Report

Lab 3 Investigation By: Christopher Mayol

First we open the image.dd file in autopsy and make a new case. Then we check and calculate the md5 hash of the image file which most match with the hash in the lab instructions.

Our image passes the integrity check.

We proceed to analysis the disk

Current Directory: C:/

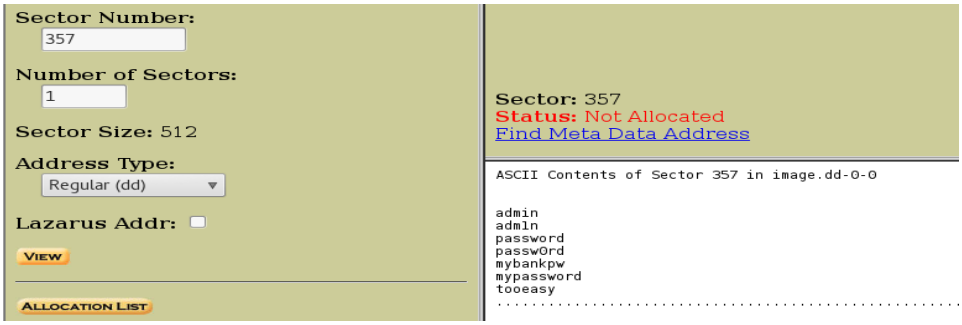
ADD NOTE GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CREATED	SIZE	UID	GID	META
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	3072	0	0	261940
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	3072	0	0	261941
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	261939
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	261942
	d / d	Documents/	2013-10-09 21:11:24 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 21:10:14 (EDT)	4096	0	0	4
	d / d	Music/	2013-10-09 15:09:06 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 15:09:06 (EDT)	4096	0	0	10
	d / d	Pictures/	2013-10-09 21:11:42 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 21:03:06 (EDT)	4096	0	0	6
	d / d	Programs/	2013-10-09 16:14:20 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:14:20 (EDT)	4096	0	0	8

We find some very interesting directories Documents, Pictures, and Programs.

	d / d	./	2013-10-09 21:11:24 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 21:10:14 (EDT)	4096	0	0	4
	r / r	About Hunter College - Hunter College - Acalog ACMSâ€¢.pdf	2013-10-09 18:17:42 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:25:12 (EDT)	69648	0	0	661
✓	r / r	Computer Science - BA - Hunter College - Acalog ACMSâ€¢.pdf	2013-10-09 18:16:22 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:25:44 (EDT)	105691	0	0	676
✓	r / r	Computer Science with Concentration in Bioinformatics - BA - Hunter College - Acalog ACMSâ€¢.pdf	2013-10-09 18:16:52 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:25:30 (EDT)	74802	0	0	670
	r / r	Hunter College Mission Statement - Hunter College - Acalog ACMSâ€¢.pdf	2013-10-09 18:18:30 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:24:56 (EDT)	58140	0	0	655
	r / r	Hunter.txt	2013-10-09 18:32:36 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:36:02 (EDT)	1988	0	0	681
	r / r	moreHunter.txt	2013-10-09 18:34:00 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 18:35:58 (EDT)	677	0	0	679
✓	r / r	pw.txt	2013-10-09 16:01:26 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:01:26 (EDT)	58	0	0	646
✓	r / r	pw.txt~	2013-10-09 16:00:52 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:00:52 (EDT)	58	0	0	648
	r / r	README.txt	2013-10-09 21:09:48 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 21:10:14 (EDT)	14	0	0	685
	r / r	topsecret.zip	2013-10-09 21:04:24 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 21:04:24 (EDT)	22477	0	0	683

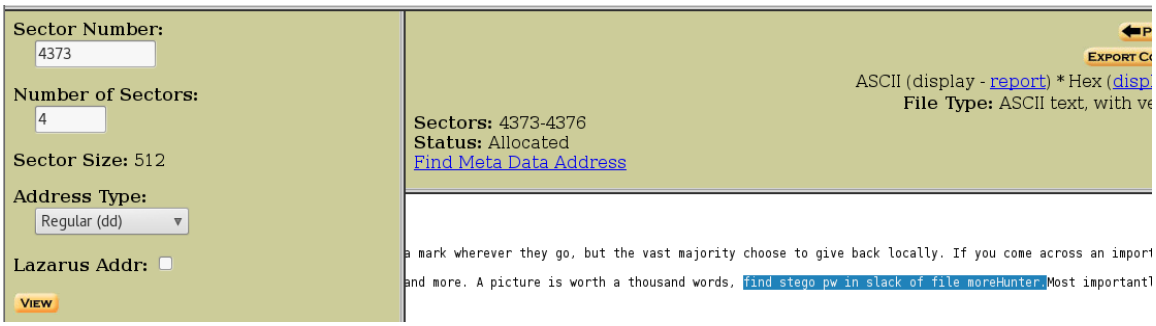
In documents we find Hunter documents and some very interesting files. The suspect deleted some files and a “pw.txt”, which sounds important. We can recover the contents of the file because we have the sector where its data is store “sector # 357”



