Kelli Kinnikin

Assignment 4

CIS425 – Fall Term 2017

Point Value: 100 points

Due Date: **In class Thursday November 16, 2017**

Submission Instruction

Please submit the hardcopy of Assignment4_lastname_firstname.pdf file along with your detailed lab notes to the instructor in lecture.

What you will need: a hosting computer with Linux/Ubuntu OS.

Using digital forensics tools/commands.

Case I:

Imagine that you are a digital forensics examiner. A FBI agent, Joe Doe, has just handed you a raw image file named image.dd along with image.md5 in which stores the MD5 hash of the original evidence. Please download the image.dd and image.md5 files from:

cis425@mathcswc.fontbonne.edu:~/image.dd

cis425@mathcswc.fontbonne.edu:~/image.md5

First I had to use these two commands to download the files into Ubuntu:

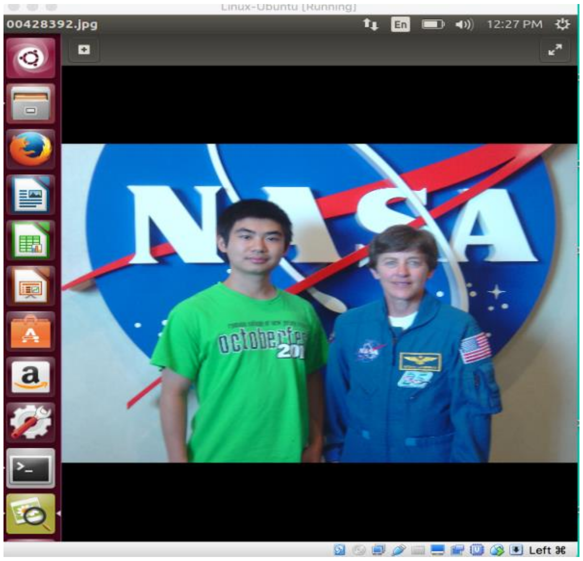
1.) “scp cis425@mathcswc.fontbonne.edu:~/image.dd ./”

2.) “scp cis425@mathcswc.fontbonne.edu:~/image.md5 ./”

You have 3 tasks:

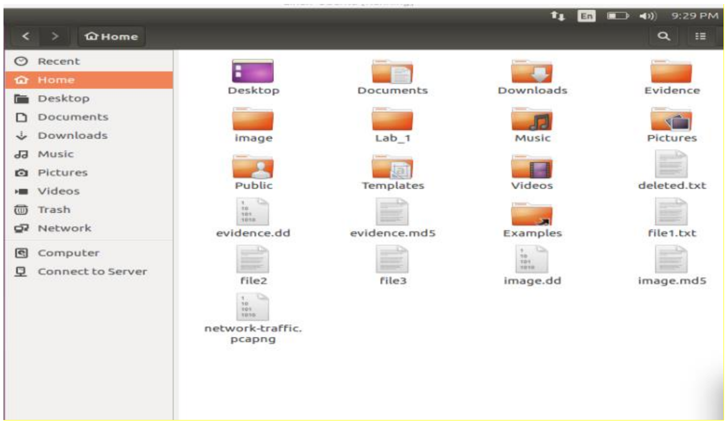
1. The suspect is accused of trespassing NASA facility without proper permission. The FBI agent seized the suspect’s computer hard drive. He asked you to find evidence which can prove that the suspect has been in the NASA facility and took a picture with one well-known astronaut named Wendy Lewis. (20 points).

- **Command:** “sudo apt-get install foremost”
- **Command:** “Foremost –t jpg –i image.dd”
- Go to home directory
- Click output folder
- Click jpg folder
- Navigate through pictures

