Baltazar, Trisia

Kellerman, Justin

Martinez, Maria

Smith, Ryan

November 28, 2018

CIS 484 Project 4

Group 6

**Digital Forensic Approach & Methodology**

In this case, we utilized the standard process followed when conducting a computer forensic investigation for law enforcement. Static acquisition and imaging of the recovered hard drive was completed and then authorized to us for examination. Our process of examination went as follows:

**Identification (1)**

Tool(s) Used: Registry Explorer, RegRipper, FTK Imager

Our first step was to verify that the hard drive belonged to the suspect, Perry Winkler. This was confirmed once we exported the system32/config folder, the users/Perry folder, and then used Registry Explorer to load all of the hives. In the SYSTEM hive, under ComputerName, we found that the computer name was “PERRYWINKLER-PC”. In the SOFTWARE hive, under CurrentVersion, we were able to determine that Perry was using a Windows 7 Professional Service Pack 1 and the registered owner is Perry. In the SAM hive, the username of an account was “Perry”, he was set as the administrator, and the password hint is “it’s your name, idiot”. The key associated with this account is “000003E8”. Also, it is the only non-built-in account on the system. Through RegRipper, we examined the SAM hive to search for more user information. The account was created on January 15, 2016 at 06:54. The last login date was Sunday, February 28, 2016. It is the default administrator user and the login count for this user is nine.

**Evidence Collection and Analysis (2)**

Tool(s) Used: Autopsy, FTKImager

Our next step was to thoroughly examine the hard drive, analyze the collected data, and comprise the most pertinent information to be presented. We found numerous images, applications, documents, and web history logs that provide evidence that Perry may be associated with drugs and other illegal activities. Using FTKImager, we first examined Partition 2. JPG image files of drugs, guns, and sports cars were discovered.

 root/users/Perry/Pictures:

There was also a picture of a contact named “rick”. Everything within this folder is from 1/26/2016.

“da stuff”

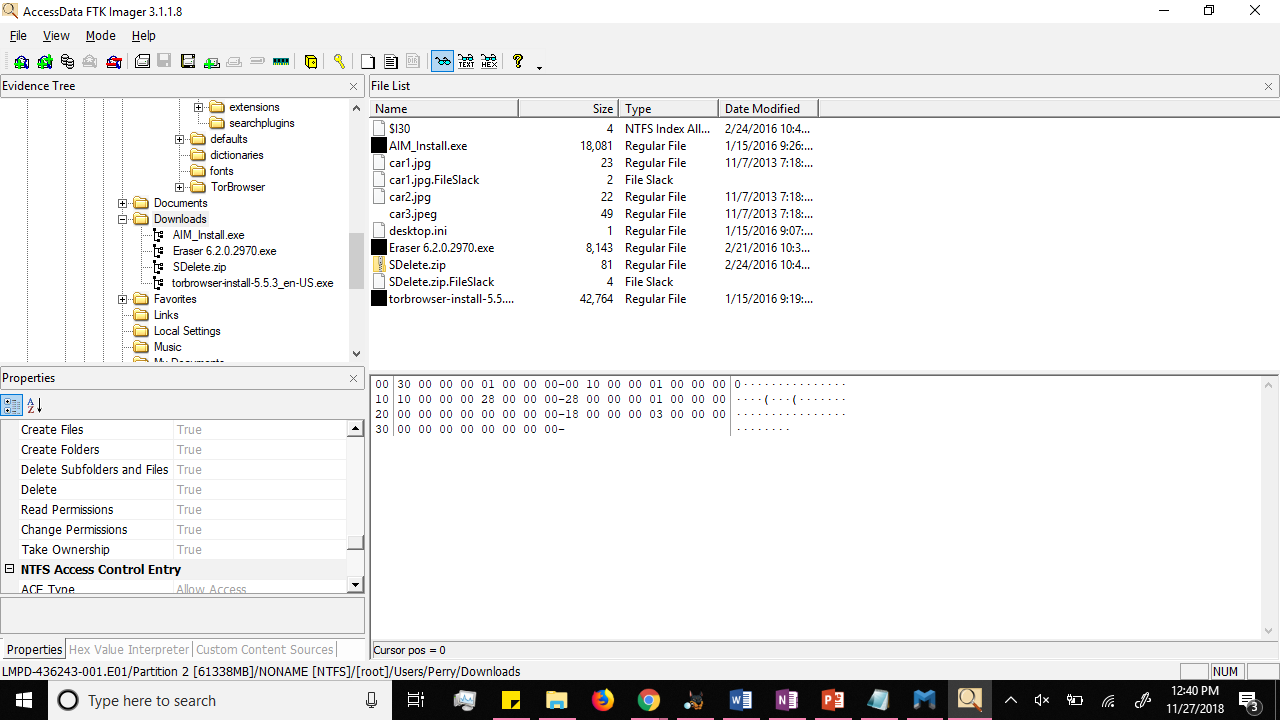
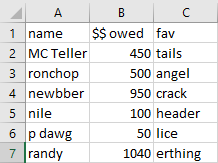
“mike’s desk”

