

Table of Contents

Brief Rundown.....	1
Question 1 Response.....	1
Question 2 Response.....	3
Question 3 Response.....	6
Question 4 Response.....	8
Question 5 Response.....	9
Question 6 Response.....	10

Brief Rundown

Throughout this investigation I will be answering 6 questions each listed in the table of contents above. I was able to gather evidence by loading the image on FTK Imager and mounting the image to my desktop workstation to examine/parse files. The dates I give will be in MM-DD-YYYY format.

List of Tools Used: FTK Imager, Registry Explorer, Microsoft Excel, Autopsy, VirusTotal

Question 1 Response

Using Registry Explorer to examine the registry keys of the image, I was able to determine that Perry was the registered owner of the machine that the hard drive was running on. I found this along with other information about the system. Perry was using the Windows 7 Professional Version 6.1 operating system.

Values				
Drag a column header here to group by that column				
Value Name	Value Type	Data	Value Slack	Is Deleted
CurrentVersion	RegSz	6.1	33-00-32-00	
CurrentBuild	RegSz	7601	5C-00	
SoftwareType	RegSz	System	33-00-32-00-5C-00	
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-0A-18-00	
InstallDate	RegDword	1452892015		
RegisteredOrganization	RegSz			
RegisteredOwner	RegSz	Perry	73-00-20-00-55-00-73-00-65-00-72-00-00-00-64-6F	
SystemRoot	RegSz	C:\Windows	00-00-00-00-00-00	
InstallationType	RegSz	Client	00-00-00-00-00-00	
EditionID	RegSz	Professional	2A-01	
ProductName	RegSz	Windows 7 Professional	2A-01-68-05-2A-01	
ProductId	RegSz	00371-177-0000061-85507	00-00-00-00	
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-37-31-2D-31-37-37-2D-30-30-30-...		
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-30-00-33-00-37-00-31-00-2D-00-30-0...		
CurrentBuildNumber	RegSz	7601	74-00	
BuildLab	RegSz	7601.win7m1_rtm.101119-1850	30-00	

Type viewer	Slack viewer	Binary viewer
Value name	RegisteredOwner	
Value type	RegSz	
Value	Perry	

Below is a screenshot that proves Perry has interacted with the machine. Below shows when Perry last accessed and modified the contents in his user directory. C:\Users\Perry

AccessData FTK Imager 4.3.1.1

File View Mode Help

Evidence Tree

- ProgramData
- Recovery
- System Volume Information
- Users
 - All Users
 - Default
 - Default User
 - Perry
 - AppData
 - Application Data
 - Contacts
 - Cookies
 - Desktop
 - Documents
 - Downloads
 - Favorites
 - Links
 - Local Settings
 - Music
 - My Documents
 - NetHood
 - Pictures
 - PrintHood
 - Recent
 - Saved Games

File List

Name	Size	Type	Date Modified
AppData	1	Directory	1/15/2016 9:06:57 PM
Application Data	1	Reparse Point	1/15/2016 9:06:57 PM
Contacts	1	Directory	2/24/2016 10:44:32 PM
Cookies	1	Reparse Point	1/15/2016 9:06:57 PM
Desktop	1	Directory	2/24/2016 10:54:31 PM
Documents	1	Directory	2/28/2016 3:47:37 PM
Downloads	1	Directory	2/24/2016 10:47:45 PM
Favorites	1	Directory	1/15/2016 9:07:08 PM
Links	1	Directory	1/15/2016 9:07:06 PM
Local Settings	1	Reparse Point	1/15/2016 9:06:57 PM
Music	1	Directory	1/15/2016 9:07:06 PM
My Documents	1	Reparse Point	1/15/2016 9:06:57 PM
NetHood	1	Reparse Point	1/15/2016 9:06:57 PM

Properties

Name	Perry
File Class	Directory
File Size	256
Physical Size	256
Date Accessed	2/28/2016 3:47:21 PM
Date Created	1/15/2016 9:06:57 PM
Date Modified	2/28/2016 3:47:21 PM

Question 2 Response

Inside the LMPD-436243-001\Partition 2\NONAME


[NTFS]\[root]\Users\Perry\Pictures folder there are two images that display money and illegal drugs. The images are each titled “da stuff.jpg” and “mike’s desk.jpg”. Inside the Recycle bin there are 3 images found that show guns. The recycle bin directory is found at LMPD-436243-001\Partition 2\NONAME [NTFS]\[root]\\$Recycle.Bin\ S-1-5-21-3461440871-1589894493-1829873476-1000\ which contains the three images. This isn’t conclusive evidence on its own but could assist the police with matching evidence.


