Rahul Prithu
CSCI 395 – Digital Forensics
Lab 3

Case Background:

The chair's assistant at the Computer Science Department has had suspicions on a Professor leaking secret CS information to other departments. The chair's assistant found a disk that may contain evidences to prove that someone is in-fact leaking CS Department secrets as well as who the leaker is.

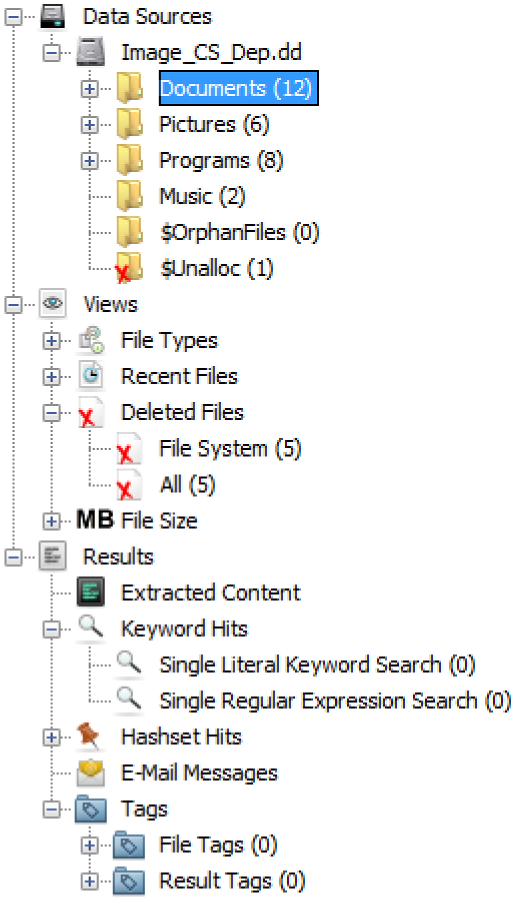
I have been assigned to this case. I was given access to the disk image to investigate it and report my findings.

I was also given MD5 hash to confirm that no data was changed in between:
b41cc17b42abb8f70b2ba8d030551c72

Analysis:

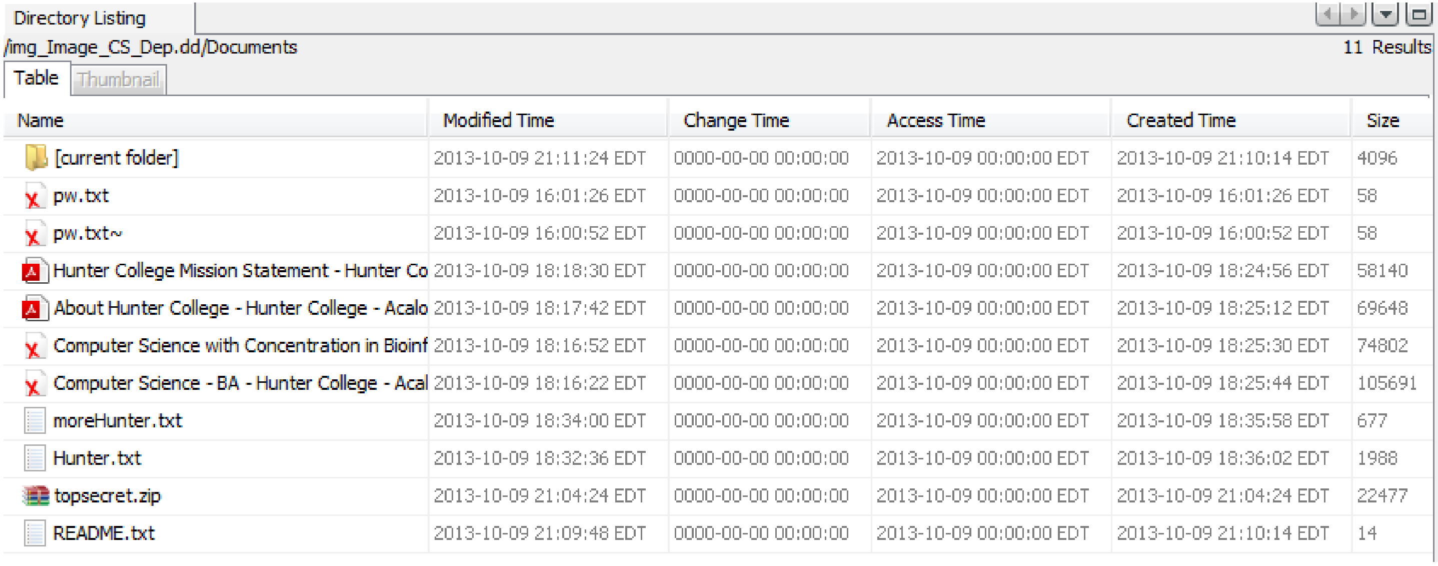
- Autopsy:

Running it on Autopsy revealed these files:



- Data Sources
  - Image_CS_Dep.dd
    - Documents (12)
    - Pictures (6)
    - Programs (8)
    - Music (2)
    - $OrphanFiles (0)
    - $Unalloc (1)
- Views
  - File Types
  - Recent Files
  - Deleted Files
    - File System (5)
    - All (5)
  - MB File Size
- Results
  - Extracted Content
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Tags
    - File Tags (0)
    - Result Tags (0)

Opening up the first of the 4 main directories, Documents:



Directory Listing

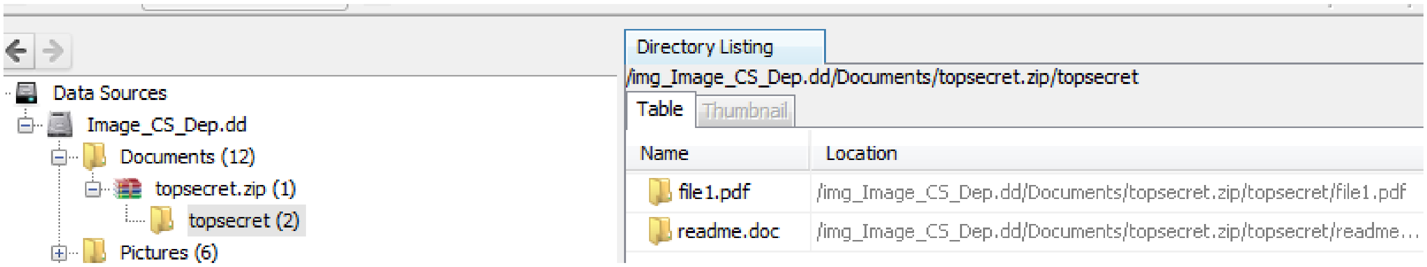
/img_Image_CS_Dep.dd/Documents

11 Results

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2013-10-09 21:11:24 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:10:14 EDT	4096
pw.txt	2013-10-09 16:01:26 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 16:01:26 EDT	58
pw.txt~	2013-10-09 16:00:52 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 16:00:52 EDT	58
Hunter College Mission Statement - Hunter Co	2013-10-09 18:18:30 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:24:56 EDT	58140
About Hunter College - Hunter College - Acalo	2013-10-09 18:17:42 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:25:12 EDT	69648
Computer Science with Concentration in Bioinf	2013-10-09 18:16:52 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:25:30 EDT	74802
Computer Science - BA - Hunter College - Acal	2013-10-09 18:16:22 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:25:44 EDT	105691
moreHunter.txt	2013-10-09 18:34:00 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:35:58 EDT	677
Hunter.txt	2013-10-09 18:32:36 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 18:36:02 EDT	1988
topsecret.zip	2013-10-09 21:04:24 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:04:24 EDT	22477
README.txt	2013-10-09 21:09:48 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:10:14 EDT	14