In root/users/Perry/Downloads there are 3 JPG image files of cars, two of which are broken down in “car1” and “car2” and a small red car in “car3”. In root/users/Perry/Desktop there is a JPG image file of a golden gun titled “in my dreams” and a sports car named “the one.”

In root/users/Perry/Documents, there is a picture of a toilet’s open tank with a Prego Sauce jar dated 05/05/2007. Which we can assume hides either more marijuana or money. There is also an image of stacks of $100 bills and coins named “need mo”. In root/Recycle .Bin/ S-1-5-21-3461440871-1589894493-1829873476-1000, we found pictures that Perry attempted to delete. Here, there are pictures of guns in files “$RMMADTL”, “$ROECCL3”, and “$RJRJMDV0” and a sports car in “$R844694I”. The image of the toilet tank with the Prego jar may also give clues as to how Perry hides these drugs. These pictures indicate that Perry is involved with drugs and is a dangerous suspect as he may likely be armed. He also has access to varying transportation through the images of broken down cars meaning that he is on the move and may be difficult to track down.

“100\_6317(Small)”

**Evidence Deletion and Plan(3+5)**

Within the directory, we also found that Perry downloaded three suspcisous applications: Tor web browser, Eraser 6.2.0.2970, and SDelete. Tor is known by many as a tool to access the “dark web” and can be used to conceal user activity information and hides your physical location. Under Tor, there is an extension of HTTPS-Everywhere which encrypts your online activity. Eraser is an advanced security tool for windows which allows you to completely remove sensitive data from your hard drive by overwriting it. SDelete is a command line utility that “allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk”. [1] There are also a few documents found on the PC. There are 3 letters addressed to a person of interest Rick Shoner. Perry has a total of 4 contacts, Rick Shoner is the only one located in his Documents folder and the only person he seems to be communicating with the most. The letters were found by conducting a LNK file analysis on the recent files for user Perry. Using LECmd, we found two out of three letters that were sent to Rick. The first letter is an RTF file named “Letter”. It was created on 2/16/2016 and was last accessed on 2/17/2017. It is also found under Perry’s Documents folder in FTKImager. The second letter, “letter2.lnk”, was not in the Documents folder with the others. Assuming it was deleted, we used FTKImager and went in root/Recycle .Bin/ S-1-5-21-3461440871-1589894493-1829873476-1000 and found one RTF file,“$RSU8VAG”, from 2/21/2016. Its date fits between the dates that “Letter” and “Letter3” were made. The third letter is an RTF file as well and was created on 2/27/2016. It was last accessed on 2/27/2016. These letters confirm that they are trying to hide information and/or actions taken. The purchase of prepaid credit cards was most likely done to avoid being traced by transactions. The “stuff” Perry may be indicating is marijuana, based on the images found in the hard drive, because they are trying to get rid of something in the kitchen and the bedroom. Another document that is of interest is under root/users/Perry/Documents there is an XLSX file. This seems to keep track of transactions, more specifically money owed by each person and the type of drug they purchased.

