Project 4

CIS 484-75

Group 4

Natalie Starck, Cameron Little, Xander Eisert, Adam Schweitzer

As a team of digital forensic examiners, we were assigned to a Louisville Metro Police Department (LMPD) investigation involving a suspected drug dealer named Perry Winkler. LMPD attempted to search Perry's place of residence though he appeared to have left the scene before they got there. A hard drive from a computer was found outside the residence and subsequently imaged using forensically sound measures. That forensic image was given to us for analysis which will be presented in this following report.

Before beginning the extraction and analysis portion of the investigation, we reviewed the questions that were posed to us to carry out the required tasks. For each question, we determined relevant artifacts we may need to examine to obtain that information. This includes items such as LNK files, jump lists, registry hives, etc. Then as we went through each question, we would reference this as a guide as well as look in other locations in case there happened to be further relevant information. Next, once the forensic image file was downloaded on our workstation, we made sure to verify it to make sure nothing had gone awry during the download process. To view and extract artifacts and evidence from the forensic image we utilized AccessData FTK Imager version 4.2.1.4.

Task 1 – Identifying the owner or user of the computer

First, we determined basic facts about the system such as, operating system version, registered owner, computer name, user accounts, etc. to address the first task which poses to look for identifying information to determine the owner or user of the computer and if the computer appeared to have been used by Perry Winkler. In order to determine this, we first examined the forensic image within FTK Imager and within the Partition 2\[root]\Users folder that displays a list of directories for each user, there was a directory named Perry. Next, we extracted all the registry hives from their respective locations in FTK Imager. Then using Registry Explorer

version 1.5.2.0 we analyzed the SYSTEM hive as this contains information related to the system such as computer name and time zone information. Finding this information helped explain further about the potential owner and user. As ControlSet001 was the active control set within the SYSTEM hive we used the following path to obtain the computer name: SYSTEM\ControlSet001\Control\ComputerName\ComputerName. The computer name is PERRYWINKLER-PC. Afterward, using Registry Explorer as well as RegRipper version 2.8 we analyzed the SOFTWARE hive as it is particularly important because it contains general owner information. Using RegRipper, we found the registered owner among other information such as OS version, service pack number, and installation date under the CurrentVersion key. The full path for this key is: SOFTWARE\Microsoft\Windows NT\CurrentVersion. The registered owner value is named Perry. This piece of information is important as it confirms Perry is the owner of the computer. Remaining within the SOFTWARE hive we traversed to the ProfileList subkey. This key is important to this task as it contains a list of user accounts on the system and is a good way to associate a SID with a username. The full key path is: SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Once at the ProfileList subkey, we looked at each SID and found the last one was associated with a user account named Perry. The account's SID is S-1-5-21-3461440871-1589894493-1829873476-1000. Lastly, to further confirm that Perry Winkler is indeed the owner and user of this computer we examined the SAM hive using RegRipper. The SAM hive contains valuable information related to local user accounts. There were several accounts including Administrator, Guest, and Perry. The Administrator and Guest accounts were disabled. The user SID for the Perry user account matches the SID listed in the SOFTWARE hive's ProfileList subkey indicating they are the same account. The account does not require a password, but there is a password hint indicating it would be the user's name. The Perry user account was last logged in on Sunday Feb 28, 2016 at 15:45:38 UTC. This may be helpful to