I immediately found a password protected zip named “topsecret.zip”.
Going inside it showed two files:

- file1.pdf
- readme.doc



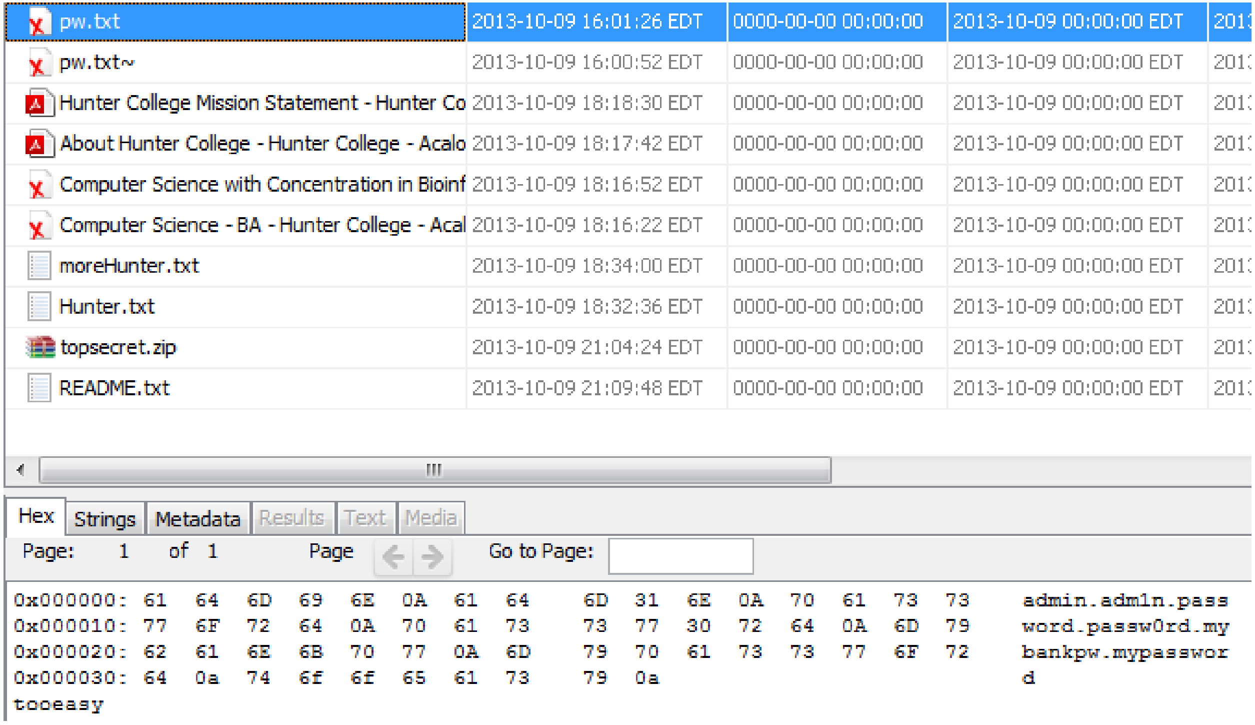
Data Sources
Image_CS_Dep.dd
Documents (12)
topsecret.zip (1)
topsecret (2)
Pictures (6)

Directory Listing

/img_Image_CS_Dep.dd/Documents/topsecret.zip/topsecret

Name	Location
file1.pdf	/img_Image_CS_Dep.dd/Documents/topsecret.zip/topsecret/file1.pdf
readme.doc	/img_Image_CS_Dep.dd/Documents/topsecret.zip/topsecret/readme...

There is also a file called “pw.txt”, perhaps this has the password to the zip.



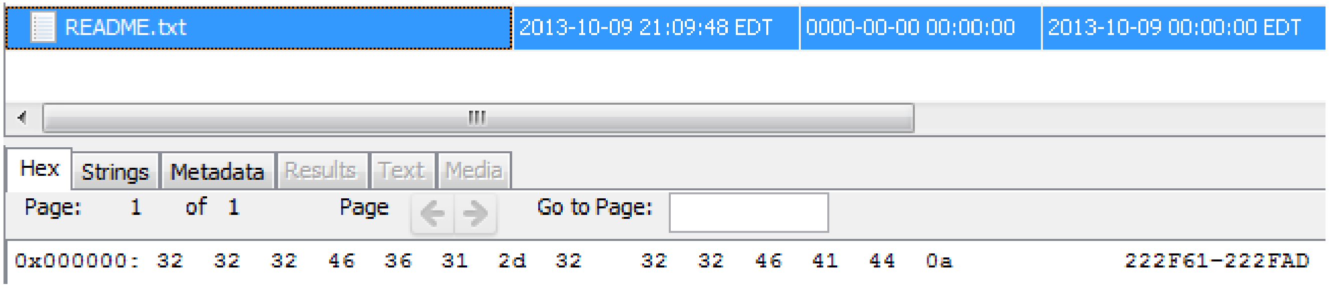
pw.txt	2013-10-09 16:01:26 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
pw.txt~	2013-10-09 16:00:52 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
Hunter College Mission Statement - Hunter Co	2013-10-09 18:18:30 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
About Hunter College - Hunter College - Acalo	2013-10-09 18:17:42 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
Computer Science with Concentration in Bioinf	2013-10-09 18:16:52 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
Computer Science - BA - Hunter College - Acal	2013-10-09 18:16:22 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
moreHunter.txt	2013-10-09 18:34:00 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
Hunter.txt	2013-10-09 18:32:36 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
topsecret.zip	2013-10-09 21:04:24 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201
README.txt	2013-10-09 21:09:48 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	201

Page: 1 of 1 Page Go to Page:

```
0x000000: 61  64  6D  69  6E  0A  61  64   6D  31  6E  0A  70  61  73  73    admin.adm1n.pass
0x000010: 77  6F  72  64  0A  70  61  73   73  77  30  72  64  0A  6D  79    word.passw0rd.my
0x000020: 62  61  6E  6B  70  77  0A  6D   79  70  61  73  73  77  6F  72    bankpw.mypasswor
0x000030: 64  0a  74  6f  6f  65  61  73   79  0a                            d
tooeasy
```

I went through the other files in Autopsy, they didn't have any valuable information. Most of them were information regarding Hunter College.

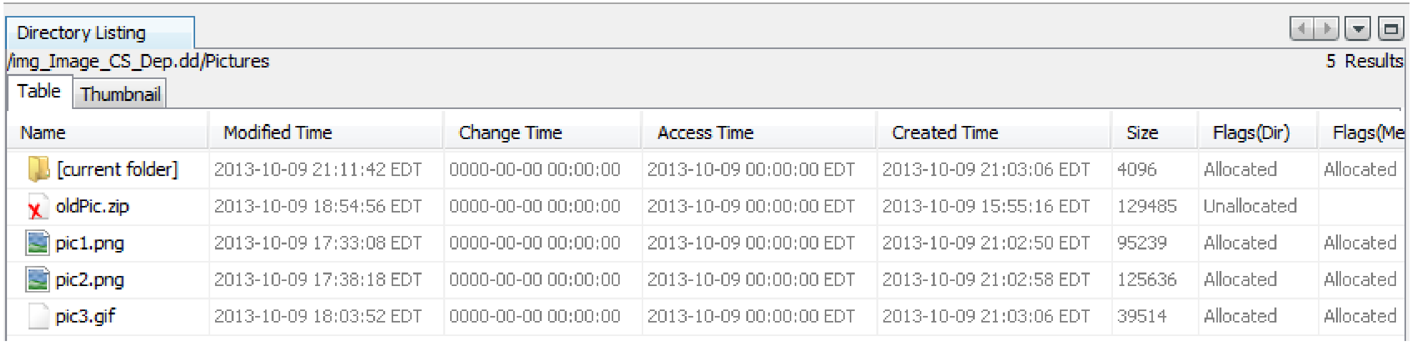
Except for one file: README.txt
It contains a string of what appears to be hexadecimal addresses.