“Letter”

*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*

*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*

“$RSU8VAG”

*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*

“Letter3”

“Book2”

As shown, it is very clear evidence that Perry has been actively trying to hide or delete incriminating evidence from his computer. We see more attempts of him trying to hide his illegal activity in his web history. Using Autposy under Results/Extracted Content/Web Search, we see multiple Bing and Google searches that showcase his attempts to hide any evidence. He searches for “how to get rid of (computer) evidence, “how to set up scheduled task,” “get rid of files,” “eraser,” “sdelete,” and “evidence eliminator.” Here he looks up the two applications he downloaded, Eraser and SDelete. We also see that he is looking up instructions on how to set up scheduled tasks.

Perry did create a scheduled task named “delete”. This task would execute “C:\Windows\SDelete\delete.bat” when there was a failed logon to the system.

The web history also shows that Perry visited southwest.com, an airline site. He accessed this site on 2/24/2016, around the dates that the letter was sent. This further supports all evidence presented so far; Perry and Rick are accomplices who have made plans to go on the run. This information gives a potential lead to the LMPD force, since they could look into flights around this date and get more information from his passport or potentially request to look into CCTV at plausible airlines. With FTKImager, under root/Users/Perry/Documents, we see a folder labeled “nice.” In this folder are two image files, “fjireskfes.bmp” and “Iguazu-falls.jpg”. Iguazu Falls is located in South America in Misiones Province, Argentina. This could point to a possible location that Perry will go to. After working through Partition 2, we next decided to examine the unallocated space on the hard drive and also successfully carved the main hard drive. Using the prefetch files and PECmd we were able to determine:

Ran TOR.exe and Torbrowser-install.exe 1?15/@016 21:20. This shows that he did install a Tor browser.

Used a program called Eraser.exe ran it 5 times. Eraser is a program that deletes sensitive information completely. This shows the Perry has deleted files using an Eraser program.

Has used Dropbox so there is potential evidence stored in the cloud. Dropboxupdate.exe has been run 14 times.

He uses Firefox and explorer browsers.

Wordpad.exe was ran 6 times on 2/27/2016 15:13.

Has used AOL-messaging 1/15/2016 21:26. And used AOL install messenger. Last run at 1/15/2016 21:27

Rick Shoner is one of Perry’s contacts and Rick uses an aol account and evidence shows that Perry download AOL messaging.

Received: from mta.email.aol.com (mta.email.aol.com [74.124.68.45])

by mtain-mf01.r1000.mx.aol.com (Partner Internet Inbound) with ESMTP id DA9533800046A

for <perrywin232k@aol.com>; Sun, 28 Feb 2016 09:08:15 -0500 (EST)

Received: from [186.210.54.196] ([186.210.54.196:2269] helo=THDMMTA25PUMP3)

by pc1udsmta1n25 (envelope-from <rickyboy579@aol.com>)

(ecelerity 2.2.2.45 r(34222M)) with ESMTP

id 57/7A-18696-E5614725; Sun, 28 Feb 2016 07:07:14 -0300

Date: Sun, 28 Feb 2016 09:08:16 -0500 (EST)

Message-Id: <Kilauea216670-69235-1739513301-2-1024@flonetwork.com>

From: "P Dawg" <rickyboy579@aol.com>

Reply-To: "Rick Shoner" <rickyboy579@aol.com>

To: perrywin232k@aol.com

Subject: it's time

MIME-Version: 1.0

Content-Type: text/plain; charset=us-ascii

Content-Transfer-Encoding: 7bit

X-From: Rick Shoner

X-To: Perry Winkler

I 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.

Next we used Arsenal to mount the image and used Photorec to file carve. Within the “unallocated space” there were two folders. The following data was found in unallocated space/00000048/:

This recovered email found in unallocated space/0000048 confirms that Perry is going to attempt to travel by plane. It also allows us to infer that either Rick has already flown on Southwest Airlines, or that the two of them plan to use that airline once they meet up. Additional evidence recovered in unallocated space is a map of South America, which supports our earlier suggestion that Rick and Perry may be going there.

