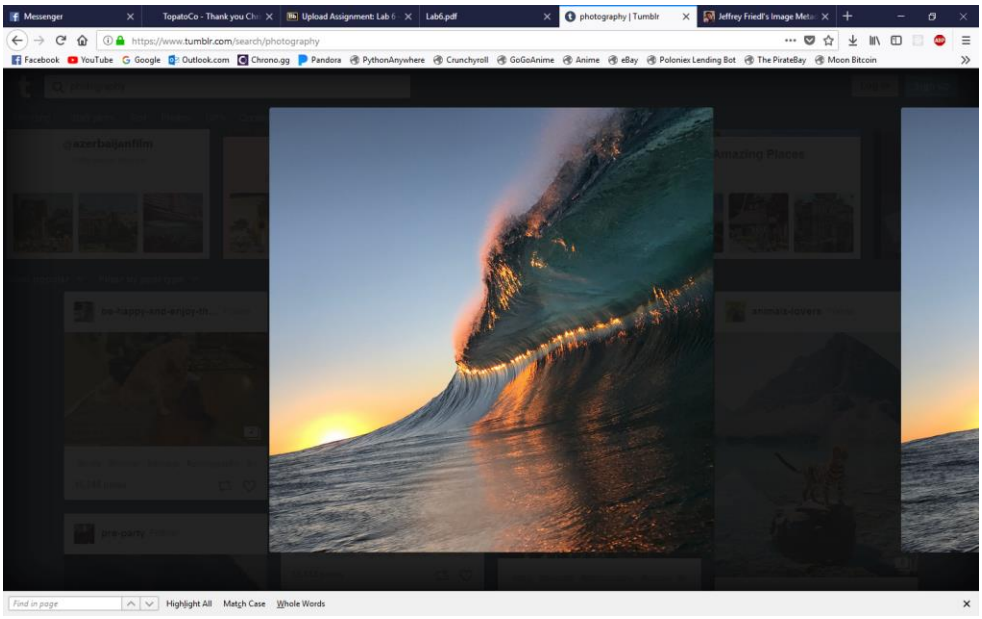
DFSC1316: Digital Forensic and Information Assurance I