README.txt	2013-10-09 21:09:48 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT

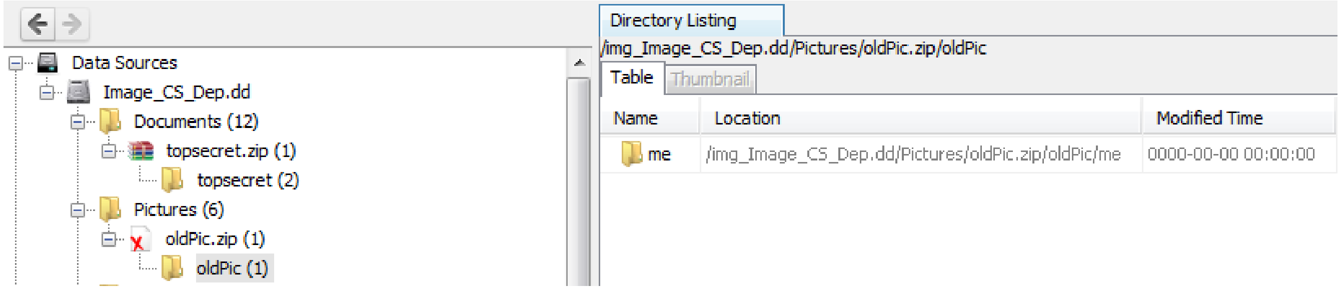
```
0x000000: 32  32  32  46  36  31  2d  32    32  32  46  41  44  0a          222F61-222FAD
```

Moving to the next main directory, Pictures, revealed 3 images. Two images were png (pic1: light refracton, pic2: flatiron building) and the third was a gif (pic3: marshmallow pizza).



Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Me
[current folder]	2013-10-09 21:11:42 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:03:06 EDT	4096	Allocated	Allocated
oldPic.zip	2013-10-09 18:54:56 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 15:55:16 EDT	129485	Unallocated	
pic1.png	2013-10-09 17:33:08 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:02:50 EDT	95239	Allocated	Allocated
pic2.png	2013-10-09 17:38:18 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:02:58 EDT	125636	Allocated	Allocated
pic3.gif	2013-10-09 18:03:52 EDT	0000-00-00 00:00:00	2013-10-09 00:00:00 EDT	2013-10-09 21:03:06 EDT	39514	Allocated	Allocated

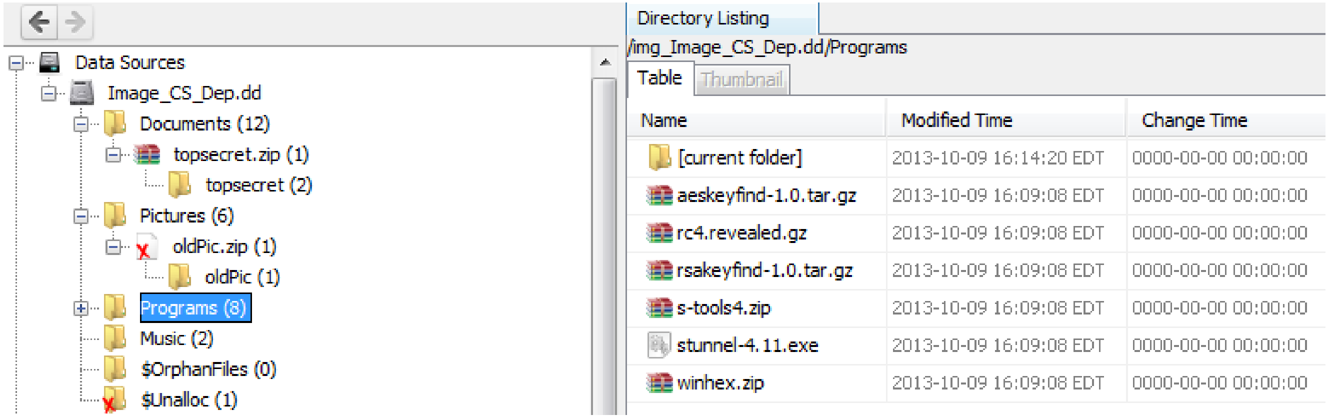
There is also traces of a deleted zip called "oldPic.zip". It is still available in the disk, so I exported it out of Autopsy. This too is password protected.



```
Data Sources
  Image_CS_Dep.dd
    Documents (12)
      topsecret.zip (1)
        topsecret (2)
    Pictures (6)
      oldPic.zip (1)
        oldPic (1)
```

Name	Location	Modified Time
me	/img_Image_CS_Dep.dd/Pictures/oldPic.zip/oldPic/me	0000-00-00 00:00:00

In the Programs folder, I found a number of programs.

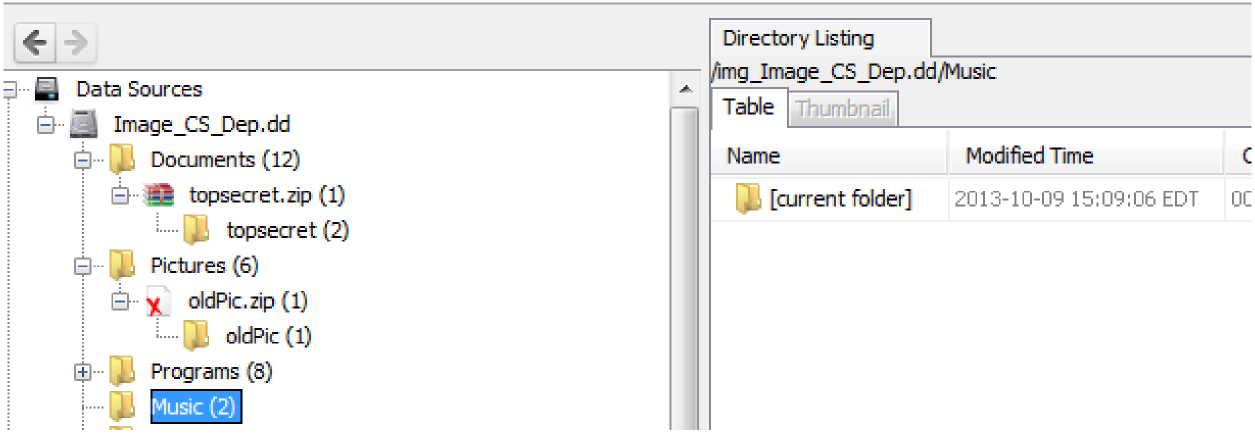


```
Data Sources
  Image_CS_Dep.dd
    Documents (12)
      topsecret.zip (1)
        topsecret (2)
    Pictures (6)
      oldPic.zip (1)
        oldPic (1)
    Programs (8)
    Music (2)
    $OrphanFiles (0)
    $Unalloc (1)
```

Name	Modified Time	Change Time
[current folder]	2013-10-09 16:14:20 EDT	0000-00-00 00:00:00
aeskeyfind-1.0.tar.gz	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00
rc4.revealed.gz	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00
rsakeyfind-1.0.tar.gz	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00
s-tools4.zip	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00
stunnel-4.11.exe	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00
winhex.zip	2013-10-09 16:09:08 EDT	0000-00-00 00:00:00

Upon running them, I came across a steganography software called “S-Tools”. Steganography is used to hide messages inside image and audio files. Interesting.

