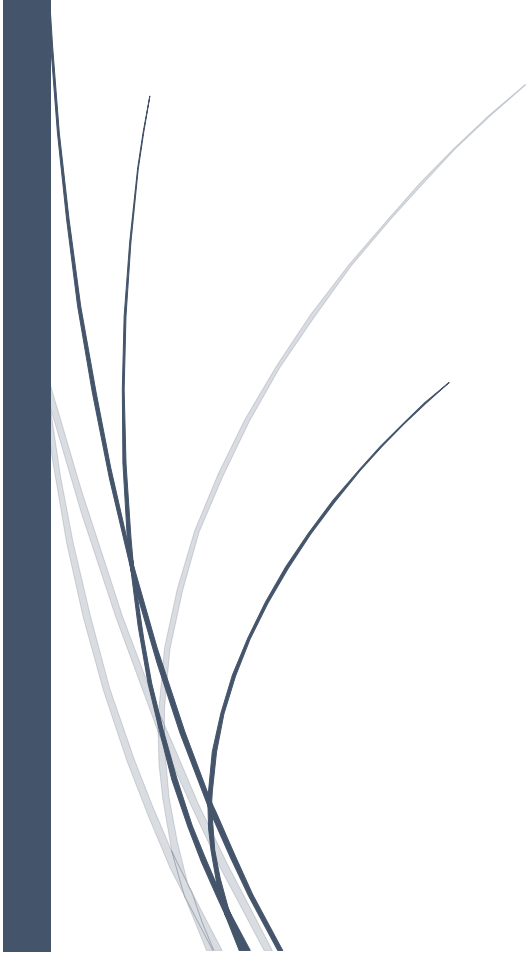
4/18/2016

CIS 484 Project 4

Paige Fenwick
Daniel McGrath
Joseph Meyer
Michael Moser



Introduction

As a team of forensic investigators, we have been tasked with analyzing the found hard drive of a known suspect in a police investigation. The suspect, Perry Winkler, tried to destroy the found hard drive which has lead us to believe there may be useful information to his whereabouts and his actions. Before investigating the hard drive, we verified the image using FTK Imager. Using a variety of forensic tools, including Autopsy 4.0.0, FTK Imager, WinHex, Recycle Bin Parser and more, we compiled documentation about the presumed past and future plans of Mr. Winkler. The following documentation will cover the found device information, any illegal findings, such as images of illegal activities, internet and browser history, any external devices that were added to the device, and any future plans that Mr. Winkler had that will help us lead to his discovery. Finally, we will document any additional findings and offer a summary of our inferences based on these findings.

1. What identifying information did you find on the hard drive to help determine the owner or user of the computer?

To be able to determine the owner of the computer we used FTK Imager to extract the SAM hive under “Partition 2\NONAME [NFTS]\root\Windows\System32\Config”. From there, we used RegRipper to look for system information. By looking in the SAM Hive Registry we found information related to computer name as well as the TCP/IP Hostname. The picture below shows a screenshot of what we found.

```
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = PERRYWINKLER-PC
TCP/IP Hostname = PERRYWINKLER-PC
----------------------------------------
```

After looking into the SAM Hive we looked at the Software Hive to validate the registered owner of the computer. The Software Hive was also found under "Partition 2\NONAME [NFTS]\root\Windows\System32\Config". By looking at it, we found the registered owner to be Perry as shown by the screenshot below.

```
RegisteredOrganization :
CurrentVersion : 6.1
CurrentBuild : 7601
CurrentBuildNumber : 7601
CSDBuildNumber : 1130
RegisteredOwner : Perry
SoftwareType : System
InstallationType : Client
SystemRoot : C:\Windows
PathName : C:\Windows
EditionID : Professional
CSDVersion : Service Pack 1
CurrentType : Multiprocessor Free
ProductName : Windows 7 Professional
ProductId : 00371-177-0000061-85507
```

