Technische Universität Wien

188.922 Digital Forensics

Lecturers: Dipl.Inf. (FH) Karsten Theiner and DI Dr. Martin Schmiedecker

Teaching Assistant: Christoph Kraus

Assignment 2: Filesystem

Bruno André Moreira Rosendo

e12302727

Due Date: November 28, 2023

Submitted: November 28, 2023

Contents

1 Purpose **1**

2 Findings (Befund) **2**

3 Analysis (Gutachten) **12**

3.1 What information was stolen? Try to find as much evidence for stolen information and document it 12

3.2 Which persons were involved in the case? 12

3.3 Is there any further information that may be helpful regarding the ongoing investigations? 13

3.4 What operating system was used? 13

3.5 What is the computer's name? 14

3.6 When was the operating system installed, when was it running the last time? 14

3.7 What is the SID (Security Identifier) for the user Peter? 18

3.8 Can you find traces of malware on the system? 18

3.8.1 What kind of malware is it and how did you find it? 18

3.8.2 Which data is affected? 19

3.8.3 Is it possible to restore the affected data? 20

4 Literature Cited **22**

1 Purpose

This assignment aimed to assist Indiga, a video game company, in conducting an inquiry into their latest game, Snipper. During a recent meetup, a rival company presented one of their new games, and Sabrina, a designer at Indiga, noticed striking resemblances between the game's main character and her own concept. This incident prompted a legal investigation due to various similarities between Indiga's game and the competitor's offering. This assignment was undertaken as part of a Digital Forensics course, wherein students were assigned the role of forensic analysts responsible for conducting this fictional investigation.

To kickstart the process, the students were given an image in the qcow format, containing the system simulating the Windows 7 home computer used by Peter, a developer at Indinga and the primary suspect in the investigation. Throughout the study, a select group of employees are regarded as subjects, including Anna (director and founder of Indiga), John (co-director, founder, and lead developer), Iris (developer), Sabrina, and Peter.

This project's primary challenge is acquiring proficiency in the techniques for retrieving, analyzing, and documenting information from a system integral to a particular dataset. The work encompassed tasks such as file carving, recovering deleted files, and other procedures commonly encountered in digital forensics cases. The Autopsy software was suggested for analysis, providing hands-on experience in digital forensics for the participating students.

2 Findings (Befund)

After downloading and extracting the computer's image, and prior to anything else, it is important to hash the image to guarantee that any modifications made to it do not alter its content in any manner. To ensure the ability to return to the initial state, one option could be to redownload it; however, a safer approach is to duplicate its contents into a new file. The hashes of both files were stored and compared throughout the investigation:

```
md5sum DigitalForensic_AssignmentImage\ Clone.vbox > hash_vbox.txt
md5sum DigitalForensic_AssignmentImage\ Clone.qcow > hash_qcow.txt
cat hash_vbox.txt
2929ffe0abf8ab5560807e50a1eb85f8  DigitalForensic_AssignmentImage Clone.vbox
cat hash_qcow.txt
77e90c0dc979c0adcb0714d93b20b310  DigitalForensic_AssignmentImage Clone.qcow
```

After hashing the image, the initial step involved utilizing VirtualBox (v6.1.38) to access a copy of the system. A Windows 7 environment became visible upon booting, presenting three available users: Gary, Peter, and StuffAccount. Peter, our primary suspect, was the only user protected by a password. Exploring the files within one of the public user accounts yielded intriguing information. It became evident that numerous files had either been deleted or corrupted, necessitating specialized software for recovery.

Additionally, noteworthy files related to character ideas and designs were discovered, suggesting a potential connection to the stolen information. One of the items, in Figure 1, comprises a sketch of a character design, bearing Sabrina's signature in the upper right corner, evidently tied to the ongoing investigation. Accompanying the drawing are notes alluding to a discussion involving Anna and John. Notably, the file's name includes a date, indicating a capture on August 23rd. Contrarily, inspection of the file metadata discloses its actual creation date as August 24th, as shown in Figure 2. This particular file is archived within the *C://Private/Work/Info* directory.

