

Project 4

Perry Winkler Computer Examination

LMPD Detective

Lawrence Pumphrey IV

## *Case Background*

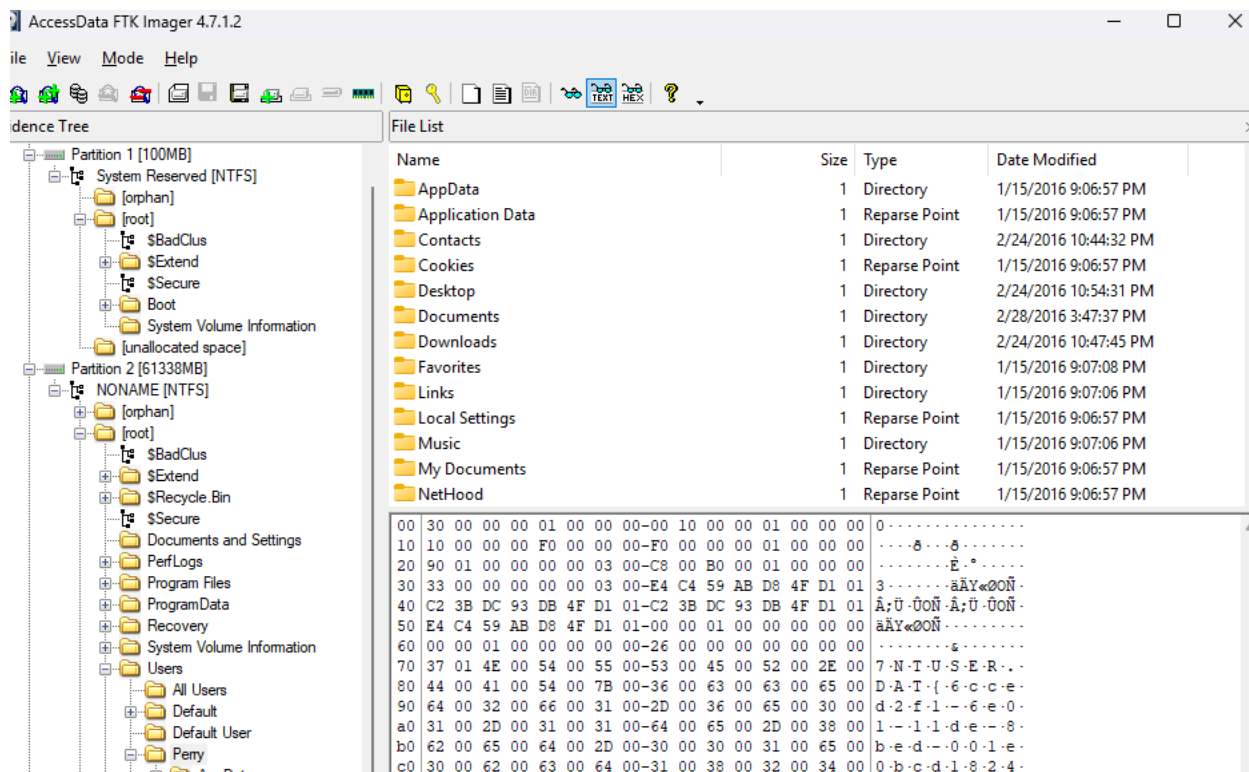
I have been tasked with investigating a computer found in a dumpster behind Perry Winkler's abandoned residence. After LMPD obtained a warrant to search Winkler's residence, nothing was found except for the damaged computer. There is no sign of Winkler or any evidence aside from what I was able to pull from the computer's hard drive. Using the FTK Imager initially to locate as much information as possible, while I used Autopsy to perform a forensic autopsy on the file. Autopsy displays the same information as FTK Imager and much more. FTK Imager allows me to manually sort through files throughout the hard drive in an evidence tree, while Autopsy allows me to manually sort that information as well as perform its analysis for me to view. These are the 2 tools I used to perform my examination and will be referenced throughout the report.

