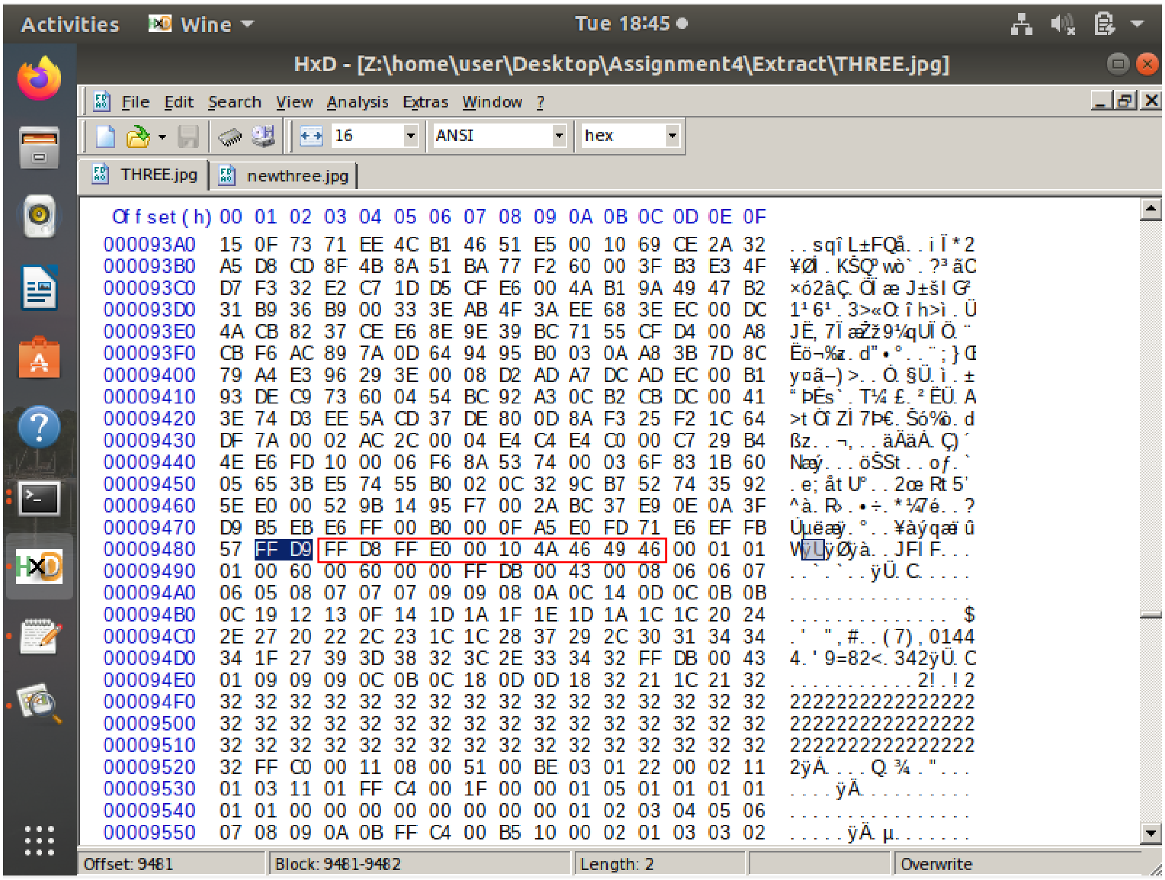

Activities
Terminal
Tue 17:50
user@Ubuntu1804: ~/Desktop/Assignment4/Extract
File Edit View Search Terminal Help

```
Contains cryptogaphy which may be subject to local laws.

Passphrase:
Pass phrase wrong.
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ wine ~/Desktop/win-tools/jphide\ a
nd\ Stegbreak/jpseek.exe TWO.jpg secret.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:
Pass phrase wrong.
user@Ubuntu1804:~/Desktop/Assignment4/Extract$ wine ~/Desktop/win-tools/jphide\ a
nd\ Stegbreak/jpseek.exe TWO.jpg secret.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/Assignment4/Extract$
```


Activities
Text Editor
Tue 17:51
user@Ubuntu1804: ~/Desktop/Assignment4/Extract
File Edit View Search Terminal Help
Open
secret.txt
~/Desktop/Assignment4/Extract
Save
How.txt
secret.txt

```
Unitary
Executive
ChristianBale
AmyAdams
AlisonPil
LilyRabe
```

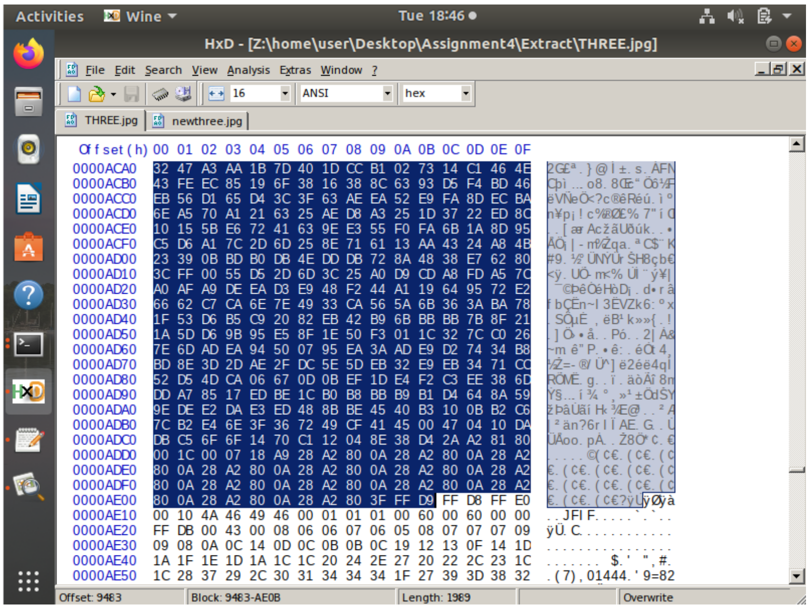
I noticed a pattern from this. The instructions given in the How.txt was for each image file. For instance, the first instruction was for ONE.bmp, the 2nd instruction was for TWO.jpg and the 3rd instruction would be for THREE.jpg and so on. Since JPseek and Stegbreak did not return anything for THREE.jpg, I opened the THREE.jpg in the HexEditor. Command: wine ~/Desktop/win-tools/HxD.exe. I noticed that there were multiple JPEG headers and footers found in THREE.jpg file. That meant that another jpeg image file was hidden within the THREE.jpg file.