File List

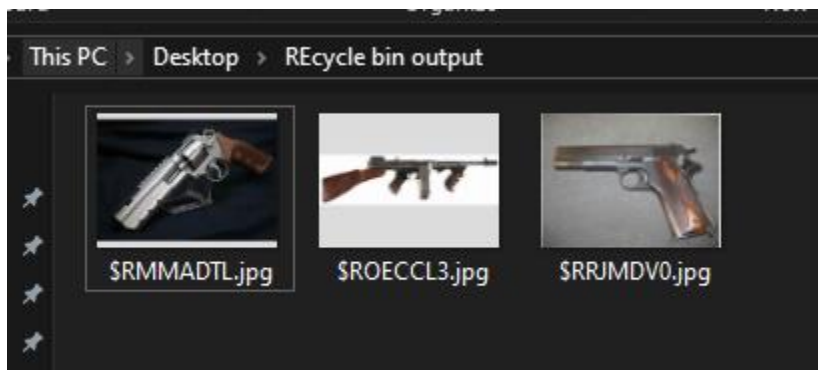
Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	1/26/2016 9:48:50 PM
cc.jpg	10	Regular File	1/26/2016 8:39:44 PM
cc.jpg.FileSlack	3	File Slack	
da stuff.jpg	58	Regular File	1/26/2016 8:41:36 PM
desktop.ini	1	Regular File	1/15/2016 9:07:06 PM
Funny_Cat_Pics_(200).jpg	109	Regular File	1/15/2016 9:11:21 PM
Funny_Cat_Pics_(200).jpg.FileSlack	4	File Slack	
mike's desk.jpg	70	Regular File	1/26/2016 8:42:24 PM
rick.jpg	54	Regular File	1/26/2016 8:43:28 PM
rick.jpg.FileSlack	3	File Slack	
rocky.jpg	61	Regular File	1/15/2016 9:12:12 PM
rocky.jpg.FileSlack	4	File Slack	

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	1/26/2016 9:48:50 PM
cc.jpg	10	Regular File	1/26/2016 8:39:44 PM
cc.jpg.FileSlack	3	File Slack	
da stuff.jpg	58	Regular File	1/26/2016 8:41:36 PM
desktop.ini	1	Regular File	1/15/2016 9:07:06 PM
Funny_Cat_Pics_(200).jpg	109	Regular File	1/15/2016 9:11:21 PM
Funny_Cat_Pics_(200).jpg.FileSlack	4	File Slack	
mike's desk.jpg	70	Regular File	1/26/2016 8:42:24 PM
rick.jpg	54	Regular File	1/26/2016 8:43:28 PM
rick.jpg.FileSlack	3	File Slack	
rocky.jpg	61	Regular File	1/15/2016 9:12:12 PM
rocky.jpg.FileSlack	4	File Slack	







Evidence Tree

[root]

\$BadClus

\$Extend

\$Recycle.Bin

S-1-5-21-3461440871-158989

\$Secure

Documents and Settings

PerfLogs

Program Files

ProgramData

Recovery

System Volume Information

Users

All Users

Default

Default User

Perry

AppData

Application Data

Contacts

Cookies

Desktop

Tor Browser


Documents

Downloads

Favorites

File List

Name	Size	Type	Date Modified
\$INDKRDO.contact	1	Regular File	2/24/2016 10:44:32 PM
\$IOECCL3.jpg	1	Regular File	2/21/2016 10:21:53 PM
\$IRJMDV0.jpg	1	Regular File	2/21/2016 10:21:46 PM
\$ISU8VAG.rtf	1	Regular File	2/28/2016 3:47:37 PM
\$R84694i.jpg	7	Regular File	1/26/2016 9:52:16 PM
\$RMMADTL.jpg	6	Regular File	1/26/2016 9:51:23 PM
\$RNDKRDO.contact	2	Regular File	2/16/2016 10:11:23 PM
\$RNDKRDO.contact.FileSlack	3	File Slack	
\$ROECCL3.jpg	5	Regular File	1/26/2016 9:51:23 PM
\$RRJMDV0.jpg	7	Regular File	1/26/2016 9:51:23 PM
\$RRJMDV0.jpg.FileSlack	2	File Slack	
\$RSU8VAG.rtf	1	Regular File	2/21/2016 10:24:38 PM
desktop.ini	1	Regular File	1/15/2016 9:07:00 PM



