

## **Project 4: Forensic Examination**

Yen Hsieh Hsu

College of Business, University of Louisville

CIS 484-50: Computer Forensics

Professor Jason Hale

December 5, 2022

## **Table of Contents**

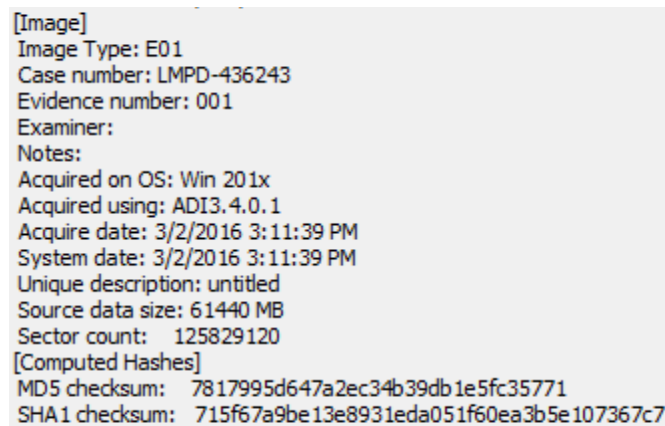
<b>Introduction &amp; Case Background</b>	<b>2</b>
<b>System Information &amp; Device Ownership</b>	<b>3</b>
<b>Evidence</b>	<b>4</b>
Association with drugs or illegal activities	4
Track covering or evidence deletion	6
Additional items/devices	8
Escape plans	9
<b>Additional Information/Evidences</b>	<b>11</b>
<b>Tools Used</b>	<b>13</b>

## Introduction & Case Background

The Louisville Metro Police Department's drug enforcement team has been after a suspected drug dealer, Perry Winkler, for several months. The LMPD obtained a search warrant to search Winkler's residence, but the suspect was no longer there. No useful evidence could be found after searching his residence as it seems that Winkler cleared the place before leaving. A damaged desktop PC was found outside of the residence, where the hard drive was able to be recovered intact, and potential evidence could be recovered from it. In this report, I will detail the ownership of the device, evidence associated with the case, potential escape routes or plans, and the steps in collecting the information.

