Jackson Mundy

CIS 484

December 2, 2024

Project 4

As a forensic analyst I have been tasked with scrubbing through this image of a computer's drive. We hope to determine pertinent information that can aid the LMPD in this case. I will be looking for evidence in areas such as recent documents because it will contain LNK files, the registry system hive for information regarding connected devices, and other various commonly used directories. The hopes are that the computer can be linked backed to Perry Winkler, and that the files and information about the system can provide insight and evidence on what Perry was involved in. There are many different applications that could accomplish the necessary tasks to ascertain the desired information, but I will be using FTK Imager and Autopsy as they provide a comprehensive overview of the information I need to access.

1. The first bit of information I found on the disk image to identify the user of the computer was in Partition 2 of the disk image. The path “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry” is located on the partition mentioned earlier.  Also, the text of this link file contains a path suggesting that the pc name is ‘perrywinkler-pc’ and can be found at the path

|  |  |
| --- | --- |
|  | ‘/img\_LMPD-436243-001.E01/vol\_vol3/Users/Perry/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/1b4dd67f29cb1962.automaticDestinations-ms/Desktop.lnk’ |

This was found via Autopsy along with the SID S-1-5-21-

3461440871-1589894493-1829873476-1000, which was in the Software\Microsoft\Windows

NT\CurrentVersion\ProfileList subkey. The pc name ‘perrywinkler-pc’ can also be found in the computer name key. Just based on this alone, one could conclude that Perry Winkler used this computer due to the name of the user matching the first name of the suspect.

1. Yes, there is some evidence also found using FTK Imager that could lead one to believe that Perry Winkler was involved in illegal activities. The biggest giveaway was that this computer had the Tor browser downloaded on it through the User “Perry”. Tor is notorious for being the browser that grants you access to what is known as the ‘Dark Web’. The Dark Web allows for people to access an underground side of the internet that deals with almost anything the user wants. A big use for the Dark Web is drug trafficking/ selling. The path to the browser is “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Desktop/Tor Browser”.

Based upon further inspection I found evidence that Perry used the search engine Bing to find information on theft type software and untraceable emails. The searches also reveal that he was interested in stealing tax refunds and committing identity theft. This information was located in an Excel workbook, the path is “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Documents/Book2.xlsx.FileSlack” Upon further discovery the Excel Book located in Perry’s document directory contains a list of names, amount ($) owed, and a tab called ‘favs’. Potentially hinting at customers and their favorite drugs since I saw one of the items listed was ‘crack’. The pathway to find this is “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Documents/Book2.xlsx”.

The Documents directory contains letters seemingly to a person named Rick who is an accomplice as Perry is asking him for aid on how to cover their tracks as he believes they’re going to get caught. This Rick can be the Rick Shoner contact that is found in the Documents folder. In that contact there is an email address “[rickyboy579@aol.com](mailto:rickyboy579@aol.com)” that can be linked back to Rick and was used for communications between the two. The paths to both of the letters are “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Documents/Letter.rtf” and “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Documents/Letter3.rtf”.

Also, within the Documents there is a picture that seems to hide some substance in a mason jar inside the toilet, this can be found at “LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/Users/Perry/Documents/100\_6317 (Small).JPG”. Using Autopsy I found an image of a bag of weed and another one containing a bag of weed and money. This could be some of the products that Perry was distributing based on other information. Also, there is an image of credit cards which Perry mentioned in a letter to Rick. The file path to find all these images is ‘/img\_LMPD-436243-001.E01/vol\_vol3/Users/Perry/Pictures’. The file names are ‘cc.jpg’, ‘da  stuff.jpg’, and ‘mike’s desk.jpg’. Based on all this evidence one could conclude that Perry was involved in illegal activities and had help as well.

1. Yes, there is evidence of Perry Winkler looking to delete information. This path ‘LMPD-436243-001.E01/Partition 2[61338MB]/NONAME [NFTS]/[root]/$Recycle.Bin/S-1-5-21-3461440871-1589894493-1829873476-1000/$RSU8VAG.rtf’ displayed a rich text file that shows that Perry got instructions on how to run tasks on the computer from someone presumably Rick and used it to destroy content on the laptop. This file also tells us that Perry was planning on trying to escape. I found this by using the FTK Imager and sifting through the recycling bin.