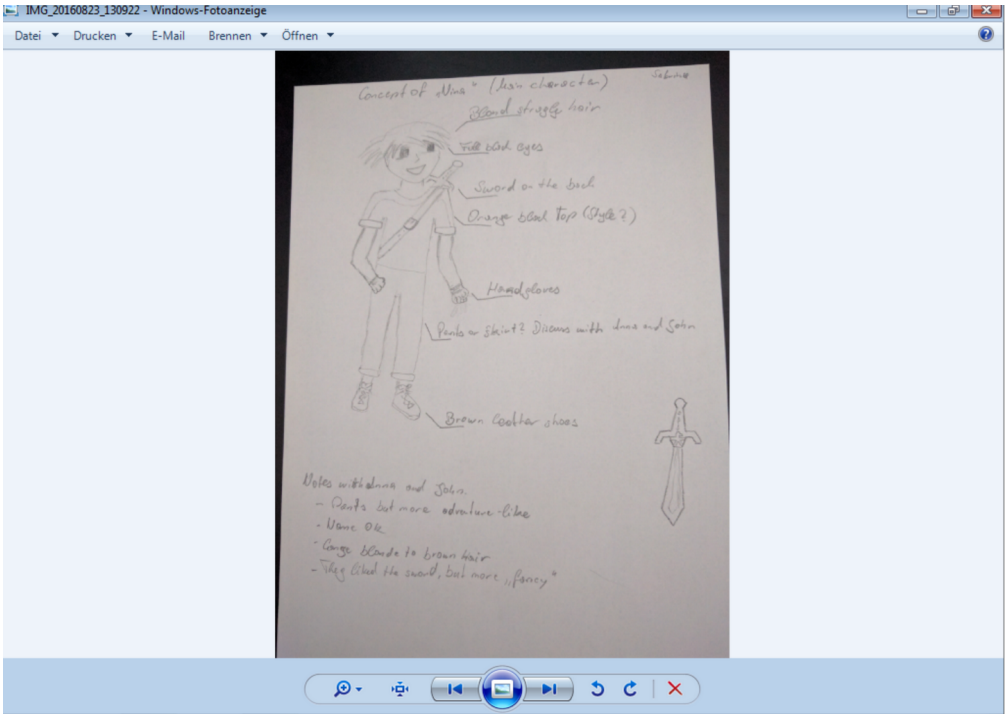


Figure 1: Character design present on the computer

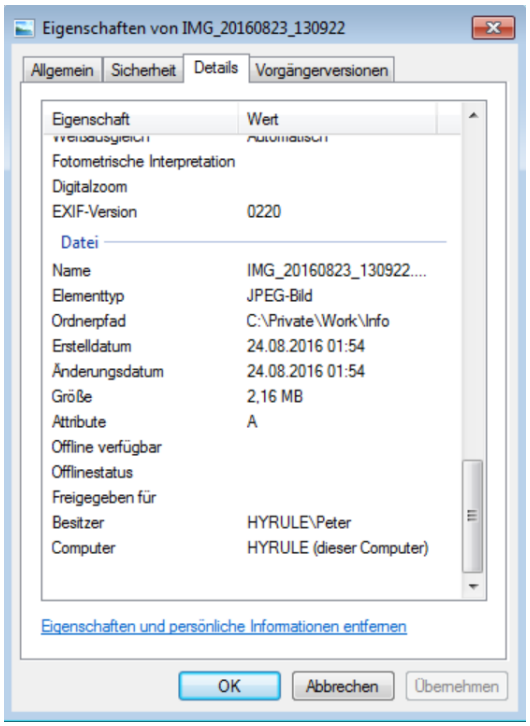


Figure 2: Metadata of the design's image

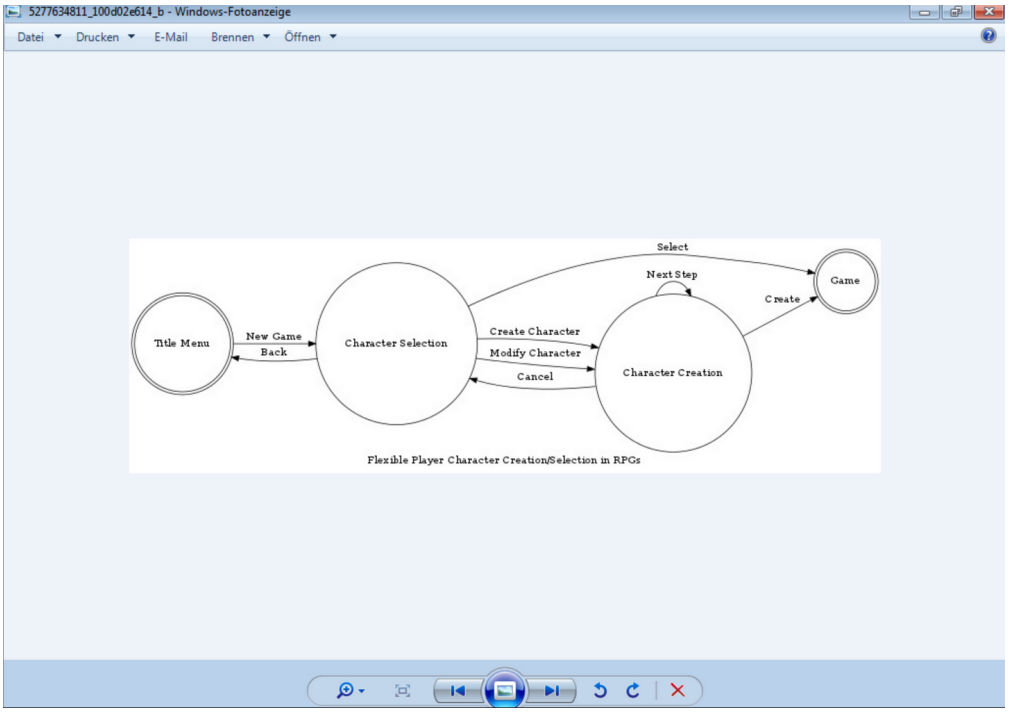


Figure 3: Flowchart for a character creation process

Within the system, additional noteworthy information relevant to the assignment's questions includes details like the operating system version, installation date, Peter's user SID, and the computer's name. A comprehensive explanation of these findings will be provided in section 3.

Subsequently, the next phase involved employing the Autopsy (v4.21.0) software for image analysis, file carving, and the recovery of deleted files, including the SHA-1 key specified in the assignment. Excluding some challenges in the setup and a few unsuccessful executions, this stage proved to be a time-consuming process, spanning approximately 15 hours to completion.