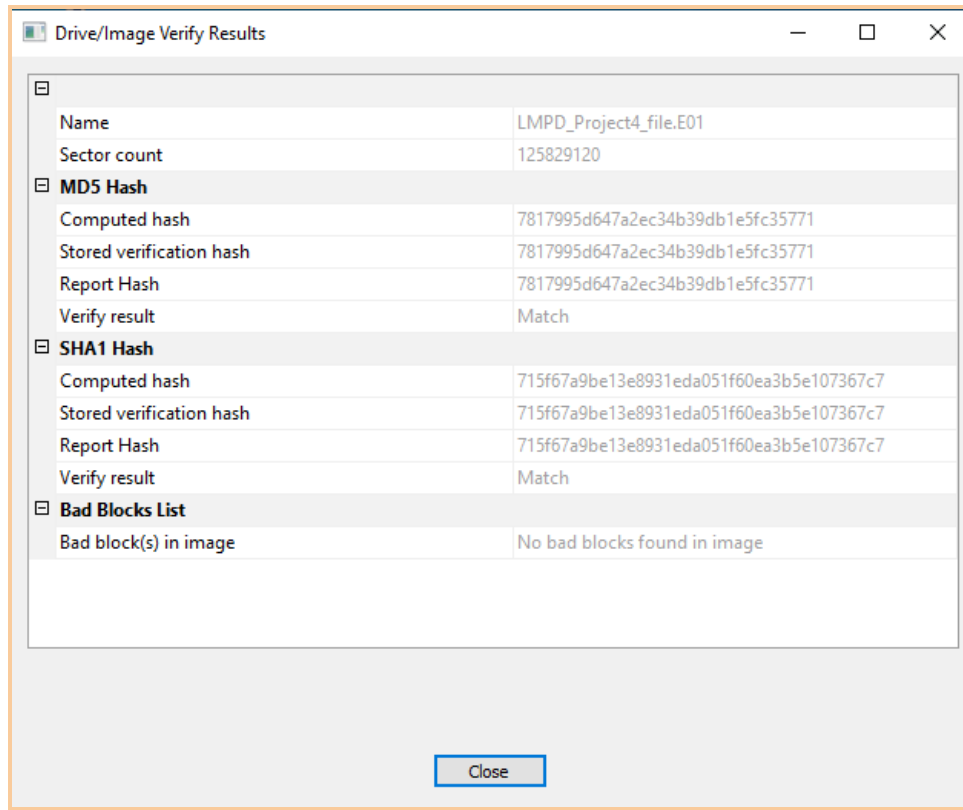
## Data Integrity

To start, the FTK Imager is used to create, verify and display the results of the verification. The hash values retrieved are compared and can determine whether any data has been lost or tampered with during transport to the lab. The computed MD5 and SHA1 hashes are displayed below:



```
[Image]
Image Type: E01
Case number: LMPD-436243
Evidence number: 001
Examiner:
Notes:
Acquired on OS: Win 201x
Acquired using: ADI3.4.0.1
Acquire date: 3/2/2016 3:11:39 PM
System date: 3/2/2016 3:11:39 PM
Unique description: untitled
Source data size: 61440 MB
Sector count: 125829120
[Computed Hashes]
MD5 checksum: 7817995d647a2ec34b39db1e5fc35771
SHA1 checksum: 715f67a9be13e8931eda051f60ea3b5e107367c7
```

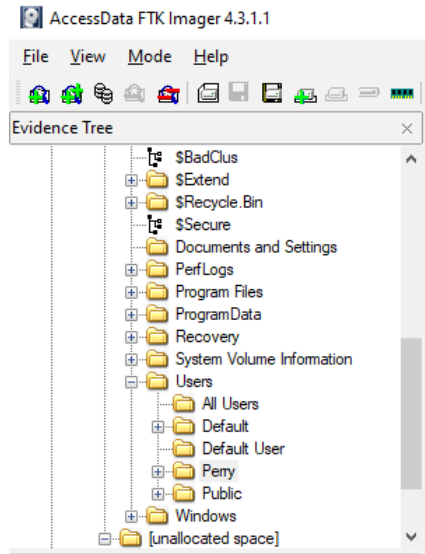
For the case file, after creating the image with FTK Imager it is verified that all the hash values are the same, meaning that the file has not been tampered with or lost, and is the original data of the device that was found at the scene.



## System Information & Device Ownership

The image information (shown in first picture) from FTK Imager already determines that the operating system is Windows. Using Autopsy, the specific version of Windows the suspect is using is Windows 7 Professional. Both FTK Imager and Autopsy shows that the user of the device is Perry Winkler, with the device name being PERRYWINKLER-PC. Registry Explorer can be used to confirm the above data too.