LMPD perhaps representing around the last time the user was at their residence. The parsed output from the SAM hive is displayed below. This and the previously mentioned items confirm the owner and user of the computer is Perry Winkler.

```
Username        : Perry [1000]
SID             : S-1-5-21-3461440871-1589894493-1829873476-1000
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Fri Jan 15 21:06:54 2016 Z
Name            :
Password Hint   : it's your name, idiot
Last Login Date : Sun Feb 28 15:45:38 2016 Z
Pwd Reset Date  : Fri Jan 15 21:06:54 2016 Z
Pwd Fail Date   : Wed Feb 24 22:50:54 2016 Z
Login Count     : 9
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

Task 2 – Evidence of drugs or other illegal activities

Next, we moved onto addressing the task of finding evidence on the computer that the user may have been associated with drugs or other illegal activities. The bulk of the substantial evidence we found was gathered using FTK Imager and confirmed with other artifacts like LNK files. The LNK files were viewed within Microsoft Excel and parsed with LECmd.exe. In the folder Partition 2\[root]\Users\Perry\Documents, there is an Excel workbook simply titled “Book2”. The book seems to contain the nicknames of clients, the money they owe, and their preferred drug. A screenshot of it is included below.

	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
8			

Instances of contacts were found by examining this path in FTK Imager: Partition 2\[root]\Users\Perry\Contacts. It contains three contacts: Perry, Larry Spitz, and Rick Shoner.

The Perry contact relates to the current suspect, so the information is less relevant. Larry Spitz's and Rick Shoner's email addresses were extracted from within FTK Imager when clicking on their name. Their emails are spitzmeister@rocketmail.com and rickyboy579@aol.com, respectively. They could be potential clients or accomplices. More will be discussed about potential accomplices further in the report. Furthermore, when examining the RecentDocs key within the NTUSER.DAT hive, only Rick Shoner and Perry display, potentially showing some information was removed. The path to see this information is: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.contact.

In addition, within the previously mentioned path Partition 2\[root]\Users\Perry\Documents, also contains two letters written by Perry and addressed to Rick. The first, titled "Letter", was first created on February 16, 2016 at 22:04:56 UTC as indicated in the LNK file Target Created time that equates to the time the actual file was created. Letter.rtf was last modified on February 16th, 2016 at 22:04:56 UTC as indicated in the LNK file Source Modified time. This document alludes to "getting rid of the stuff in the kitchen and bedroom" and seems to also contain a request for advice on how to get rid of his computer. The next letter, called "Letter3", was last modified on February 27th, 2016 at 15:13:43 UTC also indicated in the LNK file Source Modified time. It was first created February 27th, 2016 at 15:13:39 UTC as stated by the Target Created time within the LNK file output. It is much more nervous in tone than "Letter", containing several "where are you?"s. Perry also tells Rick that he purchased some credit card numbers, photos of which exist at this path: Partition 2\[root]\Users\Perry\Pictures\cc.jpg. Additionally, two photos of marijuana and money are in that same Pictures folder ("mike's desk.jpg" and "da stuff.jpg"). A screenshot of the two photos are included below.

Also, in the documents folder on FTK Imager is a timestamped photo of a jar in the tank of a toilet. The full path to this image is: Partition 2\[root]\Users\Perry\Documents\100_6317 (Small).JPG. The timestamp is from 2007, around 9 years before the discovery of Winkler's computer, but this could be a reference photo that he used for inspiration. It might be in the best interest of investigators to search the tank of any toilet in Mr. Winkler's house.

We found another interesting piece of evidence in the NTUSER.DAT registry hive. In the TypedURLs key is evidence that Perry attempted to search for the phrase "how to skim credit cards", but mistakenly typed his query into the Internet Explorer address bar instead of the search bar. The full key path is NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs.

Task 3 – Evidence of user trying to cover tracks or delete evidence