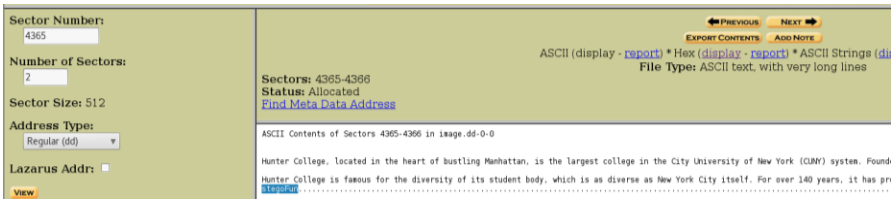
We recovered the contents of the pw file which contains some passwords which means the suspect probably encrypted some files.

Autopsy allows us to export the data in to a raw file, since we know it’s name and file extension we can fully recover the file.

In the hunter.txt file we find a hidden message. The suspect implement steganography to hide data.



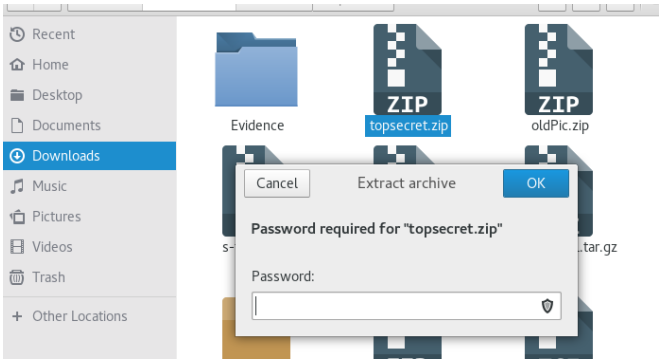
“find stego pw in slack of file moreHunter.” This is infact a secret message that points us to a password.



In “moreHunter.txt” we find what appears to be another password at the end of the file. “stegoFun”

Moving on we will find a “topsecret.zip” file which sounds classified and highly suspicious.

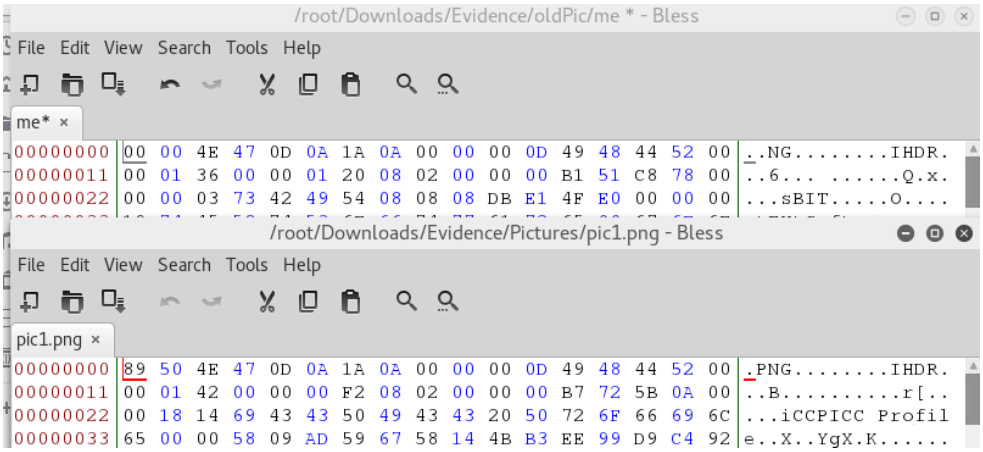
The directory entry is 683, and we noticed right away that the contents of this compressed folder is in sectors 4901-4944. Knowing this we can extract the folder and attempt to find the evidence we need.