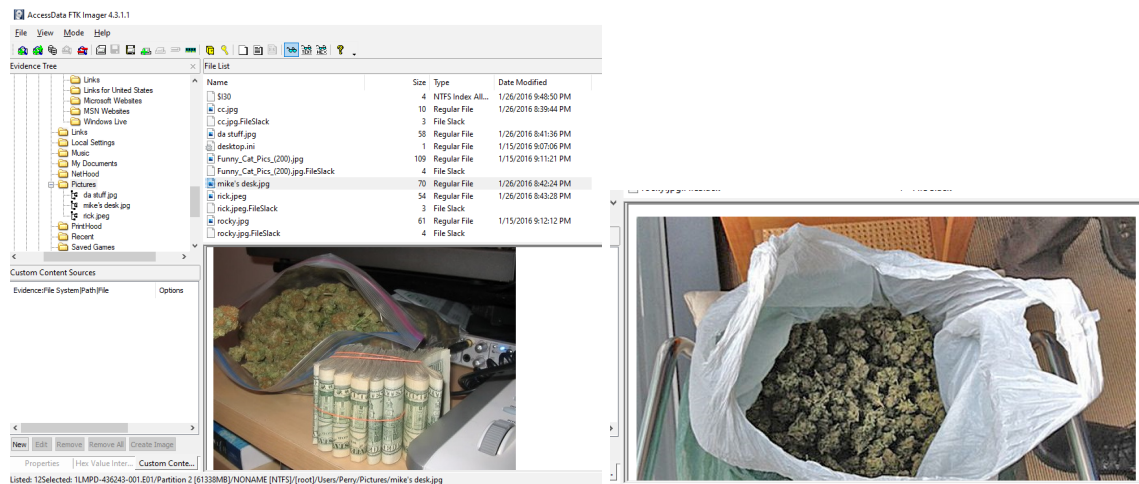
Operating System Information											
Table Thumbnail Summary											
Source Name	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory	Data Source	Program Name	Date/Time
SYSTEM				PERRYWINKLER-PC		Windows_NT	x86	%SystemRoot%\TEMP	LMPD-436243-001.E01		
SOFTWARE									LMPD-436243-001.E01	Windows 7 Professional Service Pack 1	2016-01-15 16:06:55 E



## Evidence

### *Association with drugs or illegal activities*

After mounting the image in FTK imager and exploring it, in Users/Perry/Pictures we have 1 picture of credit cards, and 2 related to drugs. Although the photos of the credit card cannot prove the suspect to be selling drugs, the photos of the actual drugs are incriminating.



Next, using Autopsy, a letter directed towards Rick was found on Users/Perry/Documents. Winkler expresses his worry about the police suspecting them, which he mentions about getting rid of the stuff, assuming drugs, in the kitchen and bedroom. He also mentions about the computer, which can refer to erasing the evidence.

Listing									
/img_LMPD-436243-001.E01/vol_3/Users/Perry/Documents									
Table Thumbnail Summary									
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag
[current folder]				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-01-15 16:06:57 EST	56	Alloc
[parent folder]				2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-01-15 16:06:57 EST	256	Alloc
emails				2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-27 10:27:02 EST	152	Alloc
My Music				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Alloc
My Pictures				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Alloc
My Videos				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Alloc
nice				2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:25:38 EST	504	Alloc
100_6317 (Small).JPG				2013-11-07 14:18:42 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-12 15:59:32 EST	70389	Alloc
Book2.xlsx				2016-02-16 16:00:56 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-16 16:00:30 EST	8438	Alloc
desktop.ini				2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	402	Alloc
Letter.rtf				2016-02-16 17:08:03 EST	2016-02-16 17:08:03 EST	2016-02-16 17:04:49 EST	2016-02-16 17:04:49 EST	374	Alloc
Letter2.rtf				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-21 17:22:11 EST	2016-02-21 17:22:11 EST	472	Unal
Letter3.rtf				2016-02-27 10:16:14 EST	2016-02-27 10:16:14 EST	2016-02-27 10:13:39 EST	2016-02-27 10:13:39 EST	475	Alloc
need mo.jpg				2012-04-06 12:03:46 EDT	2016-02-16 17:04:09 EST	2016-02-16 17:04:09 EST	2016-02-12 15:59:41 EST	38937	Alloc
Rick Shoner.contact				2016-02-16 17:09:15 EST	2016-02-16 17:09:27 EST	2016-02-16 17:09:15 EST	2016-02-16 17:09:15 EST	1291	Alloc

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Indexed Text

Translation

Page: 1 of 1

Page

Go to Page:

{\rtf1\ansi\deff0{\fonttbl{\f0\fnil{\fcharset0 Calibri;}}\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\sa200\sl276\smult1\lang9\fs22 Rick,\par 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 figuer this out.\par Signed,\par Perry\par