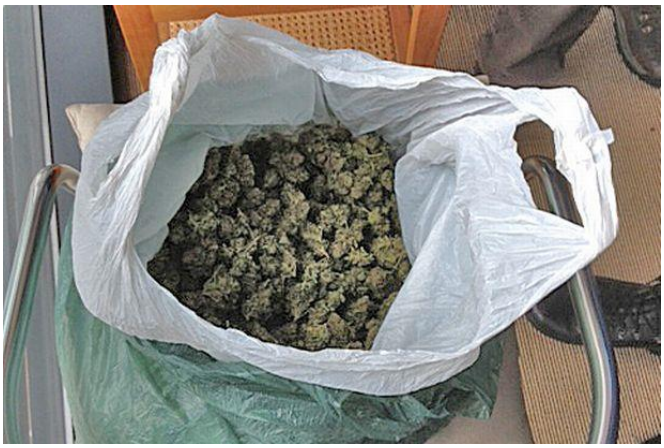
Last but not least we checked the Software Hive again for the name of the user on the C:\ drive. As you can see below, Perry's name as well as his SID were discovered.

```
Path      : C:\Users\Perry
SID       : S-1-5-21-3461440871-1589894493-1829873476-1000
```

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

We found a lot of evidence from the computer that talked about drugs and illegal activities. We looked under Perry's pictures and documents folders for personal information

related to the case. There are two pictures that can unmistakably be considered as “illegal activities.” The first one is a picture of Weed/Marijuana titled “da stuff.jpg.” This particular file was found under Perry’s picture folder using FTK imager.



The second is a picture of Weed/Marijuana with several bundles of money titled “mike’s desk.jpg.” This particular file was also found under Perry’s picture folder using FTK imager.

As there are only 4 states in the U.S. that allow the use of recreational weed and even then, only to a certain amount, it is easy to determine that these pictures may deal with illegal activities. Also, the fact that there is a bundle of money right next to the weed may mean that there is drug trading going on.

Additionally, we also found an excel file under Perry's documents folder which contained a list of people he owes money to, including an entry for $950 for "crack." Now, owing people money is not illegal… but owing people money for "crack" is most certainly illegal since Crack Cocaine is considered very illegal and dangerous. Lastly, we found a picture of a toilet tank with the lid off showing the inside. This could mean absolutely nothing, however it could also be used as a hiding place for drugs and other illegal items. The following picture was found in Perry's documents folder using Autopsy.

We also found a carved image file (under Views > File Types > Images) of some sort of homemade 'bomb' using Autopsy. We looked in carved files since they pertain evidence that was once on the computer. Since bombs are usually associated with danger or illegal activities, we can comfortably say that whoever was involved in making it was most likely up to no good.

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

There is a fair share of evidence both that Perry was trying to cover and his tracks and delete evidence from the found device. In terms of covering his tracks, a variety of web searches were found in Autopsy 4.0.0. Some of the most prevalent web searches that Perry performed were through Bing between the dates of 2/21/2016 and 2/24/2016. The first search was looking for the Eraser program. Eraser is a tool used to erase files stored on the hard drive. About 30 minutes after this search, the Eraser software was downloaded to the Perry user account on this image. On this same day, Perry ran a search regarding CCleaner and navigated to a website called magnetforensics.com. He accessed an article called 'Oh No, the Suspect Ran CCleaner to get Rid of the Evidence'. Shortly afterwards, Perry downloaded CCleaner to his device. A few days later on 2/24/2016, Perry performed another Bing search for 'how to set up a schedule task'. Scheduled task in windows can be created for every log on or every log off on a machine. This can either open a program or even empty the recycle bin upon the completion of one of these tasks. On the same night, Perry also searched for 'what is a batch file'. A batch file, when ran in the command line, will execute a series of tasks that is set in the file by the user. These tasks can include deleting files, running a program, such as Eraser or CCleaner, or other variety of tools available to the user. All of the above web searches were found using Autopsy under the following path: results>extracted content>web searches.

