|  |
| --- |
| Project 4 |

|  |
| --- |
| Emily Green, Ryan Logue, Caleb DeSpain, and Joseph Eckl  4-17-2016 |

Table of Contents

[Investigation Summary 2](#_Toc6307304)

[Methodology 3](#_Toc6307305)

[Analysis 4](#_Toc6307306)

[File and Folder Analysis 4](#_Toc6307307)

[1. What identifying information did you find on the hard drive to help determine the owner or user of the computer? Does the computer appear to have used by Perry Winkler? 4](#_Toc6307308)

[2. Is there any evidence on the computer that the user may have been associated with drugs or other illegal activities? 5](#_Toc6307309)

[3. Is there any evidence that the user may have been trying to cover their tracks or delete evidence from the computer? 6](#_Toc6307310)

[4. Can you identify any additional items (such as USB devices) that may contain pertinent evidence? If so, what are they? Include as much identifying information about each device as possible. 7](#_Toc6307311)

[5. Is there any evidence on the computer that the user may have been planning to go on the run? If so, can you determine where the user was planning to go? 7](#_Toc6307312)

[a. If the user was planning to run, is there evidence that anyone might be traveling with them? If so, can you determine the identity of the accomplice(s)? 7](#_Toc6307313)

[6. What other evidence did you locate on the computer that may assist LMPD in its investigation (e.g. files that point to additional leads, accomplices, or any other activity not targeted by the initial investigation)? 9](#_Toc6307314)

# Investigation Summary

In 2016 we were given a search warrant of Perry Winkler's residence on suspicion of drug dealing activities. After the search warrant, we obtained a copy of the suspect’s hard drive. We used this disk image to find out more information about Perry Winkler’s activities and his possible location.

After looking through the disk image, we were able to discover evidence of possible drug dealing activities because the disk image contained pictures of marijuana, and an excel document named ‘Book2’ that was used to store clients. We also found a downloaded Tor browser that could have been used to buy and sell drugs over the internet.

Also during the investigation, we found that Perry had tried to destroy evidence on his computer by looking for wiping programs and downloading two wiping programs. Perry looked at Evidence eliminator, vanish.com, and IndoCleaner. He downloaded Eraser and $Delete. He was also using services that kept his communications private like anonymouse.org, which he used for their anonymous emailing service. He was also interested in remailers, which enable you to send emails without revealing your true email address.

We found that Perry had several communications with Rick Shoner named ‘Letter’, ‘Letter2’, and ‘Letter3’. We also find a final communication called ‘It’s time’ from Rick to Perry telling Perry that he was in the hotel lobby and telling Perry to book a flight on United Airlines. However, we think Perry may have taken a Southwest flight. We believe Perry may have fled to the Iguazu Falls area in South America.

Perry also had other evidence on his computer like two flash drives a SanDisk Cruzer and a Kingston DT 100 G2 that may contain valuable evidence to the investigation.

# Methodology

Our methodology was to begin by verifying the disk image by taking an MD5 hash. Then we began by looking at the disk image in a general sense. We use FTK imager to view the disk image and browse the second partition looking for information on Perry. We assumed the easiest place to start would be in the folder labeled ‘Perry'. This gave us basic information about the user. We found his contacts, pictures of drugs, an excel spreadsheet of customers, and showed us that he had downloaded multiple wiping programs (via his ‘Downloads' folder). We also used RegExplorer, $IParse, HxD, JLECmd, and LECmd to gather more general info about user activity on the disk image.

From this basic information that we were able to grab from the ‘Perry’ folder on the disk image, we were able to begin a more detailed search using Autopsy. Once the disk image was loaded into Autopsy we looked at the files we were able to carve. From that, we found the communication between Rick and Perry that said Rick was in a hotel lobby and giving Perry instruction on how to leave the country and wire money to him. The carved files also gave more info about what Perry had been doing on his computer. For example, he was looking at other wiping programs and anonymous email service.

Autopsy also gave us the ability to sort the information contained in the disk image. This was useful in creating a more detailed search. For example, we sorted by file extension which enabled us to quickly find file extensions that might be useful such as .mbox, .exe, .png, .jpeg, etc. We were also able to narrow down our search using Autopsy because of the keyword search.