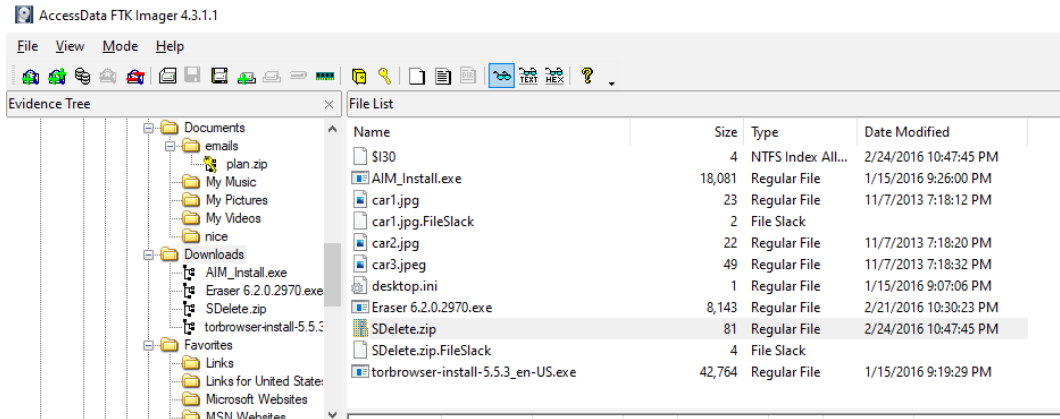
Additionally, in an Excel file named Book2 stored in Users/Perry/Documents, a client list was found. The spreadsheet contained the name of the buyer, amount they owe the dealer, and

their favorite drugs. This evidence is very important as it shows that the suspect is indeed selling drugs.

	A	B	C	D
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				
9				

#### *Track covering or evidence deletion*

There are very clear signs of track covering and evidence deletion. The first sign is the presence of the suspect having downloaded Eraser 6 and SDelete, which can be seen on Users/Perry/Downloads on FTK Imager. Heading on to Autopsy, in “Installed Programs” it is shown that the software Eraser 6 was installed on the device. Then searching on the web history, there are inquiries on how to remove traces of activities on the computer, and other similar searches that can let us conclude that the suspect has removed important information/evidence from the computer.



Listing						
Installed Programs						
Table	Thumbnail	Summary				
Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	Dropbox v.3.16.1	2016-02-24 22:58:47 EST	LMPD-436243-001.E01
SOFTWARE			0	Dropbox Update Helper v.1.3.35.1	2016-02-24 22:56:58 EST	LMPD-436243-001.E01
SOFTWARE			0	Big Air War v.1.0	2016-02-24 22:54:31 EST	LMPD-436243-001.E01
SOFTWARE			0	Eraser 6.2.0.2970 v.6.2.2970	2016-02-21 22:34:18 EST	LMPD-436243-001.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2016-02-21 22:33:21 EST	LMPD-436243-001.E01
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2016-02-21 22:33:14 EST	LMPD-436243-001.E01
SOFTWARE			0	Microsoft .NET Framework 4 Client Profile v.4.0.30319	2016-02-21 22:32:30 EST	LMPD-436243-001.E01

Listing									
Web History									
Table	Thumbnail	Summary							
Source Name	S	C	O	URL	Date Accessed	Referrer URL	Program Name	Domain	Username
index.dat				http://www.ehow.com/how_4676367_remove-traces-activity-computer.html&rc=j&fr...	2016-02-16 22:15:09 EST		Internet Explorer		Perry
index.dat		1		http://www.ehow.com/how_4676367_remove-traces-activity-computer.html	2016-02-16 22:15:13 EST		Internet Explorer	ehow.com	Perry
index.dat		1		http://www.bing.com/search?q=eraser&src=IE-SearchBox&FORM=IE8SRC	2016-02-21 22:26:51 EST		Internet Explorer	bing.com	Perry
index.dat		1		http://commandwindows.com/favicon.ico	2016-02-24 22:45:09 EST		Internet Explorer	commandwindows.com	Perry
index.dat		1		http://www.bing.com/search?q=how+to+set+up+scheduled+task&src=IE-SearchBo...	2016-02-24 22:45:11 EST		Internet Explorer	bing.com	Perry
index.dat				file/Users/Perry/Downloads/SDelete.zip	2016-02-24 22:47:45 EST		Internet Explorer		Perry

From the letter in the previous section, Winkler indicated that he needs to get rid of the evidence on the computer. Another letter was found. It is a deleted letter named Letter2. The letter shows Winkler thanking Rick, meaning that evidence was deleted. Also, there was a mention of a 'task thing' which is assumed to be the scheduled task of the computer.



