Tyler Cole, Vince Patrick, Bharadwaj Jagatheesan, Volody Bestiyanets

CIS 484 - Project 4 Report

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?**

There are several pieces of evidence that provide us with insight as to who the owner/user of this computer is. There is a username called “Perry” in the windows installation on the second partition of the disk. The machine name, as denoted in the ComputerName key in the SYSTEM registry hive, of the computer is “PERRYWINKLER-PC.” “Perry” is also listed as the default user name in the Winlogon key of SOFTWARE hive of the registry. All of these pieces of evidence suggest that the owner or user of this machine was Perry Winkler.

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

There are three pictures of firearms and a picture of a car located in the Recycle Bin for the Perry user account. It also appears, as revealed in Autopsy’s examination of the web searches made on the machine, as though he searched in the address bar of his browser for “how to skim credit cards”. There is another picture called “in my dreams.jpg” on Perry’s Desktop, which is a picture of a firearm as well. This is complemented by the “the one.jpg” file that is a picture of a sports car. Additionally, there is a file in the Perry user account’s Documents folder called “need mo.jpg”, which is an image of a large quantity of money. While these images are not directly related to illegal activity, they could serve as condemning when combined with other images and evidence, such as images of drugs. For example, it is a felony to possess drugs and guns in many states, and so this information could be useful later on.

There is a picture, located in the Perry user account’s Pictures folder, labeled cc.jpg, which is an image of credit cards, as well as an image labeled da stuff.jpg in the same folder, which is a picture of what appears to be a bag containing marijuana. The mike’s desk.jpg file

located in the same folder, has is another image of what appears to be marijuana accompanied by a large amount of money. In the Documents folder of the Perry User account there is a file labeled Book2.xlsx. It is a spreadsheet with what appears to be customers, their respective money owed, and drug preference of choice.

	A	B	C
1	name	$$ owed	fav
2	MC Teller	450	tails
3	ronchop	500	angel
4	newbber	950	crack
5	nile	100	header
6	p dawg	50	lice
7	randy	1040	erthing

Additionally this message was found in the Perry account's Document folder in a file called Letter3.rtf, indicating potential purchasing of stolen credit cards:

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

All of these items of evidence either directly proves or tangentially supports the notion that Perry, and potentially others, are engaged in illegal activity. Additional incriminating evidence is discussed later on in this report, such as the user deleting evidence and trying to cover their tracks, and evidence that the user and potential accomplices are going on the run.

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

There is a Tor Browser LNK file which could mean that Perry is attempting to cover up his tracks by using a browser that runs communications through a network of relays around the globe. There is also evidence from LNK files that a program called sdelete which, allows the

user to securely delete files, has been run on the machine. In the AppData folder, there is data for a program called Eraser 6 that removes sensitive data from the hard drive by overriding it several times, and evidence of it being ran is corroborated in LNK, JMP, and Prefetch files. Additionally, in the Run key in the SOFTWARE hive, it shows that at restart, the Eraser.exe program is set run, which indicates that the suspect is attempting to erase evidence at startup. Additionally, Dropbox is also being run at startup, and Dropbox could be used to transfer important evidence to the cloud and other machines.

The USBStor registry key in the SYSTEM hive lists some devices, but they all have DeviceHackFlags set instead of the standard information stored there, which is an indication of a potential virus, or that the user (or something else) attempted to write-block the connected devices, potentially in an attempt to hide information about the connected USB devices. The Tor Browser, as revealed by examining prefetch files, was run a single time, perhaps to do some encrypted browsing of sensitive webpages. It was last ran at 1/15/2016 9:20:41 PM. According to the corresponding prefetch file, ERASER.EXE was ran 5 times, indicating that it was potentially used to securely delete sensitive information. It was last ran at 2/28/2016 3:47:04 PM. Additionally, according to Autopsy analysis, Eraser shows up as an installed program on the system and it was installed on 2/21/2016 5:34:22.

In Perry\Documents there is a file labeled Letter.rtf which contains this content:

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 indicates that the suspect might have destroyed certain incriminating evidence. Additionally, in the web history for the Perry User account, there are several searches indicating that whoever was using the machine was attempting to cover their tracks, searching for things

like “how to get rid of evidence”, “get rid of files”, “sdelete”, “how to get rid of computer evidence”, “evidence eliminator”. There are other suspicious searches such as “how to batch script”, “what is a batch file”, and “how to set up scheduled task”. These searches were found in a combination of looking at the TypedURLS key of the NTUSER.dat hive and looking through the web searches and web history section of the Autopsy report of the forensic image. There are other searches such as “remove traces activity computer” and “hide evidence on a computer” which support the idea that the user was trying to cover their tracks.