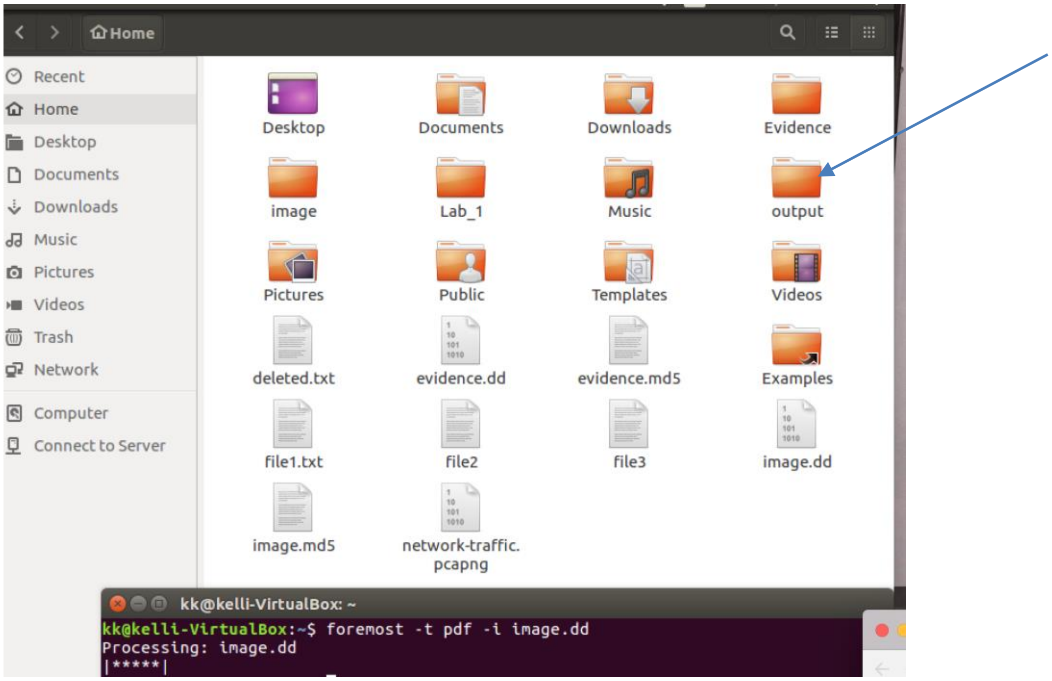


2. Please find all the pdf files whose author/creator is Ernie Chan. (10 points)

Before I could use the command: “foremost –t pdf –i image.dd”, I had to delete the output folder that was created when I used the command “foremost –t jpg –i image.dd” in question number 1. That command was used to find jpg images and I now want to find pdf files.



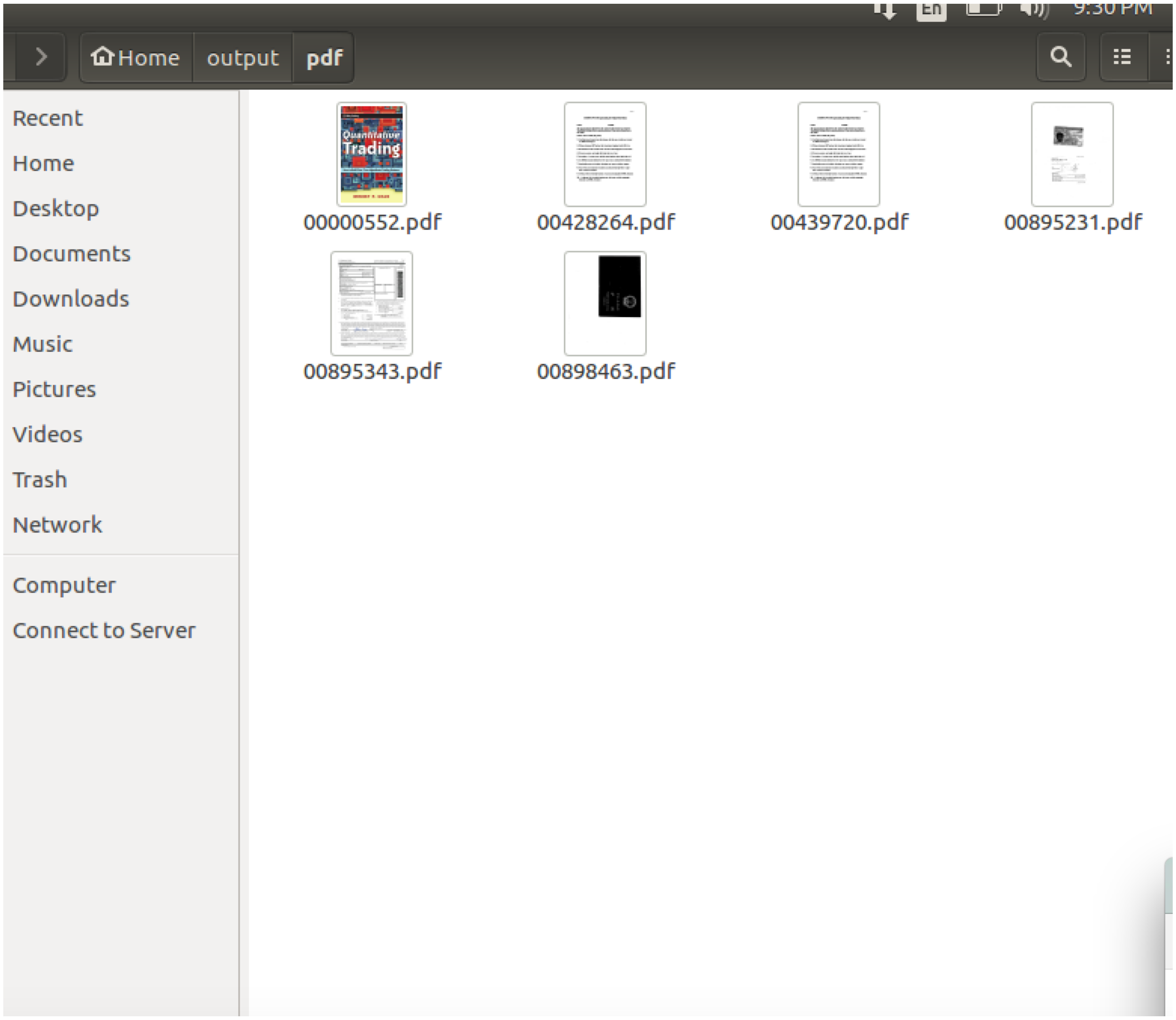
What happened when I used the "foremost –t pdf –i image.dd" command.