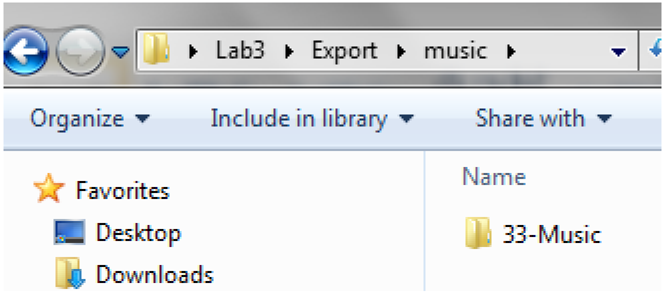
The last directory Music, was apparently found to be empty.



/img_Image_CS_Dep.dd/Music

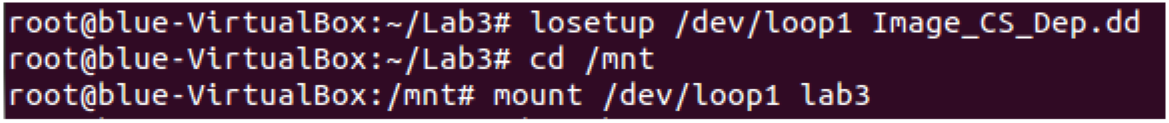
Name	Modified Time	C
[current folder]	2013-10-09 15:09:06 EDT	0C

Exporting it out of Autopsy revealed another empty folder called “33-music”.

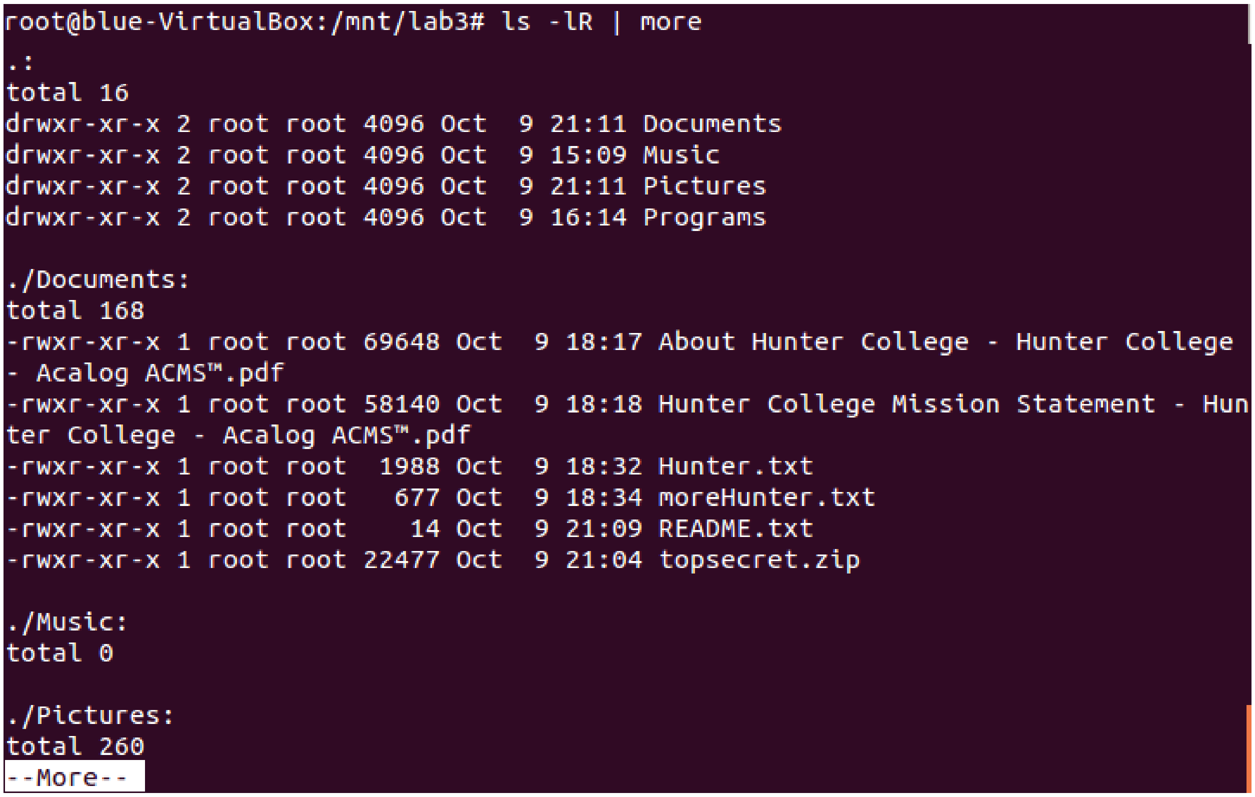


- Mounting Disk Image:

I mounted the image file on my Linux machine to dig deeper into the files.



```
root@blue-VirtualBox:~/Lab3# losetup /dev/loop1 Image_CS_Dep.dd
root@blue-VirtualBox:~/Lab3# cd /mnt
root@blue-VirtualBox:/mnt# mount /dev/loop1 lab3
```

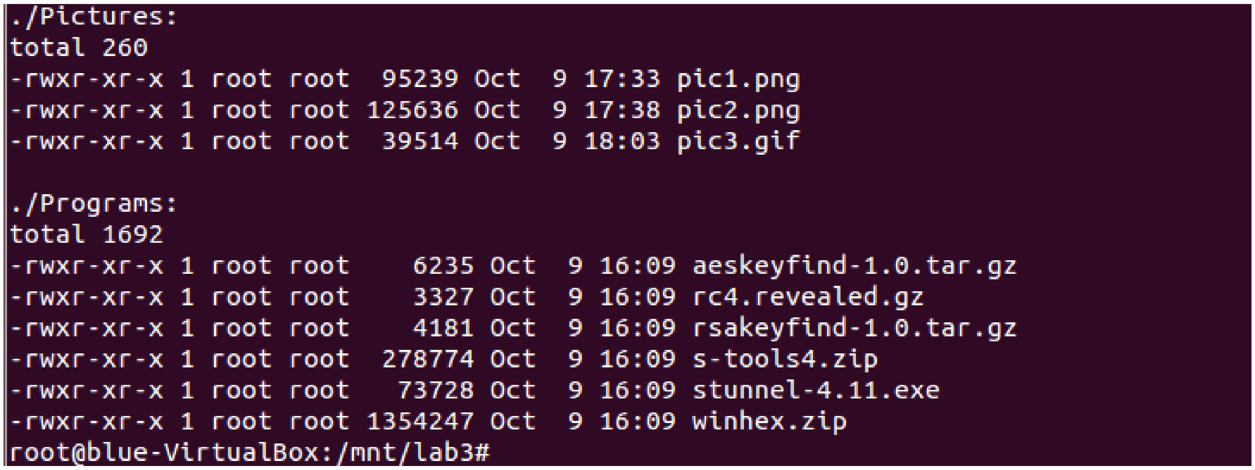


```
root@blue-VirtualBox:/mnt/lab3# ls -lR | more
.:
total 16
drwxr-xr-x 2 root root 4096 Oct  9 21:11 Documents
drwxr-xr-x 2 root root 4096 Oct  9 15:09 Music
drwxr-xr-x 2 root root 4096 Oct  9 21:11 Pictures
drwxr-xr-x 2 root root 4096 Oct  9 16:14 Programs

./Documents:
total 168
-rwxr-xr-x 1 root root 69648 Oct  9 18:17 About Hunter College - Hunter College
- Acalog ACMS™.pdf
-rwxr-xr-x 1 root root 58140 Oct  9 18:18 Hunter College Mission Statement - Hun
ter College - Acalog ACMS™.pdf
-rwxr-xr-x 1 root root  1988 Oct  9 18:32 Hunter.txt
-rwxr-xr-x 1 root root   677 Oct  9 18:34 moreHunter.txt
-rwxr-xr-x 1 root root    14 Oct  9 21:09 README.txt
-rwxr-xr-x 1 root root 22477 Oct  9 21:04 topsecret.zip

./Music:
total 0

./Pictures:
total 260
--More--
```