Activities
Wine
Tue 18:45
HxD - [Z:\home\user\Desktop\Assignment4\Extract\THREE.jpg]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
THREE.jpg
newthree.jpg

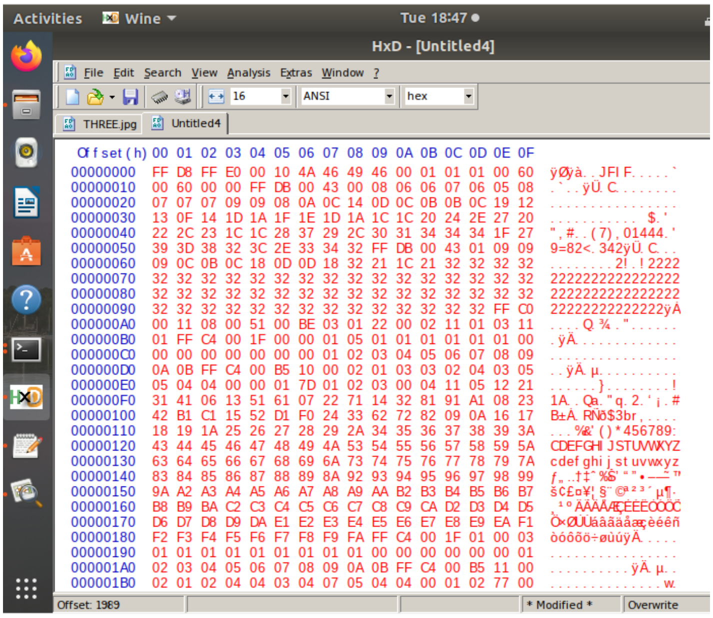
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000093A0  15 0F 73 71 EE 4C B1 46 51 E5 00 10 69 CE 2A 32
000093B0  A5 D8 CD 8F 4B 8A 51 BA 77 F2 60 00 3F B3 E3 4F
000093C0  D7 F3 32 E2 C7 1D D5 CF E6 00 4A B1 9A 49 47 B2
000093D0  31 B9 36 B9 00 33 3E AB 4F 3A EE 68 3E EC 00 DC
000093E0  4A CB 82 37 CE E6 8E 9E 39 BC 71 55 CF D4 00 A8
000093F0  CB F6 AC 89 7A 0D 64 94 95 B0 03 0A A8 3B 7D 8C
00009400  79 A4 E3 96 29 3E 00 08 D2 AD A7 DC AD EC 00 B1
00009410  93 DE C9 73 60 04 54 BC 92 A3 0C B2 CB DC 00 41
00009420  3E 74 D3 EE 5A CD 37 DE 80 0D 8A F3 25 F2 1C 64
00009430  DF 7A 00 02 AC 2C 00 04 E4 C4 E4 C0 00 C7 29 B4
00009440  4E E6 FD 10 00 06 F6 8A 53 74 00 03 6F 83 1B 60
00009450  05 65 3B E5 74 55 B0 02 0C 32 9C B7 52 74 35 92
00009460  5E E0 00 52 9B 14 95 F7 00 2A BC 37 E9 0E 0A 3F
00009470  D9 B5 EB E6 FF 00 B0 00 0F A5 E0 FD 71 E6 EF FB
00009480  57 FF D9 FF D8 FF E0 00 10 4A 46 49 46 00 01 01
00009490  01 00 60 00 60 00 00 FF DB 00 43 00 08 06 06 07
000094A0  06 05 08 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B
000094B0  0C 19 12 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24
000094C0  2E 27 20 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34
000094D0  34 1F 27 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43
000094E0  01 09 09 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32
000094F0  32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
00009500  32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
00009510  32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32
00009520  32 FF C0 00 11 08 00 51 00 BE 03 01 22 00 02 11
00009530  01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01 01
00009540  01 01 00 00 00 00 00 00 00 00 01 02 03 04 05 06
00009550  07 08 09 0A 0B FF C4 00 B5 10 00 02 01 03 03 02