Found via Autopsy ‘/img\_LMPD-436243-001.E01/vol\_vol3/Users/Perry/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/ZEUKYOGF/’ this path is a screenshot that shows that a file was deleted. As mentioned beforehand there had been communications between Perry and Rick around removing evidence off Perry’s system, the conversations took place via a deleted email between “[perrywin232k@aol.com](mailto:perrywin232k@aol.com)” and “[rickyboy579@aol.com](mailto:rickyboy579@aol.com)”. The email was about removing computer evidence by using task scheduler. Softwares such as Eraser, SDelete, and Evidence Eliminator are existent on the laptop under the Perry account. This can be further backed up by some of the search history on the web. Some of the web history includes going on sites to use anonymous emailing and covering of evidence.

1. I have found a total of 8 USB Devices to have been attached to the computer. 4 being related to VMware and only one being a Virtual USB Hub the others being Virtual Mouse. 2 being RootHubs and 1 is a Cruzer and the other is a Kingston DataTraveler flash drive.  The Kingston DataTraveler having the ID 0013729B678DEB20C51F0216 and the Cruzer having the ID 20035001811625714CA7.

The Kingston flash drive is 2GB and suggests that there was data being stored on there that could contain more information that aids the investigation. It can be seen that these devices were used to transfer files when you match up their connection times with some of the files. This is evident with the fact the last modified date of the image “mike’s desk.jpg” corresponds to the attached date on the Cruzer drive. Looking over LNK files further confirms this as the LNK file for “mike’s desk.jpg” leads back to the ‘E:’ drive rather than Perry’s ‘C:’ drive.

1. Through my investigation I have found evidence lending to the fact that Perry was intent on escaping with Rick. In one of the letters shared between the two, Perry expresses his excitement as he says that he cannot wait to get out of this place (seemingly the country). This letter can be found in the RecycleBin as Perry was attempting to cover some of his communications. The reason I stated that it seems that Perry and co are wanting to flee the country is because there are png photos that could be used to counterfeit passports. Obviously, the use of passports is for entry into other countries.

The aforementioned prepaid credit cards that were mentioned in the letters between Rick and Perry could also be used as the means to purchase the tickets since they won’t be traced back to them. One could be led to believe that Perry will use Southwest Airlines as means of transportation but when viewing the email conversation between Perry and Rick found at “/vol\_vol3//$CarvedFiles/f0252768.mbox” you can see that the intended airline was United and there was said to be a money transfer as well. Rick wanted to stay anonymous as he communicated via a hotel lobby computer.

Within the carved files I was able to find a picture that was a map of South America. This prompted me to go back and find the photo of the waterfall, Iguazu Falls, which is found at “[root]/Users/Perry/Documents/nice/”. Iguazu Falls is located in South America near Brazil and Argentina. Connecting these two bits of information will allow for one to conclude that the arranged meeting area is within South America. The same image was also found “[root]/Users/Perry/AppData/Local/Eraser 6” prompting one to believe that this was meant to be secret.

1. I don’t know how much value these photos will be but there are multiple photos of guns, and extravagant cars that can show inside the mind of Perry Winkler. The photos show that he desired a very rich lifestyle that some can attribute to being acquired through illegal means. The money, guns, and cars are very braggadocious and extravagant. One could reference this to drug lords from pop culture media.  There isn’t necessarily anything illegal about having these pictures especially since some appear to be stock photos taken off the web. These pictures should be used in conjunction with the more crucial evidence that has been discussed.

Besides the pictures I found more contacts in the ‘[root]/Users/Perry/Contacts’ location. The contacts located in the Contacts directory belong to Rick Shoner, Perry, and Larry Spitz. In the Recycling Bin I found an additional contact belonging to a Mary Reister. There wasn’t much useful information within the contacts besides standard information. When going through the images, there were a few photos of people that could be meant to represent some of the people involved, but there isn’t evidence to suggest that.

Through my analysis I have found hard evidence that links Perry Winkler to illegal activity and found even more information to provide a thorough outline of his plan and the help he received. Perry was anxious that he was soon to be caught and received aid from his accomplice Rick Shoner, as seen through emails and various letters, to discard physical and logical evidence. Some of the evidence was uncovered and yielded results showing that he had dealings in drugs, theft, and planned on fleeing the country to meet up with Rick down in South America near the border of Brazil and Argentina.