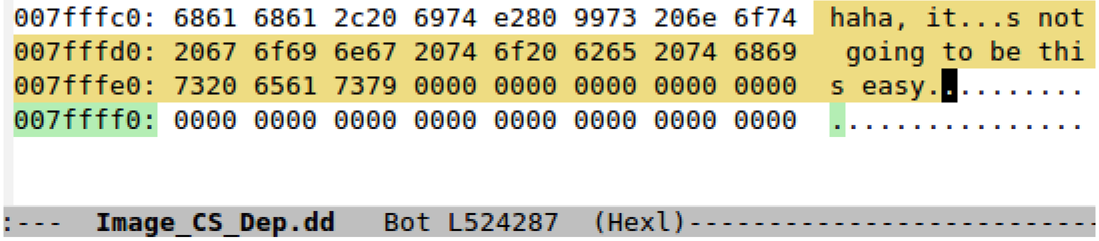


```
./Pictures:
total 260
-rwxr-xr-x 1 root root  95239 Oct  9 17:33 pic1.png
-rwxr-xr-x 1 root root 125636 Oct  9 17:38 pic2.png
-rwxr-xr-x 1 root root  39514 Oct  9 18:03 pic3.gif

./Programs:
total 1692
-rwxr-xr-x 1 root root    6235 Oct  9 16:09 aeskeyfind-1.0.tar.gz
-rwxr-xr-x 1 root root    3327 Oct  9 16:09 rc4.revealed.gz
-rwxr-xr-x 1 root root    4181 Oct  9 16:09 rsakeyfind-1.0.tar.gz
-rwxr-xr-x 1 root root  278774 Oct  9 16:09 s-tools4.zip
-rwxr-xr-x 1 root root   73728 Oct  9 16:09 stunnel-4.11.exe
-rwxr-xr-x 1 root root 1354247 Oct  9 16:09 winhex.zip
root@blue-VirtualBox:/mnt/lab3#
```

Same files as Autopsy showed.

I opened the disk image in Emacs. Jumping straight to the end revealed this message:

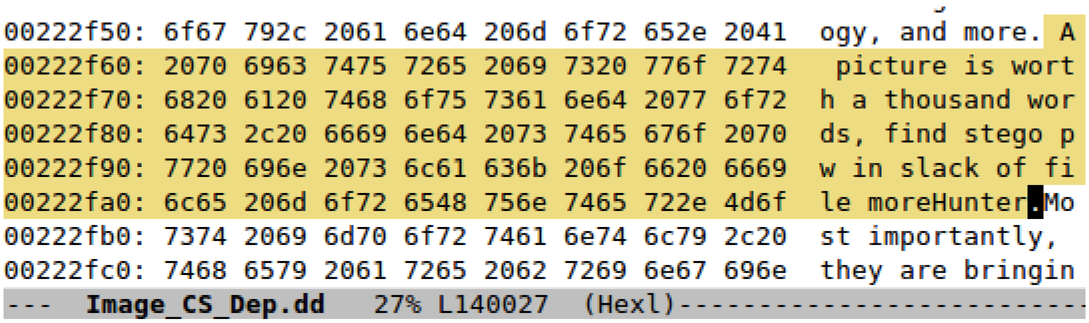


```
007fffc0: 6861 6861 2c20 6974 e280 9973 206e 6f74  haha, it...s not
007fffd0: 2067 6f69 6e67 2074 6f20 6265 2074 6869   going to be thi
007fffe0: 7320 6561 7379 0000 0000 0000 0000 0000  s easy..........
007ffff0: 0000 0000 0000 0000 0000 0000 0000 0000  ................


:---  Image_CS_Dep.dd    Bot L524287   (Hexl)-------------------------
```

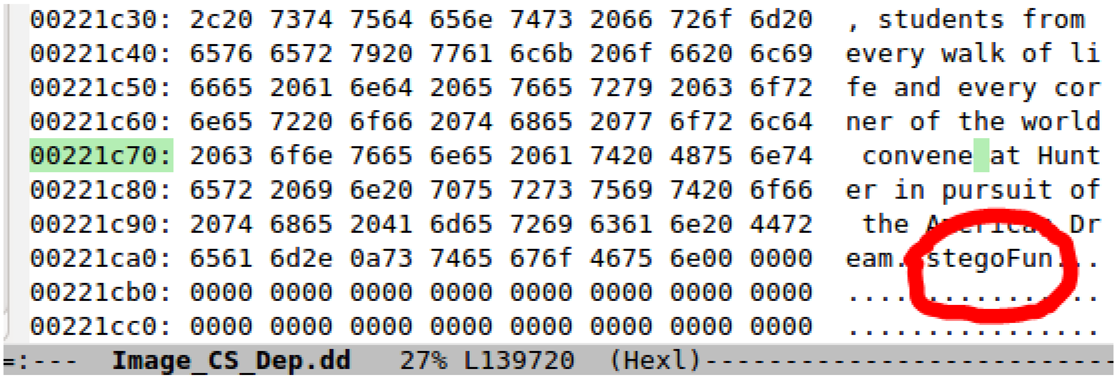
Looks like the leaker has indeed taken precautions incase the disk was lost.

I searched for the hexadecimal addresses, and came upon the phrase: “a picture is worth a thousand words, find stego pw in slack of file moreHunter”



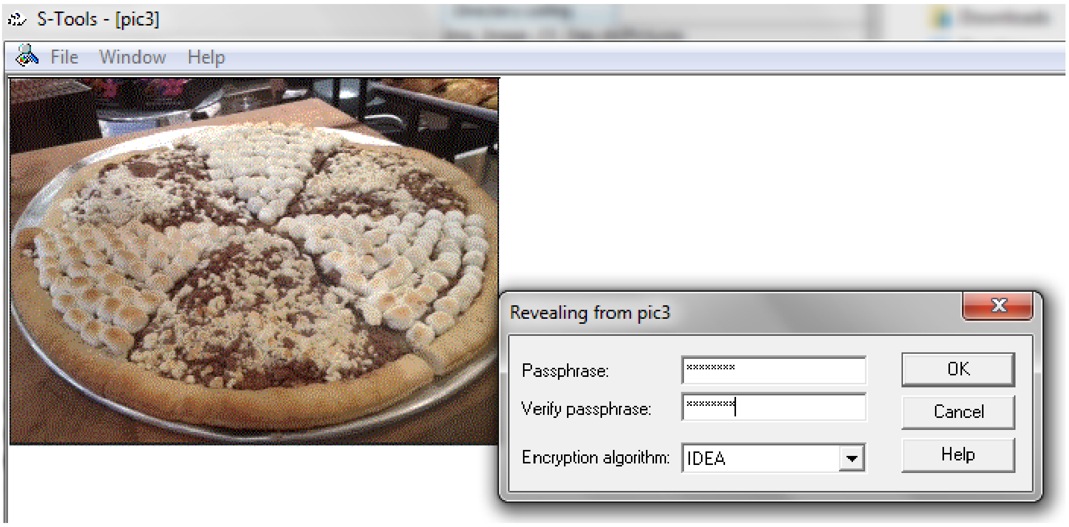
```
00222f50: 6f67 792c 2061 6e64 206d 6f72 652e 2041  ogy, and more. A
00222f60: 2070 6963 7475 7265 2069 7320 776f 7274   picture is wort
00222f70: 6820 6120 7468 6f75 7361 6e64 2077 6f72  h a thousand wor
00222f80: 6473 2c20 6669 6e64 2073 7465 676f 2070  ds, find stego p
00222f90: 7720 696e 2073 6c61 636b 206f 6620 6669  w in slack of fi
00222fa0: 6c65 206d 6f72 6548 756e 7465 722e 4d6f  le moreHunter.Mo
00222fb0: 7374 2069 6d70 6f72 7461 6e74 6c79 2c20  st importantly,
00222fc0: 7468 6579 2061 7265 2062 7269 6e67 696e  they are bringin
---  Image_CS_Dep.dd    27% L140027   (Hexl)-------------------------
```