Lab 6 Windows Operating System Forensics

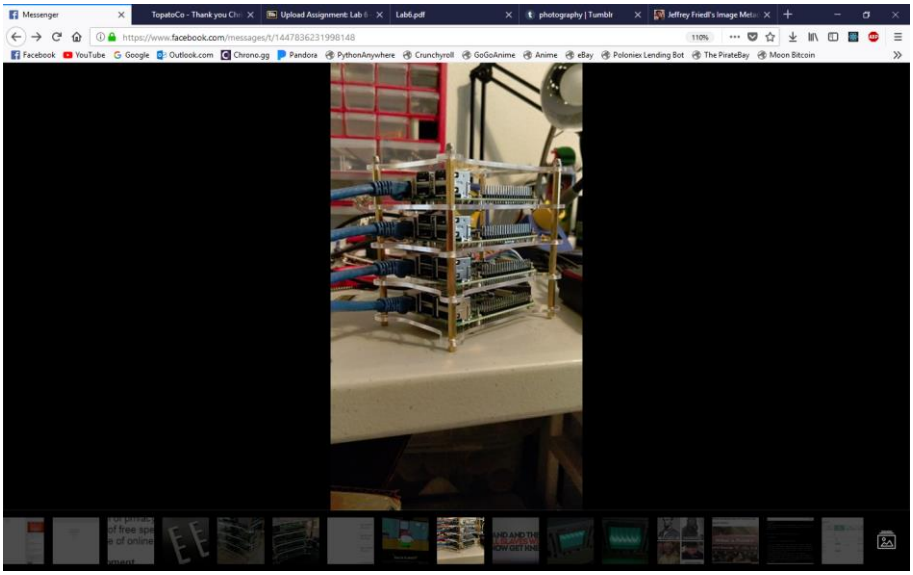
Lab 6.1: Metadata investigation

Tumblr



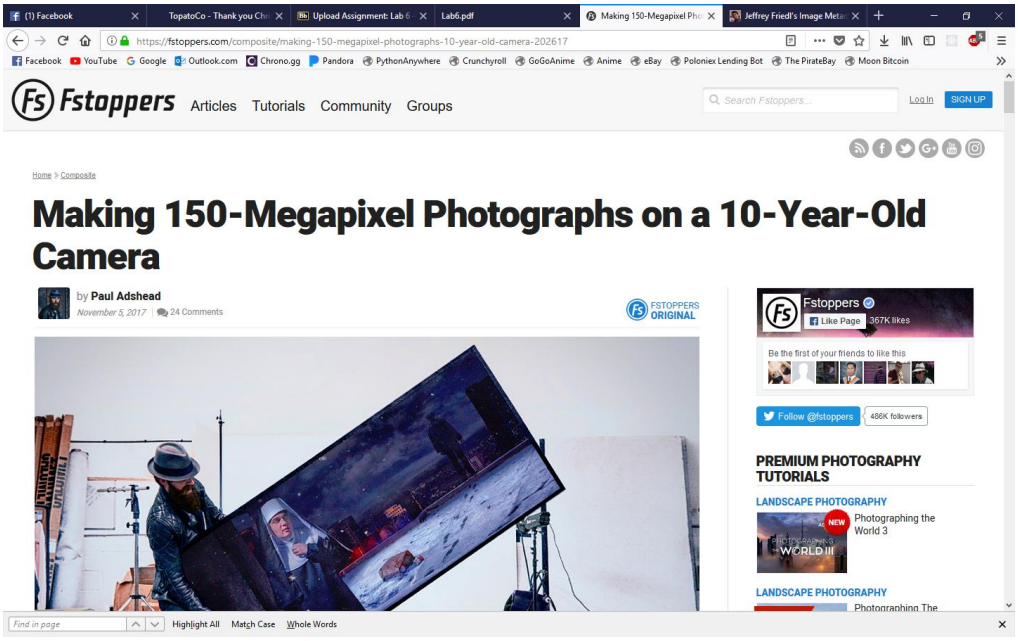
I could I saved the link to the image and processed it with “Jeffrey's Image Metadata Viewer”. I could not find any exif data.

Facebook



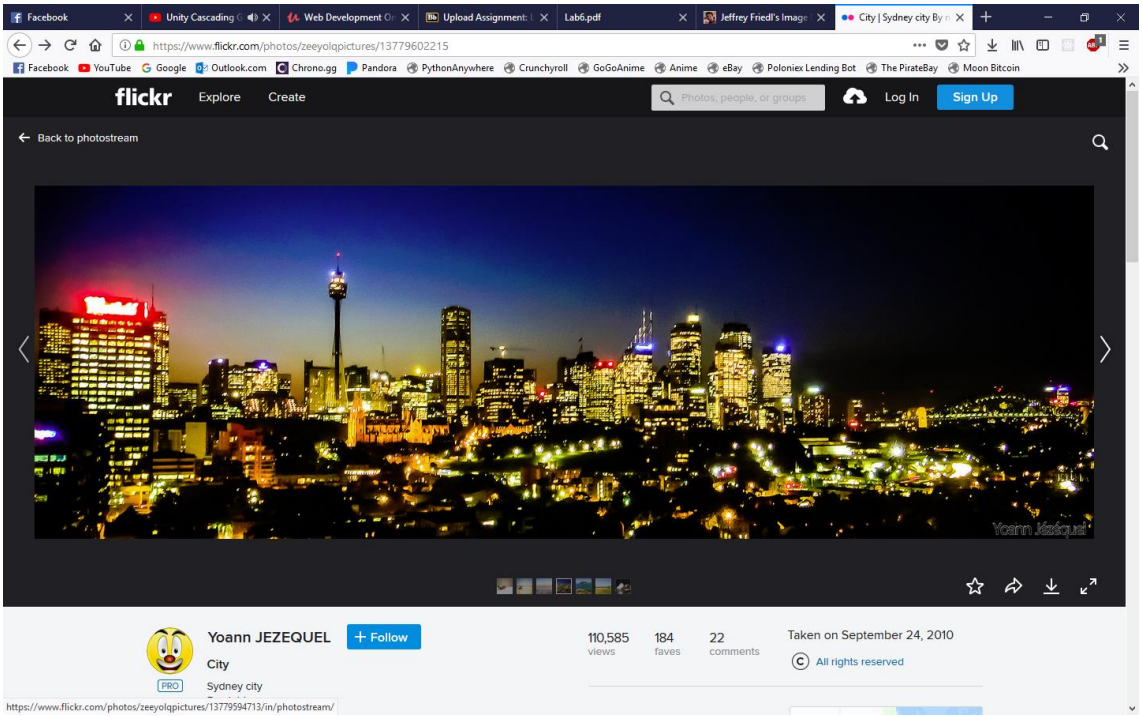
I used the same process for Facebook message photos. I could not find any exif data.

