Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

Project 4

You are a digital forensic examiner working for the Louisville Metro Police Department. A drug enforcement team has been after a suspected drug dealer, Perry Winkler, for several months. After finally obtaining a warrant to search Mr. Winkler's residence, LMPD arrives at the residence only to find an abandoned home. A first response team scours the home for any evidence as to Mr. Winkler's whereabouts, but the residence has been cleared of any useful evidence. After searching the dumpster outside the residence, a desktop PC is located and recovered. The desktop tower had been damaged – possibly in an attempt to render the data from the computer unreadable – but the hard drive is luckily intact. The hard drive from the computer is imaged using forensically sound measures and turned over to you in order to conduct a digital forensic examination. The lead investigator believes that the key to Mr. Winkler's whereabouts lies somewhere in the data collected from the computer. You are tasked with determining answers to the following questions regarding the computer recovered from the dumpster:

1. ***What identifying information did you find on the hard drive to help determine the owner of the computer?***
    - *Using the program*: **FTK Imager**
        - The first thing I did was load the image into FTK Imager to confirm that the device belonged to Mr. Winkler. One of the users of the computer is named **Perry**. Next I verified that the hash values matched so I could be certain that the image I downloaded is complete.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- *Using the program*: **Autopsy**
  - I switched over to Autopsy since it possesses the ability to carve images, and I found the file structure easy to use. I first searched for information regarding Mr. Winkler. I followed the path: DataSources/LMPD-436243-001.E01/vol3/$Recycle.Bin and Perry's SID in the recycling bin: **S-1-5-21-3461440871-1589894493-1829873476-1000**.
  - After poking around, I located a NTUSER.DAT file under Perry's user folder (img/LMPD-436243-001.E01/vol_vol3/Users/Perry). I then clicked on the file and moved to the Application tab. Under CMI-CreateHive{6A1C4018-979D-4291-A7DC-7AED1C75867C} I followed the path Software/Microsoft/Windows Media/WMSDK/General and located the ComputerName: **PERRYWINKLER -PC** and VolumeSerialNumber: **0xd86dc3e7**.
- *Using the program*: **Autopsy** and **LECmd**
  - When looking for data stored on USB devices I used Autopsy and navigated to C:\Users\ Perry\AppData\Roaming\Microsoft\Windows\Recent and extracted the LNK files. I then used LECmd to extract the metadata into a .csv file. I discovered a VMWARE machine with the MAC address of **00:0c:29:ee:c9:2a**. There is an Intel device with the MAC address is **a4:4e:31:46:b1:d0**. Both are associated with perrywinkler-pc.

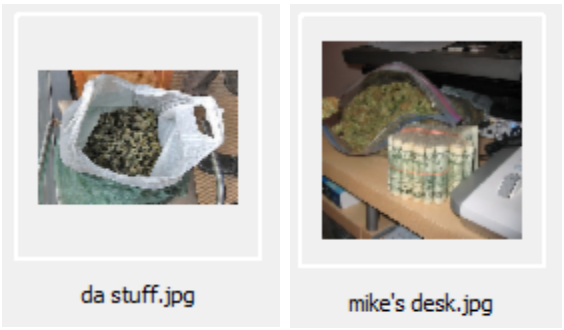
2. ***Is there any evidence on the computer that the user may have been associated with drugs or other illegal activities? Incriminating images, "client" lists, web history related to illegal activity, etc.***

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- *Using the program*: **Autopsy**
  - I started looking for any images that displayed nefarious or criminal activity. Luckily, some were recovered along with system icons. I followed the path: img/LMPD-436243-001.E01/vol3/Users/Perry/Pictures and located the files **da stuff.jpg** and **mike's desk.jpg** that were photos of cash and weed. Under Results/Extracted Content/EXIF the Metadata tab helped me determine that the photo **mike's desk.jpg** was taken on a Canon Powershot A60 camera.
    - 

  - I then switched to the Views file path to find more recovered images: Views/File Types/By Extension/Images Bin. I found three photos of guns: **th.jpg**, **thCAV3V9F6.jpg**, and **awesome.jpg**.
    - 

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- While I had the file types open I followed the path: Views/File Types/Documents/Office and found a file named **Book2.xlsx**. The contents suggest clients owe Perry money for drugs and illegal activities. In the metadata the Last-Author is **Lars**.

