Austin Marino

Week 3 – Lab 3 Digital Forensics

CYB 339 – Cyber Operation Tools

Professor Morales

Contents

[Introduction 2](#_Toc118193)

[Results and Analysis 2](#_Toc118194)

[Networks 3](#_Toc118195)

[Recycle Bin 3](#_Toc118196)

[PDF Metadata 4](#_Toc118197)

[Image Metadata 5](#_Toc118198)

[Skype Data 6](#_Toc118199)

[Firefox Data 7](#_Toc118200)

[Conclusion 7](#_Toc118201)

[References 9](#_Toc118202)

# Introduction

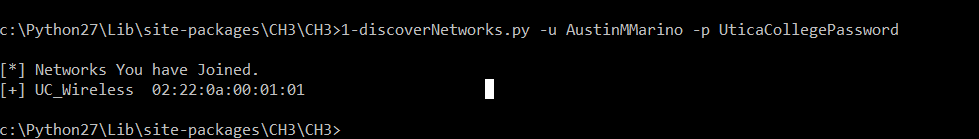
Computer Forensics and data analysis is a key component to being successful in both information security and crime investigation. Digital Forensics is a form of forensic science that focuses on the study and recovery of data found within a digital storage device. These storage devices are commonly known as computers, smart phones, tablets and many other devices used on a day to day basis. In this lab, the student will be utilizing Python scripts to discover metadata and personal information that is left within a computer storage device. In non-computer forensics, this can be referred to as trace evidence and falls under Locard’s principal of “Evidence is always left at the scene of the crime”. The student will be exploring many different types of data, from Firefox browsing history, to skype call conversation information.

# Results and Analysis

## Networks

In this portion of the lab, the student will visit the website <http://wigle.net> and create an account. This site allows a user to find physical locations from an access point in which a computer had been previously connected to. This may not seem like much information, but this allows an investigator to have a possible location as to where a cyber crime had been committed from. In image 3.1, the device tested was previously connected to a network named UC\_Wireless and provides a MAC Address of the router on the network. With an account being created on Wigle.net, the script constructed in Violent Python can now be utilized. The command *1-discoverNetworks.py -u AustinMMarino -p UticaCollegePassword* will receive data linked to the device registered on the account.

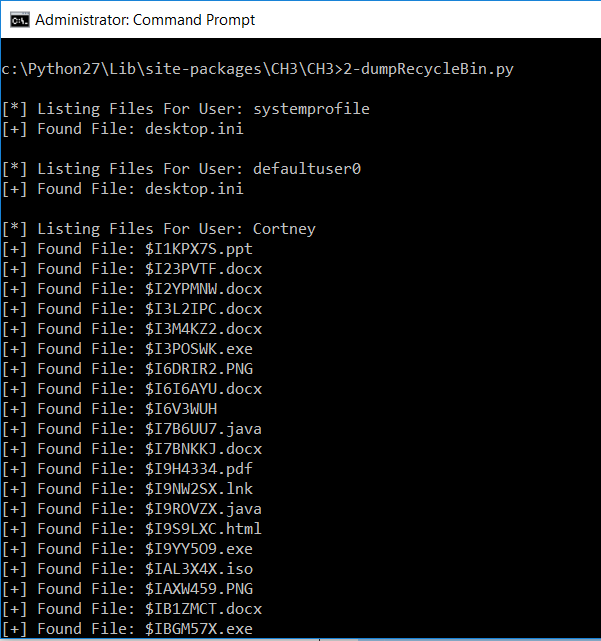
(Image 3.1)



## Recycle Bin

The Windows recycle bin is a key place to look while investigating a device for hidden or deleted data. Most users think once you delete something it is gone forever. However, running a simple script in Python can pull the full contents of the Recycle Bin. Running *2-dumpRecycleBin.py* pulls the entire contents and files in which have been “deleted” from the drive and sent to the bin. Refer to image 3.2 to see a small portion of the deleted files in the users recycle bin.