Going to the end of the file “moreHunter” in the image file gave me my next clue, “stegoFun”.



```
00221c30: 2c20 7374 7564 656e 7473 2066 726f 6d20  , students from
00221c40: 6576 6572 7920 7761 6c6b 206f 6620 6c69  every walk of li
00221c50: 6665 2061 6e64 2065 7665 7279 2063 6f72  fe and every cor
00221c60: 6e65 7220 6f66 2074 6865 2077 6f72 6c64  ner of the world
00221c70: 2063 6f6e 7665 6e65 2061 7420 4875 6e74   convene at Hunt
00221c80: 6572 2069 6e20 7075 7273 7569 7420 6f66  er in pursuit of
00221c90: 2074 6865 2041 6d65 7269 6361 6e20 4472   the American Dr
00221ca0: 6561 6d2e 0a73 7465 676f 4675 6e00 0000  eam..stegoFun...
00221cb0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00221cc0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
=:---  Image_CS_Dep.dd    27% L139720   (Hexl)-------------------------
```

I ran the gif file in the S-Tools program, and provided the password “stegoFun”, which made way to a hidden text file called “Password.txt”

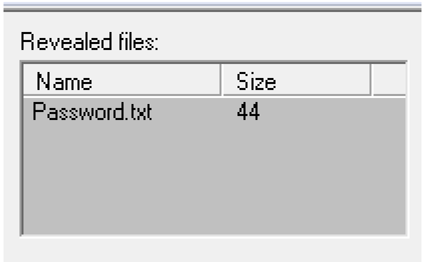


Passphrase: ********

Verify passphrase: ********

Encryption algorithm: IDEA

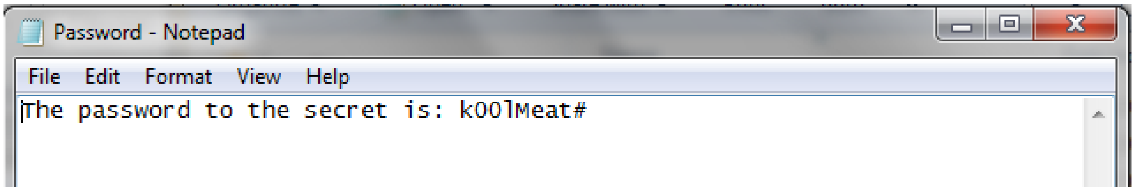
Revealed This File:



Revealed files:

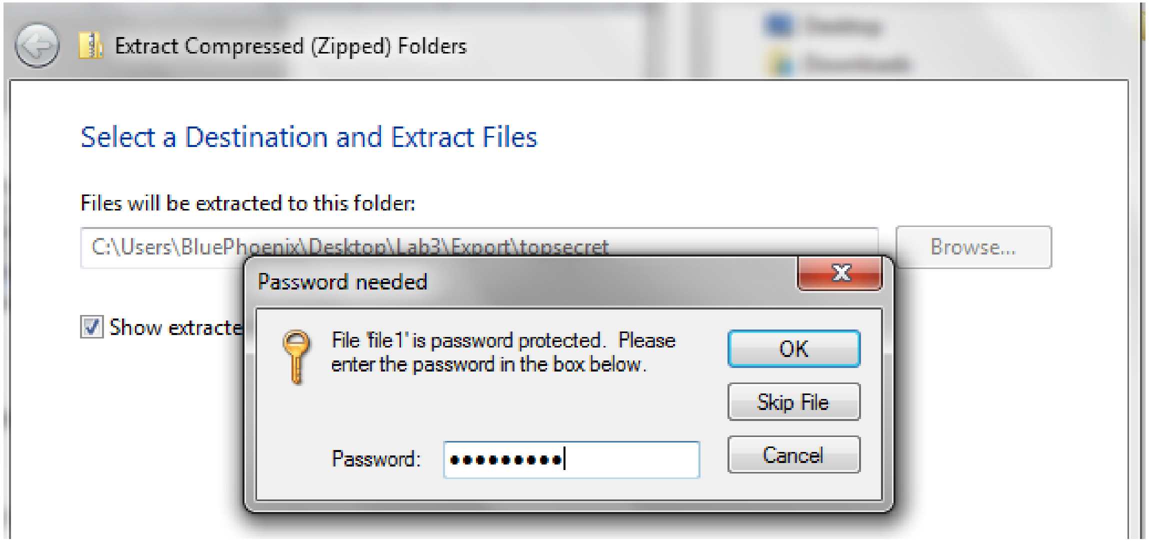
Name	Size
Password.txt	44

Inside “Password.txt”:



```
The password to the secret is: k00lMeat#
```

Trying the password inside “Password.txt” opened up “topsecret.zip”.



Select a Destination and Extract Files

Files will be extracted to this folder:

C:\Users\BluePhoenix\Desktop\Lab3\Export\topsecret

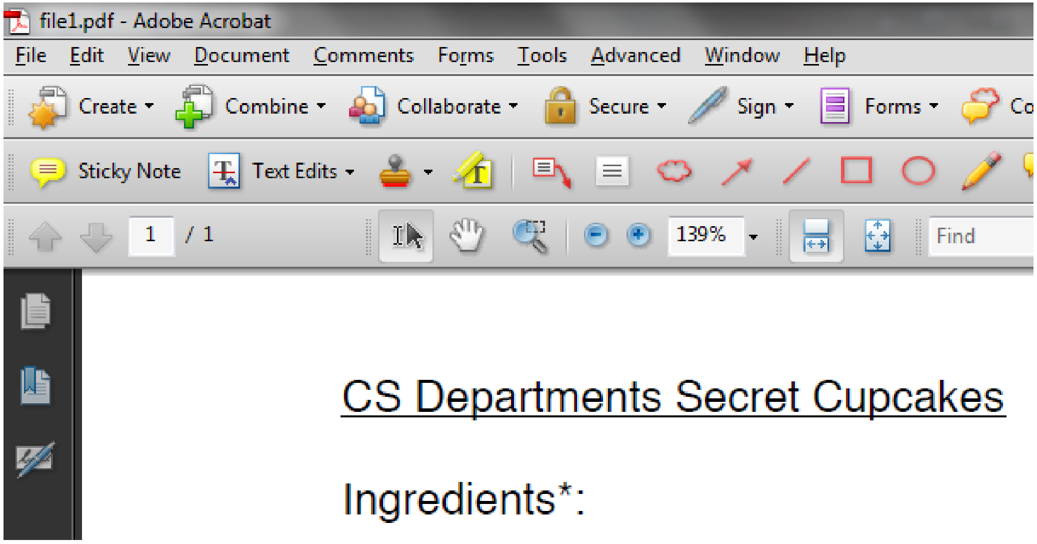
☑ Show extracte

File 'file1' is password protected. Please enter the password in the box below.