Sheet1

name	$$ owed	fav
MC Teller	450	tails
ronchop	500	angel
newbber	950	crack
nile	100	header
p dawg	50	lice
randy	1040	erthing

3. ***Is there any evidence that the user may have been trying to cover his tracks or delete evidence from the computer? Running secure erase programs, deleting files, etc.***

- *Using the program*: **Autopsy**
  - My first thought was to search through Perry's recycle bin. Most users assume this will completely remove a file from their PC. I followed the path: Results/Extracted Content/Recycling Bin. There is a message that suggests that Perry was trying to delete evidence and may have an accomplice. I found a file named **$RSU8VAG.rtf** containing a file from C:\Users\Perry\Document/**Letter2.rtf** that reads as follows:

Rick,
Thanks for your help! I will do wat you said with the task thing on the computer. Im glad you printed instructions for me or i woudl never figure it out lol. **anyways ill destroy this** and will look for your email with further instructions. cant wait to ditch this place!
Yours truly,
Perry

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- I was still trying to find deleted files so I followed the path: Views/Deleted/Files/File System. I then searched for "Rick" as a keyword. There is a message that suggests that Perry was trying to cover his tracks. I found a file named **Letter.rtf** that reads as follows:

  Rick,
  I think there onto us. What shud I do ? I know about **getting rid of the stuff** in the kitchen and bedroom but what about the computer? Please call me - i need to fugure this out.
  Signed,
  Perry

- I located a NTUSER.DAT file under Perry's user folder img/LMPD-436243-001.E01/vol3/Users/Perry. I then clicked on the file and moved to the Application tab below. A new path structure was displayed named CMI-CreateHive{6A1C4018-979D-4291-A7DC-7AED1C75867C}. I then started opening each folder I could see.
  - Under the path: Software/Microsoft/Windows/BitBucket/Volume/{094cd53b-bbe4-11e5-b7db-806e6f6e6963} I found a file named **NukeOnDelete**. BitBucket is an online Git-based source code repository hosting service. Perry may have downloaded and run code that is intended to destroy his PC.
- I then moved to see his downloaded files. I followed the path: img/LMPD-436243-001.E01/vol3/Users/Perry/Downloads and found a file named **sdelete.exe**. SDelete is a free command line tool that users can use to delete files securely so that they cannot be recovered anymore. This program may have been used to delete data.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

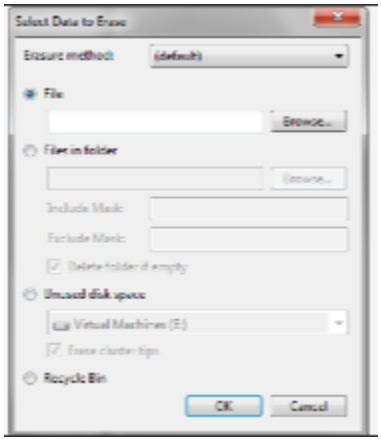
- Next, I wanted to check his web cookies to see if other data erasing programs were listed. I followed the path: Results/Web Cookies. I found Internet Explorer cookies for **eraser.heide.ie/** and **evidence.eliminator.en.softonic.com/**.
- After viewing his cookies I wanted to see if any web searches were recovered. I followed the path: Results/Web Search. Notable searchers on bing.com and google.com include: how to get rid of evidence, what is a batch file, download dropbox, sdelete, how to batch script, evidence eliminator, how to get rid of computer evidence, eraser, get rid of files, how to set up a scheduled task, and get rid of files.
- After I viewed his web searches I started opening all of the listed folder paths. I followed the path: Results/Extracted Content/Interesting Items/Interesting Files and I found **Tor Browser** which is an encryption program.
- I then followed the path: Results/Extracted Content/Installed Programs and I found Dropbox and Eraser. In addition, following Views/File Types/Executable/.exe displays the file **Dropbox.exe** and **Eraser.exe**.
- While checking his photos in the path: Views/File Types/By Extension/Images I found several screenshots. They are small but seem to show steps for deleting files. They are: image8.png, image11.png, image18.png, image14.png, image6.png, image13.png, image10.png, image12.png, image2.png, and image4.png.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- 

4. ***Can you identify any additional items (such as USB devices) that may contain pertinent evidence? Identify any devices and evidence of any files accessed on those devices.***

