Project 4

CIS 484-75

Blaine Ford, Madison Martin, Sagar Tamang, Samuel Akinfenwa

Project Overview:

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 or user of the computer? Does the computer appear to have used by Perry Winkler?

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

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

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.

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? 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)?

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)?

## Question 1 :

The information that was used to verify the computer was used by Perry Winkler was using FTK Imager. The path was LMPD-436243-001.E01/Partition 2 [61338MB]/NONAME [NTFS]/[root]/Users/Perry with a user SID of S-1-5-21-3461440871-1589894493-1829873476-1000.

We used Registry Explorer to look at different registry hives to see if Perry Winkler was a user account on the Hard Drive. Looking through the software hive, the first thing we looked at was was the CurrentVersion at the path \Partition 2\[root]\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion and the stated RegisteredUser is Perry. We then dove deeper and looked at \Partition 2\[root]\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList\ and found a user named Perry with the same SID of S-1-5-21-3461440871-1589894493-1829873476-1000.

We used RegRipper to look through the SAME hive and found that the user “Perry” had logged on 9 times and the last logon was Sunday February 28 at 15:45:38 2016.

Lastly, we found signed documents from Perry.

## Question 2 :

By using FTK Imager, you could explore the image and see what was on it. After looking through the hard drive image, yes, there was evidence that the user was associated with drugs and other illegal activities. We found under \Users\Perry\Downloads he has downloaded “Eraser 6.2.0.2970” which is an application used to delete files. By seeing this, you can determine that Perry is trying to completely delete illegal evidence. Located on \Users\Perry\Desktop, there is a photo named “in my dreams” that is a photo of a gun. He also has a download for a Tor Browser which is tied to access to the dark web. Within \Users\Perry\Pictures, there is a picture labeled “100\_6317 (Small).jpg that illustrates a jar of Prego spaghetti sauce hidden in the base of a toilet. This is very likely a hiding spot for evidence. We found an Excel spreadsheet named “Book2.xlsx” which looks to be a list of clients who purchase drugs, showing how much money they owe Perry, and their favorite drug. Lastly, we found a Word Document under \Users\Perry\Documents named “Letter3.rtf” that is written by Perry to Rick Shoner. Within this document, Perry shows his level of concern of getting caught performing such illegal activities and how he plans to hide his evidence “in the kitchen and bedroom”. He also asks Rick what to do with the computer.

## Question 3 :

We found that the current version of the operating system is Windows 7 Professional and the install date was 2016-02-15 21:06:55. We found this under the software hive and looking at \Microsoft\Windows NT\Current Version.

We found this information valuable because after looking at the web history in Autopsy, there were two URL’s “ietld:hku.hk” and “ietld:jobs.cz” that shows they were created and accessed on 2010-11-20 16:00:31 EST and they modified and changed on 2016-01-15 16:07:09 EST which is converted to be the same time as the OS install date. Seeing this makes you believe that Perry was trying to install a fresh version of Windows 7 to cover up any evidence.

There were some Word Documents found under \Users\Perry\Documents that seemed suspicious. One was named “Letter.rtf” and said;

“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 letter is showing Perry is nervous by saying “i think there onto us” and he is asking Rick his opinion on what he should do with the computer.

The next letter to Rick, named “Letter3.rtf” found in the same folder. This is still showing the same level of concern.

“Rick,

What should I do? I havent 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 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”

We parsed the $Recycle Bin using $I\_Parse and found six files that Perry had tried to delete. We used the built in File Carving in Autopsy and discovered the six files that were deleted in Results\Extracted Content\Recycle Bin. four of the six files were pictures. One was a vehicle and the other three were weapons. Another deleted item was contact information for “Mary Resiter”. The last file was “Letter2.rtf”. This file was deleted on 02/28/2016 15:47:37 UTC. Below is the contents of this deleted letter.

“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”

Based on his letter to Rick, it sounds like Rick had given Perry some instructions on how to destroy the computer in order to hide the “task thing on the computer”.

With this information, we wanted to look at programs that are scheduled to run. We looked at the Software Registry Hive using Registry Explorer. We went to \Partition 2\[root]\Windows\System32\config\SOFTWARE: Microsoft\Windows\CurrentVersion\Run the program Eraser.exe is executed from "C:\Program Files\Eraser\Eraser.exe" -atRestart. The program Eraser is used to cover up files on a hard drive by overwriting them multiple times.

Perry is trying to delete and hide his illegal activity.

Question 4 :

Yes we found two USB devices that have been connected to the suspects computer by using USBSTOR. These two devices were USB Flashdrives. One was a Kingston DT 101 G2 and the other was a SanDisk Cruzer. Using LECmd, we found two image files named “car1.jpg” and “car2.jpg” that were stored on a removable device. These pictures of these cars could be cars that could have been stolen and used in illegal activities. Another image found was a picture of Mike’s desk. This picture shows what looks like marijuana and a large roll of money. In the background, there looks to be a computer which may contain more evidence of criminal activity.

## Question 5 :

Looking at TypedURL in the NTUSER.DAT hive using registry explorer, a recent website URL visited was <http://southwest.com/>.

Using Autopsy and looking at \Results\Extracted Content\Recent Documents for Rick Shoner we found an email; [rickyboy579@aol.com](mailto:rickyboy579@aol.com), which only seems logical to trace back to Rick. We used Autopsy again to find any emails associated with that email. We found an email being sent from this email to [perrywin232k@aol.com](mailto:perrywin232k@aol.com), which would connect to Perry Winkler. This email has a title of “its time”. The email is as follows:

“I finally made it here. I'm using the hotel lobby computer so this can't 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.”

The IP Address 186.210.54.196 associated with the email came from Brazil. This makes us believe that Perry is traveling to Brazil to meet with Rick, based upon the email and the IP Address.

## Question 6 :

We found a file under \Users\Perry\Documents\emails that is zipped named “plan.zip” that has been corrupted. Even though this file was not retrievable, it makes us suspicious of what this “plan” was. We found the download of the TOR Browser to be unusual too. The two deleted contacts, Mary Reister ([mreister@gmail.com](mailto:mreister@gmail.com)) and Larry Spitz ([spitzmeister@rocketmail.com](mailto:spitzmeister@rocketmail.com)) make us believe that these were some of the contacts that Perry had dealt with in the past, and no longer does. The LMPD may want to try to track down those two people and find out what dealings they had with Perry. Under the Web Search in Autopsy, Perry searched “how to get rid of computer evidence” , or something similar several times. This makes it obvious he was trying to hide the actions taken on the machine.

## Conclusion :

After looking through the Hard Drive given to us by the LMPD, we have determined that the computer was owned and or used by Perry Winkler. During our investigation, we found pictures of drugs, guns, and hiding spots for the drugs and weapons under a user profile named “Perry”. We found evidence of a fresh install of the Windows OS to try to cover up some of the evidence as well. There were applications Perry tried to download, such as Eraser and SDelete to destroy any evidence. Finding the contact information for Rick Shoner, we discovered his email and found emails being sent from Rick to Perry about getting a flight to his location. The IP address of the email traces to Brazil, and from the recent web searches of [www.southwest.com](http://www.southwest.com), we believe Perry took a flight to Brazil to meet up with Rick, which may be where they currently are.