Project 4 - Group 3

Kyle Casson, Roby Pile, Emily Shader, Tim Spurlock, and Mason Wuest

Who is the owner/user of the computer?

- System name (located in the TEMP folder under the root) was found to be PERRYWINKLER-PC.

- Operating system owner was identified to be Perry (found in the Windows folder).

- Under the Users folder of the drive we found the user accounts on the system to be: Default, Default User, Perry, and Public
    - Only account that appeared to be used/ have data stored was the Perry account

- In the LogonUI directory of the SOFTWARE hive we found the last logged on user to be Perry on Sunday, February 28, 2016 at 15:45:28 EST.

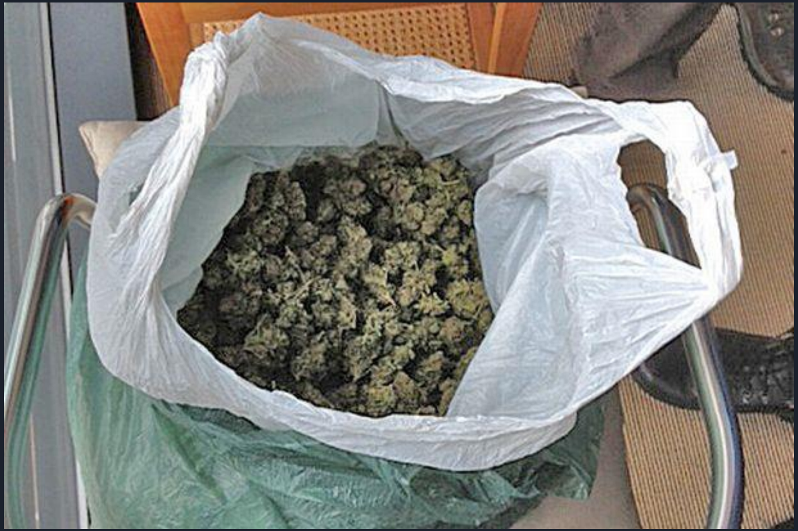
Evidence of Drugs and/or Illegal Activities

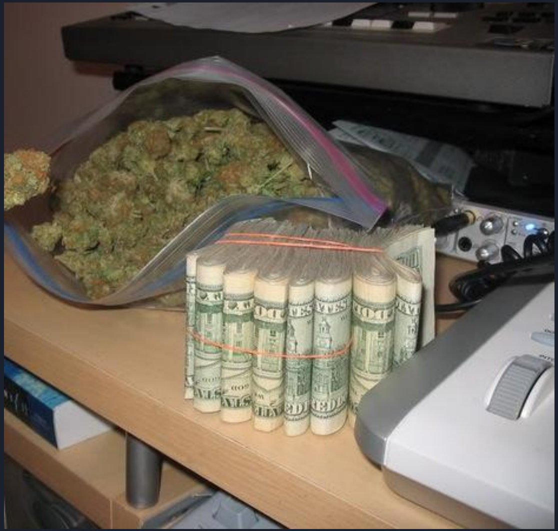
1. Excel book dated February of 2016, found containing records referencing possible substance names and amount owed by other people who are cited via aliases
2. Photos of what appears to be marijuana under the names “da stuff” and “mikes_desk”
3. Conversations with Rick Shoner which refers to buying credit card numbers online, and getting rid of things in a bedroom, kitchen as well as his computer.

Book2’s Content

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

“\Users\Perry\Pictures\da stuff.jpg” & “\Users\Perry\Pictures\mike’s desk.jpg”





Evidence of Covering Tracks and Evidence Deletion

- Tools installed on the system for cleanup (SDelete, Eraser, Evidence Eliminator)
- Scheduled tasks for those tools
- Files found in the recycle bin, deleted by user Perry
- Search History on elements of evidence covering
- Usage of TOR browser

Other Devices

- 2 Flash devices connected to the system.
- Methods of linking Volume Serial Numbers to Device Serial Numbers
- Files confirmed to be on these drives

