Homework 3 Report

Used software:

- OS Win10 64bit
- AccessData FTK Imager 4.2.0.13
- Autopsy 4.12
- Registry Explorer 0.8.1
- AccessData Registry Viewer 2.0

Suspect system and profile:

By looking at the OS Information in Autopsy, we find out that the used system is Windows 10 Pro 64bit using NTFS file system.

The suspect is probably a Russian speaker as he has many language parameters set to Russian. There is also an auto fill value in Russian. He is located in Estonia, as the systems' files timestamps indicates the Estonian time zone.

The suspect personality can be described as violent and criminal. We can first of all notice the pictures he has on his Desktop, which are all of either murder scene or corpses. Then we also the web searches which are mostly related to crime or violence, like "murder victims", "skimmers for sale" or "cannabis".

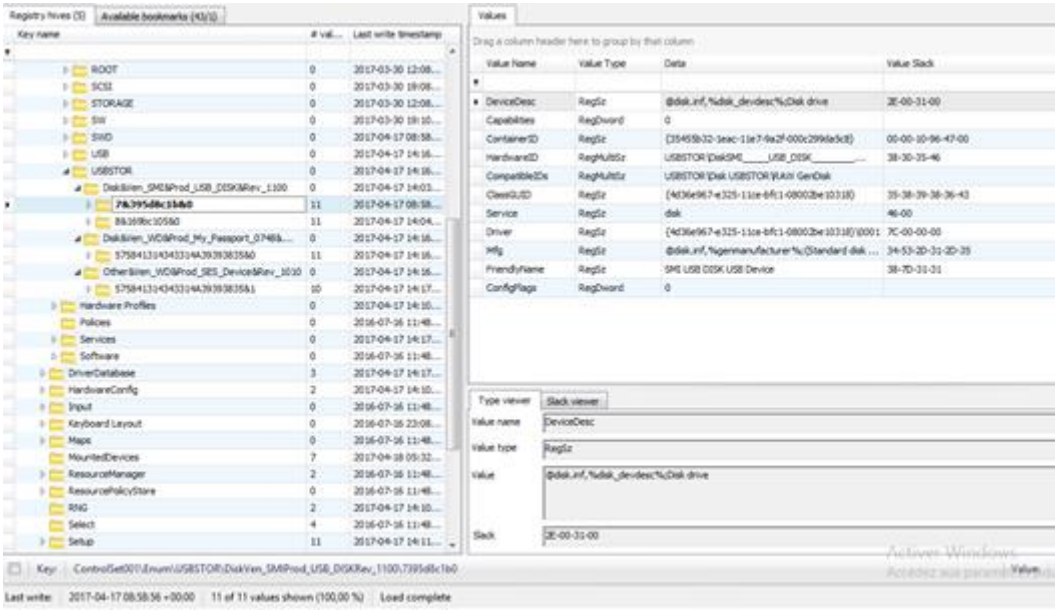
Questions:

1) The only user profile found besides the "default users" such as "Public" and "All Users" is: User

2) I get the Registry Files hives from /root/vol_vol7/Windows/System32/config

By using Registry Explorer for the hive SYSTEM, /ROOT/ControlSet001/Enum/USBSTOR, we can get the following used USB storage devices:

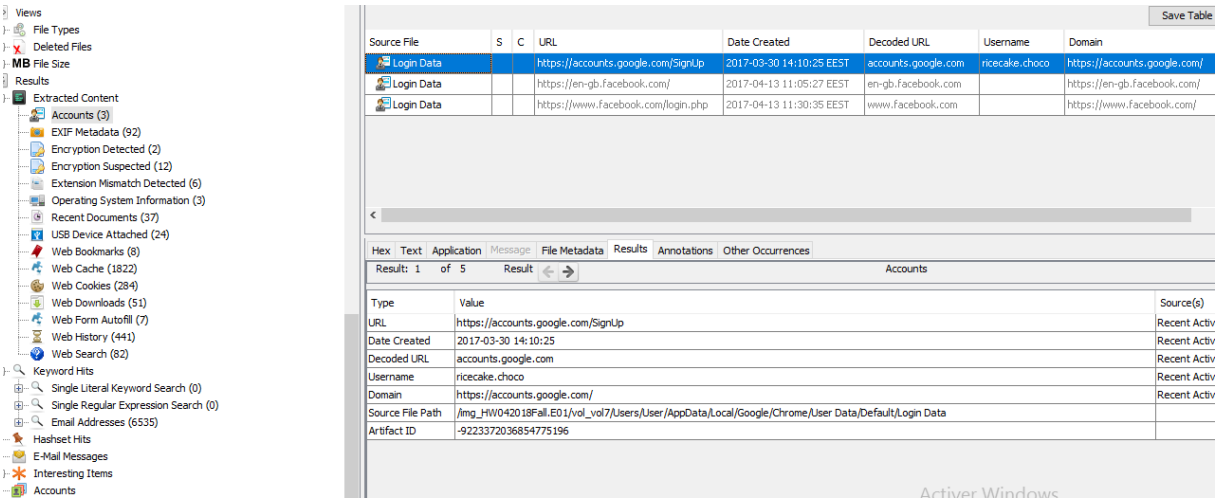
- SMI USB DISK USB Device ➔ Last used on 17/04/2017 at 14:04:02 UTC+0
- WD My Passport 0748 USB Device ➔ Last used on 17/04/2017 at 14:16:02 UTC+0
- <Unknown name> ➔ Last used on 17/04/2017 at 14:17:41 UTC+0



3) By looking at the extracted accounts in Autopsy, we can already find a Gmail account ricecake.choco@gmail.com. The suspect also has a Facebook account.

The in the Web Form Auto fill, we find the following accounts:

evil.doctor202@gmail.com



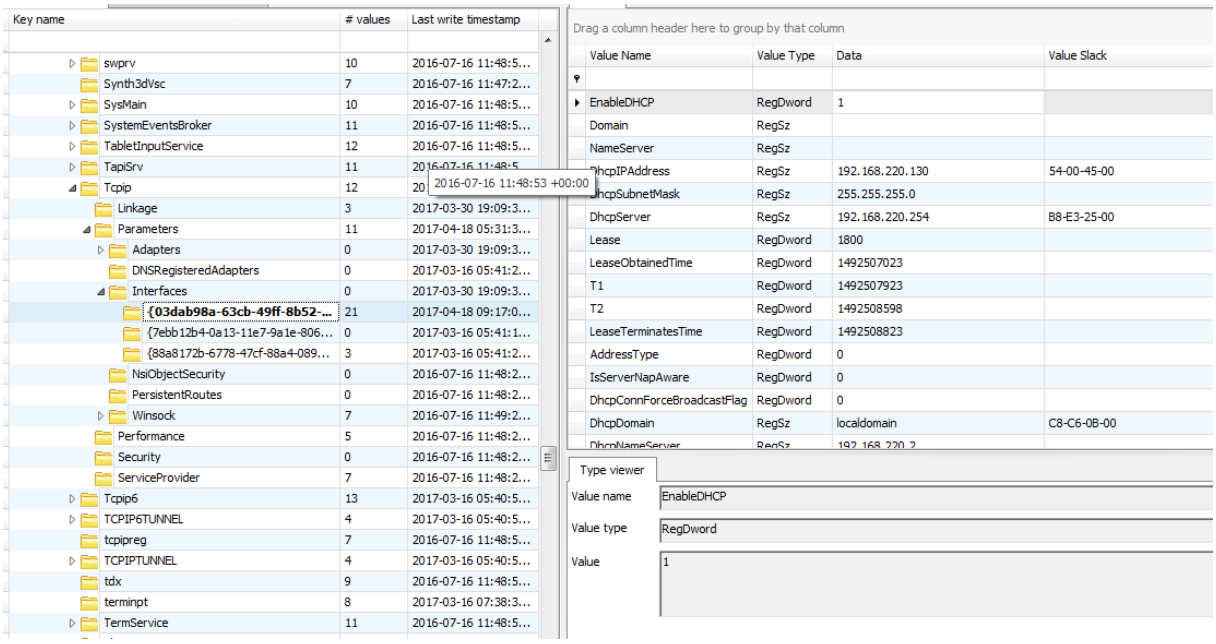
The suspect also has the Skype accounts “ricecake.choco” and “doctor.evil159”. Related skype discussions could be extracted (see “skype” evidence folder). Files