*Question 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 been used by Perry Winkler?*

To answer the question of who owns this computer and did Perry Winkler ever used the computer was simple. The computer belongs to Perry Winkler and is named "PERRYWINKLER-PC". All of this information was found by using FTK Imager to inspect the provided disk image. In FTK Imager, once the file is properly loaded and the evidence tree is present, under **Partition 2**→**Root**→**Users** there is a folder named "Perry". This folder is very important to the rest of the case as it contains a large amount of evidence that will be referenced

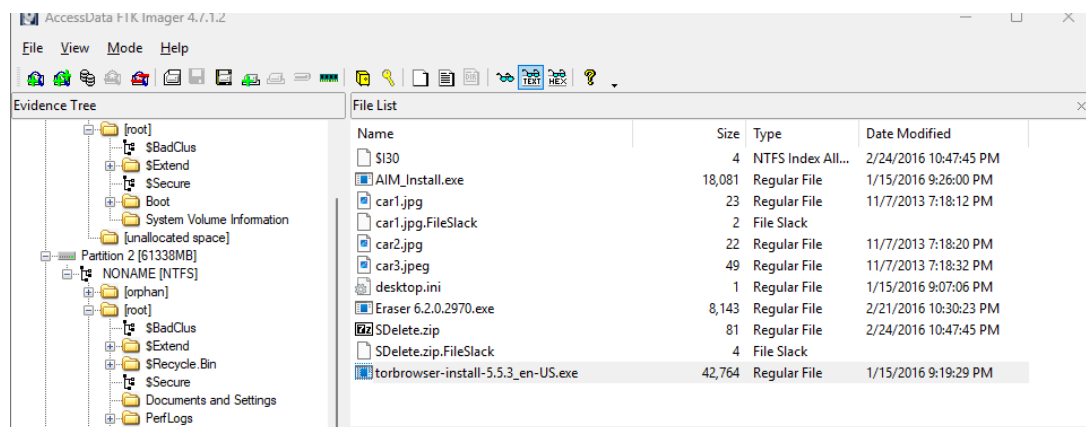
later in the report. Alternatively, in several files' metadata, the device is referenced as PERRYWINKLER-PC like below.

```
Windows Update
C:\Windows\
PERRYWINKLER-PC
WORKGROUP
?kDK
\\?\Volume{094cd53b-bbe4-11e5-b7db-806ef6e6963}\
\\?\Volume{094cd53b-bbe4-11e5-b7db-806ef6e6963}\
(C:)
```



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

Revisiting the “Perry” folder under “user”, as previously mentioned, has a large amount of evidence. You can find this folder in FTK Imager by going to **Partion 2→root→Users\Perry\Downloads**. My thought process behind this part of the investigation is that I just found what would be my file explorer when searching through the “Perry” folder. This helped me to better navigate and understand what I’m looking at/for. In the downloads folder, 3 specific .exe files point to some sort of illegal activity. Tor Browser was one and it reroutes network traffic through various IPs to essentially hide anything the user is searching. While the main use has been for accessing the dark web and searching for illegal things, there are other uses like going around a country's censorship to view the internet. However, the other 2 files, Sdelete and Eraser, both work on removing data from unallocated, allocated, or hard drive space. It’s more likely that Tor Browser was installed to not leave a trail when searching and the other two to delete any evidence that may be left behind.



Moving to the documents folder(**Partion 2→root→Users\Perry\Documents**) there are several incriminating files including Book2.xlsx, which is an Excel file that seems to have a list of names, how much money they owe, and their drug of choice. What makes this document interesting is that a user “Lars” made the last edit on this document. The identity of Lars has not

been found yet, but it's reasonably believed to be Larry Spitz who is one of the other contacts on Perry's computer.

Sheet1

name	\$\$ owed	fav
MC Teller	450	tails
ronchop	500	angel
newbber	950	crack
nile	100	header
p dawg	50	lice
randy	1040	erthing

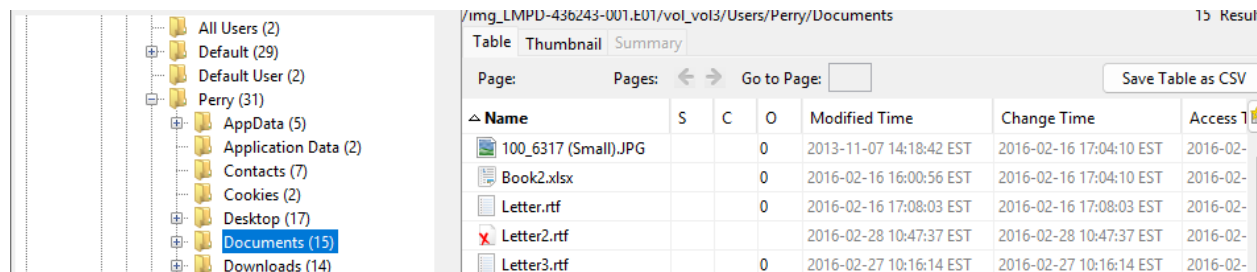
Sheet2

Sheet3

-----METADATA-----

Application-Name: Microsoft Excel  
Application-Version: 12.0000  
Author: perry  
Content-Type: application/vnd.openxmlformats-officedocument.spreadsheetml.sheet  
Creation-Date: 2010-07-22T14:00:10Z  
Last-Author: Lars

There are also 2.rtf files named Letter and Letter3, along with a contact for Rick Shoner inside the documents folder. Later, doing some snooping in the recycling bin(**Partion 2**→ **root** → **\$Recycle.Bin**) I came across Letter2. When I began examining the files on Autopsy Letter2 showed with the other documents, but was denoted as delete/in the recycling bin within the documents folder. Transcripts for Letter, Letter2, and Letter 3 are provided through the Autopsy tool below:



The screenshot shows the Autopsy tool interface. On the left, a file system tree is displayed with the following structure:

- All Users (2)
- Default (29)
- Default User (2)
- Perry (31)
  - AppData (5)
  - Application Data (2)
  - Contacts (7)
  - Cookies (2)
  - Desktop (17)
  - Documents (15)
  - Downloads (14)

The 'Documents' folder is selected. On the right, a table lists the files in the Documents folder:

Name	S	C	O	Modified Time	Change Time	Access Time
100_6317 (Small).JPG			0	2013-11-07 14:18:42 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST
Book2.xlsx			0	2016-02-16 16:00:56 EST	2016-02-16 17:04:10 EST	2016-02-16 17:04:10 EST
Letter.rtf			0	2016-02-16 17:08:03 EST	2016-02-16 17:08:03 EST	2016-02-16 17:08:03 EST
Letter2.rtf				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST
Letter3.rtf			0	2016-02-27 10:16:14 EST	2016-02-27 10:16:14 EST	2016-02-27 10:16:14 EST

**Letter.rtf:** 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

**Letter2.rtf:** 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

**Letter3.rtf:** 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 supposed to be all prepaid too so we are set! lol well i hope your safe and will look for your email.

Sincerely,

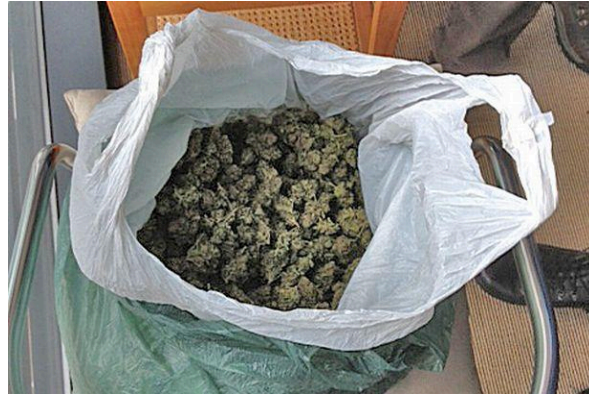
Perry

Based on the evidence provided it is safe to treat Rick as an accomplice. The specifics behind his role are not known yet but the involvement is there. Rick helps Perry get rid of the evidence as well as provides information on the next steps to escape. In Letter3 Perry says he purchased

credit cards that Rick told him to purchase. An image of those cards was found amongst several other incriminating images including one called da stuff.png and mikes desk.png that display drugs.



Cc.png



da stuff.png



mikes desk.png - Taken with Canon Powershot A60

As I mentioned earlier the recycling bin contained letter 2.rtf but there was other evidence in the same location. There was a deleted contact for Mary Reister who at this time I can't find any

other information aside from the contact information. Several images of firearms are present in the recycling bin as well.

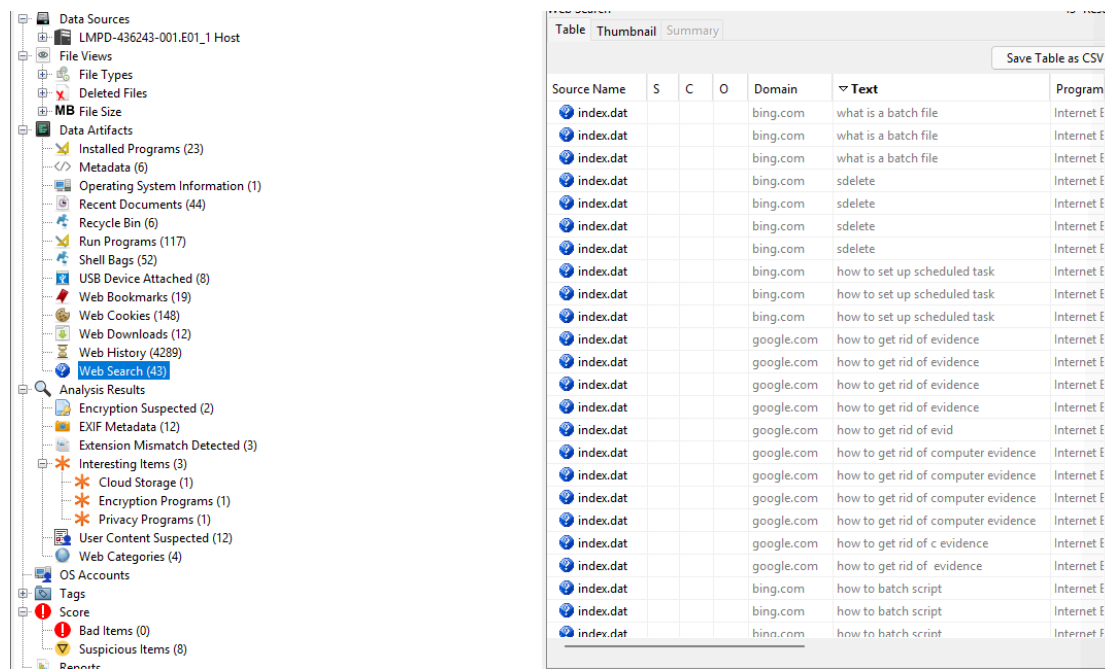


*3. Is there any evidence that the user may have been trying to cover their tracks or delete evidence from the computer?*

The installation of Sdelete and Eraser tools is clear enough evidence for covering their tracks and deleting evidence. The tools were mentioned earlier but neither received in-depth description or their features. Sdelete is a command line tool that deletes files and erases data from unallocated space. Eraser is a tool that removes sensitive data from hard drives on a computer. These 2 tools



on their own are evidence enough to prove that Perry was trying to clear his tracks and delete evidence. In the 3 letter files, he is also talking to Rick about destroying evidence in the bathroom and kitchen as well as what to do with the computer. Upon my examination using autopsy, there were 43 web searches and the majority had to do with deleting, erasing, or destroying evidence. As Perry progressed in finding the answers to destroying evidence, the questions he was asking began to change but they all are connected. Sdelete being a command line utility likely required Perry to learn how to batch script which correlates the searches of “What is a batch file” and “How to batch script”. For Eraser to regularly delete files you have to install a scheduling agent to make the task for Eraser. This correlates the “How to set up scheduled task” search to the Eraser search and program being installed.



The screenshot shows the Autopsy software interface. On the left is a sidebar with a tree view of data sources and file views. The 'Web Search' category is selected, showing 43 results. On the right is a table of search results. The table has columns for Source Name, S, C, O, Domain, Text, and Program. The results show multiple instances of 'index.dat' files from 'bing.com' and 'google.com' with search terms related to batch files, sdelete, and scheduled tasks.

Source Name	S	C	O	Domain	Text	Program
index.dat				bing.com	what is a batch file	Internet E
index.dat				bing.com	what is a batch file	Internet E
index.dat				bing.com	what is a batch file	Internet E
index.dat				bing.com	sdelete	Internet E
index.dat				bing.com	sdelete	Internet E
index.dat				bing.com	sdelete	Internet E
index.dat				bing.com	sdelete	Internet E
index.dat				bing.com	how to set up scheduled task	Internet E
index.dat				bing.com	how to set up scheduled task	Internet E
index.dat				bing.com	how to set up scheduled task	Internet E
index.dat				google.com	how to get rid of evidence	Internet E
index.dat				google.com	how to get rid of evidence	Internet E
index.dat				google.com	how to get rid of evidence	Internet E
index.dat				google.com	how to get rid of evid	Internet E
index.dat				google.com	how to get rid of computer evidence	Internet E
index.dat				google.com	how to get rid of computer evidence	Internet E
index.dat				google.com	how to get rid of computer evidence	Internet E
index.dat				google.com	how to get rid of computer evidence	Internet E
index.dat				google.com	how to get rid of c evidence	Internet E
index.dat				google.com	how to get rid of evidence	Internet E
index.dat				bing.com	how to batch script	Internet E
index.dat				bing.com	how to batch script	Internet E
index.dat				bing.com	how to batch script	Internet E

Source Name	S	C	O	Domain	▼ Text	Program
index.dat				google.com	how to get rid of c evidence	Internet E
index.dat				google.com	how to get rid of evidence	Internet E
index.dat				bing.com	how to batch script	Internet E
index.dat				bing.com	how to batch script	Internet E
index.dat				bing.com	how to batch script	Internet E
index.dat				google.com	how	Internet E
index.dat				bing.com	helicopter game download	Internet E
index.dat				bing.com	helicopter game download	Internet E
index.dat				bing.com	helicopter game download	Internet E
index.dat				bing.com	helicopter game download	Internet E
index.dat				bing.com	get rid of files	Internet E
index.dat				bing.com	get rid of files	Internet E
index.dat				bing.com	get rid of files	Internet E
index.dat				bing.com	evidence eliminator	Internet E
index.dat				bing.com	evidence eliminator	Internet E
index.dat				bing.com	evidence eliminator	Internet E
index.dat				bing.com	evidence eliminator	Internet E
index.dat				bing.com	eraser	Internet E
index.dat				bing.com	eraser	Internet E
index.dat				bing.com	eraser	Internet E
index.dat				bing.com	eraser	Internet E
index.dat				bing.com	download dropbox	Internet E
index.dat				bing.com	download dropbox	Internet E
index.dat				bing.com	download dropbox	Internet E

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.

There are 8 USB devices attached:

1. VMware USB Hub - This is likely to be either item 4 or 5 aligning with the same process items 6-8 being introduced to a virtual environment.

Items 2 and 3 are both USB Flash drive devices. Both only holding a few gigabytes of space could still be packed with a large amount of evidence. If any USB devices could be of high importance it would be one of these two.

2. Toshiba Corp Kingston DataTraveler 102/2.0 / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick
3. SanDisk Corp. Cruzer

Items 4 and 5 are USB Root Hubs which have several USB ports and allow for devices to properly be read by the computer.

4. ROOT\_HUB20 - 5&299e1c9f&0
5. ROOT\_HUB - 5&3bb57b&0

Items 6-8 are each a USB Mouse that was used in VMware. Having a mouse hooked up to a device doesn't always mean it will be connected when working inside a virtual environment like VMware so you have to sync it. Given that each of the devices have different ID's they are probably 3 different devices that have been used.

6. VMware Virtual Mouse - 6&b77da92&0&1
7. VMware Virtual Mouse - 7&2a7d3009&0&0000
8. VMware Virtual Mouse - 7&2a7d3009&0&0001

*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)?*

I located a file in the same documents folder(**Partion 2→root→Users\Perry\Documents**) as mentioned several times throughout the report. There was a folder called “emails” and inside there was an encrypted file “plan.zip” that I was unable to open but somebody with more skills in encryption from the department should easily be able to access it. On the entire drive, it was the only file encrypted to this extent that I came across. While I cannot open the document to see its contents, it being the only zip file of its type on the drive isn’t a coincidence. I believe Rick Shoner and Larry Spitz are both accomplices with Rick leaning more into the head honcho role. Seeing as Perry has constantly asked Rick for help and the next steps in Letter, Letter2, and Letter3 in addition to another I found using autopsy searching through emails between Rick and Perry. In this email, Rick is writing to black which in the past has been Perry writing to Rick. He tells Perry he landed and is using a hotel lobby computer to send the email. He also tells Perry he will wire him money to his Western Union account, to destroy any remaining evidence, board the United flight as they discussed, and he will see him soon. It is evident that Rick and Perry are working together and likely fleeing together.

Listing

ickyboy579@aol.com

5 Results

Table

Thumbnail






Summary



Page: 1 of 1

Pages: < >

Go to Page:

Save Table as CSV

Source Name	S	C	O	Keyword	Keyword R
 f0252768.mbox				rickyboy579@aol.com	(\{?)[a-zA-Z]
 Rick Shoner.contact				rickyboy579@aol.com	(\{?)[a-zA-Z]
 Unalloc_134478_106102784_6900195328			0	rickyboy579@aol.com	(\{?)[a-zA-Z]
 Rick Shoner.contact				rickyboy579@aol.com	(\{?)[a-zA-Z]
 f0252768.mbox				rickyboy579@aol.com	(\{?)[a-zA-Z]

Data Artifacts		Analysis Results	Context	Annotations	Other Occurrences
Hex	Text	Application	File Metadata		OS Account
Strings	Extracted Text	Translation			
Page: 1 of 1	Page	 	Go to Page:		Script: Latin - Basic
<p>Received: from mta.email.aol.com (mta.email.aol.com [74.124.68.45]) by mta.in-mf01.r1000.mx.aol.com (Partner Internet Inbound) with ESMTP id DA9533800046A for &lt;perrywin232k@aol.com&gt;; Sun, 28 Feb 2016 09:08:15 -0500 (EST)</p> <p>Received: from [186.210.54.196] ([186.210.54.196:2269] helo=THDMMTA25PUMP3) by pc1udsmta1n25 (envelope-from &lt;rickyboy579@aol.com&gt;) (ecelerity 2.2.2.45 r(34222M)) with ESMTP id 57/7A-18696-E5614725; Sun, 28 Feb 2016 07:07:14 -0300</p> <p>Date: Sun, 28 Feb 2016 09:08:16 -0500 (EST)</p> <p>Message-Id: &lt;Kilauea216670-69235-1739513301-2-1024@flonetwork.com&gt;</p> <p>From: "P Dawg" &lt;rickyboy579@aol.com&gt;</p> <p>Reply-To: "Rick Shoner" &lt;rickyboy579@aol.com&gt;</p> <p>To: perrywin232k@aol.com</p> <p>Subject: it's time</p> <p>MIME-Version: 1.0</p> <p>Content-Type: text/plain; charset=us-ascii</p> <p>Content-Transfer-Encoding: 7bit</p> <p>X-From: Rick Shoner</p> <p>X-To: Perry Winkler</p> <p>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.</p>					

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)?

The encrypted file “plan.zip” has information in the OS account using Autopsy that tells the password, a hint, settings, and more information that if I was stronger in encryption I believe I could open. Other examiners who are much more familiar with this field given this information could/should be able to decrypt this file. I’ll note that Rick Shoner is likely to know the whereabouts of Perry Wilkins. What we’ve learned about Rick from Perry’s PC alone is enough to begin an investigation into him as an accomplice. The other contacts Larry Spitz and Mary Reister would be worth looking into. In the Book2.xlsx file Lars is the name of the last author which could potentially be Larry Spitz and Mary’s contact info was deleted alongside other evidence in the recycling bin. All 3 have their contacts with their emails highlighted and a picture of the man believed to be Rick. You can find these contacts in FTK Imager by going to

**Partion 2 → root → Users\Perry\Contacts.**

Name	Size	Type
plan.zip	1	Reg
plan.zip.FileSlack	4	File

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	2/24/2016 10:44:32 PM
desktop.ini	1	Regular File	1/15/2016 9:07:06 PM
Larry Spitz.contact	2	Regular File	2/16/2016 10:10:19 PM
Larry Spitz.contact.FileSlack	3	File Slack	
Perry.contact	67	Regular File	1/15/2016 9:07:00 PM
Perry.contact.FileSlack	2	File Slack	
Rick Shoner.contact	2	Regular File	2/16/2016 10:09:34 PM
Rick Shoner.contact.FileSlack	3	File Slack	

Name	S	C	O	Modified Time	Change Time	Access Time
plan.zip			0	2016-02-28 10:47:53 EST	2016-02-28 10:48:38 EST	2016-02-28 10:47:53 EST
[parent folder]				2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST	2016-02-28 10:47:37 EST
[current folder]				2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST	2016-02-28 10:49:13 EST

Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Hex	Text	Application	File Metadata	OS Account
<b>Basic Properties</b> Login: Perry Full Name: Address: S-1-5-21-3461440871-1589894493-1829873476-1000 Type: Creation Date: 2016-01-15 16:06:54 EST Object ID: 199  <b>LMPD-436243-001.E01_1 Host Details</b> Last Login: 2016-02-28 10:45:38 EST Login Count: 9 Administrator: True Password Hint: it's your name, idiot Password Fail Date: 2016-02-24 17:50:54 EST Password Settings: Password does not expire, Password not required Flag: Normal user account Home Directory: C:/Users/Perry  <b>Realm Properties</b> Name: Unknown Address: S-1-5-21-3461440871-1589894493-1829873476 Scope: Domain Confidence: Known				

**Book2.xlsx Properties**  
 General Digital Signatures Security Details Previous Versions

Property	Value
<b>Description</b>	
Title	
Subject	
Tags	
Categories	
Comments	
<b>Origin</b>	
Authors	perry
Last saved by	Lars
Revision number	
Version number	
Program name	Microsoft Excel
Company	
Manager	
Content created	7/22/2010 10:00 AM
Date last saved	7/22/2010 10:00 AM
Last printed	
<b>Content</b>	

**Mary Reister** - <?xml version="1.0" encoding="UTF-8"?>

```
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:MSP2P="http://schemas.microsoft.com/Contact/Extended/MSP2P">
  <c:CreationDate>2016-02-16T22:10:39Z</c:CreationDate><c:Extended xsi:nil="true"/>
  <c:ContactIDCollection><c:ContactID
c:ElementID="1e41b2db-4868-4701-adfc-20f4fca75e19"><c:Value>2db4c467-5551-4a17-bee0-
59880ce29f13</c:Value></c:ContactID></c:ContactIDCollection><c:EmailAddressCollection><c
:EmailAddress
c:ElementID="a1b7491e-10a8-4728-b0c2-9ec0e39fb66b"><c:Type>SMTP</c:Type><c:Address
>mreister@gmail.com</c:Address><c:LabelCollection><c:Label>Preferred</c:Label></c:Label
Collection></c:EmailAddress><c:EmailAddress
c:ElementID="5224881f-5fd4-4815-a2af-76a658fba437"
xsi:nil="true"/></c:EmailAddressCollection><c:NameCollection><c:Name
c:ElementID="376245a8-8f65-41ec-b23b-97db03337fbb"><c:FormattedName>Mary
Reister</c:FormattedName><c:FamilyName>Reister</c:FamilyName><c:GivenName>Mary</c:
GivenName></c:Name></c:NameCollection><c:PhotoCollection><c:Photo
c:ElementID="4d12c2aa-3695-41b7-b516-505b49eb25a9"><c:LabelCollection><c:Label>UserTi
le</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection></c:contact>
```