Password: ●●●●●●●●●●

Eureka! Someone IS selling secret CS Department information.

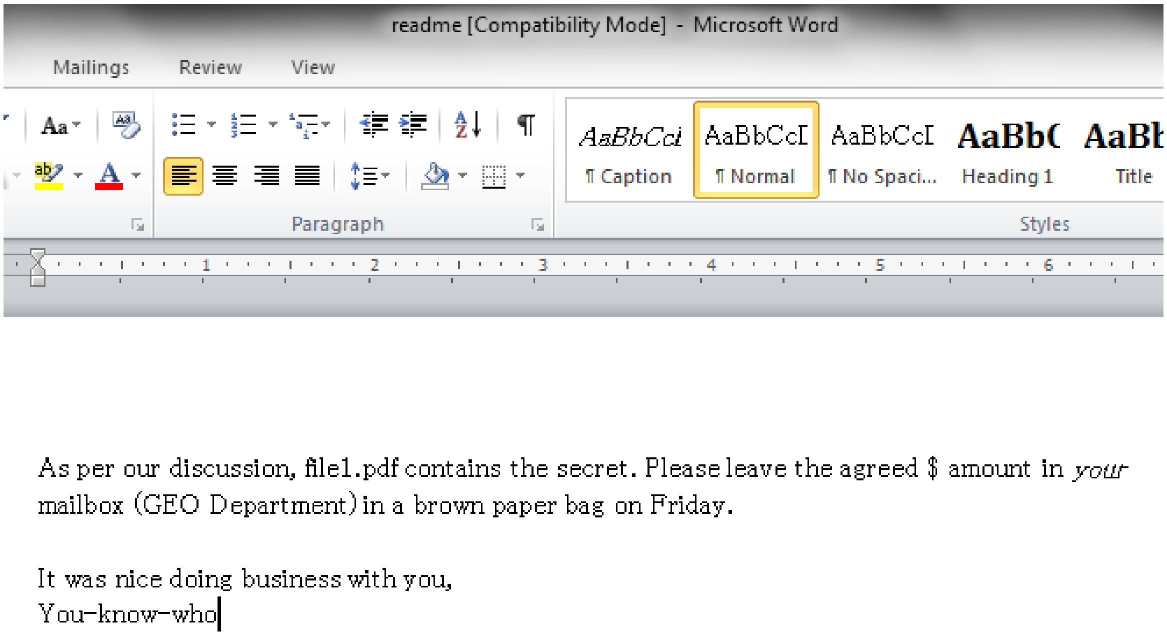
file1.pdf:



CS Departments Secret Cupcakes

Ingredients*:

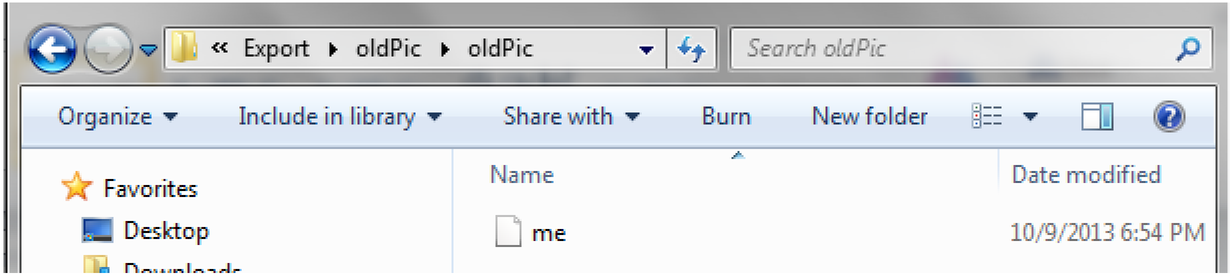
readme.doc:



As per our discussion, file1.pdf contains the secret. Please leave the agreed $ amount in *your* mailbox (GEO Department) in a brown paper bag on Friday.

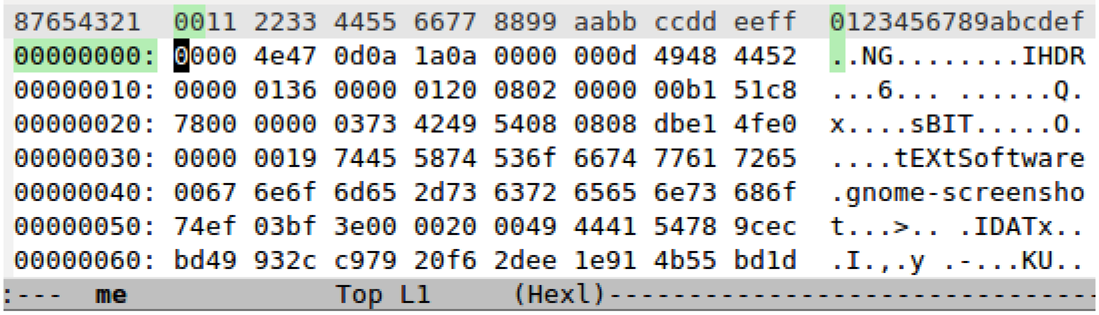
It was nice doing business with you,
You-know-who

The password did not work for "oldPic.zip" however. So, I went back to the passwords in "pw.txt" file. "mypassword" opened up "oldPic.zip". There was a file inside named "me".



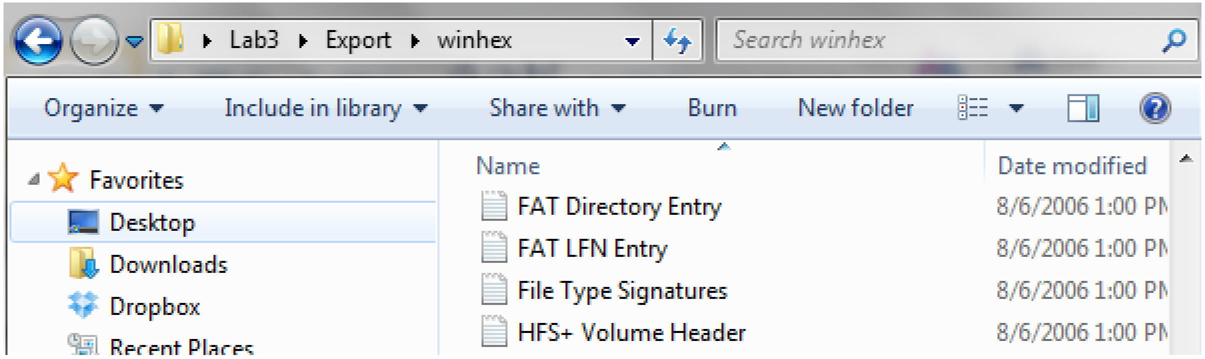
Name	Date modified
me	10/9/2013 6:54 PM

Opening "me" in hex editor shows that the first two bytes have been distorted.