The file, LMPD-436243-001\Partition 2\NONAME

[NTFS][root]\Users\Perry\Documents\Letter.rtf was also found which is a document in the form of a letter that is signed by Perry and addressed to Rick. Rick's email is

rickyboy579@aol.com if the police need it and his full name is Rick Shoner. In the letter,

Perry states "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"

desktop.ini

1

Regular File

1/15/2016 9:07:06 PM

Letter.rtf

1

Regular File

2/16/2016 10:08:03 PM

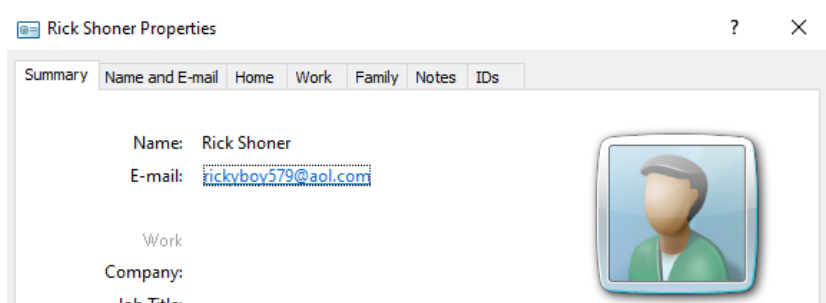
Letter3.rtf

1

Regular File

2/27/2016 3:16:14 PM

```
{\rtf1\ansi\deff0{\fonttbl{\f0\fnil\foharset0 Calibri;}}
{\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\sa200\sl276\slmult1\lang9\fofs22 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 fugure this out.\par
Signed,\par
Perry\par
}
```



The file path LMPD-436243-001\Partition 2\NONAME

[NTFS]\[root]\Users\Perry\Documents\Book2.xlsx is another document in the form of an Excel sheet which could be used to prove illegal dealings. In the screenshot below the Excel document has a list of names with money owed, and favorite type of what is possibly drugs.

	A	B	C	D	E	F	G
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							

Question 3 Response

The file LMPD-436243-001\Partition 2\NONAME

[NTFS]\[root]\Users\Perry\Downloads\Eraser 6.2.0.2970.exe has a hash value that matches the Eraser program which is used to permanently delete files from a machine. I found this out by looking up the MD5 hash value on VirusTotal. The executable was last accessed on 2/21/2016 10:30:07 PM and was created on 2/21/2016 10:30:07 PM and the owner of the executable is Perry.

desktop.ini 1 Regular File 1/15/2016 9:07:06 PM

Eraser 6.2.0.2970.exe 8,143 Regular File 2/21/2016 10:30:23 PM

SDelete.zip 81 Regular File 2/24/2016 10:47:45 PM

SDelete.zip.FileSlack 4 File Slack

torbrowser-install-5.5.3_en-US.exe 42,764 Regular File 1/15/2016 9:19:29 PM

Properties

Archive True

NTFS Information

MFT Record Number 3,748 (3837952)

Date Changed (MFT) 2/21/2016 10:30:23 PM

Resident False

Offline False

Sparse False

Temporary False

Owner SID S-1-5-21-3461440871-158

Owner Name Perry

File distributed by Eraser

14af5f5285081437c5792bac5eba3c9aa868f935f8bb11065e388393ffa2b910

Eraser Setup Bootstrapper

Size 7.95 MB

Last Analysis Date 16 days ago

peexe detect-debug-environment via-tor overlay signed direct-cpu-clock-access checks-user-input known-distributor runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Perry also had Tor Browser installed on the computer which is a browser known to be used to hide traces of user data. This browser is also commonly used to access deep/dark web websites which could possibly be used to buy illegal goods or used to communicate about illegal dealings. Tor Browser is popular for criminals and other purposes due to the application encrypting all web traffic of the user. In both Autopsy and FTK Imager, you can find instances of Tor. In the screenshot below there is Tor's executable and Installer in the run programs portion of the Data Artifacts in Autopsy.

