
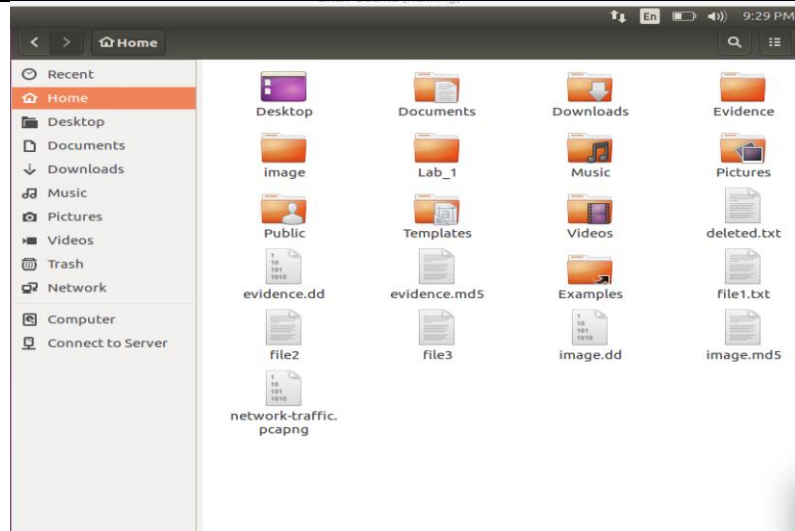


## Laboratory Notes

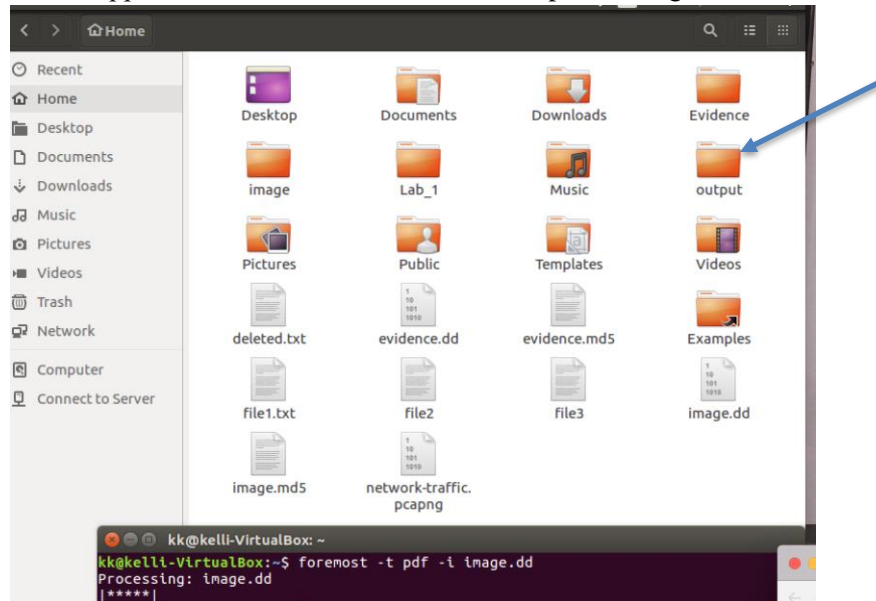
Assignment Number: \_\_\_\_4\_\_\_\_ Examiner Name: \_\_\_\_Kelli Kinnikin\_\_\_\_