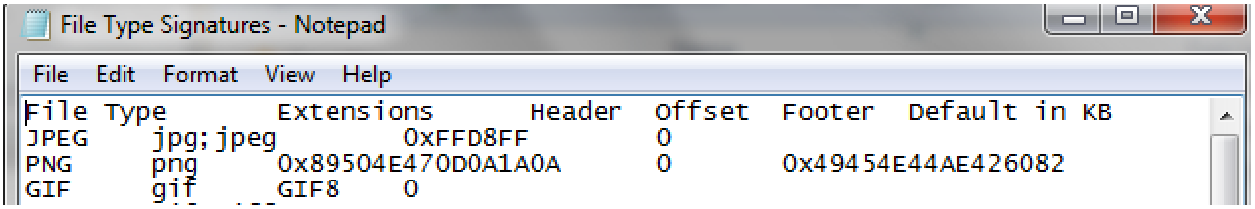


```
87654321  0011 2233 4455 6677 8899 aabb ccdd eeff  0123456789abcdef
00000000: 0000 4e47 0d0a 1a0a 0000 000d 4948 4452  ..NG........IHDR
00000010: 0000 0136 0000 0120 0802 0000 00b1 51c8  ...6... ......Q.
00000020: 7800 0000 0373 4249 5408 0808 dbe1 4fe0  x....sBIT.....O.
00000030: 0000 0019 7445 5874 536f 6674 7761 7265  ....tEXtSoftware
00000040: 0067 6e6f 6d65 2d73 6372 6565 6e73 686f  .gnome-screensho
00000050: 74ef 03bf 3e00 0020 0049 4441 5478 9cec  t...>.. .IDATx..
00000060: bd49 932c c979 20f6 2dee 1e91 4b55 bd1d  .I.,.y .-...KU..
:---  me          Top L1     (Hexl)-----------------------------
```

Comparing the next few bytes with the signatures in "File Type Signatures.txt" inside winhex:



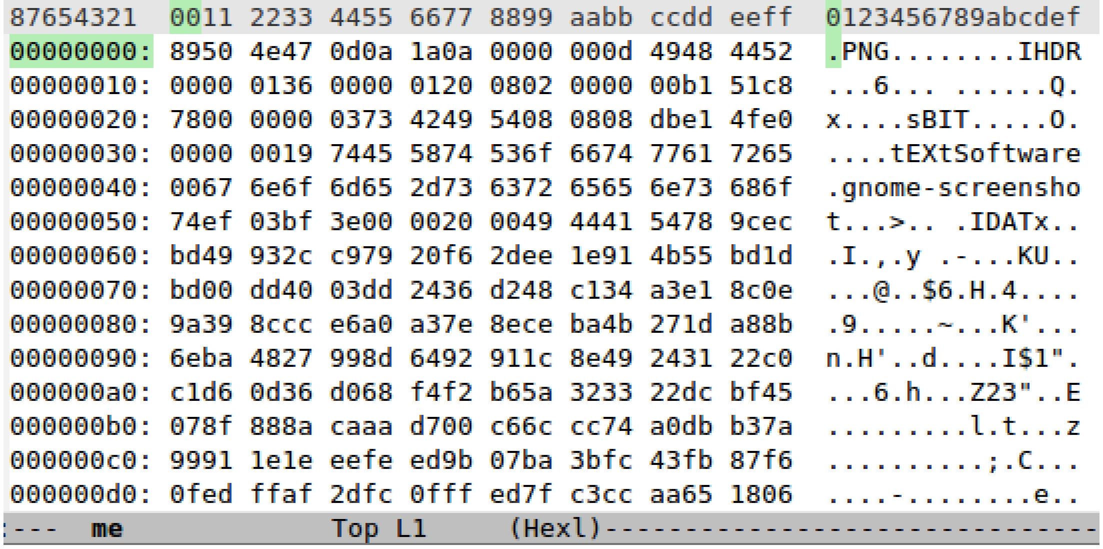
Name	Date modified
FAT Directory Entry	8/6/2006 1:00 PM
FAT LFN Entry	8/6/2006 1:00 PM
File Type Signatures	8/6/2006 1:00 PM
HFS+ Volume Header	8/6/2006 1:00 PM



```
File Type       Extensions       Header    Offset   Footer   Default in KB
JPEG      jpg;jpeg        0xFFD8FF         0
PNG       png       0x89504E470D0A1A0A     0        0x49454E44AE426082
GIF       gif       GIF8      0
```

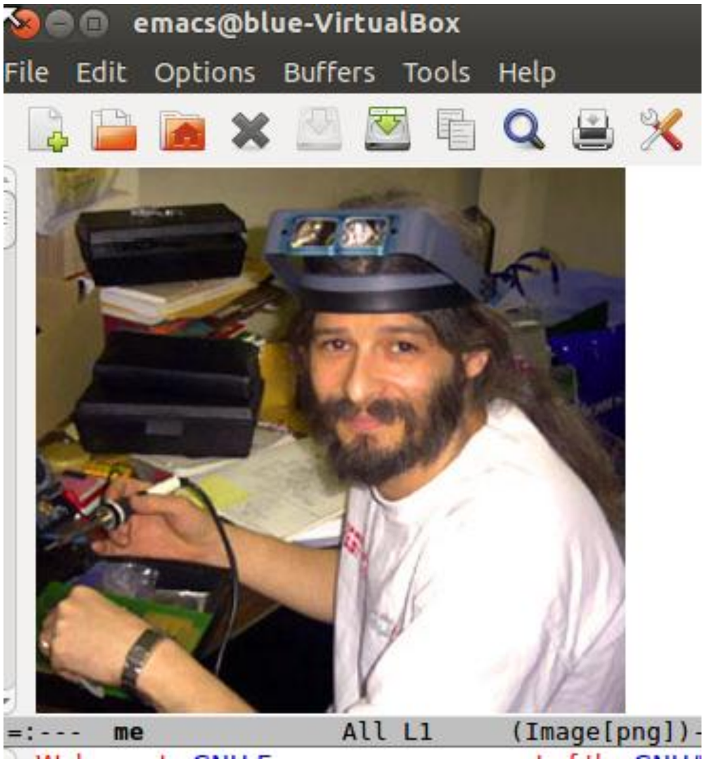
Shows that it is a PNG file.

The changing the first two bits, the file is renamed as .png and opened with photo viewer…



```
87654321  0011 2233 4455 6677 8899 aabb ccdd eeff  0123456789abcdef
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
00000010: 0000 0136 0000 0120 0802 0000 00b1 51c8  ...6... ......Q.
00000020: 7800 0000 0373 4249 5408 0808 dbe1 4fe0  x....sBIT.....O.
00000030: 0000 0019 7445 5874 536f 6674 7761 7265  ....tEXtSoftware
00000040: 0067 6e6f 6d65 2d73 6372 6565 6e73 686f  .gnome-screensho
00000050: 74ef 03bf 3e00 0020 0049 4441 5478 9cec  t...>.. .IDATx..
00000060: bd49 932c c979 20f6 2dee 1e91 4b55 bd1d  .I.,.y .-...KU..
00000070: bd00 dd40 03dd 2436 d248 c134 a3e1 8c0e  ...@..$6.H.4....
00000080: 9a39 8ccc e6a0 a37e 8ece ba4b 271d a88b  .9.....~...K'...
00000090: 6eba 4827 998d 6492 911c 8e49 2431 22c0  n.H'..d....I$1".
000000a0: c1d6 0d36 d068 f4f2 b65a 3233 22dc bf45  ...6.h...Z23"..E
000000b0: 078f 888a caaa d700 c66c cc74 a0db b37a  .........l.t...z
000000c0: 9991 1e1e eefe ed9b 07ba 3bfc 43fb 87f6  ..........;.C...
000000d0: 0fed ffaf 2dfc 0fff ed7f c3cc aa65 1806  ....-........e..
-:---  me            Top L1     (Hexl)-------------------------------
```

And the moment we've been waiting for…


emacs@blue-VirtualBox
File Edit Options Buffers Tools Help
=:--- me   All L1   (Image[png])-

It's **ERIC SCHWEITZER.**