TOR.EXE-AD4EDB11.pf	TOR.EXE	/USERS/PERRY/DESKTOP/TOR BROWSER/BROWSER/T...	2016-01-15 16:20:41 EST	1	Prefetch File	LMPD-436243-001.E01
TORBROWSER-INSTALL-5.5.3_EN-U-E10E4DA8.pf	TORBROWSER-INSTALL-5.5.3_EN-U		2016-01-15 16:20:05 EST	1	Prefetch File	LMPD-436243-001.E01

Using Autopsy, I was also able to sort the web searches in order of the dates they were performed. From 02-16-2016 to 02-24-16 there were numerous web searches relating to ways to get rid of evidence. Here is a screenshot below:

Generate Report Close Case								
Listing								
Web Search								
Table Thumbnail Summary								
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
index.dat				google.com	how	Internet Explorer Analyzer	2016-02-16 22:14:14 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evid	Internet Explorer Analyzer	2016-02-16 22:14:16 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evidence	Internet Explorer Analyzer	2016-02-16 22:14:18 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evidence	Internet Explorer Analyzer	2016-02-16 22:14:18 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evidence	Internet Explorer Analyzer	2016-02-16 22:14:26 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of c evidence	Internet Explorer Analyzer	2016-02-16 22:14:26 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of computer evidence	Internet Explorer Analyzer	2016-02-16 22:14:51 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of computer evidence	Internet Explorer Analyzer	2016-02-16 22:14:51 EST	LMPD-436243-001.E01
index.dat				bing.com	evidence eliminator	Internet Explorer Analyzer	2016-02-21 22:26:23 EST	LMPD-436243-001.E01
index.dat				bing.com	evidence eliminator	Internet Explorer Analyzer	2016-02-21 22:26:23 EST	LMPD-436243-001.E01
index.dat				bing.com	eraser	Internet Explorer Analyzer	2016-02-21 22:26:51 EST	LMPD-436243-001.E01
index.dat				bing.com	eraser	Internet Explorer Analyzer	2016-02-21 22:26:51 EST	LMPD-436243-001.E01
index.dat				bing.com	get rid of files	Internet Explorer Analyzer	2016-02-21 22:27:56 EST	LMPD-436243-001.E01
index.dat				bing.com	get rid of files	Internet Explorer Analyzer	2016-02-21 22:27:56 EST	LMPD-436243-001.E01
index.dat				bing.com	eraser	Internet Explorer Analyzer	2016-02-24 22:39:02 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evidence	Internet Explorer Analyzer	2016-02-24 22:39:02 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of computer evidence	Internet Explorer Analyzer	2016-02-24 22:39:02 EST	LMPD-436243-001.E01
index.dat				bing.com	evidence eliminator	Internet Explorer Analyzer	2016-02-24 22:39:02 EST	LMPD-436243-001.E01
index.dat				bing.com	eraser	Internet Explorer Analyzer	2016-02-24 22:39:03 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of evidence	Internet Explorer Analyzer	2016-02-24 22:39:03 EST	LMPD-436243-001.E01
index.dat				google.com	how to get rid of computer evidence	Internet Explorer Analyzer	2016-02-24 22:39:03 EST	LMPD-436243-001.E01
index.dat				bing.com	get rid of files	Internet Explorer Analyzer	2016-02-24 22:39:03 EST	LMPD-436243-001.E01
index.dat				bing.com	evidence eliminator	Internet Explorer Analyzer	2016-02-24 22:39:03 EST	LMPD-436243-001.E01
index.dat				bing.com	what is a batch file	Internet Explorer Analyzer	2016-02-24 22:44:44 EST	LMPD-436243-001.E01