There is also evidence, in Autopsy web searches and history, of the downloaded SDelete.zip from download.sysinternals.com/files/SDelete.zip, helping to corroborate evidence of that software’s use. Additionally revealed from the web searches and history, there is evidence that the user was looking up batch file scripting, accessing answers to questions such as “whats the best way to get rid of all evidence on my computer” on the question site Quora, and “how remove traces activity computer” on the tutorial site eHow. There is also evidence in Autopsy web searches and history of the suspect downloading Tor, Eraser, another wiping program called Evidence Eliminator, as well as Dropbox. Again, Dropbox could have been used to upload and transfer sensitive files. The user was also browsing forensics forums, trying to deal with issues such as suspects running CCleaner to hide evidence at www.magnetforensics.com/computer-forensics/oh-no-the-suspect-ran-ccleaner-to-get-rid-of-the-evidence/&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwj88Ky1hsvLAhVosoMKHamBDv8QFgghMAI&usg=AFQjCNEQOdDKK5wb8hbWq5iGae3eGIKhqQ.

It also appears the user had the allin1convert toolbar installed, which is a known browser-jacking piece of malware.

When examining the scheduled tasks located at Windows\System32\Tasks on the machine, one labeled “delete” is present. It runs a batch file called delete.bat located in C:\Windows\SDelete. The author of the task is PERRYWINKLER-PC\Perry, and it is enabled to fire on windows Event ID=4625, which is the event ID associated with failed login attempts. The

delete.bat file associated with this event has a single command line of “sdelete -qrsz c:\”. This launches the sdelete.exe in C:\Windows\SDelete with the flags -qrsz specifying the C: drive. The flags set the .exe to not print any errors when run, recurse subdirectories (meaning that the secure delete is ran on every folder and subfolder on the specified drive), and to allow zero free space, meaning it is meant to througohuly and quietly delete these files. Sdelete is an application that can securely remove files from computers, making them difficult to recover by overwriting and renaming files and their associated clusters up to 26 times, while at the same time overwriting unallocated free space. Essentially if someone fails to log in, the contents of the C: drive are erased.

There are several image files that were carved by Zutopsy that seems to indicate that the user was following a guide with several steps to help cover their tracks and to provide anonymity. Identified as, f0239048.jpg, f0239328.jpg, f0238688.jpg, f0243536.jpg, f0243936.jpg, f0244360.jpg, the images appear to give instructions on how to things like download the Tor browser, use vanish.org, and send anonymous emails through the site http://anonymouse.org. Many of these have large red arrows and watermarks indicating that the images came from a wikihow guide.

The following message, located at Perry\Documents\Letter2.rtf contains this text:

> 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

This could indicate the suspect was working with someone named Rick, and was instructed by this person on how to delete evidence. Several other suspicious messages beginning with ‘Letter’, such as Perry\Users\Letter3.rtf, are addressed to ‘Rick’, and there are several other items of evidence that link Perry with someone named Rick Shoner.

All of these pieces of evidence serve to thoroughly support the notion that the user was attempting to cover their tracks, and to delete/obfuscate data on the machine.

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.

When examining accessed files via LNK files, a user appears to have attached an E: drive to the machine which classified as a removable storage media. This is corroborated by several other pieces of evidences, such as the presence of the E: drive in ShellBags.

From event viewer we discovered that two USB devices have been connected to the system, one Sandisk Cruzer with a serial number of 20035001811625714CA7&0 and a Kingston with a serial number of 0013729B678DEB20C51F0216&0. Unfortunately, in the registry the EMDMgmt key located in the SOFTWARE hive and USBStor key in the SYSTEM hive did not contain much helpful data. EMDMgmt was empty, and USBStor lists some devices, but they all have DeviceHackFlags set instead of the standard information stored there, which is an indication of a potential virus, or that the user (or something else) attempted to write-block the connected devices. The E: drive appears to have contained files car1.jpg, car2.jpg, and Mike's Desk.jpg, the latter of which is of marijuana. Unfortunately we were unable to link the E: drive with a specific removable device.

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)?

We found the following message in the Perry User account's recycle bin folder. It was originally located at C:\Users\Perry\Documents\Letter2.rtf. It suggests that Perry was working

with someone named Rick, and that they were both planning to go somewhere (Recycle Bin):

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

The following message, located at Perry\Documents\Letter.rtf contains this message, which is also suspicious:

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 could indicate the suspect was working with someone named Rick, and was instructed by that person on how to cover up evidence. Several other suspicious messages beginning with 'Letter', such as Perry\Users\Letter3.rtf, are addressed to 'Rick'.

Additionally, we found a picture in Users\Perry\Documents\Nice labeled iguazu-falls.jpg. This is an area located in Argentina, on the border with Brazil, potentially the location the suspect might be planning on escaping to in order to escape potential legal prosecution.It also appears as though Perry visited southwest.com which is the website for the airline of the same name, which was revealed through analyzing the TypedURLs in the NTUSER.dat registry key.