Listing

/img\_LMPD-436243-001.E01/vol3/Users/Perry/Documents

15 Result

TableThumbnailSummary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-01-15 16:06:57 EST	56	Allocated	Allocated	unknown	/img_LMPD-436
[parent folder]				2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-01-15 16:06:57 EST	256	Allocated	Allocated	unknown	/img_LMPD-436
emails				2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-27 10:27:02 EST	152	Allocated	Allocated	unknown	/img_LMPD-436
My Music				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436
My Pictures				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436
My Videos				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436
nice				2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:25:38 EST	504	Allocated	Allocated	unknown	/img_LMPD-436
100_6317 (Small).JPG				2013-11-07 14:18:42 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-12 15:59:32 EST	70389	Allocated	Allocated	unknown	/img_LMPD-436
Book2.xlsx				2016-02-16 16:00:56 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-16 16:00:30 EST	8438	Allocated	Allocated	unknown	/img_LMPD-436
desktop.ini				2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	402	Allocated	Allocated	unknown	/img_LMPD-436
Letter.rtf				2016-02-16 17:08:03 EST	2016-02-16 17:08:03 EST	2016-02-16 17:04:49 EST	2016-02-16 17:04:49 EST	374	Allocated	Allocated	unknown	/img_LMPD-436
Letter2.rtf				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-21 17:22:11 EST	2016-02-21 17:22:11 EST	472	Unallocated	Unallocated	unknown	/img_LMPD-436
Letter3.rtf				2016-02-27 10:16:14 EST	2016-02-27 10:16:14 EST	2016-02-27 10:13:39 EST	2016-02-27 10:13:39 EST	475	Allocated	Allocated	unknown	/img_LMPD-436
need mo.jpg				2012-04-06 12:03:46 EDT	2016-02-16 17:04:09 EST	2016-02-16 17:04:09 EST	2016-02-12 15:59:41 EST	38937	Allocated	Allocated	unknown	/img_LMPD-436
Rick Shoner.contact				2016-02-16 17:09:15 EST	2016-02-16 17:09:27 EST	2016-02-16 17:09:15 EST	2016-02-16 17:09:15 EST	1291	Allocated	Allocated	unknown	/img_LMPD-436

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

StringsIndexed TextTranslation

Page: 1 of 1PageGo to Page:

Script: Latin - Basic

{\rtf1\ansi\def\fonttbl{\f0\fnil\charset0 Calibri;}} {\Vgenerator Msftedit 5.41.21.2510;}viewkind=uc1\pard\sa200\sl276\simult1\lang9\fo\fs22 Rick,\par 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!\par Yours truly,\par Perry\par