In addition to the identified carved and deleted files, the generated report yielded numerous artifacts crucial for the ongoing investigation. These included user profiles, web history, emails, operating system information, among other valuable data. The subsequent action involved utilizing Autopsy's image tool to scrutinize all images and bookmark those

deemed noteworthy. Apart from encountering the previously noted character design, a lot of content surfaced, featuring various biking-related materials, designs associated with other game characters like Ivan, flowers, content related to viagra, and images of *Game of Thrones* characters, the significance of which will become clearer as the investigation progresses.

Utilizing Autopsy's file browser, we can navigate to the files associated with the user Peter. By accessing *Users/Peter/AppData/Roaming/Peter1983/*, a wealth of information concerning Peter's received, sent, drafted, and deleted emails becomes accessible, proving to be a crucial resource for the ongoing investigation. Within this email repository, there is correspondence directed to an email address named *briennefan@openmailbox.org*, allegedly a romantic interest of Peter. Examining their communication reveals details indicating that this email address belongs to Iris. The exchanged messages unveil that Peter and Iris went on a date, followed by Iris requesting Peter to share a picture of Sabrina's design art. This art, initially intended only for Anna and John, was known to Peter as it was displayed on Sabrina's desk. One notable email dated August 24th records Peter admitting to sending the aforementioned image, followed by a frustrated inquiry from Peter regarding Iris's sudden change in behavior. Initially, there was a suspicion that this email might be an impersonation of Iris. However, it is crucial to acknowledge that the sender references real-life events, indicating a high likelihood that this communication is indeed from the Indigo developer herself.

Their conversation can be found below. Note that the date and time of the emails are not realistic, since this is a fictitious investigation, so they were excluded.

```
Iris:
Hihi
Hi Peter, now we can chat. ;)


Peter:
```

Hey, nice! Puh the traffic today was terrible... Hope you had a nice ride. :)

Iris:

Yeah no problem at all. Say, do you want to go for a drink someday? ;)

Peter:

Sure, let's discuss the details at work. :)

==========

Peter:

Hey, it felt like one, hope do not take it wrong, that I call our meeting a date.

Iris:

I'm ok with that :)

I also think, that it was a date :)

But it should be a thing between us two and we should keep it as a secret at work. ;)

Peter:

Sure thing :)

==========

Iris:

Hey, can you do me a favor?

Have you seen some design concepts of sabrina?

Peter:

Nope, not really. She only shows it to anna and john, but I know,

that she keeps it in her desk. Why?

Iris:

Can you get a copy for me? I'm very interested in it :)

Peter:

Hehe why don't you just wait until she presents the first 3d model?

Sometimes she let her drawings unlocked on her table,

but I don't think, that I should copy them :/

Iris:

I'm very impatient.

Please do it for me, maybe I will reward you with another date? ;)

Peter:

Uhm ok, I'll look what I can do for you :)

Peter:

Hope I do nothing wrong with that, but here the desired item

==========

Peter:

Hey did I do something wrong? You've been acting strange lately... :(

```
================================================================================
```

```
Peter:
Anna and john asked me today, if I leaked some information about our
work. I denied everything, I don't want you to get into trouble. What
have you done with the desired item from Sabrina. Please answer me
Iris, I don't want to discuss this at Work.
```

Another noteworthy email interaction occurs approximately a week later with *techsupportguy@mailinator.com*, illustrated in Figure 4. In this exchange, Peter seeks assistance, as his files were unexpectedly transformed into MP3s, accompanied by peculiar messages bearing the label *"IMPORTANT INFORMATION"*. Conducting a keyword search for this phrase leads to the discovery of an HTML preview (with hash *6206c793f428a56dfb15407654016a01)* indicative of a ransomware incident, as depicted in Figure 5.

