Project 4 CIS 484-77

BENjamin BENOIT, MAXWELL JONES, SAVANAH KENNEDY, WILL GRISE

**Project Overview:**

The Louisville Metro Police Department has recovered a desktop PC on March 2, 2016 from a suspected drug dealer, Perry Winkler a few months ago. The desktop was found in the dumpster and was slightly damaged, but the hard drive was still intact. We are tasked to find the location of Perry Winkler and any evidence Perry Winkler tried to get rid of.

The questions we have been tasked to answer are:

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)?

Immediately after downloading the LMPD-436243-001.E01 image, we imported the image into FTK Imager and verified that the hash values matched to ensure image integrity so that nothing was lost or dropped during the image download. The computed and stored hash matched.

MD5 Computed Hash – 7817995d647a2ec34b39db1e5fc35771

MD5 Stored Verification Hash – 7817995d647a2ec34b39db1e5fc35771

The programs used for this analysis were FTK Imager, Autopsy, Arsenal Image Mounter, $I\_Parse, Registry Explorer, RegRipper, LECmd, JLECmd, PECmd, Excel for parsed data, Notepad, XML Notepad, Notepad++.

**Question 1**

Using FTK Imager you are able to see one of the user's name being Perry. This is found in the path 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.

The similar system was used to check to see if the user was on the system. The tool used for this part was Registry Explorer v1.5.1.1 where we looked at the different registry hives to see if Perry Winkler was a user on this computer. Looking at the Software Hive, the first thing we looked at in the Software Hive was the CurrentVersion at the path \Partition 2\[root]\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion and the stated RegisteredUser is Perry. Continuing with the Software Hive we looked at the path \Partition 2\[root]\Windows\System32\config\SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList\ you find a user named Perry with the same SID of S-1-5-21-3461440871-1589894493-1829873476-1000 as the user found in FTK Imager.

Lastly looking at the image in Autopsy and going to Results\Extracted Content\Operating System Information we can see the machine name is PERRYWINKLER-PC. This corresponds to the parsed information in the JLECmd and the LECmd files where the MachineID and Hostnames is also PERRYWINKLER-PC.

Lastly, we used RegRipper and pointed it to the SAM hive and saw that the user profile Perry was logged on 9 times and last logged in on Sun Feb 28 15:45:38 2016.

There are also documents signed from Perry.

**Question 2**

Using FTK Imager, we mounted the given hard drive image. We then explored the mounted image.

Yes, on Users/Perry/Pictures he has pictures of credit cards, drugs such as marijuana, and money that appears to be earned through selling drugs. Under /Users/Perry/Downloads folder he has downloaded an executable for Eraser 6.2.0.2970, which is used to delete files. This could mean that Perry is regularly deleting incriminating evidence. He also has downloaded a Tor Browser executable, which is sued to access the dark web. On /Users/Perry/Desktop there is a photo called “in my dreams.jpg” that is of a gun. Under Users/Perry/Documents there is a picture called 100\_6317 (Small).JPG that shows a Prego spaghetti sauce jar hidden in the base of a toilet. This hiding spot likely has incriminating evidence. Also, under /Users/Perry/Documents there is an Excel sheet titled “Book2.xlsx” which appears to be a “client list” that shows customers who buy drugs, the amount of money they owe, and their favorite drug. Under /Users/Perry/Documents there is a Word Document titled “Letter.rtf” that is a letter written by Perry Winkler to Rick Shoner. Winkler expresses worry that getting caught performing illegal activities and his plans to hide evidence such as “stuff in the kitchen and bedroom.” He asks Rick what to do about the computer. Under /Users/Perry/Documents there is a Word Document called “Letter3.rtf.” This letter is also to Rick Shoner and written by Perry Winkler. It mentions that Winkler bought prepaid credit card numbers shown to him from Shoner.

A Custom Destination jump list for Internet Explorer was generated using JLECmd. It showed that on 1/15/2016 21:10

**Question 3**

Taking some of the information from one of the analyses from an earlier question, when looking at the SOFTWARE Hive and looking at \Microsoft\Windows NT\CurrentVersion the system is running Windows 7 Professional where the installation date was 2016-01-15 21:06:55 Unix/Posix (32 bit). This was somewhat interesting because when looking through all the Web History in Autopsy there are two URL’s “ietld:hku.hk” and “ietld:jobs.cz” that says they were Accessed and Created on 2010-11-20 16:00:31 EST and they were Modified and Changed on 2016-01-15 16:07:09 EST which converted is the same time as the operating system installation date. There are a few other default files that have similar data. This may mean Perry Winkler did a fresh install of Windows 7 Professional to try to cover up some tracks beforehand.