### Date & Time

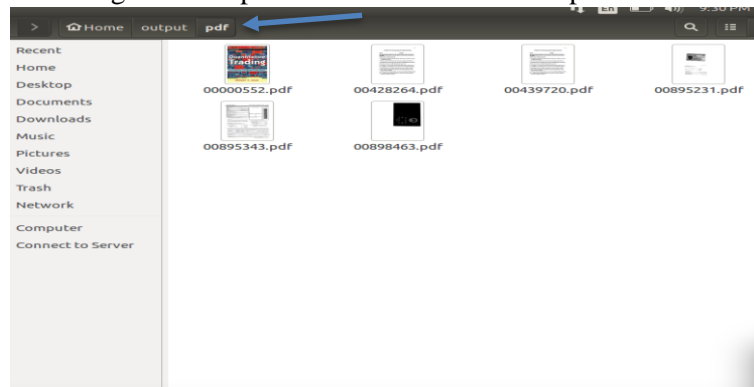
11/14/17 3:00 pm	<p>First, I had to use these two commands to download the files into Ubuntu:</p> <ol style="list-style-type: none"><li>1.) <code>"scp cis425@mathcswc.fontbonne.edu:~/image.dd ./"</code></li><li>2.) <code>"scp cis425@mathcswc.fontbonne.edu:~/image.md5 ./"</code></li></ol>
11/14/17 3:07 pm	<p>Next, I needed to find a picture that the suspect took with a well-known astronaut named Wendy Lewis.</p> <ul style="list-style-type: none"><li>• <b>Command:</b> <code>"sudo apt-get install foremost"</code></li><li>• <b>Command:</b> <code>"foremost -t jpg -i image.dd"</code>(this creates an output folder)</li><li>• Go to home directory</li><li>• Click the output folder</li><li>• Click the subfolder jpg folder</li><li>• Navigate through pictures</li></ul> 
11/14/17 3:21 pm	<p>Next, I needed to find all the pdf files whose author/creator is "Ernie Chan".</p> <ul style="list-style-type: none"><li>• NOTE: Before I could use the command: <code>"foremost -t pdf -i image.dd"</code>, I had to delete the output folder that was created when I used the command <code>"foremost -t jpg -i image.dd"</code>. That command was used to find jpg images and I now want to find pdf files.</li></ul>



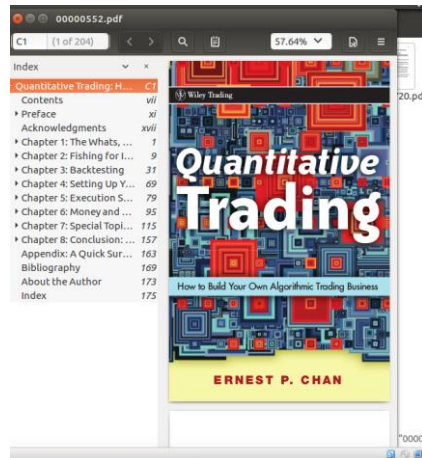
- What happened when I used the “foremost -t pdf -i image.dd” command.



- ... 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.



11/14/17  
3:36 pm



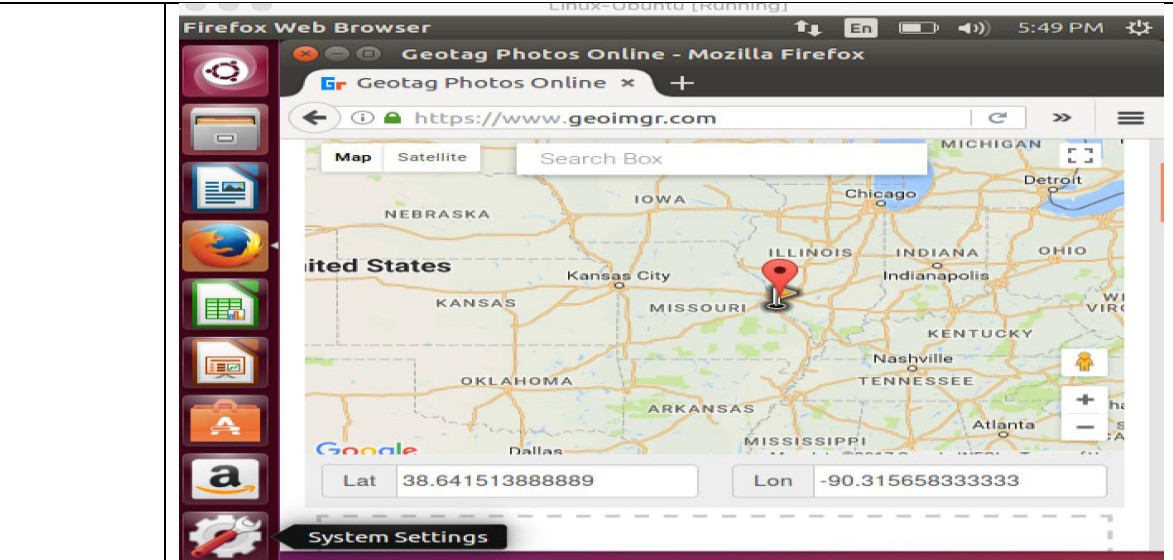
- **ANSWER: 1 PDF file entitled: QuaanitativeTrading.pdf by Ernest P.Chan**