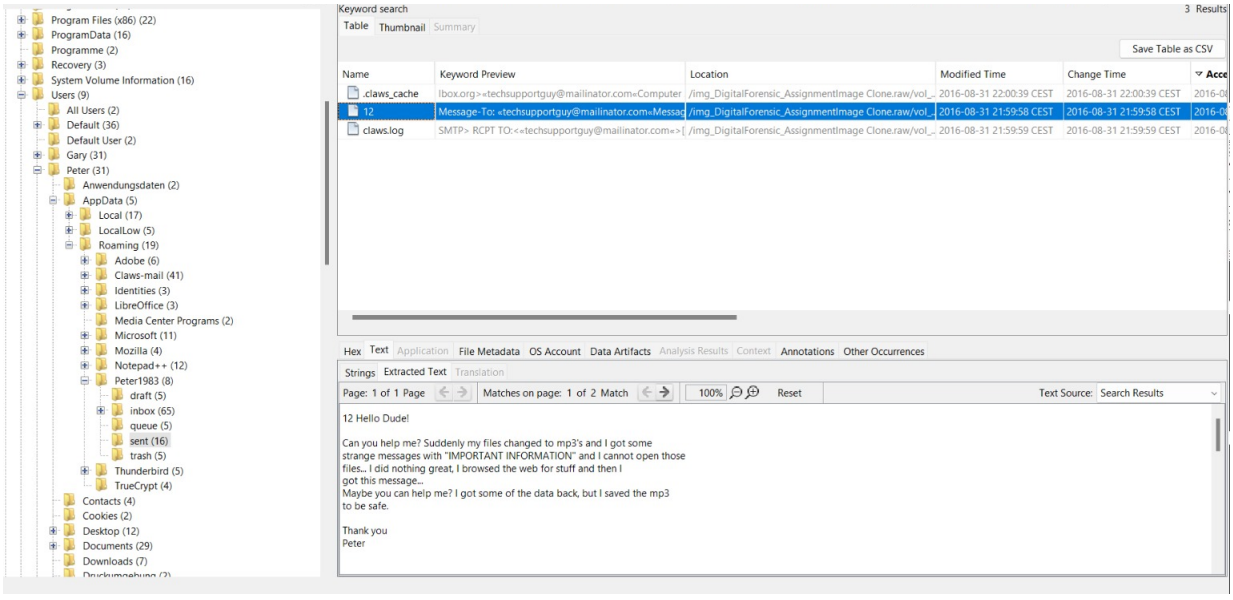


Figure 4: Email of Peter asking for technical support

Following this lead, we can try to analyze the system's web and search history. One suspicious activity was a search for a clash of clans cheat on the same day of the ransom email.

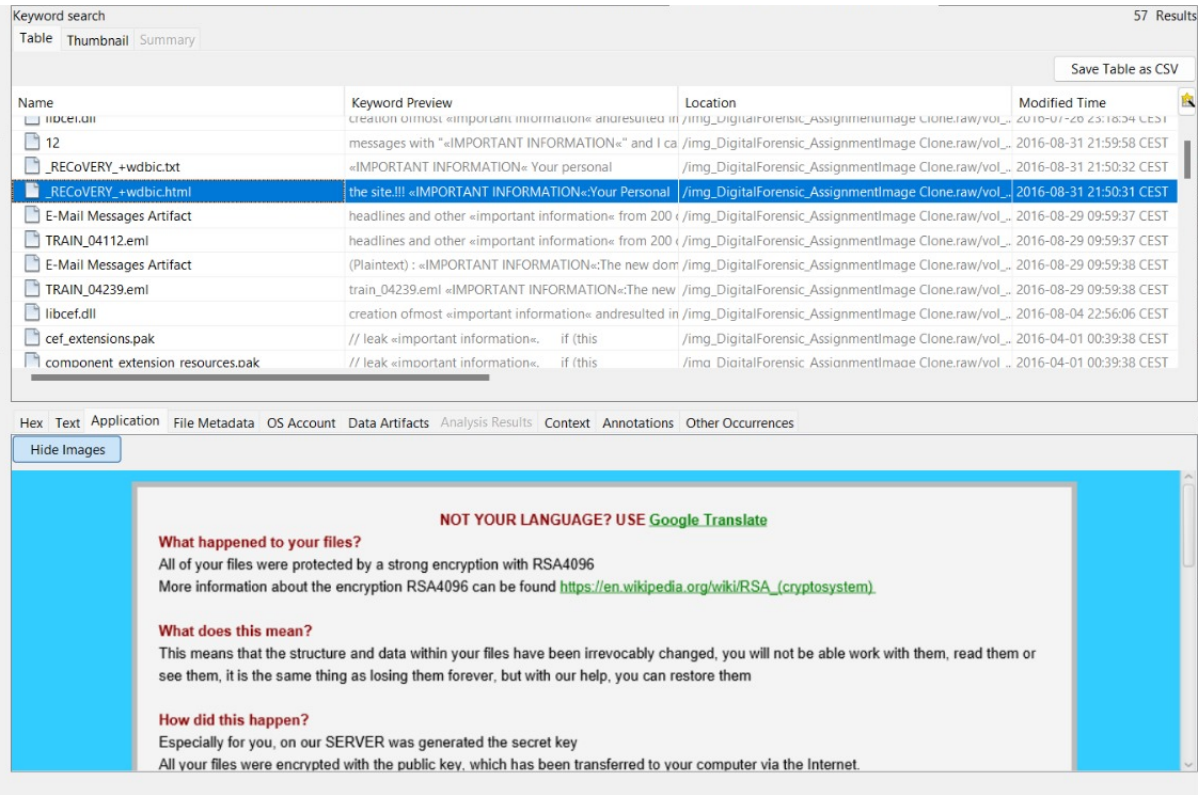


Figure 5: Malware page asking for a ransom

I then searched for the "clans" keyword and found some files related to the cheats, such as the one in Figure 6. A file named *494C3076AE2EDCDCA2493223739BF99E9FF60F1A (with hash f5c1b472e6b000bc4f7990a014fe2a31)* and a database named *places.sqlite* had the information on how and when the cheats were downloaded, including indicators to some malware named *x01.aidata*. A quick search on the web about ransomware using the MP3 extension reveals the virus to be TeslaCrypt.