Offset: 9481    Block: 9481-9482    Length: 2    Overwrite
```

So I copied the hex numbers from the beginning of the 2nd JPG header to its footer and pasted it in a new file. Then, I saved that file as newthree.jpg file. The newthree.jpg file had an openpuff configuration.

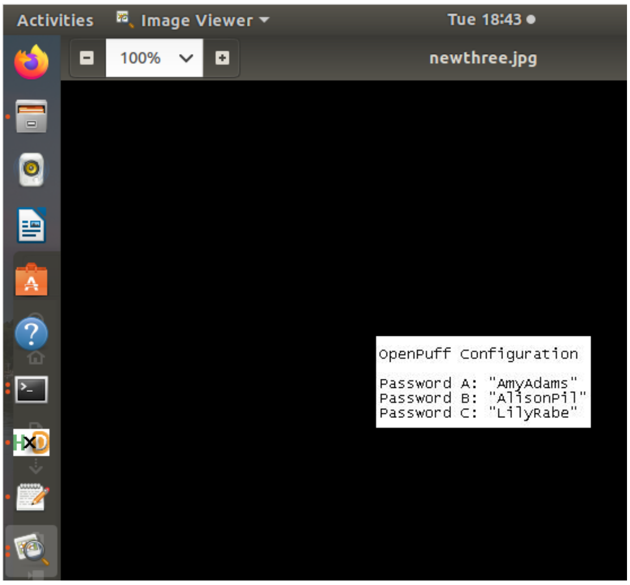


Activities
Wine
Tue 18:46
HxD - [Z:\home\user\Desktop\Assignment4\Extract\THREE.jpg]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
THREE.jpg
newthree.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000ACA0  32 47 A3 AA 1B 7D 40 1D CC B1 02 73 14 C1 46 4E
0000ACB0  43 FE EC 85 19 6F 38 16 38 8C 63 93 D5 F4 BD 46
0000ACC0  EB 56 D1 65 D4 3C 3F 63 AE EA 52 E9 FA 8D EC BA
0000ACD0  6E A5 70 A1 21 63 25 AE D8 A3 25 1D 37 22 ED 8C
0000ACE0  10 15 5B E6 72 41 63 9E E3 55 F0 FA 6B 1A 8D 95
0000ACF0  C5 D6 A1 7C 2D 6D 25 8E 71 61 13 AA 43 24 A8 4B
0000AD00  23 39 0B BD B0 DB 4E DD DB 72 8A 48 38 E7 62 80
0000AD10  3C FF 00 55 D5 2D 6D 3C 25 A0 D9 CD A8 FD A5 7C
0000AD20  A0 AF A9 DE EA D3 E9 48 F2 44 A1 19 64 95 72 E2
0000AD30  66 62 C7 CA 6E 7E 49 33 CA 56 5A 6B 36 3A BA 78
0000AD40  1F 53 D6 B5 C9 20 82 EB 42 B9 6B BB BB 7B 8F 21
0000AD50  1A 5D D6 9B 95 E5 8F 1E 50 F3 01 1C 32 7C C0 26
0000AD60  7E 6D AD EA 94 50 07 95 EA 3A AD E9 D2 74 34 B8
0000AD70  BD 8E 3D 2D AE 2F DC 5E 5D EB 32 E9 EB 34 71 CC
0000AD80  52 D5 4D CA 06 67 0D 0B EF 1D E4 F2 C3 EE 38 6D
0000AD90  DD A7 85 17 ED BE 1C B0 B8 BB B9 B1 D4 64 8A 59
0000ADA0  9E DE E2 DA E3 ED 48 8B BE 45 40 B3 10 0B B2 C6
0000ADB0  7C B2 E4 6E 3F 36 72 49 CF 41 45 00 47 04 10 DA
0000ADC0  DB C5 6F 6F 14 70 C1 12 04 8E 38 D4 2A A2 81 80
0000ADD0  00 1C 00 07 18 A9 28 A2 80 0A 28 A2 80 0A 28 A2
0000ADE0  80 0A 28 A2 80 0A 28 A2 80 0A 28 A2 80 0A 28 A2
0000ADF0  80 0A 28 A2 80 0A 28 A2 80 0A 28 A2 80 0A 28 A2
0000AE00  80 0A 28 A2 80 0A 28 A2 80 3F FF D9 FF D8 FF E0
0000AE10  00 10 4A 46 49 46 00 01 01 01 00 60 00 60 00 00
0000AE20  FF DB 00 43 00 08 06 06 07 06 05 08 07 07 07 09
0000AE30  09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12 13 0F 14 1D
0000AE40  1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 22 2C 23 1C
0000AE50  1C 28 37 29 2C 30 31 34 34 34 1F 27 39 3D 38 32

Offset: 9483    Block: 9483-AE0B    Length: 1989    Overwrite
```