Following the operating system install date, some of the surface level evidence can be found in \Users\Perry\Documents using Autopsy where there are two documents where one is titled “Letter.rtf” and the other is “Letter 3.rtf”. These documents are titled to Rick and are signed off by Perry. “Letter.rtf” was Created on 2/16/2016 22:04 and Last Modified on 2/27/2016 15:13 UTC and 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”

Here it seems Perry is beginning to get nervous because Perry believes “There onto us” and is asking Rick for help on what to do with the computer. “Letter 3.rtf” continues much of the same worry and is once again titled to Rick from Perry. “Letter 3.rtf” was Created on 2/16/2016 22:04 and Last Modified on 2/27/2016 15:13 UTC states:

“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"

Much like the first letter, we see that Perry is still worried. While doing some investigation on the image, one of the first things we saw was the $Recycle.Bin meaning there was some data that was sent to the recycling bin. We parsed the $Recycle.Bin with $I\_Parse and found there were six files that were indeed deleted. With this we were able to use the built-in File Carving in Autopsy and see the contents of the six files that were in the $Recycle.Bin found in Results\Extracted Content\Recycle Bin in Autopsy. Out of the six deleted files four were .jpg files where one was a vehicle, and the other three were weapons. The fifth item was a deleted contact of one Mary Reister, and lastly was a .rtf file which was the missing “Letter 2.rtf”. “Letter 2.rtf” was deleted on 02/28/2016 15:47:37 UTC. Its contents lead us further into what to look at next. “Letter 2.rtf” contents:

“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 off “Letter 2.rtf” it seems that Rick has supplied Perry with some instruction on how to “destroy” the computer and it has to do with the “task thing on the computer”. With this we decided to look programs that are scheduled to run. For this we look in the Software Registry Hive using Registry Explorer. Looking in the Software Registry HIVE and going to the path \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. Eraser.exe is a program used to delete information off of a hard drive by overwriting many times. This would be used to cover up the tracks of someone who is trying to hide something. Using PEDmd.exe and pointing it to \Windows\Prefetch of the image and filtering the .csv to look at Eraser.exe we were able to see that Eraser.exe was ran 5 times where the first time it was ran was on 2/21/2016 22:34 UTC and was last ran on 2/28/2016 15:47 which lines up with the Software Hive last run time. There is also documentation like a user guide on how to use Eraser which was found using Autopsy at \Views\File Types\By Extension\Documents\PDF\Eraser Documentation.pdf that was accessed on 2016-02-21 17:34:18 EST.

While continuing to shuffle through Autopsy, I stumbled upon Results\Extracted Content\Web Downloads and saw there was a .zip file for SDelete downloaded on 2016-02-17:46:40 EST. SDelete is another program that is used to delete files off the computer and is command line-based program. With it being a command line program, it would need to be ran in an executable type file. We than looked at executable files in Autopsy \View\File Types\By Extension Extension\Executables and saw in the .bat there was a “delete.bat” that was ran on 2016-02-24 17:49:31 EST where the text says “sdelete -qrsz c:\”. This is a batch file running sdelete.

While still in Autopsy we decided to investigate the Results\Extracted Content\Web Search. This showed several searches on the internet, many of these searches ranged from “how to get rid of computer evidence” to “sdelete” to “eraser”. Based on Autopsy and the time stamps it seems the searches started with “how to get rid of computer evidence” which was searched using Internet Explorer from [www.google.com](http://www.google.com) on 2016-02-16 22:14:51 EST and then continued on till sdelete was the last evidence scrubber searched with www.bing.com using Internet Explorer on 2016-02-24 22:45:36 EST

**Question 4**

Yes, according to the USBSTOR in the SYSTEM hive, there are two USB devices which have been attached the suspect’s computer. The two devices are a Kingston DT 101 G2 USB Device and a SanDisk Cruzer USB. According to LECmd, there are two image files of car1.jpg and car2.jpg which are stored on a removable device. These two images may show cars that could have been used in other illegal activities or which maybe stolen. Another image according to the LECmd is an image of Mike’s desk. The image showed what appears to be marijuana and a large roll of money. There also appears to be a computer in the background which may contain further evidence of criminal activity. This image appears to show a desk of an accomplice of Perry’s which may be involved in similar activities to Mr. Winkler. After evaluating the SYSTEM hive, located in \Windows\System32\config\ using Registry Explorer, the path G:\Windows\System32\config\SYSTEM: ControlSet002\Enum\USBSTOR\Disk&Ven\_SanDisk&Prod\_Cruzer&Rev\_1.20\20035001811625714CA7&0 showed that the SanDisk Device Serial number is 20035001811625714CA7&0. After evaluating the path G:\Windows\System32\config\SYSTEM: ControlSet002\Enum\USBSTOR\Disk&Ven\_Kingston&Prod\_DT\_101\_G2&Rev\_PMAP\0013729B678DEB20C51F0216&0 the Kingston Device Serial number was determined to be 0013729B678DEB20C51F0216&0. This allows us to identify that the Kingston drives name is Volume Label is Perry with a volume serial number of 3aa4c98b. By identifying the Kingston drive, we can infer that the Sandisk has the volume label of files and has a volume serial number of A0C9328E.