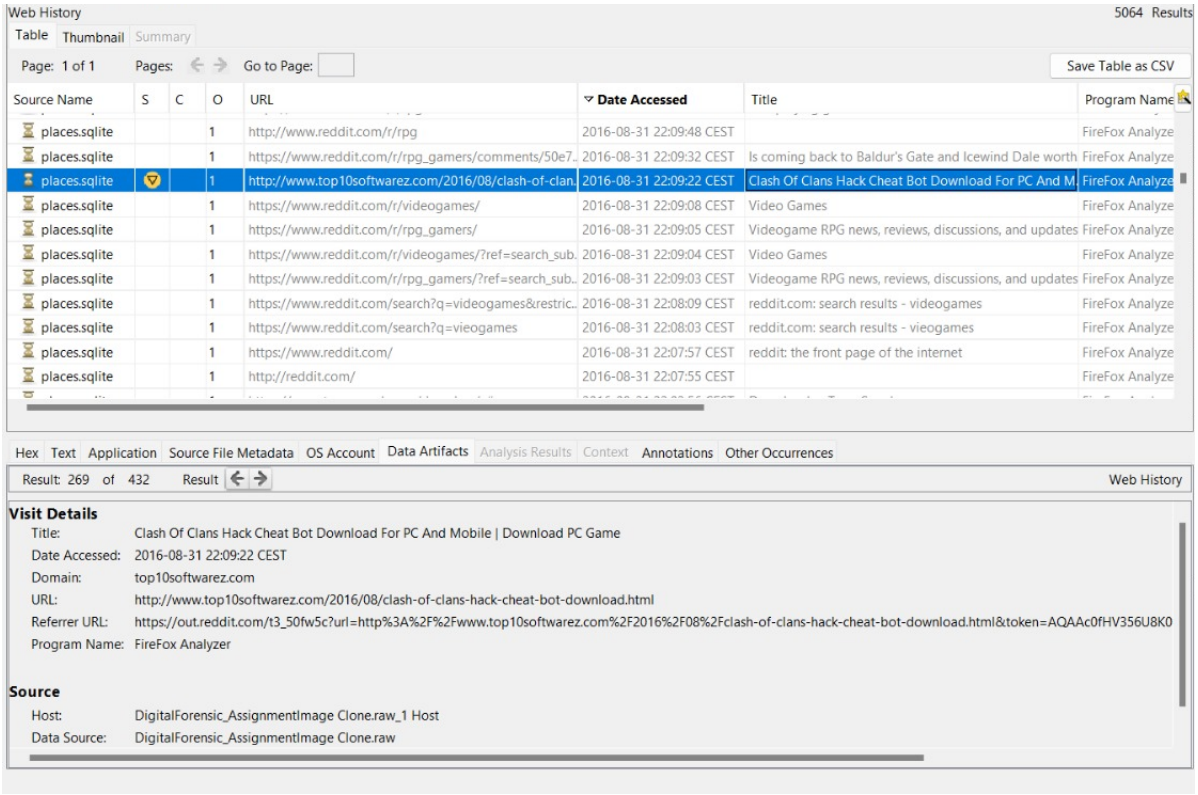


Figure 6: Evidence indicating a download of a Clash of Clans cheat

The web history reveals additional intriguing details. Specifically, there is a wealth of information related to Iris, with instances of Peter searching for her social media profiles, exploring cafes in Vienna, looking up information about flowers, and delving into the background of Brienne of Tarth from Game of Thrones, as previously noted in the image investigation. Further related information emerges through searches using keywords like *"Brienne"* or *"Iris"*, including a file titled *goog-malware-shavar.sbstore-slack*, potentially

part of Google's anti-phishing API. While this information provides added context, it is not deemed crucial for the ongoing investigation.

3 Analysis (Gutachten)

The subsequent section responds to all the assignment's specific questions and assesses the results of the investigation according to the information found in section 2.

3.1 What information was stolen? Try to find as much evidence for stolen information and document it

The stolen information consisted of a photograph of one of Sabrina's character designs shown in Figure 1, which was laying on her office desk. As detailed in section 2, Peter fell victim to emotional blackmail by Iris, compelling him to send a picture of the confidential design that, until then, only Anna and John were authorized to view. The evidence supporting this narrative includes the exchanged emails between Peter and Iris, Peter's possession of the design photo on his computer, and all the images and web searches on the system affirming Peter's emotional feelings towards Iris. There is a notable likelihood that Iris may have leaked this sensitive information beyond the confines of the company, resulting on a competing company getting access to it.

3.2 Which persons were involved in the case?

The key figures in the case were Peter and Iris, central to the acquisition and leak of the character design to an external entity. Of the remaining three individuals, Sabrina is involved due to her role as the creator of the design. While Anna and John do not play a pivotal role, they are the directors of Indigo and were aware of the design prior to the events unfolding, as depicted in Figure 1.

3.3 Is there any further information that may be helpful regarding the ongoing investigations?

The logical progression in the investigation is to delve into Iris's activities and, potentially, analyse her laptop. This step holds the promise of unearthing vital information regarding whom she shared the design with, the motivations behind such actions, and the identity of the receiving company.