Through file carving via Autopsy, we discovered a recoverable .mobx email file named f0252768.mbox which contained the following email, with the subject line "it's time":
"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 file metadata indicated an original author of P Dawg, with the email address rickyboy579@aol.com. It was sent at 2016-02-28T14:08:16 to Perry Winkler, with the email address perrywin232k@aol.com. Other interesting metadata includes the following: **Message:Raw-Header:**Reply-To: "Rick Shoner" <rickyboy579@aol.com>, **Message:Raw-Header:**X-From: Rick Shoner, **Message:Raw-Header:**X-To: Perry Winkler

This serves as evidence that Rick Shoner and Perry Winkler trying to avoid detection and destroying evidence, while taking a United Airline flight, as well as money transfers via Western Union. Additionally, the email header revealed a originating IP address of 186.210.54.196, which is registered in Brazil, and apparently owned by Algar Telecom. The secondary server which received the email is at 74.124.68.45, which is registered in Anchorage, Alaska, 99503. This could mean that Rick is in Brazil and is wiring money to Perry in Alaska, and they plan to meet somewhere else, via the mentioned united flight. Additionally, the message at Perry\Documents\Letter3.rtf indicates that Perry is waiting for contact and movement from Rick.

There is also a rick.jpeg file in the Perry sser account's Pictures folder, which is a picture of Doc Brown, a character from *Back to the Future*. In terms of other potential accomplishes, there is a contact file for someone named Mary Reister that was deleted and recovered from the Recycle Bin, indicating an email address of mreister@gmail.com. There is also a file labeled Rick Shoner.contact that existed at C:\Users\Perry\Documents and C:\Users\Perry\Contacts, as well as a file named Perry.Contact located at C:\Users\Perry\Contacts as revealed by examining LNK files. The Rick Shoner.contact lists an email address of rickboy579@aol.com , while Perry.Contact contains nothing other than the name Perry. There is another contact located at In Perry\Contacts called Larry Spitz.contact. It indicates that Larry Spitz has an email address of spitzmeister@rocketmail.com. These contacts could reveal potential accomplices or additional leads.

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)?

According to the registry key located at SOFTWARE\Microsoft\Windows NT\ CurrentVersion, the operating system on the machine is Windows 7 professional service pack 1, installed on Fri, 15 Jan 2016 21:06:55. Additionally, as revealed by examining the SAM\SAM\Domains\Account\Users registry key, the admin logon has a login count of 6. And the "perry" account has a logon count of 9. The password hint for the "Perry" is "it's your name, idiot" implying that the user account's password is either "Perry" or "Winkler."

Upon reconstructing the users EFS encryption key using a tool called mimikatz, it was revealed that the password is 'perry', which is useful in potentially avoiding the C: drive wiping event of SDelete. We recreated the EFS certificate in an attempt to decrypt and open the plan.zip file in Perry\Documents\email, and while the certificate was successfully recreated, it appears the zip file is otherwise corrupted and unopenable.Given its location and name, this may have contained incriminating evidence worthy of investigation.

Through examining the application event log, we found the user created a restore point on 2/21/2016 6:34:02 and installed Eraser on 02/21/2016 6:34:22. Moreover, from viewing the logs in Microsoft Windows DriverFrameworks UserMode the user started using the kingston drive 2/16/2016 6:03:16 and last used it 2/28/16 11:49:21 AM. Furthermore, the user first started using Sandisk on 1/26/2016 5:48:14 PM.

By examining prefetch files it appears as though Perry used Snipping tool and MS Paint 10 times each. He used a strangely named program called xpsrchvw.exe 7 times and ran RDP 6 times. As expected, the Tor browser installation file was certainly run (a single time). Additionally, it appears, through ShellBag analysis, as that the user last interacted with Tor on 1/15/2016. AIM was installed and used twice, potentially for messages that would be noteworthy. By examining prefetch files, we determined Eraser was run 5 times and Task

Scheduler was run 1 time which could mean he was scheduling file erasures regularly. ShellBags also revealed that the user accessed the program Sdelete which is used to securely wipe hard disks, and ShellBags also reveals that a user downloaded a zip file titled ‘sdelete.zip’ and extracted the contents, presumably to use the application with the same name.

Programs that have been run on the machine that appear suspicious and could require further investigation include 41470975[1].EXE which was run a single time according to its corresponding prefetch file. It is a strange and unknown program name, and it being run only once is an indicator of potentially malicious and suspicious activity according to the principle of least frequency of occurrence.

There are also Canon logo images on the volume, as discovered by Autopsy indicating that that may be the type of camera used to take some of the pictures located on the system.

There is also an image of what appears to be a can of prego pasta sauce in the back component of a toilet, dated 05/05/2007 at \Perry\Documents\100_6317.jpg. This is an odd thing, which may be worthy of investigation.