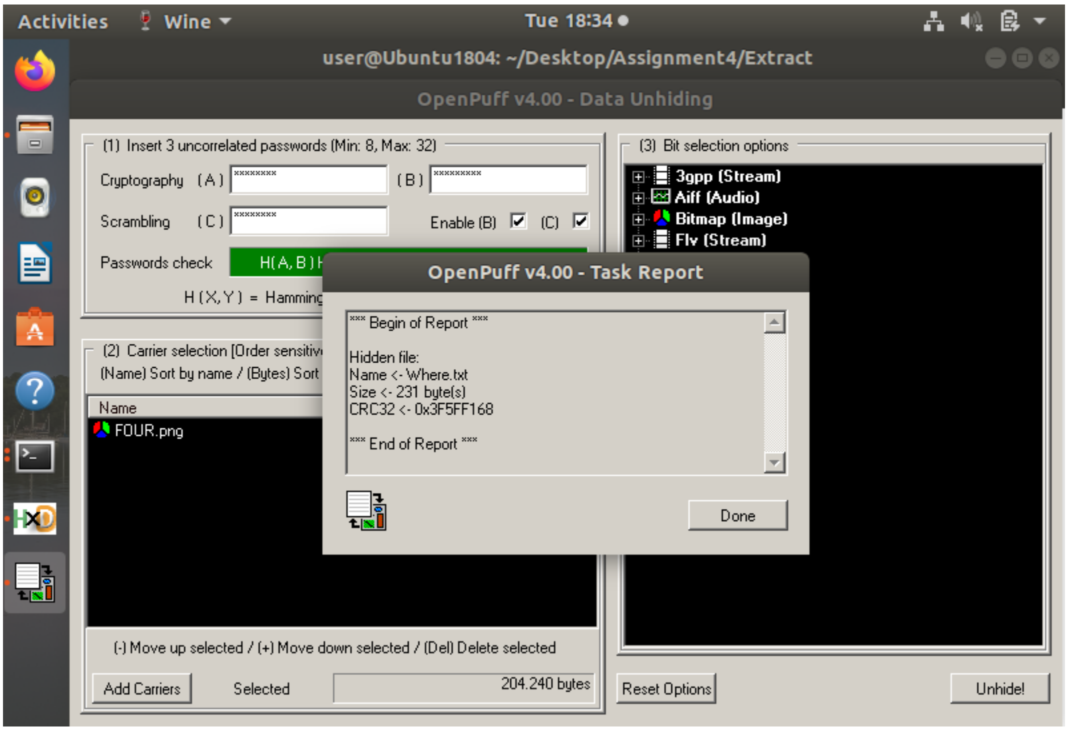


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 60  ÿØÿà..JFIF.....`
00000010  00 60 00 00 FF DB 00 43 00 08 06 06 07 06 05 08  .`..ÿÛ.C........
00000020  07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12  ................
00000030  13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20  ............ $.' 
00000040  22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27  ",#..(7),01444.'
00000050  39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09  9=82<.342ÿÛ.C...
00000060  09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32  ........2!.!2222
00000070  32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32  2222222222222222
00000080  32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32  2222222222222222
00000090  32 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C0  22222222222222ÿÀ
000000A0  00 11 08 00 51 00 BE 03 01 22 00 02 11 01 03 11  ....Q.¾.."......
000000B0  01 FF C4 00 1F 00 00 01 05 01 01 01 01 01 01 00  .ÿÄ.............
000000C0  00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09  ................
000000D0  0A 0B FF C4 00 B5 10 00 02 01 03 03 02 04 03 05  ..ÿÄ.µ..........
000000E0  05 04 04 00 00 01 7D 01 02 03 00 04 11 05 12 21  ......}........!
000000F0  31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23  1A..Qa."q.2.'¡.#
00000100  42 B1 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17  B±Á.RÑð$3br,....
00000110  18 19 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A  ...%&'()*456789:
00000120  43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A  CDEFGHIJSTUVWXYZ
00000130  63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A  cdefghijstuvwxyz
00000140  83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99  ƒ„…†‡ˆ‰Š''""•–—˜™
00000150  9A A2 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7  š¢£¤¥¦§¨©ª²³´µ¶·
00000160  B8 B9 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5  ¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
00000170  D6 D7 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1  Ö×ØÙÚáâãäåæçèéêñ
00000180  F2 F3 F4 F5 F6 F7 F8 F9 FA FF C4 00 1F 01 00 03  òóôõö÷øùúÿÄ.....
00000190  01 01 01 01 01 01 01 01 01 00 00 00 00 00 00 01  ................
000001A0  02 03 04 05 06 07 08 09 0A 0B FF C4 00 B5 11 00  ..........ÿÄ.µ..
000001B0  02 01 02 04 04 03 04 07 05 04 04 00 01 02 77 00  ..............w.
```



```
OpenPuff Configuration

Password A: "AmyAdams"
Password B: "AlisonPill"
Password C: "LilyRabe"
```

Then I launched the openpuff tool to see if I could reveal any hidden file from FOUR.png since this was the 4th instruction in the How.txt. Command: wine ~/Desktop/win-tools/OpenPuff/OpenPuff.exe. After adding all the passwords according to the configuration and pressing unhide, a text file called where.txt was found. I extracted the where.txt file to the extract directory.



Activities
Wine
Tue 18:34
user@Ubuntu1804: ~/Desktop/Assignment4/Extract
OpenPuff v4.00 - Data Unhiding
(1) Insert 3 uncorrelated passwords (Min: 8, Max: 32)
Cryptography (A)
(B)
Scrambling (C)
Enable (B) ☑ (C) ☑
Passwords check
H(A,B)
H(X,Y) = Hamming
(2) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort
Name
(-) Move up selected / (+) Move down selected / (Del) Delete selected
Add Carriers
Selected
Reset Options
Unhide!
(3) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
OpenPuff v4.00 - Task Report
Done

Cryptography (A) ******** (B) *********

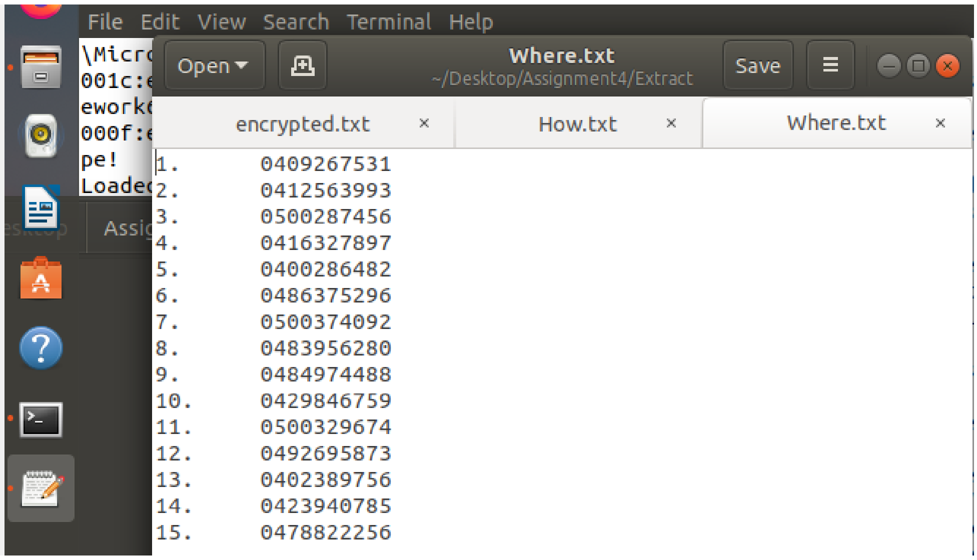
Scrambling (C) ********

Name: FOUR.png

Selected: 204.240 bytes