**Larry Spitz/Lars** - <?xml version="1.0" encoding="UTF-8"?>

```
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:MSP2P="http://schemas.microsoft.com/Contact/Extended/MSP2P">
  <c:CreationDate>2016-02-16T22:09:43Z</c:CreationDate><c:Extended xsi:nil="true"/>
```

```

<c:ContactIDCollection><c:ContactID
c:ElementID="0542ea04-b98f-49ac-9ecd-6cafb00fea83"><c:Value>734b61aa-62ef-4487-a12b-
da69761d838a</c:Value></c:ContactID></c:ContactIDCollection><c:EmailAddressCollection><
c:EmailAddress
c:ElementID="1bdf1a1b-c7e1-4b25-8d57-160bc9f654de"><c:Type>SMTP</c:Type><c:Address
>spitzmeister@rocketmail.com</c:Address><c:LabelCollection><c:Label>Preferred</c:Label
></c:LabelCollection></c:EmailAddress><c:EmailAddress
c:ElementID="8580ea4a-528a-43c8-85b0-bf5481eb7d28"
xsi:nil="true"/></c:EmailAddressCollection><c:NameCollection><c:Name
c:ElementID="5bbcec18-5742-4e29-8518-21ee53ffbd04"><c:FormattedName>Larry
Spitz</c:FormattedName><c:FamilyName>Spitz</c:FamilyName><c:GivenName>Larry</c:Giv
enName></c:Name></c:NameCollection><c:PhotoCollection><c:Photo
c:ElementID="e77d1e03-7344-47f9-b3f2-0277ef7a7986"><c:LabelCollection><c:Label>User Tile
</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection></c:contact>

```

```

Rick Shoner/Master Rick - <?xml version="1.0" encoding="UTF-8"?>
<c:contact c:Version="1" xmlns:c="http://schemas.microsoft.com/Contact"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:MSP2P="http://schemas.microsoft.com/Contact/Extended/MSP2P">
  <c:CreationDate>2016-02-16T22:08:36Z
</c:CreationDate><c:Extended xsi:nil="true"/>
  <c:ContactIDCollection><c:ContactID
c:ElementID="1dbfd5b8-0e14-4c41-8f38-9a529f658fb0"><c:Value>37aa335b-09c1-4c05-ad3a-
2a174cf3b8a9</c:Value></c:ContactID></c:ContactIDCollection><c:EmailAddressCollection><c:
:EmailAddress
c:ElementID="36216c72-30e1-46ba-aa50-7aea0bb32a09"><c:Type>SMTP</c:Type><c:Address
s>rickyboy579@aol.com</c:Address><c:LabelCollection><c:Label>Preferred</c:Label></c:La
belCollection></c:EmailAddress><c:EmailAddress
c:ElementID="f3f46041-249e-4b89-bdb4-51c883dcff51" xsi:nil="true" c:Version="2"
c:ModificationDate="2016-02-16T22:09:34Z"/></c:EmailAddressCollection><c:NameCollection>
<c:Name c:ElementID="82de8042-ec4d-4016-849d-431f885cc35c"><c:NickName>master
rick</c:NickName><c:FormattedName>Rick
Shoner</c:FormattedName><c:FamilyName>Shoner</c:FamilyName><c:GivenName>Rick</c:
GivenName></c:Name></c:NameCollection><c:PhotoCollection><c:Photo
c:ElementID="4d236d38-ac9b-4052-8121-429103c09ca7"><c:LabelCollection><c:Label>User Ti
le</c:Label></c:LabelCollection></c:Photo></c:PhotoCollection></c:contact>

```