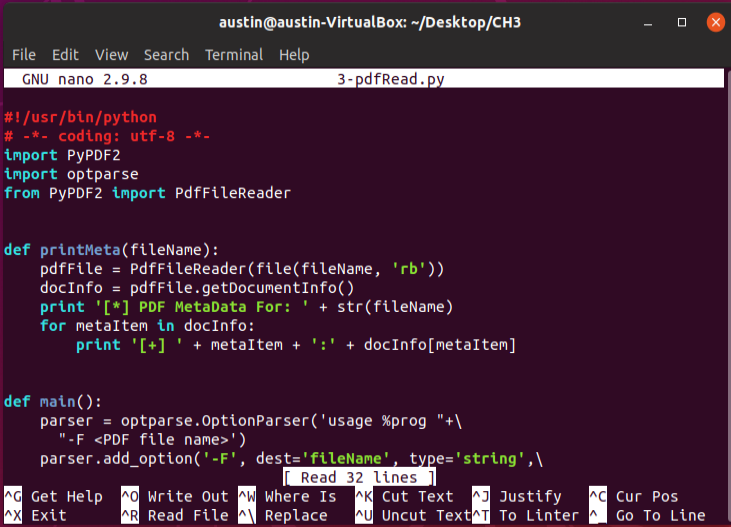
(Image 3.2)



## PDF Metadata

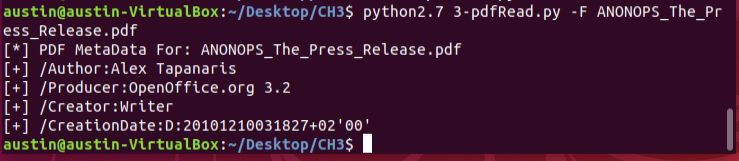
Below is the image of the source code of the PDF metadata script. The lines to be focused on here are line 3 (Image 3.3) *import PyPDF2* and line 5 (Image 3.3) *from PyPDF2 import PdfFileReader*. In the original code from the text, pyPdf was included in the source code. This module has been outdated and has been replaced with PyPDF2. To install the new module, use *pip install PyPDF2.* This will give the user access to the newest version of the Python PDF reader module.

(Image 3.3)



After the script has been edited with the proper modules, the command *wget* [*http://www.wired.com/images\_blogs/threatlevel/2010/12/ANONOPS\_The\_Press\_Release.pdf*](http://www.wired.com/images_blogs/threatlevel/2010/12/ANONOPS_The_Press_Release.pdf)will retrieve a press release containing information and will be downloaded into the virtual machine. The script constructed will strip the PDF of any important information such as author, producer, creator, dates and place them into a tabular format (Image 3.4). To run this script use *python2.7 3-pdfRead.py -F ANANOPS\_The\_Press\_Release.pdf* to find key information within this .pdf document.

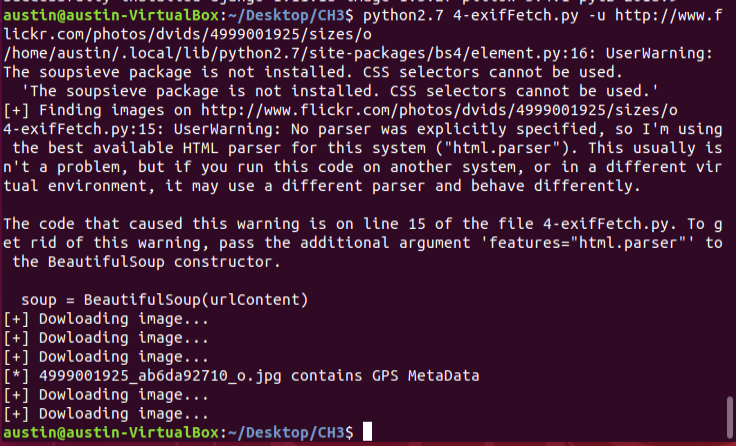
(Image 3.4)



## Image Metadata

Imaging data is highly important data to pay attention to. This data can provide a user with information such as GPS coordinates from images. During an investigation, gaining access to a physical location can allow the process of conducting searches and seizures much easier. This can also provide further information during a trial, allowing possible contradictions within alibis of criminals and also make evidence more concrete of when and where the crime was committed. The image below (Image 3.5) is scanning a target [*http://www.flickr.com/photos/dvids/4999001925/sizes/o*](http://www.flickr.com/photos/dvids/4999001925/sizes/o)for vulnerable images that still contain GPS metadata.