After finding evidence related to drugs or other illegal activities, we moved on to the third task addressing evidence that the user may have been trying to cover his tracks or delete evidence from the computer. We primarily looked for instances of secure erase programs and deleted files. First, using Registry Explorer, we examined the SYSTEM hive's AppCompatCache subkey as this tracks file name, size, and last modified time of an executable. The last modified time is not the last time of program execution. It was found within this path: SYSTEM\ControlSet001\Control\Session Manager\AppCompatCache. There are instances of

two executables that appear to be secure deletion programs: Eraser.exe and sdelete.exe. Both appear under the Downloads folder under the Perry user account and are included below.

Cache Entry Position	Program Name	Modified Time
=	eraser	=
22	C:\Program Files\Eraser\Eraser.exe	2015-09-03 20:31:44
108	C:\Users\Perry\Downloads\Eraser 6.2.0.2970.exe	2016-02-21 22:30:23
127	C:\Users\Perry\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40_Full_setup.exe	2016-02-21 22:30:25
128	C:\Users\Perry\Downloads\Eraser 6.2.0.2970.exe	2016-02-21 22:30:07

Cache Entry Position	Program Name	Modified Time
=	sdelete	=
96	C:\Windows\SDelete\sdelete.exe	2016-02-24 22:47:06
106	C:\Users\Perry\Downloads\SDelete\sdelete.exe	2016-02-24 22:47:06

Other relevant applications within the AppCompatCache subkey include Dropbox, Aim and Aol messenger related applications, and Tor web browser. Aim and Aol messenger related applications could have potential contacts and conversations. Dropbox could store other incriminating documents. Tor web browser is used for private web browsing and to maintain anonymity. It could show that the Perry user was trying to conceal their web browsing history. Several other registry hive locations show the existence of these secure erase programs such as the SOFTWARE hive's Run key, Uninstall key, and RecentDocs key. All keys were examined with Registry Explorer. The Run key shows that each time the system restarts the Eraser program is run across all user accounts and Perry is the only active account. The Uninstall key contains another confirmation of the Eraser secure deletion installer program under the Perry user account via the InstallSource value. The RecentDocs key within the .zip extension contains a reference to SDelete.zip file, another reference to the secure deletion program. Another hive containing information about the previously mentioned programs is the NTUSER.DAT hive and this is especially important because this hive is directly associated with the Perry user account. The NTUSER.DAT hive's UserAssist key shows information about executables run by a user, in our case Perry. Within this key is proof that the Eraser program was the very last executable run by

the Perry user account on February 28, 2016 at 15:47:04 UTC. We also see evidence that Perry was the one who installed Eraser.exe, as well as proof of installation and access to the Tor browser.

Under the UsrClass.DAT hive we find Shellbag information, which will be helpful for confirming other finds later. We find a device mounted to E:\, most likely a flash drive, that was last written to on February 28, 2016 at 15:47:13 UTC, just nine seconds after Perry last ran Eraser.exe on the PC. Additionally, Shellbag data shows that Perry first ran the program SDelete on February 24, 2016 at 22:47:23 UTC. Shellbags were viewed using Shellbags Explorer version 1.4.0.0.

Remaining artifacts that confirm the existence of the Eraser and SDelete programs are the Windows event logs- Application subtype, scheduled tasks, prefetch files, and LNK files. The event log shows Eraser as associated with the Perry user account by using the SID. SDelete has a scheduled task authored by the Perry user account. One of the prefetch output files shows the Eraser program was run 5 times. A LNK file exists for the SDelete zip file that contained the SDelete program.

Event logs were extracted from this path: Partition 2\[root]\Windows\System32\winevt\Logs. The path to extract the scheduled tasks is: Partition 2\[root]\Windows\System32\Tasks. Prefetch files are stored within this path: Partition 2\[root]\Windows\Prefetch. LNK files were extracted from this path: Partition 2\[root]\Users\Perry\AppData\Roaming\Microsoft\Windows\Recent. Event logs were parsed via EvtxECmd.exe (Evtx Explorer) and prefetch files were parsed with PECmd.exe. Both were viewed within Timeline Explorer version 1.0.0.0. XML Notepad 2007 was used to view the scheduled task.