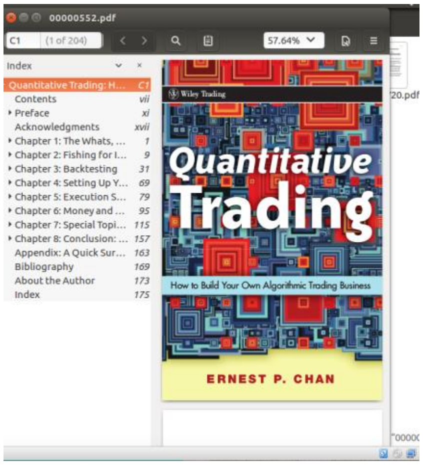
```
kk@kelli-VirtualBox:~$ foremost -t pdf -i image.dd
Processing: image.dd
|*****|
```

… it creates an output folder. Then you want to click on the output folder and navigate to the pdf subfolder to find all the pdf files on this image.dd.

Kelli Kinnikin

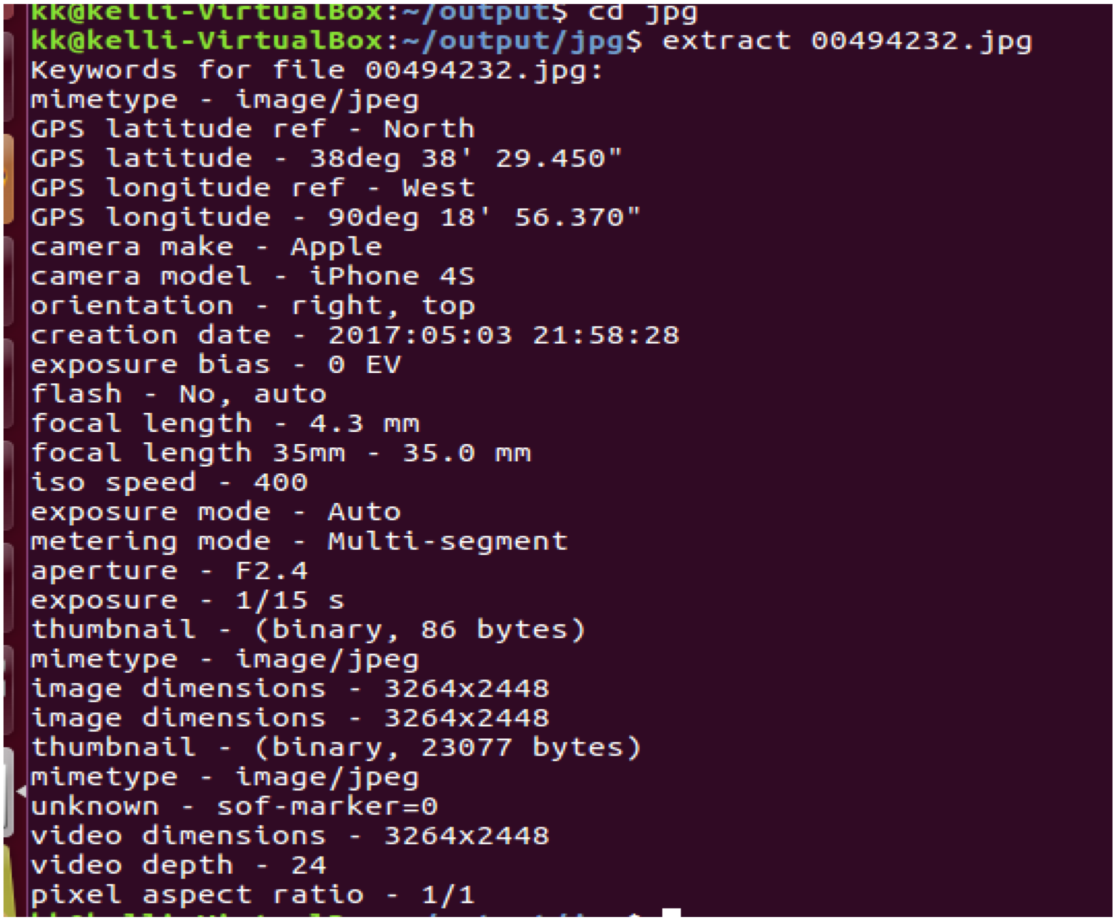


You see there are 6 pdf's but only one with the author "Ernie Chan"



ANSWER: 1 PDF Quantitative Trading

3. The suspect has taken a picture with his iPhone 4S. Agent Joe Doe asked you to find the picture and see if the picture is associate with a location. If yes, please find down the latitude and longitude of the location, the name of the location, and the turn by turn location from your home to the location (20 points).
    - **Command:** “cd output”
    - **Command:** “find . –type f –exec grep –l ‘iphone’{} \;”
    - **Command:** “sudo apt-get install extract”