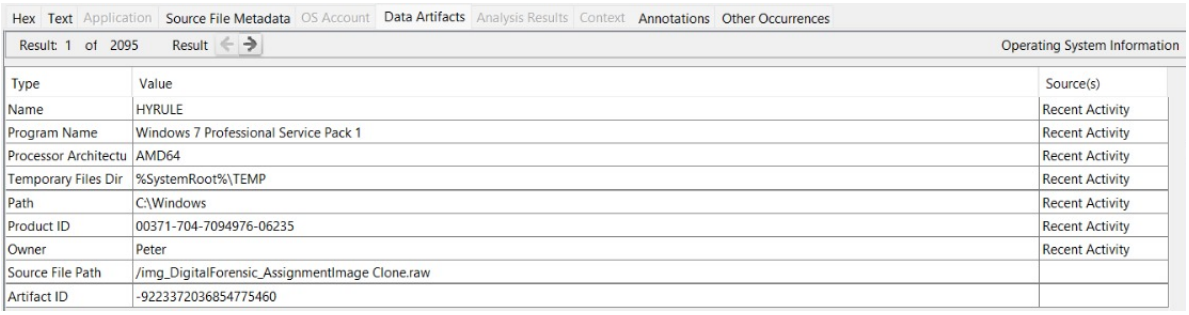
While the malware discovered on Peter's computer initially seems significant, a more thorough analysis exposes its irrelevance to the case. It turns out that Peter acquired the virus while attempting to download cheats for a video game.

An intriguing artifact meriting further exploration is the encryption software (*gdbus.exe*) identified by Autopsy. It's plausible that Peter attempted to encrypt certain files for confidentiality, although confirmation necessitates a more in-depth investigation. Additionally, there is a TrueCrypt container within Peter's files, offering potential significance if accessed.

3.4 What operating system was used?

Specific information about the operating system used can be found in one of the artifacts generated by Autopsy, seen in Figure 7. We can also confirm that the user Peter is the owner of the OS.

- **OS:** Windows 7 Professional Service Pack 1
- **CPU Architecture:** AMD64
- **Product ID:** 00371-704-7094976-06235
- **Owner:** Peter



Hex | Text | Application | Source File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Result: 1 of 2095 Result — Operating System Information

Type	Value	Source(s)
Name	HYRULE	Recent Activity
Program Name	Windows 7 Professional Service Pack 1	Recent Activity
Processor Architectu	AMD64	Recent Activity
Temporary Files Dir	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00371-704-7094976-06235	Recent Activity
Owner	Peter	Recent Activity
Source File Path	/img_DigitalForensic_AssignmentImage Clone.raw	
Artifact ID	-9223372036854775460	

Figure 7: Autopsy's artifact about the operating system

3.5 What is the computer's name?

According to Autopsy's OS artifact and the information inside the image's system, the computer's name is HYRULE, as can be seen in Figures 7 and 8.

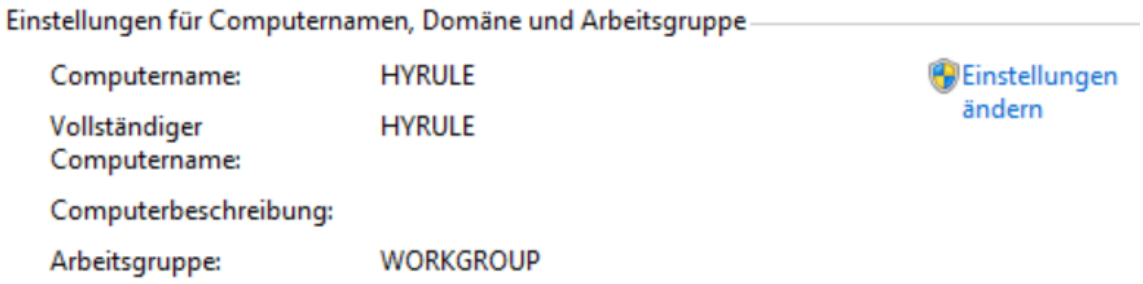


Figure 8: Information about the computer's name

3.6 When was the operating system installed, when was it running the last time?

Various methods exist to determine the installation time of the operating system. While all these methods yield the same date, the time may vary. This analysis will explore these different approaches and discuss which should be considered the definitive reference [1].

By running these commands within the *PowerShell* interface in the Windows image, we can extract the date and time of the operating system installation directly from the registry,

as shown in Figure 9. According to this method, the installation date is determined to be July 7, 2016, 00:27:42 (Thursday).

```
$date = Get-ItemProperty -Path
'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\'
|  select -ExpandProperty InstallDate


(Get-Date "1970-01-01 00:00:00.000Z") + ([TimeSpan]::FromSeconds($date))
```

Figure 9: OS installation date according to Windows' registry

However, we get a different installation time (07 July 2016, 01:27:42) when using the *SystemInfo* command on *cmd*, as seen in Figure 10. The same is true for *WMI* via the *PowerShell* by running `([WMI]'').ConvertToDateTime((Get-WmiObject Win32_OperatingSystem).InstallDate)`, as shown in Figure 11.

An alternative method for approximating the OS creation time involves examining the *"last write time"* of the client-side cache, which closely aligns with the original installation. This can be achieved through the command: `Get-Item C:\Windows\CSC`, as shown in Figure 12.

The determination of the accurate installation time is subject to debate. Regarding the first three methods, any time disparity likely arises from a timezone conversion issue when representing the installation date in a human-readable format. Consequently, all three ways should converge to 01:27:42. However, the last method provides an earlier time of 01:04. This should be considered the preferred estimate as it is appears to be the closest approximation to the actual installation time across different machines [2].