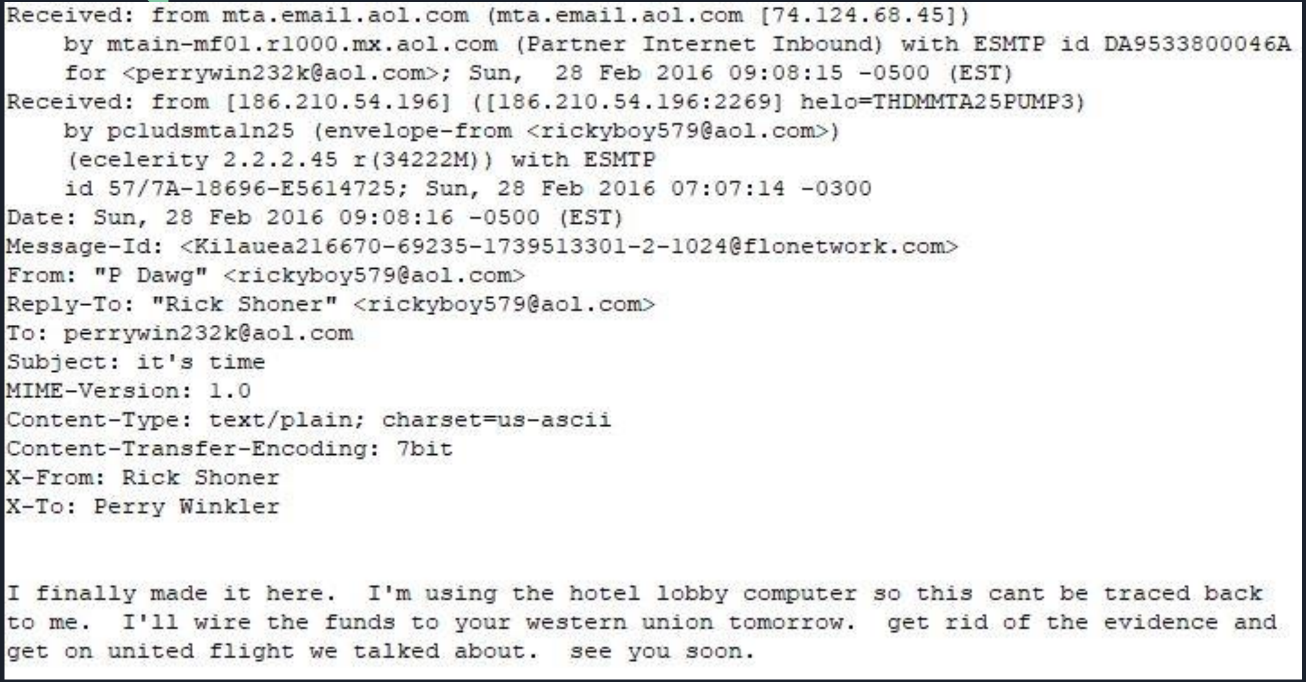
Evidence of User Planning to Run

- Map of South America found that was unallocated from the drive but recovered as a carved file using Autopsy.

- Image found under Documents in the user profile Perry called “iguazu-falls.jpg” using FTK imager. This image appears to show the Iguazu Falls waterfall located on the border of Argentina and Brazil.

- Unallocated email file was recovered as a carved file from the drive
    - IP of sender is hosted in Brazil

Carved Email File & Images



```
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.
```

Guyana
Suriname
French Guiana
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
Falkland Is.

Other Potential Evidence

- Image of tomato sauce jar in a toilet
  - No specific relevance
- Potential United flight reservation
  - Email evidence points to a potential united airlines flight
- DVD maker installation
  - No specific evidence that this program had been used
- Corrupted or encrypted Plan.zip file
  - 0 MB file unable to decrypt/open

Summary of Tools Used

- Autopsy (Version 4.9.0)
- FTK Imager (Version 4.2.0.13)
- Registry Explorer (Version 1.1.0.6)
- LECmd (Version 1.1.0.0)
- JLECmd (Version 1.1.0.0)
- Notepad++ (Version 7.5.9)
- Arsenal Image Mounter (Version 1.0.7.22)
- PECmd (Version 0.5.00)
- VSCToolset (Version 1.6)
- USB Detective (Version 1.3.0)

Questions?