    - **Command:** “cd jpg”
    - **Command:** “extract 004294232.jpg”

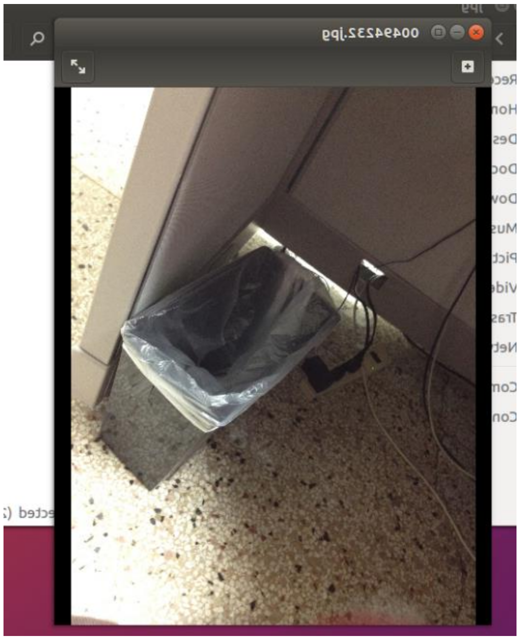


```
kk@kelli-VirtualBox:~/output$ cd jpg
kk@kelli-VirtualBox:~/output/jpg$ extract 00494232.jpg
Keywords for file 00494232.jpg:
mimetype - image/jpeg
GPS latitude ref - North
GPS latitude - 38deg 38' 29.450"
GPS longitude ref - West
GPS longitude - 90deg 18' 56.370"
camera make - Apple
camera model - iPhone 4S
orientation - right, top
creation date - 2017:05:03 21:58:28
exposure bias - 0 EV
flash - No, auto
focal length - 4.3 mm
focal length 35mm - 35.0 mm
iso speed - 400
exposure mode - Auto
metering mode - Multi-segment
aperture - F2.4
exposure - 1/15 s
thumbnail - (binary, 86 bytes)
mimetype - image/jpeg
image dimensions - 3264x2448
image dimensions - 3264x2448
thumbnail - (binary, 23077 bytes)
mimetype - image/jpeg
unknown - sof-marker=0
video dimensions - 3264x2448
video depth - 24
pixel aspect ratio - 1/1
```