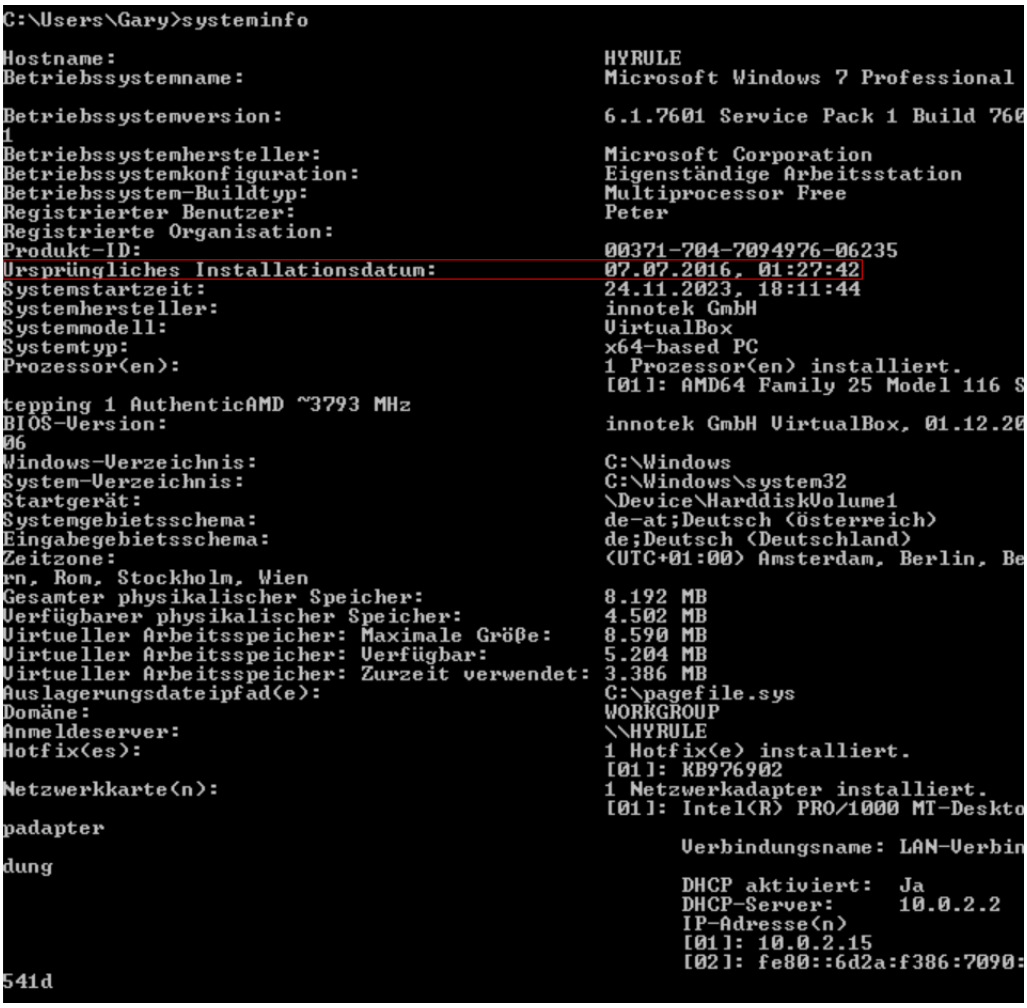


Figure 10: Output from *systeminfo*, including OS installation date

Figure 11: OS installation date according to WMI

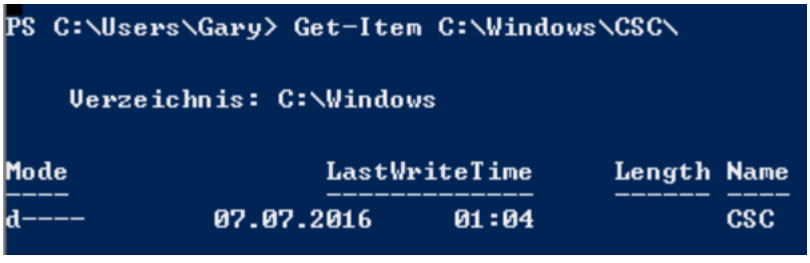


Figure 12: OS installation date according to client-side cache

Regarding the last system startup, initially, the first option was to check the last time Peter logged into the system, which was on 05-09-2016 at 15:26:40. However, this information could be misleading as the system may have been accessed by users other than Peter. For this reason, Windows Event Viewer was utilized to retrieve the last system startup [3]. Fortunately, the obtained data aligned with Peter's login time, confirming that he was indeed the last user to initiate the system boot. The result is illustrated in Figure 13 (exclude later accesses during the investigation), obtained by filtering for startup events (ID 6005), as detailed in the referenced article.