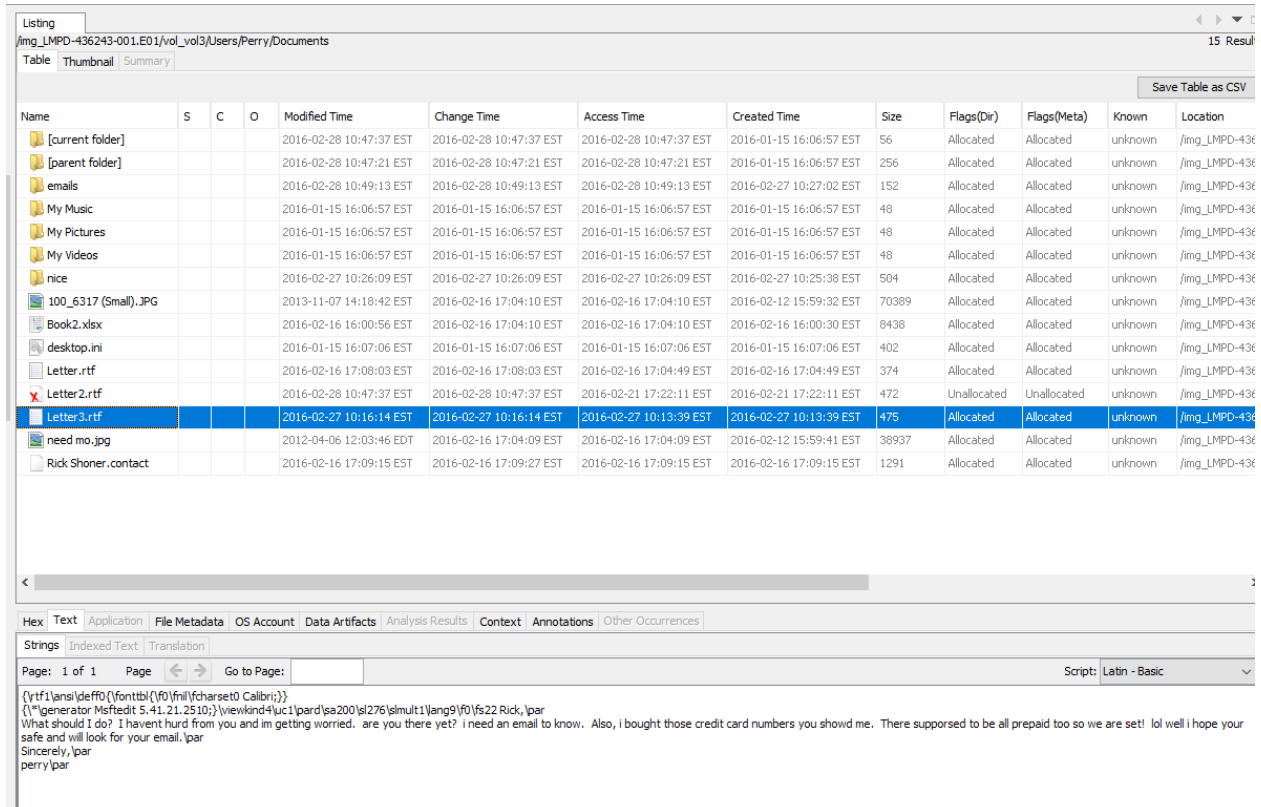
## Additional items/devices

From Autopsy, two external devices were identified. One SanDisk Cruzer and a Toshiba Kingston DataTraveler flash drive were identified. The Kingston flash drive is currently the most suspicious and may contain evidence or other important information as it was the most recent one to connect to the computer on February 28, 2016.

Listing							
USB Device Attached							
Table	Thumbnail	Summary					
Source Name	S	C	O	Date/Time	Device Make	Device Model	Data Source
SYSTEM			0	2016-02-28 10:45:22 EST		ROOT_HUB	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:22 EST		ROOT_HUB20	LMPD-436243-001.E01
SYSTEM			0	2016-01-26 16:48:11 EST	SanDisk Corp.	Cruzer	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:52 EST	Toshiba Corp.	Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / P...	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:24 EST	VMware, Inc.	Virtual USB Hub	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:23 EST	VMware, Inc.	Virtual Mouse	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:23 EST	VMware, Inc.	Virtual Mouse	LMPD-436243-001.E01
SYSTEM			0	2016-02-28 10:45:23 EST	VMware, Inc.	Virtual Mouse	LMPD-436243-001.E01

## Escape plans

There were signs that Winkler was planning to run away. The first clue was from the letters shown above where Winkler mentioned wanting to ditch the place. Later a third letter is found in the same location as the previous first letter, where Winkler is ready to leave with the cards Rick recommended him to buy.