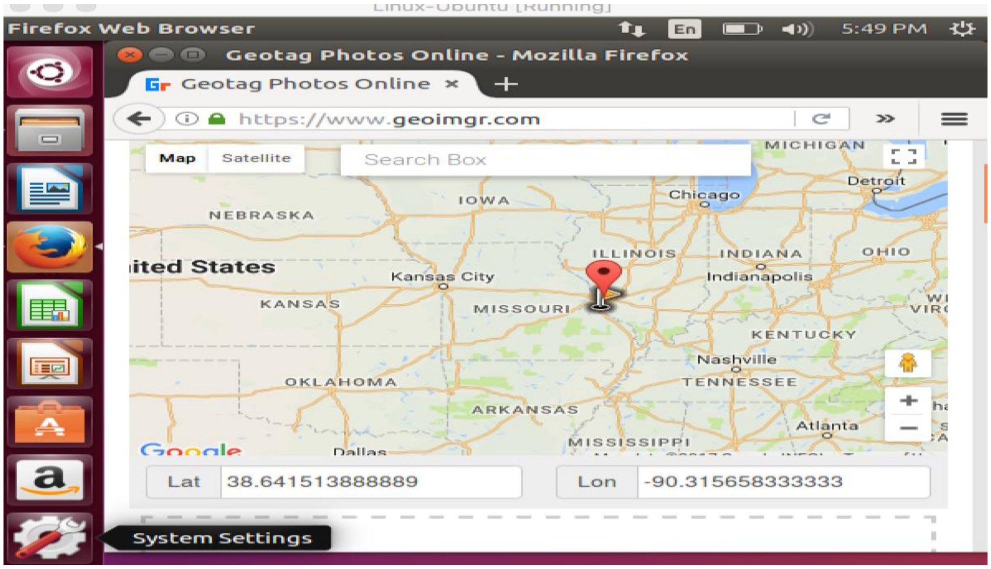
Latitude: North 38 deg 38’ 29.450

Longitude: West 90 deg 18’ 56.370

Kelli Kinnikin



- Then I went to an online tool to find the location of this .jpg image.
- I went to www.geoimgr.com and dragged the picture into the dropbox.
- I got the following results:

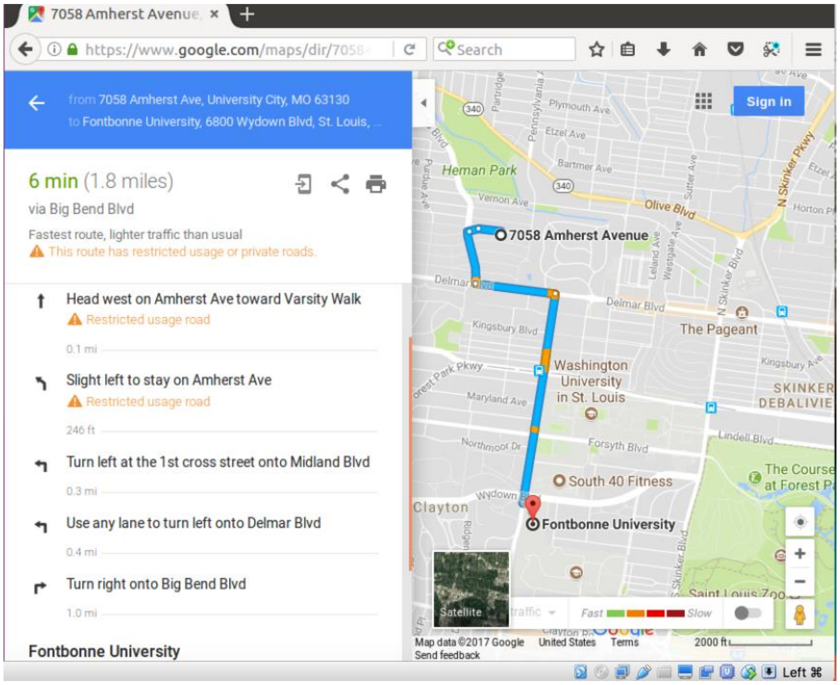


Lat 38.641513888889

Lon -90.315658333333

The location is: Fontbonne University… perhaps your office in Ryan Hall?

Turn by Turn Directions From My Home:



from 7058 Amherst Ave, University City, MO 63130
to Fontbonne University, 6800 Wydown Blvd, St. Louis, ...

6 min (1.8 miles)
via Big Bend Blvd
Fastest route, lighter traffic than usual
⚠ This route has restricted usage or private roads.

↑ Head west on Amherst Ave toward Varsity Walk
⚠ Restricted usage road
0.1 mi

Slight left to stay on Amherst Ave
⚠ Restricted usage road
246 ft

Turn left at the 1st cross street onto Midland Blvd
0.3 mi

Use any lane to turn left onto Delmar Blvd
0.4 mi

Turn right onto Big Bend Blvd
1.0 mi

Fontbonne University

Case II:

Imagine that you are a digital forensics analyst working for company A. The company's CEO email account has been hacked. You suspect that the CEO clicked a link in a phishing email and entered his or her email address and password. You obtained a network packet log file which can be viewed in Wireshark. Please download the network-traffic file from:

cis425@mathcswc.fontbonne.edu:~/network-traffic.pcapng

Your task is to find the evidence which proves that the CEO has sent his email address and password to a web server controlled by hackers. If the evidence is found, please find the following information related the hack:

First, I downloaded the file using command:

"scp cis425@mathcswc.fontbonne.edu:~/network-traffic.pcapng ./"

1. Hacker's web server's IP address and domain name. (10 points)
   107.180.57.91 domain name: primetechconsult
2. Hacker's web server software's name.
   apache server (10 points)
3. The date and time when the CEO sent his email address and password.
   Friday, Nov 2017 18:03:42 GMT (10 points)
4. The CEO's email address and password.

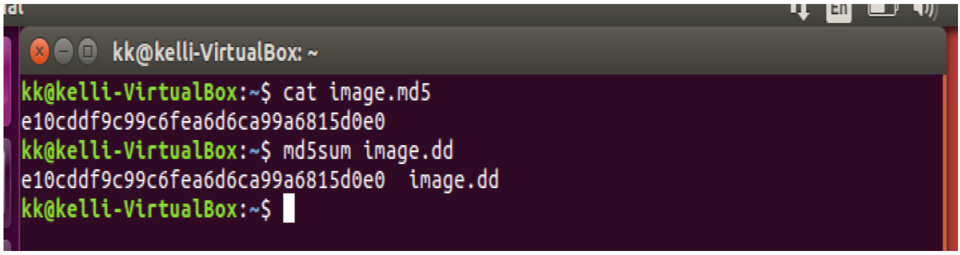
Email: gtian@fontbonne.edu **Password:**1234567890 (10 points)

5. The total number of packets involve in this incident.
   10 total packets (10 points)

Hint: the email and password are likely to be in clear text.

Please write down the detailed note for this assignment. Also verify the integrity of the image file before and after your forensics examination. You need to submit this note in class on November 16, Thursday.
Note: You MUST work individually

It is very important to check the integrity before and after your examination t o make sure there were no alterations with the original image. I used the command “cat image.md5 and “md5sum image.dd” to get each hash value. As you can see, they are the integrity of the image is secure.



```
kk@kelli-VirtualBox:~$ cat image.md5
e10cddf9c99c6fea6d6ca99a6815d0e0
kk@kelli-VirtualBox:~$ md5sum image.dd
e10cddf9c99c6fea6d6ca99a6815d0e0  image.dd
kk@kelli-VirtualBox:~$
```

.