In addition, within the parsed web searches in Autopsy, there were instances of searches like "how to get rid of evidence" and searches related to Eraser and SDelete. Web downloads showed the same programs as well. Web history showed searches and visits to websites related to the secure erase programs. Also, a search for "untraceable emails." All parsed web related history is associated with the Perry user. These same searches can be found and confirmed from custom jump list entries too. Jump lists were extracted from: Partition 2\[root]\Users\Perry\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations and parsed with JLECmd.exe. A search for a website and a visit is a clear indication the user of the system sought out that specific website.

Moving on to other artifacts, we examined the Recycle Bin next. The Recycle Bin contains files deleted by the specific user account if under their SID subfolder. We found the Recycle Bin contents from this path: Partition 2\[root]\$Recycle.Bin\ S-1-5-21-3461440871-1589894493-1829873476-1000. Once the deleted files were extracted, more specifically the $I and $R files, we parsed the $I index files within $I Parse version 1.1 since they contain the deleted file metadata. We were able to see specific images and file content within File Explorer or within FTK Imager itself. Some of the files included a rtf document along with photos of guns and a car. Letter2 once existed in the Documents folder but was deleted. The letter, last opened on February 21, 2016 at 15:13:17 UTC as indicated by the Source Modified LNK file time, thanks Rick for some advice on setting up a task on the computer and for some printed instructions and promises Rick that this will be destroyed. It's assumed the task is for SDelete since this was a scheduled task and either the letter or perhaps the computer was going to be destroyed since it was in a dumpster. The $RNDKRDO.contact deleted file contained Mary Reister's email address. This could be a potential accomplice or client.

Next, we examined deleted files within the Master File Table (MFT) using FTK Imager and carved others using Autopsy's PhotoRec Carver. If the file was solely available within the MFT record, only the file's metadata was recoverable. If file content was solely available, carving was employed. FTK Imager represents a file as deleted via a red X symbol. Initial items found as deleted were LNK files: drawing.lnk, Letter.lnk, Perry.lnk, and th.lnk. Other files found as deleted were related to the registry and were a SECURITY log file and a NTUSER.DAT file. These among other files may have been deleted by the secure erase programs mentioned earlier. There is a separate location outside of the root directory known as orphan that contains orphan files. Orphan files are those whose parent directory MFT records have been overwritten. The DropboxUninstaller.exe as well as many other files with a pyd extension are shown as deleted. Some are named win32security.pyd, win32evtlog.pyd, win32event.pyd and could be related to the Windows event logs. Using PhotoRec Carver, many images were revealed, some more relevant than others. These could be images of the suspect as well as potential clients/accomplices. They were found in Autopsy under Images/Videos then under the following path- /img_LMPD-436243-001.E01/vol_vol3//$CarvedFiles/. Another image was found within the path: Partition 2\[root]\[unallocated space]\00000048\01330004 of a suspicious item. All will be included below.

Lastly, two files were found as deleted from Autopsy, namely SDelete[1].aspx and Passport.htm, both from Temporary Internet Files, meaning they were downloaded from the Internet. Both

show attempts to hide information. The passport file may or may not be as relevant, but we cannot determine due to only the MFT record being available.

Task 4 – USB devices that contain pertinent evidence