- *Using the program*: **Autopsy**
  - After reading this question I followed the path: Results/Extracted Content/USB Device Attached since it contained USB information. I found a **Cruzer** SanDisk Corp. storage device and a **Kingston DataTraveler** 102/2.0/HEMA Flash Drive 2 GB/PNY Attache 4GB Stick Toshiba Corp. storage device.
- *Using the program*: **Autopsy** and **LECmd**
  - To find data that was stored on the devices, I navigated to C:\Users\ Perry\AppData\Roaming\Microsoft\Windows\Recent and extracted the LNK files.
  - I then used LECmd to extract the metadata into a .csv file. There are three records with the drive type of removable. The photos **car1.jpg**, **car2.jpg**, and **mike's desk.jpg** were on accessed on these devices. I navigated to Views/File Types/By Extension/Images to find the images.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- 

5. ***Is there any evidence on the computer that the user may have been planning to go on the run? If so, where? If the user was planning to run, is there evidence that anyone might be traveling with him? If so, who? Planning documents, itineraries, contacts, emails, web history, etc.***

- *Using the program*: **Autopsy**
  - While looking for deletes files, I followed the path: Views/Deleted/Files/File System and found a message that suggests that Perry was planning to run. The .rtf file containing that message that reads as follows:

    ```
    Rick,
    Thanks for your help!  I will do wat you said with the task
    thing on the computer.  Im glad you printed instructions
    for me or i woudl never figure it out lol.  anyways ill
    destroy this and will look for your email with further
    instructions.  cant wait to ditch this place!
    Yours truly,
    Perry
    ```

  - In the same path Views/Deleted/Files/File System, I searched for "Rick" as a keyword after seeing it in the first letter I found. There is a message that suggests that Perry was trying to run. I found a file named **Letter3.rtf** that reads as follows:

    ```
    Rick,
    What should I do?  I havent hurd from you and im getting
    worried.  are you there yet?  i need an email to know.
    ```

Emily Wantland

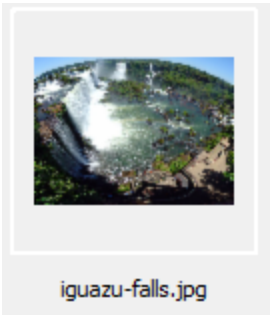
CIS 484-78

Prof. Hale

19 April 2021

```
Also, i bought those credit card numbers you showd me.
There supporsed to be all prepaid too so we are set!  lol
well i hope your safe and will look for your email.
Sincerely,
perry
```

- After looking through the deletes files I once again started opening all of the listed folder paths. I followed the path: img/LMPD-436243-001.E01/vol3/Users/Perry/Documents/nice and found a file named **iguazu-falls.jpg**. Iguazu Falls is a popular tourist destination in Brazil.



- I started to comb through the carved files in the path: DataSources/LMPD-436243-001.E01/vol3/$CarvedFiles and found a photo named **f0669024.jpg** of a map of **South America**.
- While looking for web cookies earlier at the path: Results/Extracted Content/Web Cookies, I found cookies for **southwest.com/** using Internet Explorer.
- While I had the file types open I followed the path: Views/File Types/Documents/Plain Text, and found **perry@southwest[1].txt** which suggests he had a Southwest account to book a flight.
- After looking at the Plain Text folder I switched to the HTML folder in Documents: Views/File Types/Documents/HTML. I found a document named **Passport[1].htm**.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- I started looking through the recovered email addresses to see if I could uncover any correspondence between Mr. Winkler and Rick. I followed the path: Results/Keyword Hits/Email Addresses/(\{?)[a-zA-Z0-9%+_\-]+(\,[a-zA-Z0-9%+_\-]+)*(\}?@([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4} and found **Rick Shoner.contact**. The metadata includes the FormattedName as **Rick Shoner** and the Address as **rickyboy579@aol.com**. This looks to be like Rick's full name and email address.
  - After finding Rick's email address, I navigated back to the carved files at: DataSources/LMPD-436243-001.E01/vol3/$CarvedFiles. I searched for "rickyboy579@aol.com" found the file **f0252768.mbox**. It is an email from Rick sent to Perry, or P Dawg. The metadata includes Perry's email address: **perrywin232k@aol.com**. The subject of the email is: **it's time**. The message was received on: **Sun, 28 Feb 2016 09:08:15 -0500 (EST)**. This confirms that Perry is located within the Eastern Time Zone. Lastly, there is an IP address listed for Perry's receival destination: **74.124.68.45**. The email reads:

    ```
    I finally made it here.  I'm using the hotel lobby computer so
    this cant be traced back to me.  I'll wire the funds to your
    western union tomorrow.  get rid of the evidence and get on
    united flight we talked about.  see you soon.
    ```

  - After finding Perry's IP address, I navigated to LMPD-436243-001.E01/vol3/$Unalloc/Unalloc_134476_106102784_6900195328. I used his IP address as a search key and found a file named**:** **[Unalloc_134476_106102784_6900195328]**. This file contained Rick's IP address **186.210.54.196**. This IP address is located in **Uberlândia, Brazil**.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- While checking his photos in the path: Views/File Types/By Extension/Images, I found several photos including the word passport—especially **passportcover.png**.

6. ***Identify any other evidence that you located on the computer that may assist LMPD in its investigation. If you're not sure whether or not it's important, include it!***

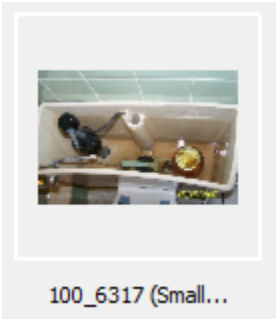
- *Using the program*: **Autopsy**
  - While checking his photos in the path: Views/File Types/By Extension/Images I located the file cc.jpg which was a photo of three credit cards in a stack. Perry confirms to Rick that he purchased credit cards in a letter.
    - 
      cc.jpg
  - While looking through all of the path folders I opened: Results/Extracted Content/EXIF Metadata. I found a file named **100_6317 (Small).JPG** that looks to be a photo of a taped-shut Prego jar in a toilet tank. The date on the photo is 05/05/2007 and it was taken on a KODAK Z650 Zoom Digital Camera.

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

- 

  - While looking through all of the path folders I opened: Views/File Types/By Extension/Archives and found a file named **plan.zip**. The File Metadata shows the path img/LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents/emails/plan.zip. This encrypted file may include the instructions that Perry references in his letters to Rick.
  - While looking through Perry's recycled files in: Results/Extracted Content/Recycle Bin, I found a filed named **$RNDKRDO.contact**. The file path was C:\Users\Perry\Contacts**Mary Reister.contact**. This may be a client. I navigated back to: Results/Keyword Hits/Email Addresses/(\{?)[a-zA-Z0-9%+_\-]+(\,[a-zA-Z0-9%+_\-]+)*(\}?@([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4} and found an email account **mreister@gmail.com** which shares the first initial and last name.
  - While taking a second look at the email addresses after finding Mary Reister at the path: Results/Keyword Hits/Email Addresses/(\{?)[a-zA-Z0-9%+_\-]+(\,[a-zA-Z0-9%+_\-]+)*(\}?@([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}, I found a contact file **LarrySpitz.contact** with the address **spitzmeister@rocketmail.com**.
  - Lastly, I wanted to see when the operating system was installed. I navigated back to the NTUSER.dat file to see the Windows Registry. I opened the application tab and started

Emily Wantland

CIS 484-78

Prof. Hale

19 April 2021

looking through the Create Hive: CMI-CreateHive{6A1C4018-979D-4291-A7DC-7AED1C75867C}. I clicked on Software/Microsoft/Windows NT and switched to the file metadata tab. There I found that the creation date is **2016-01-15 16:06:57 EST** and the latest modified date is **2016-02-28 10:49:29 EST**.

Conclusion

The hard drive image provided by the LMPD confirms that this device did indeed belong to Perry Winkler. It is probable that the suspect was engaged in criminal activity. The evidence points to gun-related violence and drug related crimes. Correspondence between Mr. Winkler and a Mr. Shoner suggests that the two are accomplices. Letters provide details about deleting evidence and fleeing the country. Mr. Shoner's IP address and photos found on the computer suggest that Mr. Winkler is headed to Brazil. A letter from Mr. Shoner instructs Mr. Winkler to take a United Airlines flight, but Mr. Winkler visited southwest.com.

In addition, several data erasing programs were found on the computer. Mr. Winkler downloaded applications to remove information from his system, but LMPD was able to recover data. After attempting to physically destroy the computer, but keeping the hard drive intact, he fled his home. It is likely that Mr. Winkler is either headed to a hotel in Uberlândia, Brazil.