```
*** Begin of Report ***

Hidden file:
Name <- Where.txt
Size <- 231 byte(s)
CRC32 <- 0x3F5FF168

*** End of Report ***
```

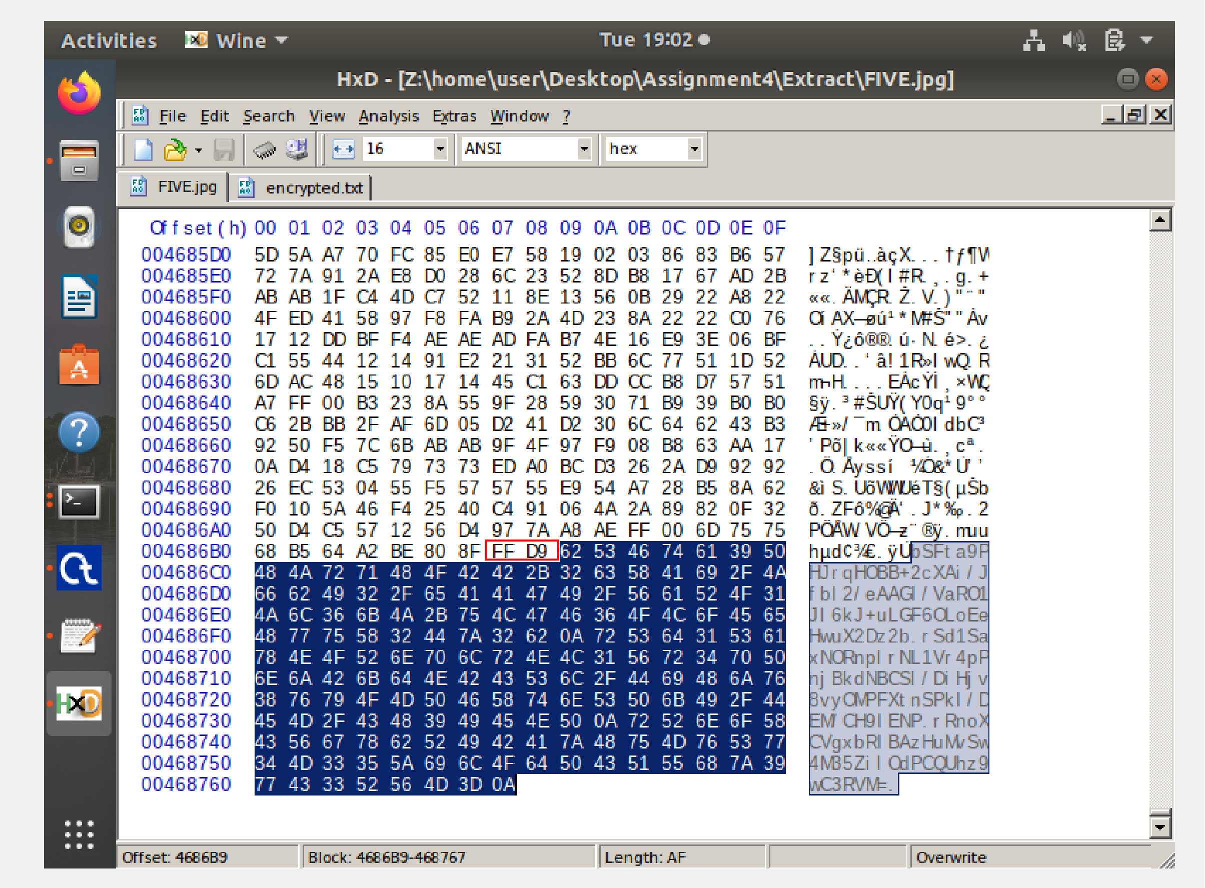
Where.txt had a list of numbers as said in the How.txt.



File Edit View Search Terminal Help
Open
Save
Where.txt
~/Desktop/Assignment4/Extract
encrypted.txt
How.txt
Where.txt

```
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
```

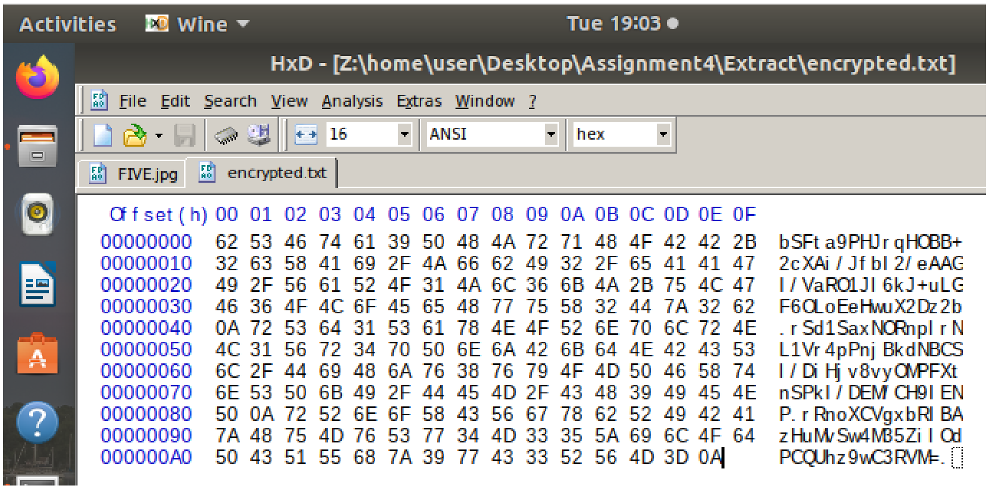
Then I continued to follow the How.txt's final instruction where it mentioned an encrypted message. Previously when I used stegbreak on FIVE.jpg it returned an error saying corrupt JPEG data bad Huffman code. So I decided to open FIVE.jpg file in hex editor. I noticed that the Jpeg footer FFD9 was not found at the end of the file but in the middle. The hex numbers after the footer looked like a message was encoded with base 64 encoding.


Activities
Wine
Tue 19:02
HxD - [Z:\home\user\Desktop\Assignment4\Extract\FIVE.jpg]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
FIVE.jpg
encrypted.txt

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

004685D0  5D 5A A7 70 FC 85 E0 E7 58 19 02 03 86 83 B6 57  ]Z§pü.àçX...†ƒ¶W
004685E0  72 7A 91 2A E8 D0 28 6C 23 52 8D B8 17 67 AD 2B  rz'*èÐ(l#R.¸.g.+
004685F0  AB AB 1F C4 4D C7 52 11 8E 13 56 0B 29 22 A8 22  ««.ÄMÇR.Ž.V.)"¨"
00468600  4F ED 41 58 97 F8 FA B9 2A 4D 23 8A 22 22 C0 76  OíAX—øú¹*M#Š""Àv
00468610  17 12 DD BF F4 AE AE AD FA B7 4E 16 E9 3E 06 BF  ..Ý¿ô®®.ú·N.é>.¿
00468620  C1 55 44 12 14 91 E2 21 31 52 BB 6C 77 51 1D 52  ÁUD..'â!1R»lwQ.R
00468630  6D AC 48 15 10 17 14 45 C1 63 DD CC B8 D7 57 51  m¬H....EÁcÝÌ¸×WQ
00468640  A7 FF 00 B3 23 8A 55 9F 28 59 30 71 B9 39 B0 B0  §ÿ.³#ŠUŸ(Y0q¹9°°
00468650  C6 2B BB 2F AF 6D 05 D2 41 D2 30 6C 64 62 43 B3  Æ+»/¯m.ÒAÒ0ldbC³
00468660  92 50 F5 7C 6B AB AB 9F 4F 97 F9 08 B8 63 AA 17  'Põ|k««ŸO—ù.¸cª.
00468670  0A D4 18 C5 79 73 73 ED A0 BC D3 26 2A D9 92 92  .Ô.Åyssí ¼Ó&*Ù''
00468680  26 EC 53 04 55 F5 57 57 55 E9 54 A7 28 B5 8A 62  &ìS.UõWWUéT§(µŠb
00468690  F0 10 5A 46 F4 25 40 C4 91 06 4A 2A 89 82 0F 32  ð.ZFô%@Ä'.J*‰‚.2
004686A0  50 D4 C5 57 12 56 D4 97 7A A8 AE FF 00 6D 75 75  PÔÅW.VÔ—z¨®ÿ.muu
004686B0  68 B5 64 A2 BE 80 8F FF D9 62 53 46 74 61 39 50  hµd¢¾€.ÿÙbSFta9P
004686C0  48 4A 72 71 48 4F 42 42 2B 32 63 58 41 69 2F 4A  HJrqHOBB+2cXAi/J
004686D0  66 62 49 32 2F 65 41 41 47 49 2F 56 61 52 4F 31  fbI2/eAAGI/VaRO1
004686E0  4A 6C 36 6B 4A 2B 75 4C 47 46 36 4F 4C 6F 45 65  Jl6kJ+uLGF6OLoEe
004686F0  48 77 75 58 32 44 7A 32 62 0A 72 53 64 31 53 61  HwuX2Dz2b.rSd1Sa
00468700  78 4E 4F 52 6E 70 6C 72 4E 4C 31 56 72 34 70 50  xNORnplrNL1Vr4pP
00468710  6E 6A 42 6B 64 4E 42 43 53 6C 2F 44 69 48 6A 76  njBkdNBCSl/DiHjv
00468720  38 76 79 4F 4D 50 46 58 74 6E 53 50 6B 49 2F 44  8vyOMPFXtnSPkI/D
00468730  45 4D 2F 43 48 39 49 45 4E 50 0A 72 52 6E 6F 58  EM/CH9IENP.rRnoX
00468740  43 56 67 78 62 52 49 42 41 7A 48 75 4D 76 53 77  CVgxbRIBAzHuMvSw
00468750  34 4D 33 35 5A 69 6C 4F 64 50 43 51 55 68 7A 39  4M35ZilOdPCQUhz9
00468760  77 43 33 52 56 4D 3D 0A                          wC3RVM=.
```

