This document will represent a report that is meant to show the result of a forensic investigation for the scenario where a local law enforcement hired me (Serafim Ciobanu) to act as an expert witness in a legal case, and provided me with some key artifacts recovered from an individual suspected of planning an armed robbery. The artifacts represent a USB image, and Registry hives. Additionally, there was a note that says “PASSWD cartoons”

The finding and conclusions of the investigation will be put in a clear way that shows whether the suspect is guilty or not.

# Summary of findings

For the investigation of the USB image (usb.dd), I will use a Kali Linux machine in order to make usage of most tools that will allow me to read data in-depth on the image.

First of all, for any precautions, I will stop the processes that might somehow override the image itself.

sudo systemctl stop udisks2.service

sudo systemctl mask udisks2.service

Then copy over the image onto the machine

Then check the md5sum to know if the image is intact

sudo md5sum usb.dd

A computer screen shot of a computer code

Description automatically generated

Which is the same as in the briefing, meaning it is intact.

And mount the image as a device

sudo losetup -fPr usb.dd –show

A screenshot of a computer

Description automatically generated

We can see that we have a FAT16 file system on the USB.

We only have 123M of space allocated, which might mean that 2M can store something else.

Then I mounted the partition

sudo mount /dev/loop0p1 /mnt/usb\_lab7

And inside there I can already see some files.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

And a hidden file. This files are important for the (quiz1) investigation. “.TheMessage.txt” “Pancakes.pdf” “TheSimpsons.pdf”

TheMessage.txt reveals a secret message that is likely to mean that the suspect was part of the plan to rob a victim along with someone else

A screenshot of a computer program

Description automatically generated

Also, System Volume Information contains information regarding the IndexerVolumeGrid, which might be useful for identifying a disk partition in Windows afterwards.

Then I managed to see the deleted files from the USB device, by using:

sudo fls -rp /dev/loop0p1

A computer screen shot of a computer program

Description automatically generated

The filename seems to be “Blueprints.jpg” (quiz2)

I managed to recover the deleted file, by doing:

sudo icat /dev/loop0p1 14 > ~/Documents/Blueprints.jpg

The contents reveal the blueprint of the “MONEY BIN” (quiz3) of Scrooge McDuck, who is a very wealthy duck.

A computer screen shot of a blueprint

Description automatically generated

So overall from the “.TheMessage.txt”, we get that the target is “SCROOGE McDUCK” who is a “pekin duck” (quiz4)

Further analysis shows that the file sizes of some files are too big.

A screenshot of a computer

Description automatically generated

In this case, I decided to check first the Pancakes.pdf, as the size is too big for a simple pancakes recipe.

By running binwalk Pancakes.pdf I managed to find that there is some embedded data inside of it.

A screenshot of a computer program

Description automatically generated

I copied the file over to my documents (cp Pancakes.pdf ~/Documents/)

and then ran:

binwalk -e Pancakes.pdf

A computer screen shot of a program

Description automatically generated

And the output shows a couple of embedded files or information inside.

If we check the contents of the file “The Plan.txt” we will find out that the first thing a crook needs is a “ski mask”. Thanks “Pancakes.pdf” for that information (quiz5)

A screenshot of a computer screen

Description automatically generated

The contents show the full plan execution for the robbery

A screenshot of a computer

Description automatically generated

The rar file contains the same file

A screenshot of a computer

Description automatically generated

The other file that is suspiciously big is called TheSimpons.jpg, and it most probably contains other information.

I decided to check it for steganography, with a tool called steghide.

And here it is where I made use of the note that said “PASSWD cartoons”, as that is a passphrase to get the content that is hidden.

A computer screen shot of a program

Description automatically generated

After running:

steghide extract -sf TheSimpsons.jpg -p cartoons

We get the image with the villains

A screenshot of a computer

Description automatically generated

Where the second villain is called “TheBeastWithin”, can be found in the file “VillainsTeamMembers.jpg”, which we got from the “TheSimpsons.jpg” using “steghide” (quiz6)

One of the last things left to do that I want to check, is when was the last time the USB stick got connected to the suspect’s PC.

To do that, I can analyze the registry hives that were also captured.

I am using registry explorer to get the information.

The path: ControlSet001\Enum\USBSTOR (SYSTEM)

And then I can look for information that regards last connected times

A screenshot of a computer

Description automatically generated

And since there is only one USB that can be seen currently, that was last connected on 24/06/2022 (quiz7), I assume it was the USB stick that we acquired image of.

# Expert opinion

As a conclusion, I can affirm that the suspect is guilty of planning an armed robbery upon the Money bin of Scrooge McDuck, taking into consideration all the possible finding that I listed in this report. That is favored by the fact that the suspect was having special files hidden inside other files, and of course messages.

The USB device was probably used to get rid of any possible (or leaving less) marks on the computer of the victim, hence there were also some ways to hide the data for anti-forensic means.