After using web searches, I went ahead and looked into the web history and found multiple instances of Perry using websites such as ehov and Wikiphow which hosted content relating to deleting evidence off of computers. Screenshot below:

index.dat		http://www.ehow.com/how_4676367_remove-traces-activity-computer.html&rc=j&frm=1&q=...	2016-02-16 22:15:09 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	http://www.ehow.com/how_4676367_remove-traces-activity-computer.html	2016-02-16 22:15:13 EST	Internet Explorer Analyzer	ehow.com	LMPD-436243-001.E01	Perry
index.dat	0	http://www.bing.com/search?q=eraser&src=IE-SearchBox&FORM=IE8SRC	2016-02-21 22:26:51 EST	Internet Explorer Analyzer	bing.com	LMPD-436243-001.E01	Perry
index.dat	0	http://commandwindows.com/favicon.ico	2016-02-24 22:45:09 EST	Internet Explorer Analyzer	commandwindows.com	LMPD-436243-001.E01	Perry
index.dat	0	http://www.bing.com/search?q=how+to+set+up+scheduled+task&src=IE-SearchBox&FORM=...	2016-02-24 22:45:11 EST	Internet Explorer Analyzer	bing.com	LMPD-436243-001.E01	Perry
index.dat		file/Users/Perry/Downloads/SDelete.zip	2016-02-24 22:47:45 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	http://www.gametop.com/category/helicopter.html	2016-02-24 22:53:09 EST	Internet Explorer Analyzer	gametop.com	LMPD-436243-001.E01	Perry
index.dat	0	http://www.gametop.com/download-free-games/big-air-war/download.html	2016-02-24 22:53:18 EST	Internet Explorer Analyzer	gametop.com	LMPD-436243-001.E01	Perry
index.dat		http://www.wikihow.com/Hide-Evidence-on-a-Computer&rc=j&frm=1&q=&esrc=s&sa=U&v=...	2016-02-16 22:14:42 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat		file/Users/Perry/Videos/Untitled.png	2016-01-26 21:46:42 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	https://dl-web.dropbox.com/installer?juno=True&juno_use_program_files=True&build_no=3.1...	2016-02-24 22:56:37 EST	Internet Explorer Analyzer	dropbox.com	LMPD-436243-001.E01	Perry
index.dat	0	https://download.sysinternals.com/files/SDelete.zip	2016-02-24 22:47:45 EST	Internet Explorer Analyzer	sysinternals.com	LMPD-436243-001.E01	Perry
index.dat	0	http://www.aol.com/	2016-01-15 21:15:19 EST	Internet Explorer Analyzer	aol.com	LMPD-436243-001.E01	Perry
index.dat	0	http://commandwindows.com/batch.htm	2016-02-24 22:45:09 EST	Internet Explorer Analyzer	commandwindows.com	LMPD-436243-001.E01	Perry
index.dat	0	http://static-hp-eus.s-msn.com/sc/2b/a5ea21.ico	2016-02-21 22:25:45 EST	Internet Explorer Analyzer	s-msn.com	LMPD-436243-001.E01	Perry
index.dat		file/car1.jpg	2016-02-16 22:03:25 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	http://www.ehow.com/feed/ehow-tech.rss	2016-02-16 22:15:12 EST	Internet Explorer Analyzer	ehow.com	LMPD-436243-001.E01	Perry
index.dat	0	http://ccm.net/rss	2016-02-21 22:26:38 EST	Internet Explorer Analyzer	ccm.net	LMPD-436243-001.E01	Perry
index.dat	0	http://www.bing.com/search?q=helicopter+game+download&src=IE-SearchBox&FORM=IE8S...	2016-02-24 22:53:02 EST	Internet Explorer Analyzer	bing.com	LMPD-436243-001.E01	Perry
index.dat		file/Users/Perry/Desktop/th.jpg	2016-02-16 22:13:30 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	https://www.southwest.com	2016-02-24 22:58:45 EST	Internet Explorer Analyzer	southwest.com	LMPD-436243-001.E01	Perry
index.dat	0	http://eraser.heidi.ie/feed	2016-02-21 22:27:19 EST	Internet Explorer Analyzer	heidi.ie	LMPD-436243-001.E01	Perry
index.dat	0	http://www.bing.com/search?format=rss&q=eraser&src=IE-SearchBox&FORM=IE8SRC	2016-02-21 22:26:51 EST	Internet Explorer Analyzer	bing.com	LMPD-436243-001.E01	Perry

Question 4 Response

In Autopsy, there are two external USBs listed with a SanDisk Cruzer being used on 01-26-2016 with a Kingston DataTraveler by Toshiba being used recently on 02-28-2016. If any USB drives of these brands are found by the police, they should be examined in case they have evidence on them. The Kingston DataTraveler is the one most necessary since it's been used most recently