11/14/17  
3:40 pm

Lastly for case I, I needed to find a picture that has been taken with an iphone 4S.

- **Command:** “cd output”
- Now that we are in the output directory, we need to go to the jpg subdirectory...
- **Command:** “cd jpg”I needed to go to this subdirectory because all the pictures are located here.
- **Command:** “find . -type f -exec grep -l ‘iphone’ {} \;”  
This will give you a list of jpg’s taken with an iphone and the 00494232.jpg came up
- **Command:** “sudo apt-get install extract”  
I installed this package so I could extract the information from the picture.
- **Command:** “extract 00494232.jpg”

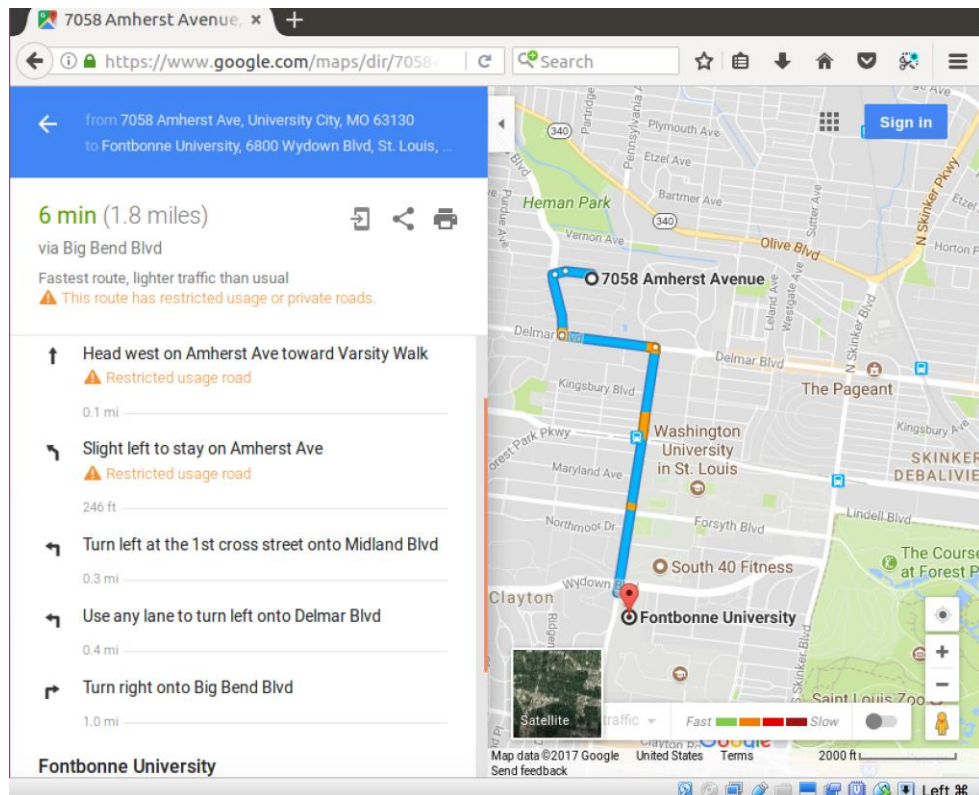
<p>11/14/17 3:45 pm</p>	<pre> kk@kali-VirtualBox:~/output\$ cd jpg kk@kali-VirtualBox:~/output/jpg\$ extract 00494232.jpg Keywords for file 00494232.jpg: mimetype - image/jpeg GPS latitude ref - North GPS latitude - 38deg 38' 29.450" GPS longitude ref - West GPS longitude - 90deg 18' 56.370" camera make - 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 </pre> <ul style="list-style-type: none"> <li>• This will give you all the information about the picture</li> </ul> <p><b>Latitude: North 38 deg 38' 29.450</b></p> <p><b>Longitude: West 90 deg 18' 56.370</b></p>  <ul style="list-style-type: none"> <li>• Then I went to an online tool to find the location of this .jpg image.</li> <li>• I went to <a href="http://www.geoimgr.com">www.geoimgr.com</a> and dragged the picture into the dropbox.</li> <li>• I got the following results:</li> </ul>
<p>11/14/17 3:50 pm</p>	

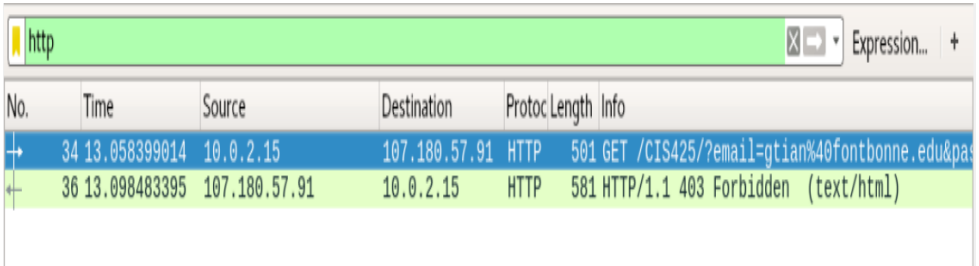
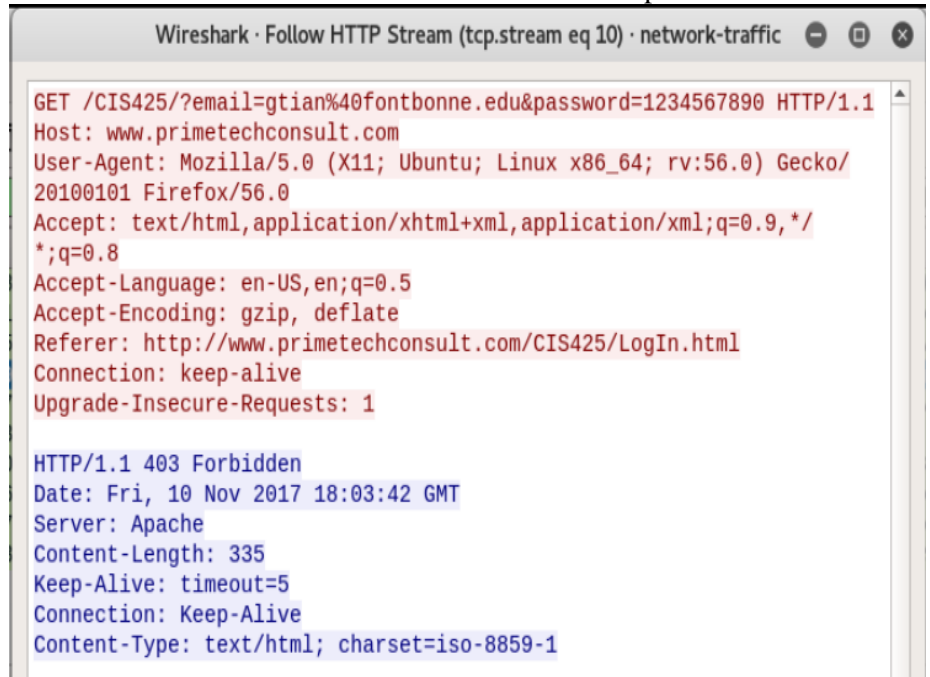


The location is: Fontbonne University... perhaps your office in Ryan Hall?

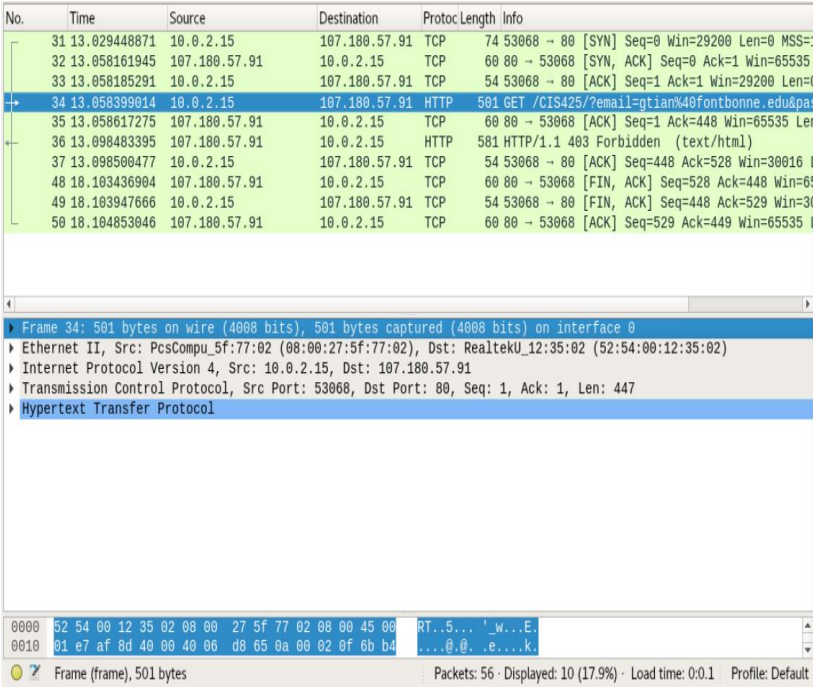
11/14/17  
4:03 pm

Turn by Turn Directions From My Home To The Image Location:



<p>11/14/17 4:07 pm</p>	<p>*****CASE II*****</p> <p>First I downloaded Wireshark packet file</p> <ul style="list-style-type: none"> <li>“scp <a href="mailto:cis425@mathcswc.fontbonne.edu">cis425@mathcswc.fontbonne.edu</a>:~/network-traffic.pcapng ./”</li> </ul>
<p>11/14/17 4:10 pm</p>	<p>Next, I opened the file in Wireshark.</p> <ul style="list-style-type: none"> <li>Since the client entered his email on a website, I wanted to filter by HTTP(website) requests.</li> </ul>  <ul style="list-style-type: none"> <li>I can see there is a GET request on packet number 34 with brief information that directs to email information.</li> </ul>
<p>11/14/17 4:20 pm</p>	<p>Next, I right clicked the packet &gt; Follow &gt; HTTP Stream.</p> <ul style="list-style-type: none"> <li>This allows me to read the information of the packets.</li> </ul> 
<p>11/14/17 4:20</p>	<ul style="list-style-type: none"> <li>With this Wireshark screen shot(above), you can get the email, password, host, date, and server information needed for case II.</li> </ul>



<p>11/14/17 4:30</p>	<ul style="list-style-type: none"> <li>Domain Name: primetechconsult</li> <li>Hacker's web server: Apache</li> <li>Date and Time: Friday, Nov 2017 18:03:42 GMT</li> <li>Email: <a href="mailto:gtian@fontbonne.edu">gtian@fontbonne.edu</a> Password: 1234567890</li> </ul>  <ul style="list-style-type: none"> <li>This screenshot gives you the IP address (107.180.57.91) and the total number of packets. To get the total number of packets you just count the info highlighted above (in green) and there are 10 total packets for this incident.</li> </ul>
<p>11/14/17 4:33pm</p>	<p>Last but not least, you should always verify the integrity (hash values) of the image before and after your examination to make sure nothing was tampered with on the original evidence.</p> <ul style="list-style-type: none"> <li>Command: “cat image.md5”</li> <li>Command “md5sum image.dd”</li> </ul> 