# Analysis

## File and Folder Analysis

### What identifying information did you find on the hard drive to help determine the owner or user of the computer? Does the computer appear to have used by Perry Winkler?

Using Registry Explorer, we investigated the System hive and in the ComputerName subkey, we were able to find that the name of the computer was PERRYWINKLER-PC. (SYSTEM: ControlSet002\Control\ComputerName\ComputerName)

Next, we looked at the Software hive in the registry. In this, we found the ProfileList subkey which lists Perry and his SID that was on the disk. (SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3461440871-1589894493-1829873476-1000) This information was useful because the SID listed in the ProfileList matches the SID listed of the user sending items to the recycling bin. Meaning that Perry is the one using the computer because his account SID matches one of the users putting files in the recycling bin. It also matches a SID listed in the Security hive under the Accounts subkey. The Software hive also lists Perry as the current owner of the computer in the CurrentVersion subkey (SOFTWARE: Microsoft\Windows NT\CurrentVersion).

Finally, we looked in the SAM hive. This hive is useful for identifying user accounts on a system and in the User subkey we found that it listed 3 users that had accounts on the computer: Admin, Guest, and Perry (SAM\Domains\Account\Users). In this subkey, it showed that Perry last logged on to the computer on 2/28/2016 at 3:45 PM and logged onto the computer a total of 9 times.

Using Autopsy, we found the listed owner of the hard drive was Perry by looking under results > Operating System Information > System. Moreover, another piece of evidence that Perry is the owner of this hard drive is that the computer listed under all event logs is ‘PERRYWINKLER-PC’ and the OS recognizes the system name as ‘PERRYWINKLER-PC’.

### Is there any evidence on the computer that the user may have been associated with drugs or other illegal activities?

The first piece of evidence that was found that Perry may be involved in illegal activity was in the registry under ‘NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedUrls’. This shows that the last thing typed in the URL bar in an Internet Explorer browser ‘how to skim credit cards’. Using Autopsy we were able to find more suspicious items that the user searched for like ‘how to steal tax refunds’. We also found that he searched for ‘how to get rid of evidence’ and ‘being watched by cops’. These items found in Autopsy in Perry’s Internet Explorer internet history and were searched for using google.com and bing.com.

Using Autopsy we found that Perry has pictures of drugs and money found in his ‘Pictures’ folder. The first picture is named ‘Mike’s desk’ that was taken on 4/2/2007 with a Canon PowerShot A60. This picture shows a bag of marijuana and cash on a table. The second picture is named ‘da stuff’ which was created on 1/26/2016 and shows a bag of marijuana in a chair. The user also had pictures of credit cards and guns on his computer. The second piece of incriminating evidence is an excel document named ‘Book2.xls’ that was found in Partition 2\NONAME\root\Users\Perry\Documents. It contains columns with names of people, ‘$$ owed', and a ‘fav' column that lists street names of different drugs. This suggests that Perry could be involved in dealing drugs. The user has a shortcut to start a TOR browser on his desktop, which is what he could have been using to help buy and sell drugs on the internet. The user also had an image of what looked like an explosive device that was discovered by using Autopsy’s file carving tool.

### Is there any evidence that the user may have been trying to cover their tracks or delete evidence from the computer?

It seems like the user was trying to destroy the evidence of their activity on their computer because the user had several wiping programs on their computer. One was $Delete and the other was Eraser. Using the Registry Explorer, we found that Perry had run the Eraser program 4 times and that it was last run on 2/28/2016 at 3:47 PM. Perry also had the Eraser program set to run at each restart of his computer. This was found in Registry Explorer in the Software hive under the Run subkey (SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

Perry was also looking at several other programs that would delete files and hide user activity on a computer. In carved files found on Autopsy, we found that Perry was looking at Vanish.com, evidence eliminator, Indocleaner, and Anonymouse.org. Perry was probably looking at anonymouse.org in order to use the anonymous email service. Perry was also looking at traceable and untraceable remailers. A remailer enables you to send and receive email while keeping your real email a secret.

The user also had several suspicious web searches like ‘being watched by the cops’, ‘how to get rid of evidence’, ‘scheduled tasks’, and ‘how to run batch files’. Perry’s search for batch files, $delete, and scheduled tasks correlated with a batch file on his computer called ‘$delete.bat’. All of these web searches were again discovered using Autopsy like mentioned before. Perry searched for these items using bing.com and google.com.