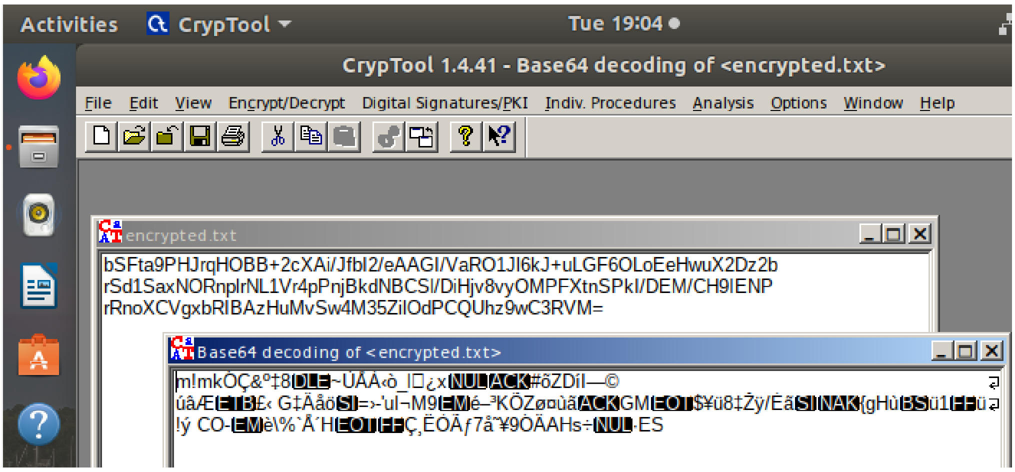
```
Offset: 4686B9    Block: 4686B9-468767    Length: AF    Overwrite
```

So I copied those hex numbers after the Jpeg footer into a new HxD file and saved it as encrypted.txt as the How.txt mentioned that this would be a ‘list’ of names.


Activities
Wine
Tue 19:03
HxD - [Z:\home\user\Desktop\Assignment4\Extract\encrypted.txt]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
FIVE.jpg
encrypted.txt

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  62 53 46 74 61 39 50 48 4A 72 71 48 4F 42 42 2B  bSFta9PHJrqHOBB+
00000010  32 63 58 41 69 2F 4A 66 62 49 32 2F 65 41 41 47  2cXAi/JfbI2/eAAG
00000020  49 2F 56 61 52 4F 31 4A 6C 36 6B 4A 2B 75 4C 47  I/VaRO1Jl6kJ+uLG
00000030  46 36 4F 4C 6F 45 65 48 77 75 58 32 44 7A 32 62  F6OLoEeHwuX2Dz2b
00000040  0A 72 53 64 31 53 61 78 4E 4F 52 6E 70 6C 72 4E  .rSd1SaxNORnplrN
00000050  4C 31 56 72 34 70 50 6E 6A 42 6B 64 4E 42 43 53  L1Vr4pPnjBkdNBCS
00000060  6C 2F 44 69 48 6A 76 38 76 79 4F 4D 50 46 58 74  l/DiHjv8vyOMPFXt
00000070  6E 53 50 6B 49 2F 44 45 4D 2F 43 48 39 49 45 4E  nSPkI/DEM/CH9IEN
00000080  50 0A 72 52 6E 6F 58 43 56 67 78 62 52 49 42 41  P.rRnoXCVgxbRIBA
00000090  7A 48 75 4D 76 53 77 34 4D 33 35 5A 69 6C 4F 64  zHuMvSw4M35ZilOd
000000A0  50 43 51 55 68 7A 39 77 43 33 52 56 4D 3D 0A     PCQUhz9wC3RVM=.
```

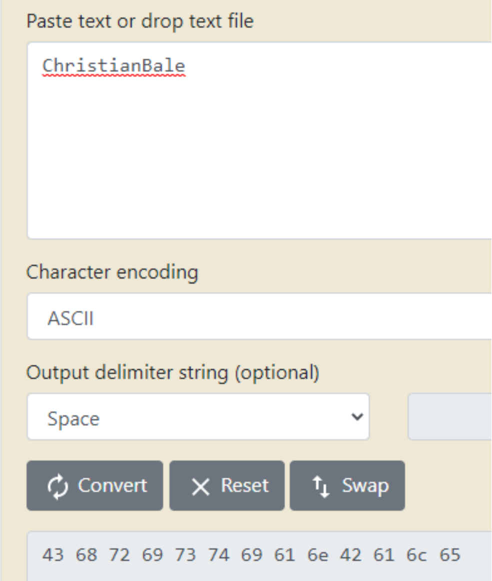
To decode the base 64 encoding and decrypt the message I used Cryptool. Command: wine /home/user/.wine/drive_c/Program\ Files\ \(x86\)/CrypTool/CrypTool.exe was used to launch the application. Opened the encrypted.txt file and decoded the message using base 64 decoding.


Activities
CrypTool
Tue 19:04
CrypTool 1.4.41 - Base64 decoding of <encrypted.txt>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
encrypted.txt
Base64 decoding of <encrypted.txt>