From searching “how to get rid of a computer hacker” to using websites like Anonymouse, which allows anonymous emails to be made, there is an abundance of evidence showing that he was trying to hide his illegal activities.

**Additional Devices (4)**

Tool(s) Used : Registry Explorer, Autopsy, LECmd

There are a couple additional items that may contain pertinent evidence. In the System hive under USBSTOR there were at least two physical devices connected to the machine. One Kingston DT 101 G2 USB with an SID of “0013729B678DEB20C51F0216&0”. One SanDisk Cruzer USB Device with an SID of “20035001811625714CA7&0”. Autopsy verified these connections.

LNK File analysis using LECmd shows that files were accessed from two removable devices. “mike’s desk.jpg” was accessed from a device with volume serial number “A0C9328E”. “car1.jpg” and “car2.jpg” were accessed from a device with volume serial number “3AA4C98B”. These volume serial numbers could be linked to the actual devices if the EMDMGmt key was present in the Software hive. The files accessed were all saved locally to Perry’s computer.

**Additional Evidence Collection and Analysis (6)**

Tool(s) Used: Autopsy, FTK Imager

We found additional data that could further aid the investigation. Starting with Partition 2. There appears to be a picture that can be associated with Rick in root/users/Perry/Picutres named “Rick.jpg”. Rick Shoner is not the only contact Perry had on his hard drive. Using FTKImager, under root/users/Perry/Contacts, we find three contacts (including Rick and Perry).Here we find Larry Spitz with the email of [spitzmeister@rocketmail.com](mailto:spitzmeister@rocketmail.com). Rick’s email is [rickyboy579@aol.com](mailto:rickyboy579@aol.com) and a nickname of “master rick.” Larry could also be a possible accomplice and possible travel partner for Perry. Another contact found in root/Recycle .Bin/244-S-1-5-21-3461440871-1589894493-1829873476-1000 under file “$NDKRDO.contact” with the information of Mary Reister. Also, under his Documents folder, there is an “email” folder that contains a zip file called “plan.” This could be the instructions and email that Perry was referring to in his letters to Rick. The file was also modified on 2/28/2017, the day after Letter, which was created and accessed on 2/28/2017. We are unable to uncover what is in this file We also found evidence that suggests he was involved with illegal activity beyond drugs. In the unallocated space we found searches for the following: “how to steal tax refund”, “how to know if you’re being watched by the cops” and articles about identity theft. We were also able to confirm a Virginia location for Perry and found an image file of a Virginia driver’s license that could be his.

Being able to identify characteristics, hobbies, etc. could be useful in the investigation. Perry seems to like cats as we find multiple cat pictures in root/users/Perry/.Pictures. He also downloaded Big Air War from gametop.com and we saw this using Autopsy under Users/Perry/Desktop. He also is very interested in crime and may have even been “inspired” by this interest to pursue more illegal activities. Additional data collected showed that he was interested in the stand out case about Natalee Holloway. Where a young woman’s suspected killer fled to South America and an impactful part of his trial included digital forensics. He was also interested in an article about a man who was charged for attempting to financially support ISIS. We confirmed these interested based upon web history and image files that we reversed image searched on Google. He was subscribed to news magazines (found subscription was USA Today) and even shared an article from CNBC about Identity Theft Refunds and Social Security, furthering supporting the previously mentioned data about taxes and refunds. There were also other web logs showing his search for personal related aspects of his life such as how to stop being single, Tinder, acne and other body issues. Based on drug dealing affiliation, emails/web activity expressing unhappiness, a special interest in true crime, and an equally eager friend, it could be concluded that and a desire for a lavish lifestyle through multiple illegal means is what Perry Winkler is trying to accomplish.

# Works Cited

|  |  |
| --- | --- |
| [1] | M. Russinovich, "https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete," 13 February 2018. [Online]. [Accessed 25 November 2018]. |