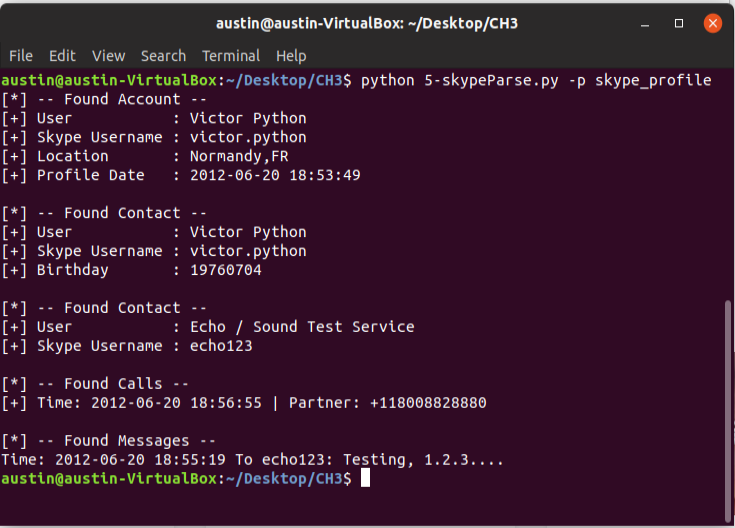
(Image 3.5)



## Skype Data

Skype is another application that stores metadata. Information such as contacts, conversations, birthdays, and time stamps are saved from individual calls and are stored in the user’s profile. This metadata can be pulled using a Python script less than fifteen lines in length and printed into a tabular format. To run this script, a target profile needs to be designated. The command (Image 3.6) *python 5-skypeParse.py -p skype\_profile* will allow the user to pull information on the designated target profile.

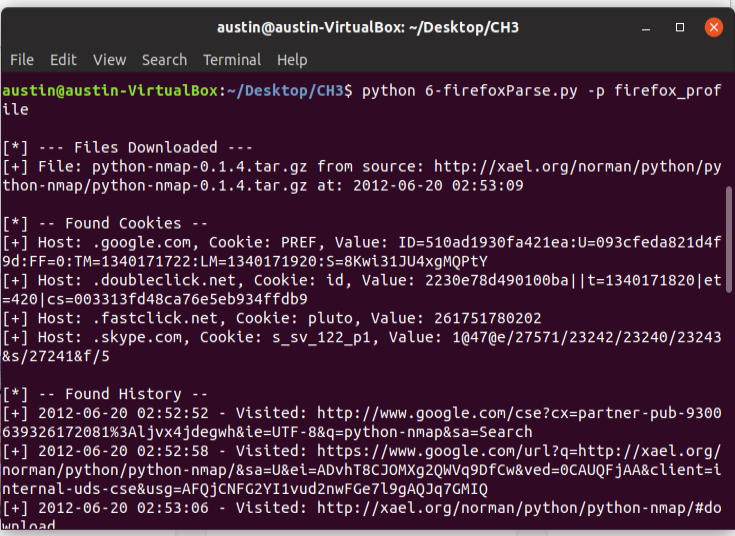
(Image 3.6)



## Firefox Data

Pulling metadata from Firefox is very similar to the Skype metadata script. This takes the users browser history instead of a user profile and prints information of websites and search history. Cookies are stored within the browser, allowing an investigator to filter through and see information on a designated target. In image 3.7, the user has Files Downloaded, Found Cookies, and Found History displayed in a readable tabular format. The script also displays data for which host the user downloaded or visited. This gives more insight to an investigation on “who, what, where, and when”.

(Image 3.7)



# Conclusion

Digital forensics has always been a big interest of mine, but I have never been given a good opportunity to actually practice it. This lab was an eye opener to a small portion of computer forensic work and what types of tools can be utilized during an investigation. Data recovery is a key component to having a successful investigation in a cyber related crime. Throughout this lab I endured many challenges and had to overcome them with a lot of online reading. During the exif metadata section, the PIL module had been outdated and was no longer supported. The textbook was very adamant on utilizing this module but unfortunately I could not find any information on it other than the module was obsolete and no longer supported. However, I did find there was a new module called “Pillow” which is backward completable with the old PIL module. This was a simple fix but took me over 3 hours to figure out. These are the downsides to taking a course of this difficulty online. It does force me to be more independent and conquer issues on my own which is always a good skill set to have in the computing industry. Another major issue I encountered was installing the PyPDF2 module in my virtual machine. When attempting to install I was receiving an error message saying the module did not exist. After reading some forum posts from fellow students, I found the solution and finally got everything up and running. After a long eight hours of constant working, I found the solutions to all the questions required. This gave me a little more insight on how difficult digital forensic work can be, but also how powerful these scripts can be. Some scripts were less than twenty lines of code and can pull very unique critical data.

# References

O’Connor, TJ “Violent Python A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers” 2013

Forum Threads on Stackoverflow:

<https://stackoverflow.com/questions/8863917/importerror-no-module-named-pil>

https://stackoverflow.com/questions/20060096/installing-pil-with-pip