related to discussions can be found under /root/vol_vol7/Users/User/AppData/Roaming/Skype/live#3aricecake.choco/chatsync/. I extracted two files 9136bb5eaa2e4193.dat and b8b61904de10813e.dat, related to chats.

4) I first looked at the Registry artefacts, in SOFTWARE/Microsoft/Windows NT/CurrentVersion/NetworkList/Profiles, but I found nothing relevant.

Then I checked the artefact SYSTEM/ControlSet001/Services/Tcpip/Parameters/Interfaces, and here I found information about an Internet connection via a DHCP server (can be a local router), but the IP addresses found are local, I didn't find the public address.

A connection was established on 18/04/2017 at 09:17:03 and the attributed local address is 192.168.220.130/24 through the gateway 192.168.220.2



5) When browsing the user's folders under /root/vol_vol7/Users/User/, we can conclude that the presence of the following web browsers:

Mozilla Firefox: We can find a profile in /root/vol_vol7/Users/User/AppData/Local/Mozilla/Firefox/Profiles/ created for some use with many relevant data and details for this use (thumbnails, cache …).

Google Chrome: We have a long list of web history (see Question 6).

Microsoft Edge: There is few history found, and besides main history since 30/03/2017 are relevant to either Firefox or Chrome. We have however Firefox and

Chrome setup files in the User's Downloads folder, so we can assume the Edge was used at first to download the other two browsers.

Internet Explorer: I found nothing to assume it has been used.

Tor Browser: We have some cache files to prove it has been used, in addition to .onion websites which can be accessed only through Tor.

6) By using the web history provided by Autopsy, we can export a CSV file of the web history. The data were exported to web_history.csv in "evidence" folder, and entries are ordered by date from the recent to the oldest. All entries were made with Chrome browser.

7) In one of the two Skype discussions found, we can get the phone number of one of the suspects' contacts: +372 689 451.

8) First of all, we find a file on the User's Desktop named links.txt. The file contains a list of Dark Web websites related to drug dealing. This can also explain why the suspect was using Tor Browser (see "drug related" evidence folder).

Second, we find webpages pages related to drug dealing in the User's Documents. One is for a command of Moroccan Hashish from a German website, and another is for a Cannabis order from an American website. In the same Documents' folder, we find pictures of this merchandise (see "drug related" evidence folder).

One of the found Skype discussions raises strong suspicions about an on-going drug sell operation. Here is the conversation text (without the special characters and encodings):

"Hi, do you have smth (something) for me

/7.33.0.105//

what do you mean

dope

yes, how much do you need

price

2600

2200

ship it on Friday

bitcoins

5 HA

or casion

casino

casino will be fine

great

let you know details by phone

+372 689 451

thnks

nice"

In this discussion, it's clear that someone is asking for some drugs (dope) from the suspect, and the suspect admits that he has some and he accepts selling him. We need to precise that data might have been omitted without the special characters. It's better to look at the complete unmodified in the Skype file 9136bb5eaa2e4193.dat (see "skype" evidence folder), this just a possible reporting of the real and complete conversation. Moreover, we can find under root/vol_vol7/Users/User/AppData/Roaming/Skype/live#3aricecake.choco/media_messaging/media_cache_v3/ a cached picture of Cannabis, the same as the one found previously in the User's Documents folder. This implies that the picture was sent by the suspect in one of his Skype conversation, may be even the one above, for marketing purposes.