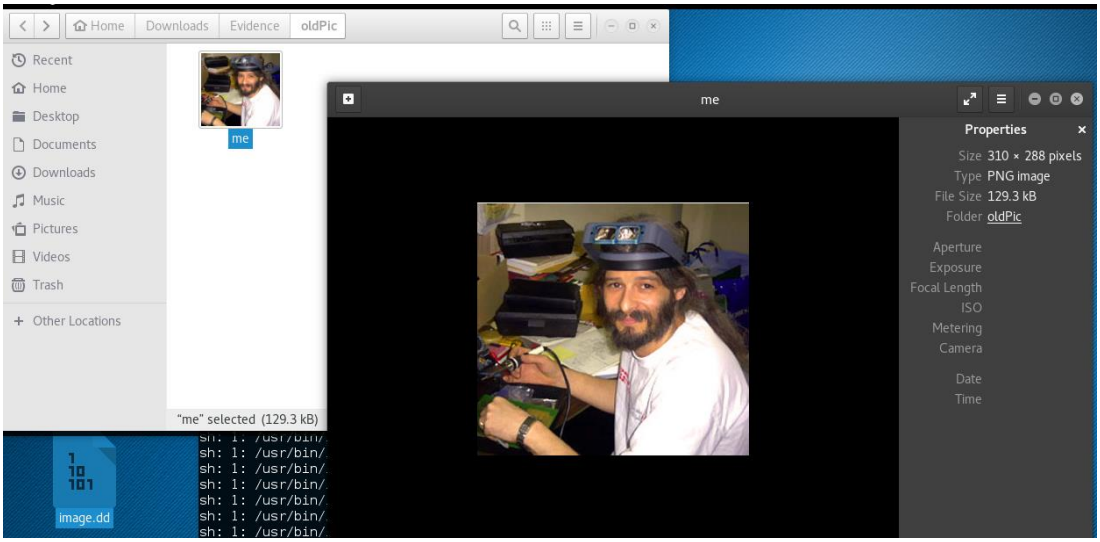
We find that the topsecret folder is encrypted with a password and sadly none of the passwords from the “pw.txt” will decrypt this folder.

Now we know that this folder contains all the evidence we need to proof that the suspect is guilty, all we gotta do is find this key.

In the Pictures folder we will find a few images and a oldPic zip file which is encrypted with a password. Good news is that the password can be found in the “pw.txt” we recovered. The password is “mypassword”. In the folder we find a “me.png” but if we try to open it it will fail because the file is corrupted. We can still recover the image by opening the file in a hexeditor.



Comparing the corrupted me.png to a working pic1.png we find that the header marker is missing 0x8950, replacing this we recover the image



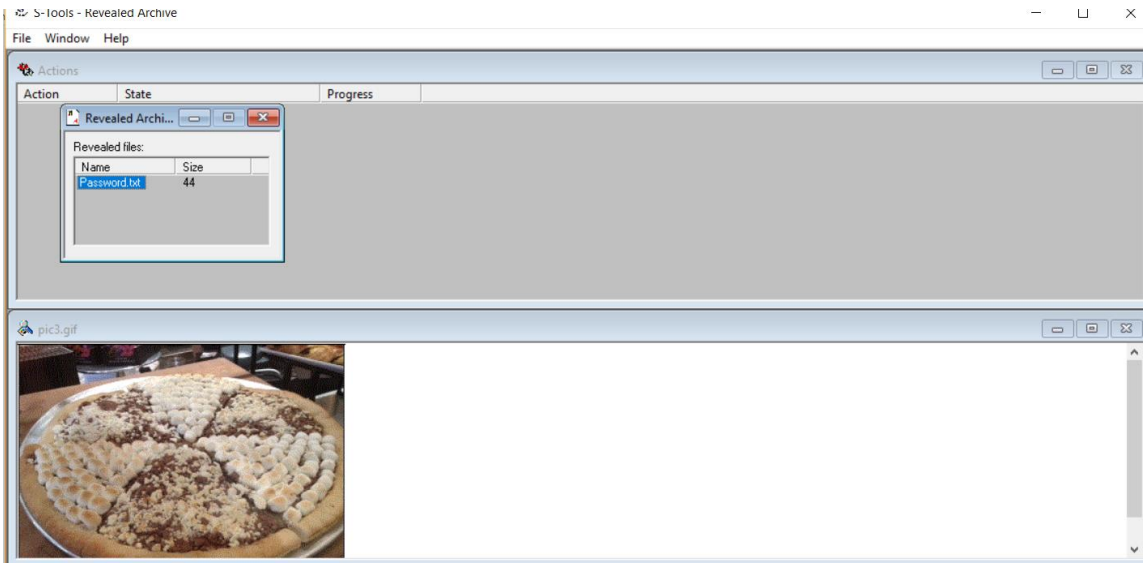
We now have a picture of the suspect.