```
bSFta9PHJrqHOBB+2cXAi/JfbI2/eAAGI/VaRO1JI6kJ+uLGF6OLoEeHwuX2Dz2b
rSd1SaxNORnplrNL1Vr4pPnjBkdNBCSI/DiHjv8vyOMPFXtnSPkI/DEM/CH9IENP
rRnoXCVgxbRIBAzHuMvSw4M35ZiIOdPCQUhz9wC3RVM=
```

```
m!mkÒÇ&º‡8DLE~ÙÅÀ‹ò_I□¿xNULACK#õZDíl—©
úâÆETB£‹ G‡Äåö SI=›-'ul¬M9EMé–³KÖZø¤ùãACKGMEOT$¥ü8‡Žÿ/ĖãSINAK{gHùBSü1FFü
!ý CO-EMè\%`Å´HEOTFFÇ,ËÒÄƒ7å˜¥9ÒÄAHs÷NUL·ES
```

It was mentioned in the How.txt that AES encryption and a simple cipher has been used. First I, decrypted the AES encryption and it prompted for a HEX number password. There were three remaining passwords (Unitary, Executive and ChristianBale) on the password list (secret.txt) that were unused. So I tried converting Unitary, Executive and ChristianBale into hex numbers using an online converting tool and used it as the password. When I used, Unitary and Executive, the output was weird and it did not look like a list of name mentioned in How.txt. But when I used ChristianBale (hex numbers) as the password, the output looked like a list.



Paste text or drop text file

ChristianBale

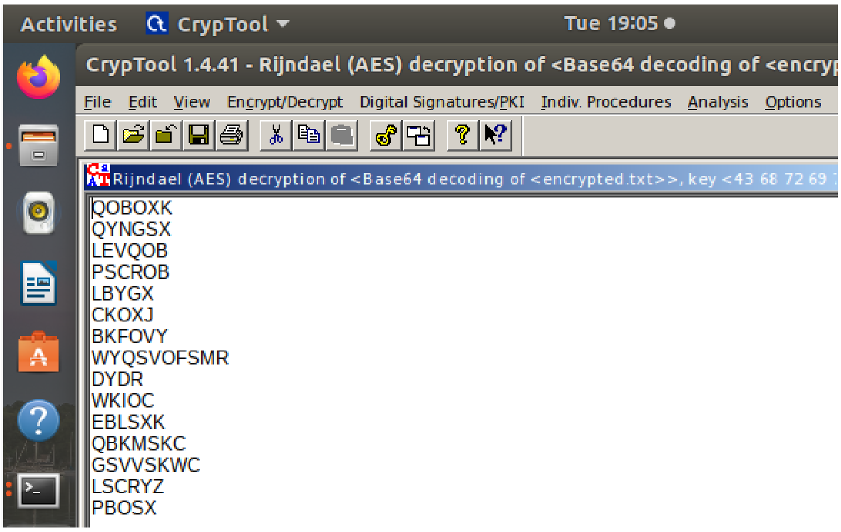
Character encoding

ASCII

Output delimiter string (optional)

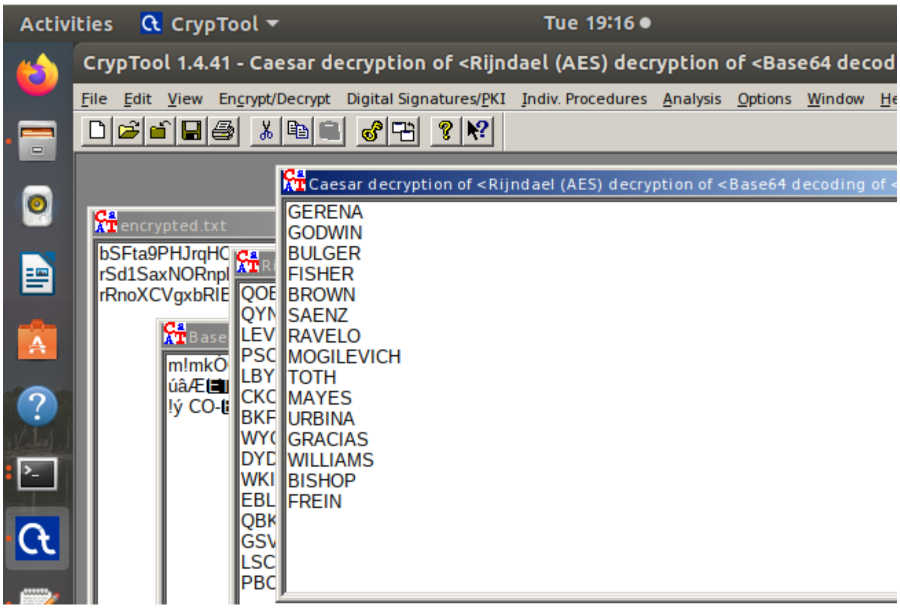
Space

```
43 68 72 69 73 74 69 61 6e 42 61 6c 65
```


Activities
CrypTool
Tue 19:05
CrypTool 1.4.41 - Rijndael (AES) decryption of <Base64 decoding of <encry
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options
Rijndael (AES) decryption of <Base64 decoding of <encrypted.txt>>, key <43 68 72 69 7

```
QOBOXK
QYNGSX
LEVQOB
PSCROB
LBYGX
CKOXJ
BKFOVY
WYQSVOFSMR
DYDR
WKIOC
EBLSXK
QBKMSKC
GSVVSKWC
LSCRYZ
PBOSX
```

Then I used Caesar cipher to decrypt the message further. Tried all of the alphabets one by one to see which was the key and found out that K was used as the key. Finally, a list of names were revealed.


Activities
CrypTool
Tue 19:16
CrypTool 1.4.41 - Caesar decryption of <Rijndael (AES) decryption of <Base64 decod
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window He
Caesar decryption of <Rijndael (AES) decryption of <Base64 decoding of <
encrypted.txt
Base