In addition to the above web history searches, Perry downloaded a variety of evidence hiding tools, including Eraser, Evidence Eliminator and CCleaner. All of these tools can be used to delete files from a system and/or clean out browser history. The above programs were found in Autopsy under results>extracted content>installed programs. Having already touched on

Eraser and CCleaner, Evidence Eliminator goes one step further by deleting hidden information from a user's hard drive that would not normally be removed.

To further prove what Perry did Autopsy prefetch files show that Perry executed Eraser software on 2/28/2016 at 10:49:30 EST. Prefetch files were found under Data Sources\LMPD-436243-001.EO1\vol_vol3\Windows\Prefetch. Worth noting, 2/28/2016 is the last day any prefetch file was executed which shows that this the last time Perry was on the computer. To go along with that, images that were file carved showed snippets of the Eraser and CCleaner software, which could point to how Perry did not want other people to know he was using them. Last but not least another carved image file showed someone on the computer went to www.vanish.org. With Eraser, CCleaner, and Evidence Eliminator already being mentioned, we believe this was yet again another way to cover his tracks.

A few other carved files that were found that pertain to covering his tracks include pictures of Anonymouse, Tor Browser, and a Wikipedia page for anonymous remailers. Anonymouse is used to keep your IP address anonymous while Tor Browser blocks all information associated with internet activity. Lastly, Anonymous remailers act in a way to block the data associated with email messages. There is no hard proof to say if Perry actually used any of these aforementioned things, but it is highly possible he did. And worth noting, because these are all carved files, no additional metadata can be found from the data.

After noting how Perry tried to cover his tracks, our discussion turns to deleted files. By using FTK Imager all recycling bin files were found by extracting the files (root\Recycle Bin) and placing upon my own computer's desktop. From there we used Recycle Bin Parser on the $I files. By doing this, we found a few questionable pictures, a specific contact, and a letter. Three of the pictures we found were of guns, while one was of a car. Each picture was originally on the

desktop of Perry's computer (C:\Users\Perry\Desktop) before he sent them to the recycling bin. The files associated with guns were "th.jpg", "thCAV3V9F6.jpg", and "awesome.jpg". th.jpg was deleted on 2/21/2016 at 18:25:18 EST, thCAV3V9F6.jpg was deleted on 2/21/2016 at 18:21:53 EST, and "awesome.jpg" was deleted on 2/21/2016 at 18:21:46 EST. The last picture, the car, was titled "WOW.jpg" and it was deleted on 2/21/2016 at 18:21:41 EST.

We also found a contact, Mary Reister (mreister@gmail.com), who was previously stored under C:\Users\Perry\Contacts but had since been sent to the recycling bin. The name of the file was simply "Mary Reister.contact". This contact was deleted on 2/24/2016 at 18:44:32 EST. Last but not least we found a letter dealing with deleting computer files with the path and name of C:\Users\Perry\Documents\Letter2.rtf. This letter was deleted on 2/28/2016 at 11:47:37 EST.

To further validate even more that Perry was trying to cover his tracks, lnk files and jumplists need to be explored. Lnk files were found in Autopsy under Results > Extracted Content > Recent. As the last noteworthy file that was sent to the recycle bin was on 2/24, I figured any files around that date would be beneficial to our evidence.

The first noteworthy file was "th.link", which was a picture of gun in recycling bin. While it was deleted on 2/21/2016 at 18:25:18 EST, it was initially accessed on 1/26/2016 at 16:51:31 EST. The next noteworthy file was "awesome.lnk", which was also one of the gun pictures mentioned before in the recycling bin. After already figuring out that the file was sent to the recycling bin from Perry's desktop on 2/21/2016 at 18:21:46 EST, this file was recently accessed on 1/26/2016 at 16:51:53 EST. The following are additional lnk files found:

-**"inmydreams"** - Picture of gold gun found on desktop - Could be a gun Perry might have wanted to buy if he had the money - Accessed on 1/26/2016 at 16:52:03 EST

-**”the one.lnk”** - Picture of exotic sports car found on desktop - Could be something Perry wanted to buy if he had the money - Accessed on 1/26/2016 at 16:52:23 EST

