Project 4

Darrell Liwanag

1.

Looking at the OS Systems acquired by using Autopsy I looked at the OS accounts listed. From there I noticed the only user on the desktop belonged to someone with the name ‘Perry’ that offers some evidence of it being ‘Perry Winkler’, the password seemed to be his name as suggested by the password hint. After further looking through recent documents in the data artifacts tab of autopsy, I discovered a LNK files I extracted some text from a Desktop.lnk stating that the ‘Perry’ user is linked to a desktop named ‘perrywinkler-pc’ which implies that user ‘Perry’ is Mr. Winkler as it uses the suspects first name. The user’s SID is S-1-5-21-3461440871-1589894493-1829873476-1000 this information was gathered under the reasoning that its SID may be linked to other incriminating evidences.

2.

After critical analysis over the system there has been pertinent information that suggest Mr. Winkler involved in illicit Drug and illegal activity. There has been three notable images found on the desktop. One labeled 100\_6317 (Small).JPG, illustrates a toilet tank with what is perceived to be a Prego pasta sauce jar holding substances other than sauces hidden in the water repository.

The second image is labeled as ‘Mike’s desk.jpg’, with the image being about 8 rolls of big bills bundled by rubber band next to a gallon Ziploc bag of marijuana. The third image labeled, ‘da stuff.jpg’, pictures a plastic grocery bag halfway filled with marijuana. Finally, after investigating the documents autopsy grouped up, I uncovered an XLS document named ‘book 2’ which has a list of clients and the amount of money owed as well as a column of their ‘Fav’ with the subjects matter being street names of differing drugs.

In addition, through FTK imager through the root, in the document section I accumulated a series of search histories put into a XLS sheet. In the aforementioned document, I uncovered a search history with the search stating, ‘ software to steal taxes’. So not only is Mr. Winkler involved with illicit drug activity but they are also interested in stealing taxes.

Finally I have found an .RTF with communications with Perry and a person named Rick through the file views/filetypes/documents/richtexts labled letters.rtf, the extracted text states:

“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”

This document alludes to the fact that an organization is onto them, meaning they have to start destroying evidence.

3.

As mentioned in in the evidence shown directly prior, the message foreshadows clues to Mr. Winkler deleting evidences and documents. With that being said, the owner of the computer failed to do so.

By using autopsy’s web history features, the web browsing history further highlighted searches related to privacy tools, including queries about using Tor and accessing a wikiHow page titled *"How to Send Anonymous Emails,"* which provided guidance on maintaining anonymity in digital communication. Additionally, the subject visited a Techwalla article titled *"How to Remove Traces of Your Activity on a Computer,"* suggesting an intent to understand methods for erasing digital footprints. In doing so, it prompted further digging into the web downloads via autopsy.

The digital evidence revealed a clear pattern of activity focused on researching and potentially implementing methods for online anonymity and the removal of digital traces. My findings present numerous downloads in software’s such as Sdelete, Eraser, and Evidence Elimination 6.0 which are all software’s used to delete files and information off of a person’s computer. In addition, I found a download of AOL and Tor browser which is an instant messaging platform designed to communicate without email trace and browse online with security, respectively.

After reviewing the prefetch files on the suspect's computer, the analysis revealed that Eraser version 6 was installed and executed on February 21, 2016, at 10:30:35 PM. The program was subsequently run five additional times between February 21, 2016, at 10:34:39 PM and February 28, 2016, at 3:47:14 PM

4.

In my investigation, I examined the Registry’s System Hive to gather information about storage devices connected to the system, a critical step in determining whether the suspect utilized external storage media for file transfers. During this analysis, I identified a Kingston Data traveler 101 G2 USB device with serial number 0013729B678DEB20C51F0216, which was connected on February 16, 2016, at 10:03:13 PM. Additionally, I found evidence of a SanDisk Cruzer USB device with serial number 200350011811625714CA7, connected on January 26, 2016, at 9:48:11 PM.

To ascertain the contents of these USB devices, I analyzed LNK files. The device with VSN 3AA4C98B had two images of a car with context insufficient to the subject matter. On the other hand, the device with the Volume Serial Number (VSN) A0C9328E contained the file from section 2’s evidence titled *"mike’s desk.jpg,"*.

Continuing my analysis in the registrys software hive, I found a link between attachment dates to specific files by cross-referencing the modified times of those files. the SanDisk drive, connected on January 26, 2016, matched with the last modification date of the *"mike’s desk.jpg"* image, supporting a direct connection between the device and the file in question.

5.

After looking through the carved and deleted files, the files hint with the two of them leaving by plane as cookies and cache suggest plane tickets searched via southwests website and united. With that initial hint, I found another email in Autopsy Fileviews/filetypes/Documents/richtexts/letter3.rtf, It denotes buying prepaid cards. The purchase of these cards implies using it to prevent being tracked since the cards are prepaid without a name.

The carved files first pointed me towards a deleted png file of a map of South America. As analysis continued I stumpled upon some png photos of a passport schematics with the following names:

A screenshot of a computer

Description automatically generated

This alludes to the idea of creating a counterfeit passport in efforts to relocate outside of American jurisdiction.

In addition to the passport photo findings, I uncovered an email in a .mbox file at /vol\_vol3//$CarvedFiles/f0252768.mbox. The email goes as follows:

A white background with text

Description automatically generated

The email was sent from accomplice, Rick Shoner with the alias ‘P Dawg’, to Mr. Winkler himself. After digging into the metadata, It seems that it was sent from a hotel computer in the middle of Brazil.

Afterwards, I stumbled across a photo of the Iguazu waterfall earlier in the analysis that I thought to be useless, but after further investigation I remembered the photo and looked up the destination and found it borders Brazil and Argentina. This photo may be a clue as to where they might set up base. In support of this notion, Eraser 6 had the same picture, meaning the user tried to delete it previously.

6.

In the midst of finding evidence for the current case, I have found possible avenues and lines of evidence that may point to accomplices or other charges.

The first avenue to approach is going through the listed contact files via root/Users/Perry/Contacts. There is Mr. Rick Shoner who seems to already be an accomplice/mastermind of this scheme. Then Larry Spitz with an email of [spitzmeister@rocketmail.com](mailto:spitzmeister@rocketmail.com). Finally, there is Mary Reister whos contact was found in the /$Recycle Bin.

The next avenue is to go over the /img\_LMPD436243001.E01/vol\_vol3/Users/Perry/AppData/Roaming/Microsoft/Crypto/RSA

File path. While scrubbing through files paths , I stumbled upon a crypto key that may provide an answer to unencrypting documents around this desktop. A screenshot of a computer

Description automatically generated

This crypto key may also point to the next lead I am about to say.

I have uncovered an encrypted zipped file named “plan.zip” that may allude to further plans about escape or erasure of data. This data was found at /img\_LMPD436243001.E01/vol\_vol3/Users/Perry/Documents/emails/plan.zip

Whilst trying to download and unzip the file, I was prompted with a message saying it “cannot open the file as a [zip] archive, is not archive” halting my investigation on this potential lead.

Finally the last possible lead comes from the carved files that showed an image of womans mugshot. The images was found at

/img\_LMPD-436243-001.E01/vol\_vol3//$CarvedFiles/f0259224.jpg

Whilst it may not amount to much, a reverse image search could be used on the image to investigate whether or not if it’s a potential suspect or accomplice.