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 4 of 8 Result < >									
USB Device Attached									
Type	Value								Source(s)
Date/Time	2016-02-28 10:45:52 EST								Recent Activity
Device Make	Toshiba Corp.								Recent Activity
Device Model	Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick								Recent Activity
Device ID	0013729B678DEB20C51F0216								Recent Activity
Source File Path	/img_LMPD-436243-001.E01/vol_vol3/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854775661								

Type	Value								Source(s)
Date/Time	2016-01-26 16:48:11 EST								Recent Activity
Device Make	SanDisk Corp.								Recent Activity
Device Model	Cruzer								Recent Activity
Device ID	20035001811625714CA7								Recent Activity
Source File Path	/img_LMPD-436243-001.E01/vol_vol3/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854775662								

Question 5 Response

In a letter found in the recycle bin specifically at LMPD-436243-001\Partition 2\NONAME [NTFS]\[root]\\$Recycle.Bin\ S-1-5-21-3461440871-1589894493-1829873476-1000\ Perry speaks about ditching a place and is signed by himself. Similarly to the letter mentioned in Question 2, Perry addresses the message to Rick. Based off of the information below, we can conclude that Rick could be travelling with Perry but this is only a possibility. Letter contents: “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”

After this letter, there was a third letter written from Perry to Rick with Perry expressing concern about not receiving communication from Ricky. This letter could be used as additional evidence that Rick was at the very least, assisting Perry with travelling somewhere. Letter contents is found at this file path LMPD-436243-001\Partition 2\NONAME [NTFS]\[root]\Users\Perry\DocumentsLetter3.rtf and is shown below: “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 showd 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

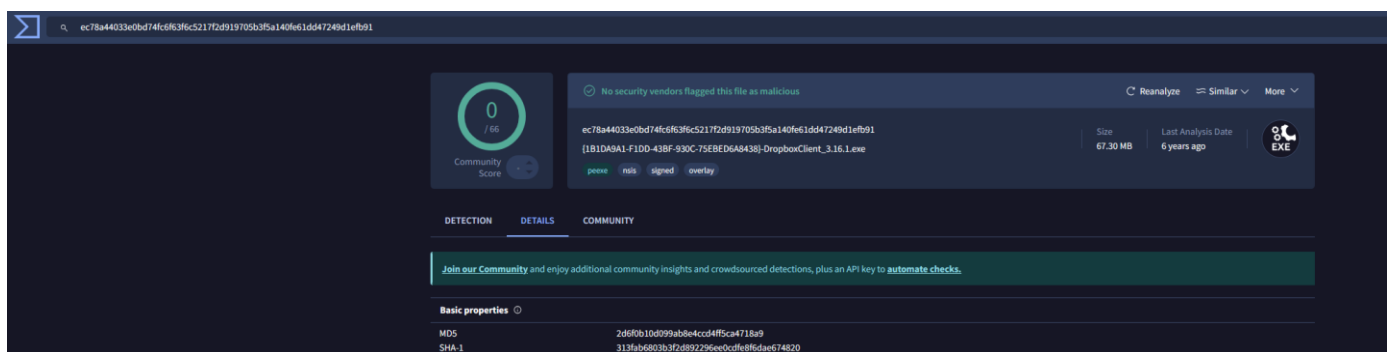
perry\par”

Question 6 Response

Another application the user had installed was Dropbox which is a cloud storage utility that could be used to store files outside of the machine or to share files with individuals or groups. The police could collaborate with Dropbox to gather additional findings. Dropbox is found in the Run Programs on the image loaded into Autopsy:

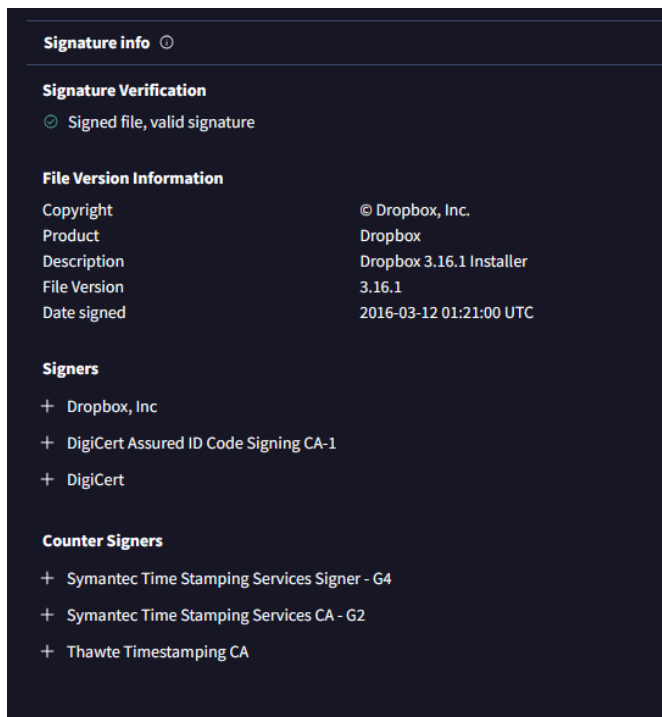
✓ DROPBOX.EXE-CD6685AF.pf		DROPBOX.EXE	/PROGRAM FILES/DROPBOX/CLIENT_3.16.1	2016-02-24 17:58:41 EST	1	Prefetch File	LMPD-436243-001.E01
✓ DROPBOX.EXE-F5354AA9.pf		DROPBOX.EXE	/PROGRAM FILES/DROPBOX/CLIENT	2016-02-24 17:58:55 EST	2	Prefetch File	LMPD-436243-001.E01
✓ DROPBOXCLIENT_3.16.1.EXE-491B5A82.pf		DROPBOXCLIENT_3.16.1.EXE		2016-02-24 17:58:30 EST	1	Prefetch File	LMPD-436243-001.E01

I copied the MD5 hash value of DROPBOXCLIENT_3.16.1.exe and loaded into VirusTotal which verified that the file was indeed an executable from Dropbox, Inc.



The screenshot shows the VirusTotal web interface for the file `DropboxClient_3.16.1.exe`. The file's MD5 hash is `ec78a44033e0bd74fc6b3f6c5217d2919705b3f5a140fe1d47249d1efb91`. The interface indicates that no security vendors have flagged this file as malicious. The file is 67.30 MB in size and was last analyzed 6 years ago. The basic properties section shows the MD5 hash as `2d6f0b10d099ab9e4cd4ff5ca471ba9` and the SHA-1 hash as `313fab6803b3f2d892296e0cfe8f6dae674820`.

Property	Value
MD5	2d6f0b10d099ab9e4cd4ff5ca471ba9
SHA-1	313fab6803b3f2d892296e0cfe8f6dae674820



At LMPD-436243-001\Partition 2\NONAME

[NTFS][root]\Users\Perry\Pictures\rick.jpeg there is also an image that is titled “rick”. This image could be of the person who Perry was speaking to in the emails and could help the police locate Rick if needed. As stated earlier, Rick’s email address is rickyboy579@aol.com.



On 02-24-2016 at 22:58:45 EST, Perry also visited the website of Southwest Airlines at <https://www.southwest.com>. If Perry and/or Rick travelled via airline, they likely used the service of Southwest Airlines and the police should reach out to Southwest Airlines for more information. This screenshot was found via Autopsy.

index.dat		file/Users/Perry/Desktop/th.jpg	2016-02-16 22:13:30 EST	Internet Explorer Analyzer		LMPD-436243-001.E01	Perry
index.dat	0	https://www.southwest.com	2016-02-24 22:58:45 EST	Internet Explorer Analyzer	southwest.com	LMPD-436243-001.E01	Perry
index.dat	0	http://eraser.heidi.ie/feed	2016-02-21 22:27:19 EST	Internet Explorer Analyzer	heidi.ie	LMPD-436243-001.E01	Perry
index.dat	0	http://www.bing.com/search?format=rss&q=eraser&src=IE-SearchBox&FORM=IE8SRC	2016-02-21 22:26:51 EST	Internet Explorer Analyzer	bing.com	LMPD-436243-001.E01	Perry

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 21 of 78 Result									

Visit Details	
Username:	Perry
Date Accessed:	2016-02-24 22:58:45 EST
Domain:	southwest.com
URL:	https://www.southwest.com
Program Name:	Internet Explorer Analyzer

Source	
Host:	LMPD-436243-001.E01_1 Host
Data Source:	LMPD-436243-001.E01
File:	/img_LMPD-436243-001.E01/vol3/Users/Perry/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat