Perry Winkler, Not Exactly A Criminal Mastermind

...

CIS 484 Forensics Project 4 - Group 2
Paige Fenwick, Daniel McGrath, Joseph Meyer, Michael Moser

The Job

- LMPD searched Perry Winkler's home
- Desktop PC located and recovered
- Hard drive intact and forensically imaged
- Tasked with figuring out answers to case

The Evidence

- Disk Image: img_LMPD-436243-001.E01 (3.98GB)
- Volume ID 2: 204800 sectors, NTFS formatted
- Volume ID 3: 125,620,224 sectors, NTFS formatted
- Volume 1 and 4 were unallocated and empty
- Image

```
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = PERRYWINKLER-PC
TCP/IP Hostname = PERRYWINKLER-PC
----------------------------------------
```

The Subject

Perry Winkler - suspected drug dealer

Known accomplices

- Rick Shoner
- Larry Spitz
- Mary Reister

Currently on the run

Findings

Information discovered

- System Information
- Criminal Activity
- Web Searches and Downloads
- Deleted/Carved Files
- Recent Files
- Connected Devices
- Where Perry is Planning to Go
- Additional Leads

System Information

- Owner of Computer
- User of Computer

```
RegisteredOrganization :
CurrentVersion : 6.1
CurrentBuild : 7601
CurrentBuildNumber : 7601
CSDBuildNumber : 1130
RegisteredOwner : Perry
SoftwareType : System
InstallationType : Client
SystemRoot : C:\Windows
PathName : C:\Windows
EditionID : Professional
CSDVersion : Service Pack 1
CurrentType : Multiprocessor Free
ProductName : Windows 7 Professional
ProductId : 00371-177-0000061-85507
```

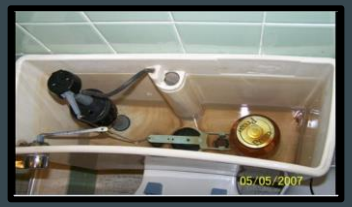
```
----------------------------------------
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = PERRYWINKLER-PC
TCP/IP Hostname = PERRYWINKLER-PC
----------------------------------------
```

```
Path        : C:\Users\Perry
SID         : S-1-5-21-3461440871-1589894493-1829873476-1000
```

Criminal Activity

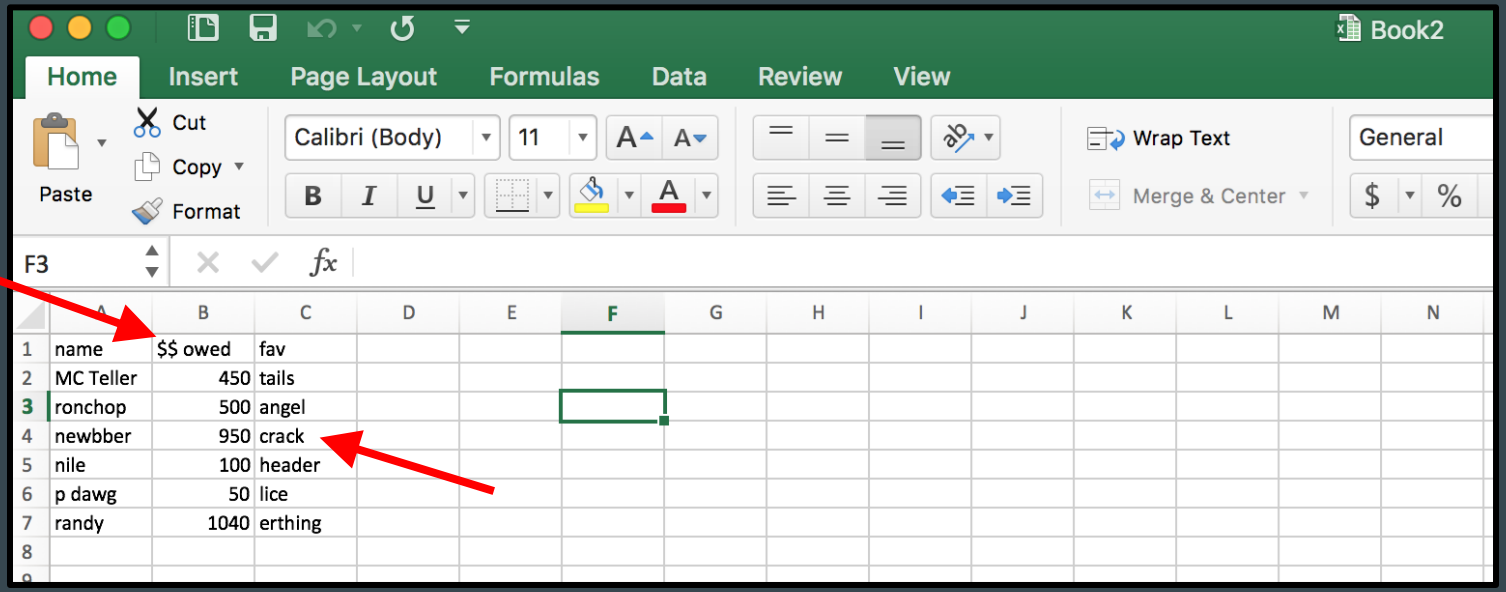
Pictures of marijuana, guns, bundles of money, and possible hiding places. (Autopsy/FTK Imager)

Carved image file of some sort of homemade ‘bomb’. (Autopsy)



Criminal Activity

Excel file under Perry's documents folder which contained a list of people he owes money to, including an entry for $950 for "crack."

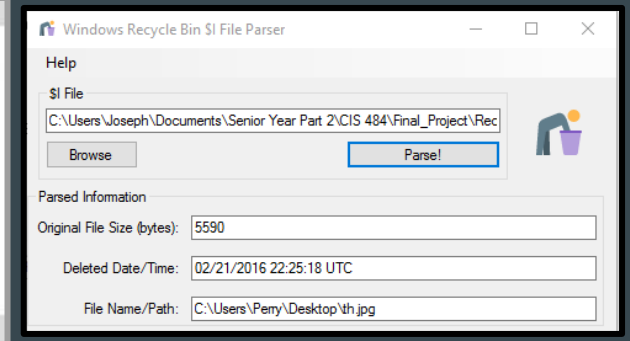


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	name	$$ owed	fav											
2	MC Teller	450	tails											
3	ronchop	500	angel											
4	newbber	950	crack											
5	nile	100	header											
6	p dawg	50	lice											
7	randy	1040	erthing											
8														

Web Searches/Downloads

- Some of the most prevalent web searches that Perry performed were through Bing between the dates of 2/21/2016 & 2/24/2016
    - 1st search: Eraser program
    - 2nd search: CCleaner, magneticforensics.com
    - Article called “Oh No, the Suspect Ran CCleaner to get Rid of the evidence.”
        - Downloaded shortly after.
    - A few days later...
        - Search for “how to set up a schedule task.”

Deleted Files



Name: Mary Reister
E-mail: mreister@gmail.com
Work
Company:
Job Title:

Rick,

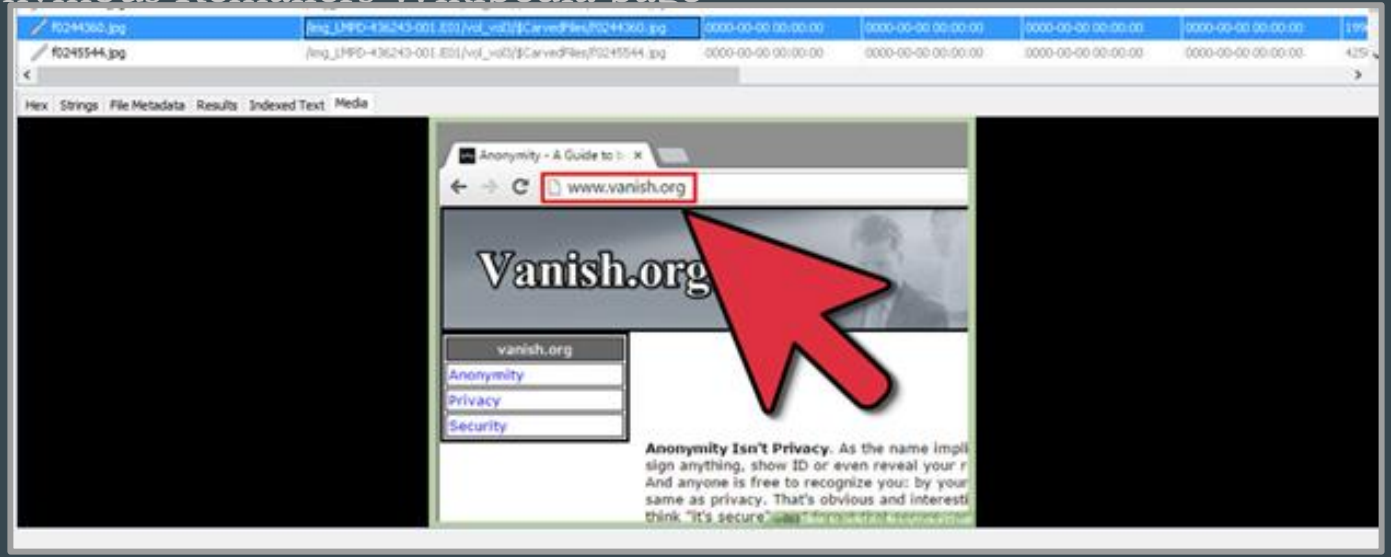
Thanks for your help! I will do wat you said with the task thing on the computer. Im glad you printed instructions for me or i woudl never figure it out lol. anyways ill destroy this and will look for your email with further instructions. cant wait to ditch this place!

Yours truly,

Perry

Carved Files

- Autopsy: Views > File Types > Images
- Eraser, CCleaner, Evidence Eliminator, Vanish.org, Anonymouse, Tor Browser, Anonymous Remailers Wikipedia page



Recent Files

- Autopsy:

Results >
Extracted Content >
Recent Documents

th.lnk	Revolver pistol - Recycle Bin	1/26/2016
awesome.lnk	Pistol - Recycle Bin	1/26/2016
inmydreams.lnk	Gold pistol - Desktop	1/26/2016
theone.lnk	Sports car - Desktop	1/26/2016
wow.lnk	Sports car - Recycle Bin	1/26/2016
mike's desk.lnk	Drugs and Money - E:\	1/26/2016
letter.lnk	Email - Documents	2/16/2016
sDelete.lnk	Zip file - Downloads	2/24/2016
letter2.rtf.lnk	Email - Recycle Bin	2/24/2016
letter.rtf.lnk	Email - Documents	2/27/2016
letter3.rtf.lnk	Email - Documents	2/27/2016
System and Security.lnk	Interesting File - Documents	2/27/2016

Letters

"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"

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

"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.\par
"Sincerely,\par
"Perry\par"

Connected Devices

Autopsy: Results > Extracted Content > Devices Attached

E:\ Drive

PERRY - Kingston DataTraveler 102 Flash Drive / HEMA Flash Drive 2 GB / PNY Attache 4GB Stick

Install Date - 2/16/2016

Device Parameters LastWrite Time - 2/28/2016

Files - SanDisk Corporation Cruzer USB Drive

"Car2.lnk"

Install Date - 1/26/2016

"Car1.lnk"

"Mike's Desk.lnk"

Device Parameters LastWrite Time - 1/26/2016

Where is Perry Planning to Go?

- Flight Plans
  - Southwest flies domestically
  - United flies internationally
  - We know Perry fantasizes about living in “paradise”
- Passport[1].html orphan file
- Beach image carved files
- Theory
  - Perry flies Southwest to connect with an international United flight

What We Think Happened

February 28th

Rick Shoner emailed Perry from hotel

Last prefetch file was ran shortly after

Been on the run since then

Police arrived at Winkler’s on March 2nd

Additional Leads

Deleted Contacts

- Mary Reister
- Larry Spitz

Batch File ran on 3/11

Plan.zip file

Tools Used

- Autopsy 4.0.0
- FTK Imager
- WinHex
- Recycle Bin Parser
- RegRipper

Conclusion

Analyzed found hard drive using a variety of tools

Perry Winkler is a person of interest in criminal activity

    Along with his partner, Rick Shoner

Believe that he is now on the run and trying to leave the country

All the found evidence can be used to bring Winkler to justice