1. Identifying Information

I found the computer name, PERRYWINKLER-PC, by checking the Operating system information using Autopsy v4.21.0. All future mentions of Autopsy will be on this version. Also, using FTK Imager v4.3.1.1, I found an account named Perry in the Users subkey under the root key. All future mentions of FTK Imager will be on this version. I checked these two different areas because each one holds pertinent information, such as account names, OS type and version, user SIDs, and so on.

2. Evidence of Illegal Activities

Using Autopsy, I found an image titled "da stuff.jpg" that shows a bag full of marijuana that was stored in the /Users/Perry/Pictures directory. I checked this directory because it is a very common location for people to store their photos, as it's easily identifiable and comes premade. Therefore, it's a likely place to find evidence. This image was found under the Users key in the Perry and Pictures subkeys. In this same location is another image called "mike's desk.jpg" which features a different bag of marijuana and a large roll of cash.

Also found through Autopsy in the /Users/Perry/Documents directory was a series of letters Perry sends to a man named Rick. I checked this directory for the same reasons as the previous one. Its easily accessible and identifiable and has a likely chance of containing useful evidence. "Letter3.rtf" mentions that he bought the credit card numbers that Rick told him to and is awaiting further instructions. The full letter is as follows:

"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"

3. Covering Tracks/Deleting Evidence

In another of the letters mentioned in section 2, that being “Letter1.rtf”, Perry states that he has already disposed of evidence that was in the bedroom and kitchen but asks for help in disposing of the evidence on his computer. The full letter is as follows:

Rick,
What should I do? I havent hurd from you and im getting worried. are you there yet? i need an email to know. Also, i bought those credit card numbers you showd me. There supporsed to be all prepaid too so we are set! lol well i hope your safe and will look for your email.
Sincerely,
Perry

Another piece of evidence I found is an email sent from perrywin232@aol to rickyboy579@aol, likely the Rick in the aforementioned letters, in which Perry states that he’ll use the task scheduler to delete his computer activity. I found this in the /$Recycle.Bin key on Autopsy. I searched this key because the recycle bin keeps the metadata of the files that are put into it and keeps them until its overwritten. Because of this, the contents of the files are recoverable.

Looking through the Installed Programs subkey under the Data Artifacts key, I found that Perry installed an application called Eraser, specifically version 6.2.0.2970 on 2/21/2016 at 10:34:18 PM EST. Seeing this, I also checked the prefetch files for this application. Prefetch files store information about applications and files that are accessed by your computer. Since Eraser is a tool used to completely wipe the data from a hard drive, I needed to know if he had run the program or not. According to the prefetch files, Eraser was run five times between 2/21/2016 and 2/28/2016. However, seeing as how the files are still recoverable, it must not have been executed correctly.

Also, his web search history showed many attempts to learn how to conceal or erase his online activity. Some examples include an ehow.com search for how to remove traces of activity on a computer, searches for using Tor browsers, how to send emails anonymously, among other things.

Lastly, in the /Users/Perry/Documents/Email directory, there was a file called "plan.zip." The file is encrypted, but it likely includes crucial details of Perry's plans, possibly including Rick and/or other accomplices.

4. **Additional Items**

Perry had two different USB drives with which he moved files back and forth. One of these USBs was a SanDisk Cruzer USB, serial number 20035001181162571 4CA7, and it likely contained the filed named "mike's desk" that was mentioned earlier due to the drive being attached the same day the file was last modified.

5. **Plans to Flee**

A file in the /Users/Perry/Documents/nice directory there's a JPG of the Iguazu Falls. This waterfall is on the Iguazu River, which sits on the border of the Argentine province of Misiones and the Brazilian state of Paraná. This on its own wouldn't be cause for concern; however, a file located at /vol_vol3//$CarvedFiles/f0252768.mbox shows an email Perry received from Rick with the IP address 186.210.54.196. This IP address is Brazilian. In the email, Rick states that he's contacting Perry from a hotel computer to avoid being traced and instructs Perry to get on a United Airlines flight. The full email is 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."

6. Other Evidence

In the Users/Perry/Contacts directory, there were two more contact not listed previously. One for a person named Larry Spitz with the email address spitzmeister@rocketmail.com, and Mary Reister with the email address mreister@gmail.com.