Next, we moved on to addressing the task of finding items like USB devices that may contain pertinent evidence. Upon further investigation of the SYSTEM hive within the registry, we discovered that two removable storage devices had been connected to the computer. The path within the SYSTEM hive is SYSTEM\ControlSet001\Enum\USBSTOR. The first storage device that was connected to the computer was a SanDisk Cruiser USB Device. This device was last inserted into the computer on January 26, 2016 at 21:48:14 UTC. The device's name, also referred to as Friendly under the SYSTEM hive, was "files" and had a serial number of: 20035001811625714CA7. After reviewing the jump lists associated with removable storage devices as the drive type and the volume label as "files," we were able to discover one photo was accessed and referenced on this drive. The local path to this item, was "E:\mike's desk.jpg." While the path is different, this references the same photo that is displayed on page 5, that depicts a substantial sum of bundled cash with what preliminary appears to be cannabis/marijuana. We were able to verify that this photo was the same one on the thumb drive due to the same volume serial number being on the .lnk file and Autopsy. This volume serial number was "A0C9328E." The next removable storage device that was located on the SYSTEM hive was a Kingston Prod DT 101 G2 USB. This device was last connected to the computer on Sunday, February 28, 2016 at 15:46:06 UTC. The serial number of this device is 013729B678DEB20C51F0216 and its friendly name was "PERRY". Since this USB device and the SanDisk Cruiser USB device were the only two removable storage devices connected to the computer, we can conclude that the Kingston Prod DT 101 G2 was the last device inserted into the computer. With the same processes used to discover files within the SanDisk Cruiser, the

same can be done within this USB device. Upon discovery, there were two .lnk files that referenced two photos within this device. These photos were labeled “car1.jpg” and “car2.jpg.” These two photos were pictures of two older model cars. They were also verified using the volume serial number of the device: “3AA4C998.” While the devices didn't have any other suspicious activity connected to them, they were both connected during the time other illicit activity was being completed on the computer.

Task 5 - Evidence of the user planning to go on the run

Was the user planning to go on the run? We think so. There is a multitude of evidence leading us to that conclusion. First, there are the 3 letters where the user, Perry, is communicating with Rick and discussing their plans. In the second letter Perry writes “cant wait to ditch this place!”, leading us to believe he is about to leave his current location. In the third letter Perry writes “are you there yet? i need an email to know”, in which it looks like his potential accomplice, Rick, is in route to the new location. We think that the “Rick Shoner.contact” file in Perry’s Documents directory reveals Rick’s full name as “Rick Shoner” and that his email address is “rickyboy579@aol.com”.

Next, we wanted to dig a bit deeper. We used Arsenal Image Mounter and VSSMount to investigate the LMPD image file for volume shadow copies. Luckily, a volume shadow copy existed! Digging into the VSC we discovered an image of a map of South America. Additionally, we found an email file called “plan.eml”. The email was sent to “perrywin232k@aol.com” and is from Rick’s suspected email address, rickyboy579@aol.com, and reads as follows:

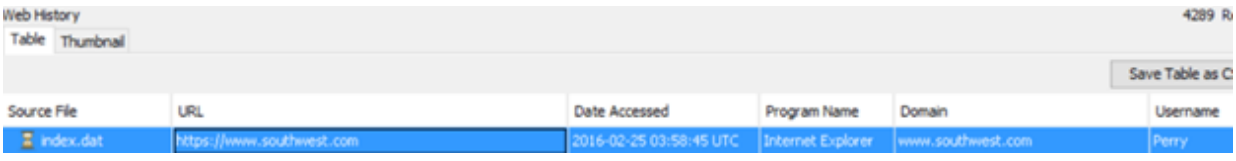
> “I finally made it here. I'm using the hotel lobby computer so this cant be traced back to me. I'll wire the funds to your western union tomorrow. get rid of the evidence and get on united flight we talked about. see you soon.”

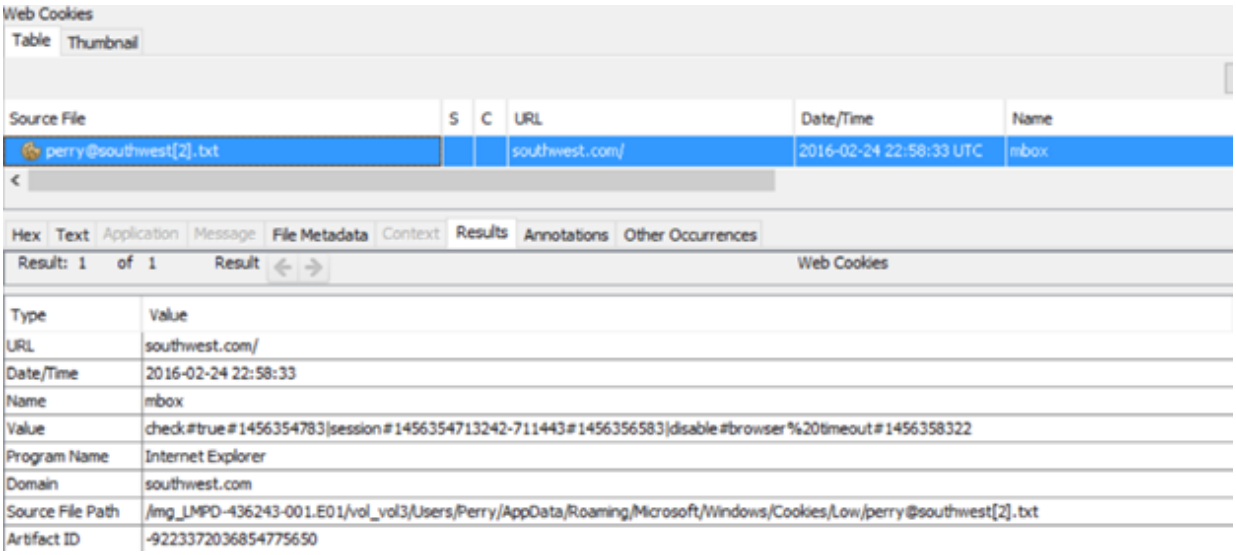
The email was received Sunday, 28th of February 2016, at 09:08:16 EST. Rick states that he's made it to the destination, which we believe is Brazil. Inspecting the "plan.eml" file with Notepad++ revealed the IP address that the email was received from: 186.210.54.196. Looking up the IP address online, we see that it is a Brazilian IP address, indicating that Rick has made it safely to a hotel in Brazil. Here is a screenshot of the "plan.eml" file as seen in Notepad++:

```
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 pcludsmtaln25 (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.
```

Lastly, using Autopsy we discovered some information through Perry's web history that indicates he was looking for flights. There is evidence that Perry visited "southwest.com", Southwest is a popular airline. However, the email from Rick suggests that Perry is to "get on united flight we talked about", not a Southwest flight. Here are screenshots of both the web cookie and web history entry in Autopsy:





Task 6 – Other evidence of potential importance

All in all, we believe the main tasks discussed previously contained their relevant evidence along with mentions of other evidence of potential importance.