Fstoppers



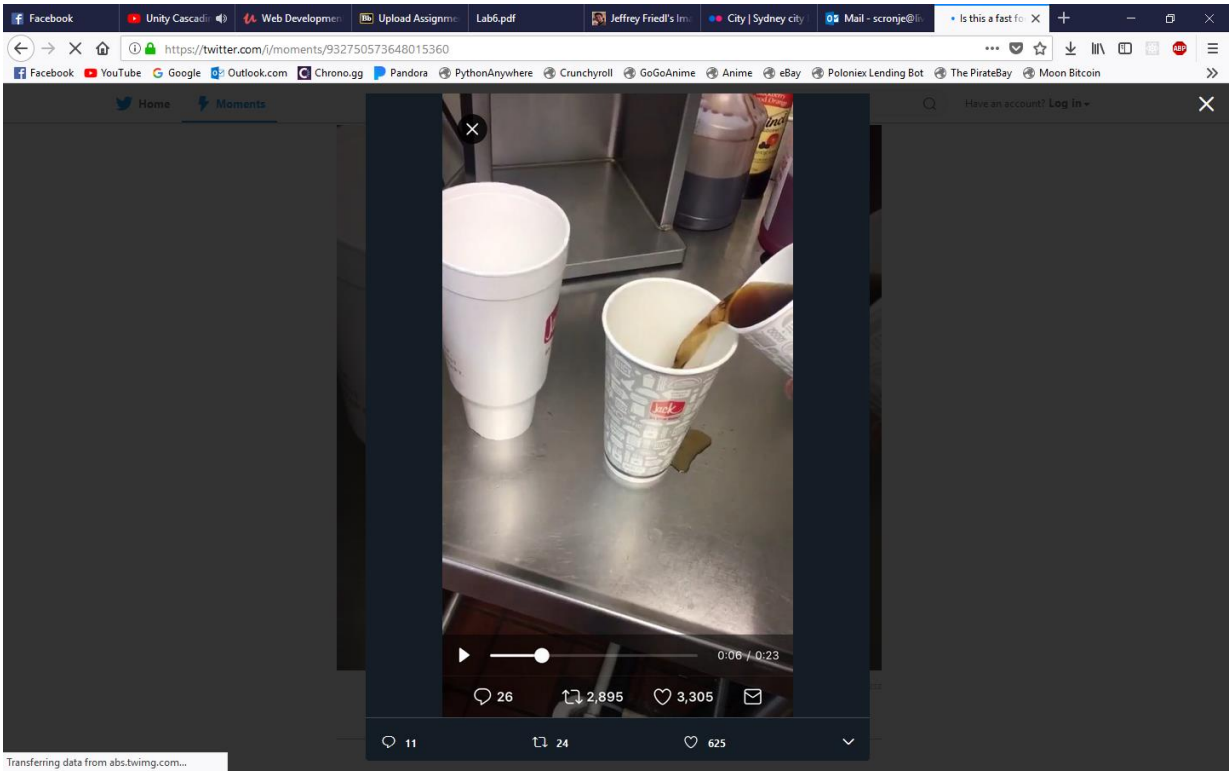
I followed the same process. This time I did find some exif information. It has been edited with Photoshop on a Macintosh on 2017/04/08.

Flickr



Again, I used the same method to find the exif information. I could not find anything for this image.

Twitter



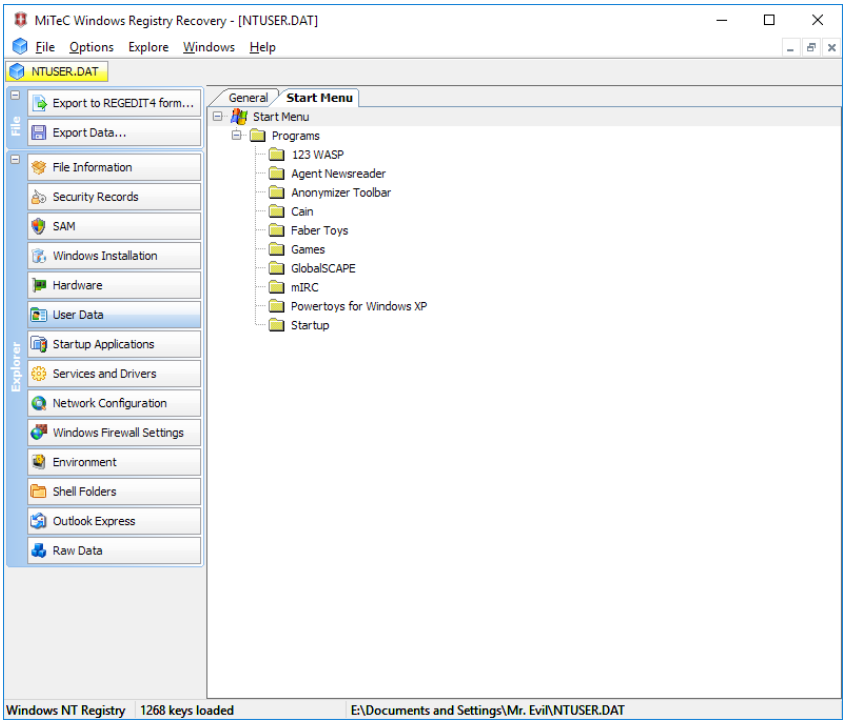
Again, for Twitter I used the same method to find the exif information. There was no information stored.

Lab 6.2 Windows Registry Forensic

Questions to answer (25 points each question):

1. Answer the question in step 11, where is the “system” file located in the C drive?
   The “system” file is located under “C:\WINDOWS\sytem32\config\system”.

2. In order Windows versions, such as Win98/XP, and Win7, when you press the “Windows” key, you will have the “Start menu” pops up. In the start menu contains many shortcuts from where you can quickly and conveniently start a program. Find out what program is contained in the “start menu” of the machine under investigation. Make a screen copy to answer this question.



3. What is Mr. Evil's email address?
   whoknowsme@sbcglobal.net

4. What is the manufacture/brand of the DVD drive of this machine?
   Toshiba