Listing  
/img\_LMPD-436243-001.E01/vol\_vol3/Users/Perry/Documents 15 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-01-15 16:06:57 EST	56	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
[parent folder]				2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-01-15 16:06:57 EST	256	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
emails				2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-27 10:27:02 EST	152	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
My Music				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
My Pictures				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
My Videos				2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	2016-01-15 16:06:57 EST	48	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
nice				2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:25:38 EST	504	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
100_6317 (Small).JPG				2013-11-07 14:18:42 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-12 15:59:32 EST	70389	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
Book2.xlsx				2016-02-16 16:00:56 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST	2016-02-16 16:00:30 EST	8438	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
desktop.ini				2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	402	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
Letter.rtf				2016-02-16 17:08:03 EST	2016-02-16 17:08:03 EST	2016-02-16 17:04:49 EST	2016-02-16 17:04:49 EST	374	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
Letter2.rtf				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-21 17:22:11 EST	2016-02-21 17:22:11 EST	472	Unallocated	Unallocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
Letter3.rtf				2016-02-27 10:16:14 EST	2016-02-27 10:16:14 EST	2016-02-27 10:13:39 EST	2016-02-27 10:13:39 EST	475	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
need mo.jpg				2012-04-06 12:03:46 EDT	2016-02-16 17:04:09 EST	2016-02-16 17:04:09 EST	2016-02-12 15:59:41 EST	38937	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents
Rick Shoner.contact				2016-02-16 17:09:15 EST	2016-02-16 17:09:27 EST	2016-02-16 17:09:15 EST	2016-02-16 17:09:15 EST	1291	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol_vol3/Users/Perry/Documents

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Indexed Text Translation

Page: 1 of 1 Page Go to Page: Script: Latin - Basic

{\rtf1\ansi\deff0{\fonttbl{\f0\fnl{\charset0 Calibri}}}{\generator Msftedit 5.41.21.2510}{\viewkind4\uc1\pard{\sa200\sl276\simult1\lang9\fd0\fs22 Rick, \par 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 showed me. There supposed 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

Additionally, with a search to his web history, an airline's website, Southwest, could be found. This may say that Winkler may be planning to fly out, possibly internationally.

index.dat	1	http://www.bing.com/search?q=helicopter+game+downlo...	2016-02-24 22:53:02 EST	Internet Explorer	bing.com	Perry	LMPD-436243-001.E01
index.dat	1	file://Users/Perry/Desktop/th.jpg	2016-02-16 22:13:30 EST	Internet Explorer		Perry	LMPD-436243-001.E01
index.dat	1	https://www.southwest.com	2016-02-24 22:58:45 EST	Internet Explorer	southwest.com	Perry	LMPD-436243-001.E01
index.dat	1	http://eraser.heidi.ie/feed	2016-02-21 22:27:19 EST	Internet Explorer	heidi.ie	Perry	LMPD-436243-001.E01
index.dat	1	http://www.bing.com/search?q=helicopter+game+downlo...	2016-02-24 22:53:02 EST	Internet Explorer	bing.com	Perry	LMPD-436243-001.E01

On Users/Perry/Documents/nice, it contains an image of Iguazu Falls, located in South America. This is a possible location Winkler may plan to run to. The location of South America is further confirmed through Autopsy or through the volume shadow copy of the drive (both reach the same results) where an email file is found. Rick, with the IP address 186.210.54.196 located in Brazil, sent the email to Winkler informing him of his current status and their plans. As a conjecture, the location they are running to is South America, most likely Brazil, where the Iguazu Falls is close by so that they can meet up.


Listing  
/img\_LMPD-436243-001.E01/vol3/Users/Perry/Documents/nice

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(t
[current folder]				2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:26:09 EST	2016-02-27 10:25:38 EST	504	Allocat
[parent folder]				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-01-15 16:06:57 EST	56	Allocat
fjreskfes.bmp				2016-02-27 10:26:01 EST	2016-02-27 10:26:09 EST	2016-02-27 10:26:01 EST	2016-02-27 10:26:01 EST	0	Allocat
iguazu-falls.jpg				2016-02-27 09:21:38 EST	2016-02-27 10:25:47 EST	2016-02-27 10:25:47 EST	2016-02-27 09:21:47 EST	496575	Allocat

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0° 22% Reset



## Additional Information/Evidences

The suspect is potentially armed. In Users/Perry/Desktop we have the “in my dreams.jpg” image which shows a firearm. Additionally, in the deleted files, images thCAV3V9F6.jpg, th.jpg, and awesome.jpg also show images of firearms. These files used to be in the same location as Users/Perry/Desktop.



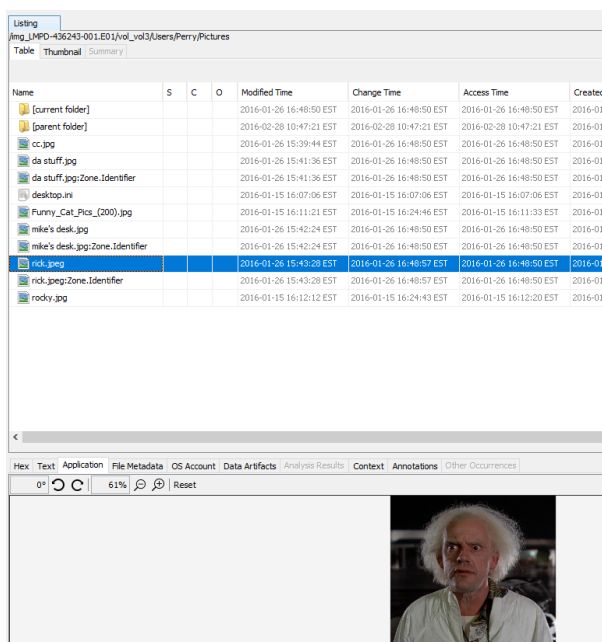
On Users/Perry/Documents/100\_6317 (Small).JPG there is a bottle of unknown items within the toilet tank. This could possibly be another piece of evidence.



On Users/Perry/Contacts, there are three main contacts: Larry Spitz, Rick Shoner, and Mary Reister. Currently there is no information on Larry Spitz and Mary Reister. Mary Reister's contact has also been deleted, which begs the question of whether she is an accomplice. As for Rick Shoner, he is determined to be an accomplice of Winkler through the email correspondence provided in the evidence above.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2016-02-24 17:44:32 EST	2016-02-24 17:44:32 EST	2016-02-24 17:44:32 EST	2016-01-15 16:07:00 EST	56	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
[parent folder]				2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-02-28 10:47:21 EST	2016-01-15 16:06:57 EST	256	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
desktop.ini			0	2016-01-15 16:07:06 EST	2016-01-15 16:07:06 EST	2016-01-15 16:07:00 EST	2016-01-15 16:07:00 EST	412	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
Larry Spitz.contact			0	2016-02-16 17:10:19 EST	2016-02-16 17:10:19 EST	2016-02-16 17:10:19 EST	2016-02-16 17:10:19 EST	1263	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
Mary Reister.contact				2016-02-24 17:44:32 EST	2016-02-24 17:44:32 EST	2016-02-16 17:11:23 EST	2016-02-16 17:11:23 EST	1256	Unallocated	Unallocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
Perry.contact			0	2016-01-15 16:07:00 EST	2016-02-16 17:11:47 EST	2016-01-15 16:07:00 EST	2016-01-15 16:07:00 EST	68374	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts
Rick Shoner.contact			0	2016-02-16 17:09:34 EST	2016-02-24 17:39:19 EST	2016-02-16 17:09:34 EST	2016-02-16 17:09:34 EST	1347	Allocated	Allocated	unknown	/img_LMPD-436243-001.E01/vol3/Users/Perry/Contacts

Lastly, there is a photo named rick.jpeg that can be found on Users/Perry/Pictures. It is unsure if this has any importance or if it is actually Rick's photo which can help us identify the appearance of the accomplice.



## **Tools Used**

A majority of the information were found by using:

- FTK Imager
- Autopsy
- Registry Explorer
- Excel
- Notepad
- Arsenal Image Mounter
- VSCMount