**Question 5**

Looking at TypedURL in the NTUSER.DAT Hive using Registry Explorer, the second most recent URL is http://southwest.com/

After finding a contact card using Autopsy looking at \Results\Extracted Content\Recent Documents for Rick Shoner and found the email associated to be rickyboy579@aol.com, we then used Autopsy again to find any emails associated with that email. We searched [rickyboy579@aol.com](mailto:rickyboy579@aol.com) at \Results\Keyword Hits\Email Addresses and found an email sent from [rickyboy579@aol.com](mailto:rickyboy579@aol.com) to [perrywin232k@aol.com](mailto:perrywin232k@aol.com) where the source file name is “f0252768.mbox” with an email title of “its time” with the contents of:

“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 first received IP address 186.210.54.196 associated with the email first came from Brazil. This has led us to suspect Perry Winkler may be traveling to Brazil to meet with Rick Shoner based on the email and the location of the IP address.

**Question 6**

Under /Users/Perry/Documents/emails there is a zip file titled “plan.zip” that is corrupted. After repairing the zip file using WinRAR the file is empty in of itself, but there is an associated plan.file-slack file which could be analyzed for possible retrieval of that data using hexeditor. Since this was outside of my knowledge area, I was unable to conduct analysis of this file. Additionally, there is a web history artifact discussing how to delete pornography off of a user's computer. Although this is speculative, a criminal using a device for pornography would not generally care about legal pornographic files being found. I also found the use of the TOR browser to be questionable. Another file ruleset.json had several strange references to pornography as well as things like girls, girl scouts. There is also a file within the TOR browser en-US.dlc which contains several pornographic words and terms. Additionally, there is evidence in the timeline portion of autopsy that shows a virtual machine being used alongside a USB device. This USB device was also being used within the virtual machine. There were also drivers for a virtual mouse. This can be a further resource of information. Evidence of Firefox and google chrome being used can also be found within this timeline, although there is no program data or program files that would normally be associated with these types of applications. There are many instances of alterations of dates of files, to time periods in the 1970’s as well alteration to the dates being past the 2060’s. These files may be of some interest. There is also evidence that the user of the device installed several plugins, NoScript and SSL everywhere being notable. The user of this device also utilized dropbox for exchanging of files. Though there are no transaction logs to analyze, there are update logs that may be of some interest. It would be safe to say that most of the activity conducted on this device utilized a combination of TOR, dropbox, and applications within the VMware utilized on this device. Two additional contacts were also found [mreister@gmail.com](mailto:mreister@gmail.com) for a Mary reister, and [spitzmeister@rocketmail.com](mailto:spitzmeister@rocketmail.com) for a Larry Spitz. There is also a collection of files which exhibit high entropy, usually indicative of cryptography being used. There are also several references to cryptography applications throughout the computer, specifically AES.

**Conclusion:**

Based off our findings from the hard drive obtained by LMDP, we believe that this device was in fact owned by Perry Winkler due to there being an account and the system name being PERRYWINKLER-PC. There was evidence of drugs related pictures and documents stating which person liked which drug on the hard drive. There is evidence that the computer may have had a fresh install of an OS as there are files that show an earlier date of creation, as well as there being actual deleted files that were able to be carved out. On top of this, there were also deletion executables such as SDelete and Eraser.exe ran several times to cover up tracks as well as letters from Perry to Rick thanking him on the instruction on how to use them. There were two USB drives that had contact with the system, one of which the volume label is named Perry. Based off a contact card for Rick Shoner we were able to trace the email address associated with the contact card to an email sent to Perry about getting a flight to his location. Based off some email header investigations we were able to find that the IP address traced back to Brazil. This maybe where they are, as the most recent TypedURL was for [www.southwest.com](http://www.southwest.com). Lastly, there were some other interesting files associated with the tor browsers downloaded, but they seem to contradict themselves as the evidence points to one topic and the actual contents point to obsolete things. There was a zip file titled “Plan.zip” but when opened it is blank. We do believe this hard drive was Perry Winkler and we believe his whereabouts are in or around Brazil, or that will be his whereabouts soon.