-**”wow.lnk”** - Picture of car found in recycling bin - Could be something Perry wanted to buy if he had the money (Why Recyling Bin?) - Accessed on 1/26/2016 at 16:52:32 EST

-**”mike’s desk.lnk”** - Picture of drugs and money found on E:\ drive (and Perry’s Pictures folder) - Shows illegal activity - Accessed on 1/26/2016 at 16:54:04 EST

-**”letter.lnk”** - Email note - Definitely shows trying to get rid of evidence - Accessed on 2/16/2016 at 17:04:56 EST

> “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.\par
> “Signed,\par
> “Perry\par”

-**”sDelete.lnk”** - Zip file in downloads folder - Believe it deals with deleting information off of the computer - Accessed on 2/24/2016 at 17:46:40 EST

-**”letter2.rtf.lnk”** Rich text file found in recycling bin (originally in documents folder) - Shows compatibility with other versions of Word and having Rick as a partner in the destruction of computer evidence - Accessed on 2/24/2016 at 17:51:14 EST

> 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

-**”letter.rtf.lnk”** - Same file as mentioned before, just in rich text format - Accessed on 2/27/2016 at 10:13:30 EST

-**"letter3.rft.lnk"** - Email file found in documents folder - Shows a possible escape plan to not get caught - Accessed on 2/27/2016 at 10:13:43 EST

> "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.\par
> "Sincerely,\par
> "Perry\par"

-**"System and Security.lnk"** - Interesting that is the last file accessed on recent documents section - Accessed on 2/27/2016 at 10:24:24 EST

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.

Various connected devices were found on the image file by looking at the Results > Extracted Content > Devices Attached section of Autopsy. A USB device that may contain pertinent evidence was the E:\ drive on the machine. By extracting the files from Autopsy, we found that this drive was once associated with Perry's USB Drive (friendly name was 'Perry'). By looking the SYSTEM and SOFTWARE Hives on RegRipper, we came across some data associated with the E:\ drive (such as friendly name). Worth noting, the SYSTEM and SOFTWARE hives were found under specific locations. The SYSTEM Hive was found under the path of SYSTEM\ControlSet001\Enum\USBStor. The SOFTWARE Hive was found under SOFTWARE\Microsoft\WindowsNT\CurrentVersion\EMDMgmt.

In terms of the actual drive, Autopsy showed that the maker of the device is Toshiba Corporation and the device model is Kingston DataTraveler 102 Flash Drive / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick. Also, the device ID is 0013729B678DEB20C51F0216. By then using the SAM and SOFTWARE hives, we found out additional information about the

drive. For instance, the InstallDate of the drive was on 2/16/2016 at 18:03:17 EST while the Device Parameters LastWrite time is 2/28/2016 at 11:46:06 EST.

Another connected device was a SanDisk Corporation Cruzer USB drive that also took up the E:\ on the computer. This connected device had a friendly name of 'files'. The device ID is 20035001811625714CA7. By using the SAM and SOFTWARE hives, we found out additional information about the drive. For instance, the InstallDate and Device Parameters Last Write times of the drive was on 1/26/2016 at 17:48:11 EST. Lastly, other connected devices included a VMware Virtual USB Hub and three Virtual Mice.

Some files that I know were on either one of the drives include "car2.lnk", "car1.lnk", and "mike's desk.lnk". These were all found in the Recent section of the imaged file in Autopsy. While I am not sure what the car lnk files showed, we believe they were simply images of automobiles. I do know though that "mike's desk.lnk" relates to an image of drugs and money. This shows that a USB drive was used for illegal activities in this investigation. And while all of these files were simply shown to be on the E:\ drive, we can presume they were on Perry's USB rather than the Files' USB device. This is because of the more recent LastWrite time.

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 him? If so, can you determine the identity of the accomplice?

Beginning on 2/24/2016, Perry starting searching for southwest.com and visiting its website. This was all found using Autopsy under the results>extracted content>web searches. Perry was visiting this site often but there was no evidence of any purchase. There were also several temporary internet files which had to do with Southwest Airlines such as "Southwest Cargo" and "Southwest Corporate Travel."

Additionally, there were multiple email correspondences with Rick Shoner that indicated that Perry was trying to leave. This could indicate that Rick Shoner was Perry Winkler's accomplice as they communicated quite frequently. The first email found, which was mentioned in a previous section of this documentation, stated that Perry "couldn't wait to ditch this place!". With the way that the email is structured, it seems as if Perry and Rick will be ditching together since Rick is 'waiting' on instructions from Perry. Additionally, Rick sent an email to Perry stating he was waiting at the hotel and that Perry should hide the evidence and meet him there. This email was found using Autopsy in the unallocated files. And upon further review of the email and file metadata, we found the IP address of the computer the email was sent on. This IP address was associated with Brazil which means Rick was in Brazil when he sent the email to Perry. Shortly afterwards, Perry performed one last prefetch file on his hard drive and no other data was found after this interaction. Finally, on Perry's user account under his Documents folder, he had a folder called emails. Upon looking into the folder, Perry had a "plan.zip file" but when trying to extract the file, the file was labeled as empty and could not be extracted. From the naming convention and the placement of the folder, it seems that Perry was keeping his emails stored here and was 'planning' to do something, which could have been to leave the area.

The only other evidence that could potentially point to where Perry and Rick might be traveling can be found by once again looking at carved files and then orphan files. After mentioning carved files before, orphan files rather are found under Views > Deleted Files > File System. In these files that have since have had all metadata deleted, partial remnants of certain files exist. Such files that may help out in this investigation include an orphan file-name related to passports ("Passport[1].html"), a carved image file of a beach and someone fishing ("f112840.png"), and an orphan file showing a hotel ("polaroid_2_aud1_hotels_160315[1].jpg").

Our best guess here is that Perry and Rick might be traveling to a different country while planning on spending the rest of their lives in paradise.

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)?

After a full overview of the found device, there are additionally items of interest that should be noted to law enforcement. First, with the web browsing history, Winkler visited dropbox multiple times throughout the year. We discovered he visited Dropbox.com multiple times through the dates of 2/20/2016 - 2/25/2016 (and atomically? ran DropboxUninstaller on 3/11 – shown under Views > Deleted Files > File System). This is of interest because during this same time, he was searching the web and downloading programs such as Eraser, Evidence Eliminator, CCleaner and other programs to potentially hide evidence. Searching his dropbox account could provide other useful information. This was found under extracted content>web history>web searches in Autopsy. Also we found emails using Autopsy that references “Sending anonymous emails” which can be correlated with doing something suspicious.

The aforementioned zip file named “plan.zip” is another file of interest as it seems suspicious, especially since we as junior forensic detectives could never get it to open nor find a program to repair the archive. We tried to a little digging but we did not see any additional file streams in WinHex. This may be worth noting because something may be hidden within this zip file which could help LMPD with its investigation.

The last thing that could point to an additional lead in the case pertains to the contact file that was found in the recycling bin. Having touched on this before, this contact’s name is Mary Reister. Her name did not come up in regards to anything else in this investigation, but as her

contact information was sent to the recycling bin for some reason, she may be able to provide useful information related to the case.

Conclusion

After careful examination of the found device, we have concluded that Perry Winkler was involved with illegal activities and is more than likely on the run from the police force. After looking through his emails, deleted files, web history and other various documents, we found a variety of images, messages between Perry and his accomplice Rick Shoner, and programs used to clean the hard drive that all point to Winkler being a drug dealer of some sort. If we had to guess, it looks as if the computer was discarded by Perry Winkler into the dumpster outside the residence on the night of 2/28. Thus, Perry has most likely been on the run since trying to meet up with Rick in Brazil. Once again, all of the above information was gathered using forensic tools such as Autopsy 4.0.0, WinHex, FTK Imager and a few other variety of tools.