Perry was also using Dropbox which could have been used to store additional files and send files to other accomplices. This suggests that the user was aware that his activities could be prosecuted by law enforcement and was suspicious that he was already being investigated/watched by police. Moreover, it shows that the user was actively trying to get rid of evidence that his computer contained.

There was also a letter written to Rick by Perry that was placed in the Recycling Bin, Perry was possibly thinking that it would remove this piece of evidence from the computer. The content of ‘Letter2’ also included Perry talking about getting rid of evidence and being given instructions on how to do so.

### Can you identify any additional items (such as USB devices) that may contain pertinent evidence? If so, what are they? Include as much identifying information about each device as possible.

There were two USB devices connected, a SanDisk Cruzer with serial number 20035001811625714CA7 and a Kingston DT 100 G2 with serial number 0013729B678DEB20C51F0216. Both of these items were found using Registry Explorer and there could be files on these devices that Perry forgot to delete that could have files that could help the investigation.

### Is there any evidence on the computer that the user may have been planning to go on the run? If so, can you determine where the user was planning to go?

### If the user was planning to run, is there evidence that anyone might be traveling with them? If so, can you determine the identity of the accomplice(s)?

Perry seems to have been in contact with several individuals, one was Rick Shoner. Rick was listed in Perry’s contacts list and his info was Partition 2\root \Users\Perry. Rick and Perry seem to have a personal relationship because Perry has him listed with the nickname ‘Master Rick’. Moreover, Rick and Perry have been in communication with each other. This is evident from Perry’s letters that he wrote him which are located in his ‘Documents’ folder and named “Letter” (created 2/16/2016 at 5:04 PM) and “Letter3” (created 2/27/2016 at 10:13 AM). Another communication to Rick was found in the Recycling Bin named “Letter2” (Created 2/21/2016 at 5:22 PM and sent to the recycling bin at 2/28/2016 10:47 AM). In these communications, Perry asks Rick for instructions on how to use the wiping programs that he has downloaded on his computer and in the second letter he specifically says, “can’t wait to ditch this place!”. Rick also sent an email back to Perry using AOL. The email was titled ‘it's time' and in the email, Rick tells Perry that he is in a hotel lobby and is going to wire Perry money and tells him to take a United flight.

**‘Letter’**

I think there onto us. Wat 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 figure this out.

**‘Letter2’**

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 would of 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

**‘Letter3’**

Rick,

What should I do? I haven’t hurd from you and im getting worried. Are you there yet? i need an email to know. Also, i bought those credit card numbers you showed me. There supposed to be all prepaid too so we are set! lol well i hope your safe and will look for your email.

sincerely,

perry

**‘It’s time’**

“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.”

Perry also looked at Southwest.com and could have possibly booked a flight on Southwest. Perry also had a folder in his ‘Documents’ that was named ‘nice’ and had a picture of Iguazu falls. He also had a picture of South America that was found in carved files using Autopsy. We think that Perry may be around the Iguaza falls area in South America.

### What other evidence did you locate on the computer that may assist LMPD in its investigation (e.g. files that point to additional leads, accomplices, or any other activity not targeted by the initial investigation)?

A carved file, f2080560.jpg found in Autopsy showed a picture of a man and woman. These people may have known Perry or the picture could be Perry himself. It would be useful to use this picture as a way to try and track down or identify people of interest. Another picture, f0259224.jpg, was found of a mugshot of a woman who may have known Perry. This person may have useful information as well. Perry also has others listed in his contacts that may have pertinent information for the investigation. Those people would be Larry Spitz, and Mary Reister.

Perry also had a suspicious zip file named, ‘plan’ but it seems like the file has been corrupted. When we tried to unzip it, we got the error, “can not open [zip] as archive, is not archive”. When we opened the file in HxD, a hexadecimal editor, to try and recover the file, we found that the file had no header or footer. In order for a zip file to be recovered, it must have either a header or a footer in order to enable us to assemble the proper header or footer the file needs. The header or footer can tell us what file zipping program was used and how the file was compressed.