Moving on to the Programs directory

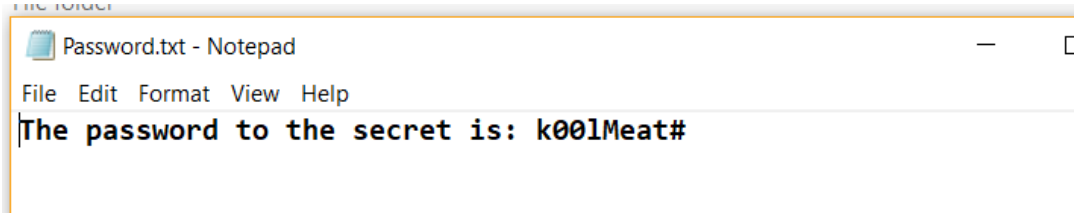
Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
	d / d	../	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	16384	0	0	2
	d / d	./	2013-10-09 16:14:20 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:14:20 (EDT)	4096	0	0	8
	r / r	aeskeyfind-1.0.tar.gz	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:13:08 (EDT)	6235	0	0	903
	r / r	rc4.revealed.gz	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:13:32 (EDT)	3327	0	0	906
	r / r	rsakeyfind-1.0.tar.gz	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:13:46 (EDT)	4181	0	0	909
	r / r	s-tools4.zip	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:14:00 (EDT)	278774	0	0	911
	r / r	stunnel-4.11.exe	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:14:10 (EDT)	73728	0	0	914
	r / r	winhex.zip	2013-10-09 16:09:08 (EDT)	2013-10-09 00:00:00 (EDT)	2013-10-09 16:14:20 (EDT)	1354247	0	0	916

Folder contains programs which look very suspicious since most of these programs use cryptography. If you compile both aeskeyfind and rsakeyfind programs using g++ and feed it the image.dd file, no keys are found sadly. The suspect uses stunnel, which might indicate that he wants to ensure his connection is very secured, which might mean he is transferring sensitive information. The Program winhex in our case is very important because is a hexeditor tool, which is how the suspect implemented stegonagraphy.

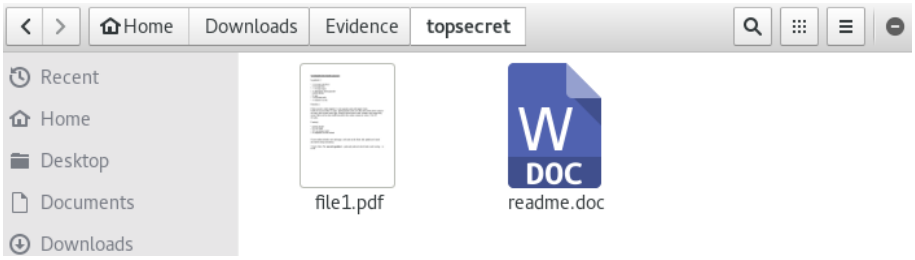
If we use s-tools we can reveal a file inside pic3.gif, which is password protected. The good thing is that we found the password before in the moreHunter.txt file “stegoFun”



Extracting the password file we get…



The password to the topsecret.zip folder “k00lMeat#” !!



Success!!

file1.pdf

CS Departments Secret Cupcakes

Ingredients*:

- 1 3/4 cups cake flour
- 1 3/4 cups flour
- 1 1/2 cups sugar
- 1 tablespoon baking powder
- 2 sticks butter
- 3 eggs
- 1 cup whole milk
- 1 teaspoon vanilla

Directions:

Preheat oven to 325 degrees F. Line cupcake pans with paper liners.
Combine in a bowl flours, sugar, baking powder and salt. Mix until combined for about 3 minutes. Add in butter and eggs. Slowly add milk and vanilla to batter until completely mixed. Bake until a cake tester inserted in the center comes out clean, 15 to 20 minutes.

Frosting*:

- 2 sticks butter
- 8 cups sugar
- 1/2 cup almond milk
- 2 teaspoons vanilla extract

Cream softened butter and add sugar, milk and vanilla. Beat with paddle until reach desired frosting consistency.

*Cook's Note: The **secret ingredient** -- preferably added to both batter and frosting -- is Love.

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

We have cracked this case wide open the suspect is indeed selling a CS secret, he is selling the **Secret cupcake formula** and the secret ingredient **Love.** The readme file gives us the location where the

transactions take place. We have gather proof to infact say with 100% confidence that the suspect is guilty!

Eric Schweitzer