```
bSFta9PHJrqHC
rSd1SaxNORnpl
rRnoXCVgxbRlE
```

```
m!mkO
úâÆ
!ý CO-
```

```
QOE
QYN
LEV
PSC
LBY
CKC
BKF
WYC
DYD
WKI
EBL
QBK
GSV
LSC
PBC
```

```
GERENA
GODWIN
BULGER
FISHER
BROWN
SAENZ
RAVELO
MOGILEVICH
TOTH
MAYES
URBINA
GRACIAS
WILLIAMS
BISHOP
FREIN
```

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.

Overview:

A drug manufacturing location was identified in a warehouse behind Roma St Station where traces of powder was found. A laptop and 4 CDs was retrieved from the warehouse. I, Sangheetha Velayutham was assigned to this case by Sandra to analyse a zip file to retrieve any important information. I received an email from Sandra containing two NTLM hash strings retrieved from the criminal's laptop and the ZIP file from one of the CDs as attachments.

Evidence Form (Figure 1-11 of the text)

Brisbane Special Investigative Unit This form is to be used for only one piece of evidence. Fill out a separate form for each piece of evidence.			
Case No:	DrugRomaSt_20092021	Unit Number:	DrugRomaSt_17
Investigator:	Sangheetha Velayutham		
Nature of Case:	Illegal 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.
123654	CD containing a suspicious ZIP file	N/A	N/A
Evidence Recovered by:	Moti	Date & Time:	10th May 2021, 3:20 am
Evidence Placed in Locker:	Evidence placed in Forensics Lab Evidence Locker by Moti	Date & Time	10th May 2021, 4.30 am
Evidence Processed by	Description of Evidence		Date & Time
Moti	Obtained the CD		10th May 2021, 3:20 am
Moti	Stored the CD in the lab's Evidence locker		10th May 2021, 4.30 am
Sandra	Analyses CD in lab.		10th May 2021, 9.30 am
Sandra	Make 3 copies of the CD. Stores 2 copies in the lab and distributes the 3rd copy to colleagues. Sends a copy of Zip file to Sangheetha Velayutham.		10th May 2021, 11.00 am
Sangheetha Velayutham	Makes a copy of zip file and it is stored on virtual machine, Directory = /Desktop/Assignment4		10th May 2021, 3.00 pm
			Page 1 of 1 <

Recommendation:

My steps should be retraced to see if the same results that I got can be obtained. Save all the retrieved files carefully to prevent tampering. There were two unused passwords in the password list (Unitary, Executive). Figure out what the two passwords are for. Maybe it can be used to access any account.

Summary of steps:

1. Made a copy of zip file to ensure integrity of file (dd tool).
2. Verified the integrity by checking the hash values with the given hash value (hashcalc tool and md5 command).
3. Used Ophcrack to crack both the NTLM hashes and obtained two passwords (DickCheney and DonaldRumsfeld).
4. Used the frackzip tool to obtain the password of the zip file (password: vice).
5. Used the password obtained from frackzip (vice) to extract all files in the zip file to another directory called Extract.
6. Stegbreak tool was used to see if there was any hidden content in the jpeg files. None was found.
7. S-Tools was used to reveal a hidden text file (how.txt) from ONE.bmp.
8. The How.txt had instructions on where important details were hidden.
9. Jpseek tool was used to reveal a password list from TWO.jpg image using one of the NTLM password (DonaldRumsfeld).
10. THREE.jpg image was opened using HxD hex editor tool. An image file was hidden within the THREE.jpg.
11. The hidden image file was extracted into a new file. The hidden image file had an openpuff configuration.
12. Openpuff tool was used to unhide hidden contents of FOUR.jpg. The openpuff configuration that was found was used and a text file (Where.txt) was revealed.
13. FIVE.jpg had a corrupt jpeg data, so it was opened in HxD tool. There was a base 64 encoded message after the JPEG footer.
14. The encoded message was then decoded using base 64 decoding in Cryptool. Then the decoded message was decrypted as the How.txt mentioned that the message was encrypted using AES algorithm.
15. Later the message was further decrypted using Caesar cipher (K as key) revealing a list of names.

What was recovered? :

Image File	**Content recovered from Image file**
ONE.bmp	**How.txt** (recovered using S-tools) – contained instructions on where important details are hidden
TWO.jpg	**secret.txt** (recovered using JPseek) - password list with 6 passwords
THREE.jpg	**newthree.jpg** (hidden image file – recovered using HxD editor) - Openpuff configuration with 3 of the passwords from secret.txt
FOUR.png	**Where.txt** (recovered using OpenPuff) – list of numbers (15 numbers)
FIVE.jpg	**encrypted.txt** (encrypted message – obtained using HxD editor and decrypted the message using Cryptool) – list of names (15 names)

Interpretation:

The How.txt was instructions for the accused to know where important details are hidden in the image files. The password list was the various passwords they used via various tools to hide information. The newthree.jpg clearly stated the openpuff password configuration. The list of numbers found in where.txt are most probably Australian mobile numbers of drug dealers/buyers/fellow drug manufacturers. The list of names found may also be of drug dealers/buyers/fellow drug manufacturers. Since there are 15 names and 15 numbers, the numbers could be the mobile number of the people who the names belong to.

Suggestions:

Firstly, contact the relevant communications service provider to check the owners of the mobile numbers obtained. The mobile numbers and the list of names can also be checked in the police database. Check if the any of the names are related to any drug incident. If the numbers belong to the list of names that was obtained, then check each people's background to see if anything relates to drug incidents. Call each of them in for questioning. Then if there are evidence connecting them to any drug incidents, their mobile numbers can be tracked to find them. If the numbers do not match the list of names we have, then call each of them in for questioning and see if they know anything related to the warehouse drug manufacturing incident.

Reference:

RapidTables (2021.) *ASCII to Hex | Text to Hex Code Converter*, RapidTables, accessed 20 September 2021.

Winzip (2021.) *Potentially Unsafe File Types*, Winzip, accessed 20 September 2021.