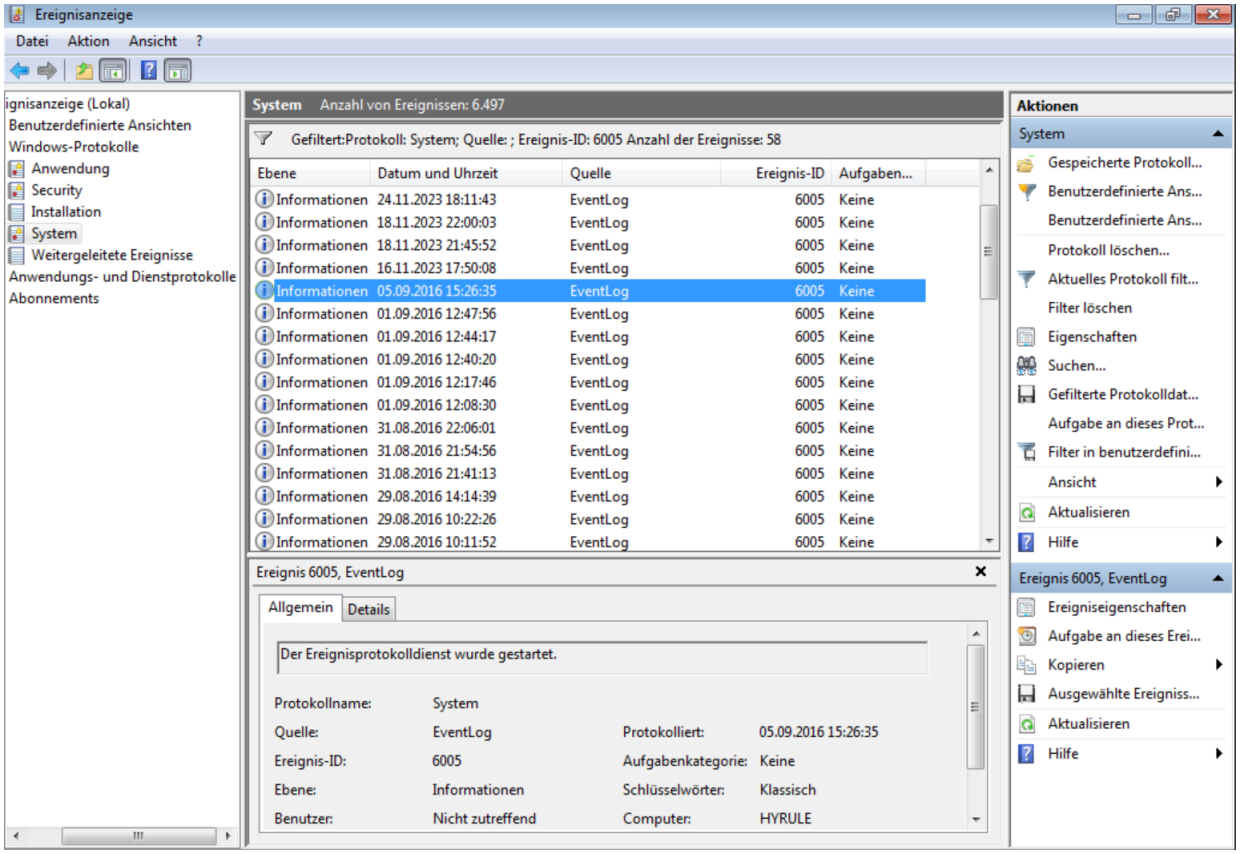


Figure 13: Event Viewer showing the startup events of the system

3.7 What is the SID (Security Identifier) for the user Peter?

We can get the SID for all users, including Peter, by running the following command inside the PowerShell of the image [4]:

```
Get-WmiObject win32_useraccount | Select name,sid
```

That said, Peter's SID is **S-1-5-21-3032217210-630098460-752710606-1001**.

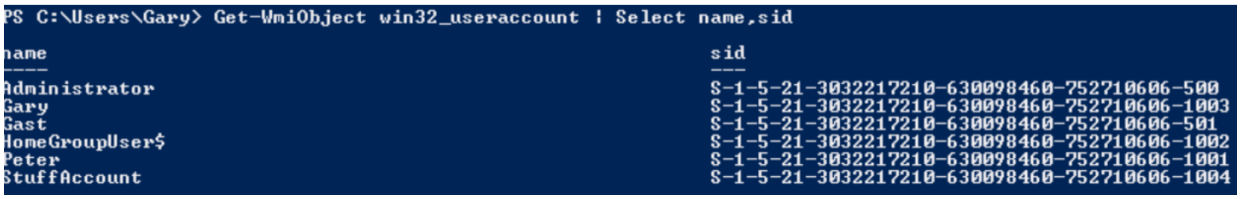


Figure 14: List of Windows' users and respective SIDs

3.8 Can you find traces of malware on the system?

Certainly, as detailed in section 2, Peter fell victim to a ransomware attack.

3.8.1 What kind of malware is it and how did you find it?

The malware that affected Peter is identified as TeslaCrypt. As detailed in section 2, this discovery stemmed from an email wherein Peter sought assistance from a "tech support guy" to recover files that had suddenly been converted into MP3s, accompanied by an unusual message. Searching for this message led to the confirmation that Peter had fallen victim to a ransomware attack. The identification of TeslaCrypt as the specific malware was facilitated by matching the message details and verifying it through the release of a master decryption key, providing a means to decrypt and affirm the correct malware association.

3.8.2 Which data is affected?

Numerous files were affected, identifiable through a search for files with an MP3 extension. Any files exhibiting an extension mismatch or corruption are very likely affected by the virus. Another indicative factor is the modification date, which should align with Peter's infection timeframe (post his attempt to download *Clash of Clans* cheats).

Table 1 presents all the affected files along with their corresponding hashes before decryption.

Table 1: Files affected by the malware

File Name	**Hash**
contactdata.csv	579dd657b961c57332e38bb21fa65b1c
Leonard_Nimoy_William_Shatner_Star_Trek_1968.JPG	5e40f617af844e4924ffe8fa35b0c778
monster_concept_art_vii_by_d_faultx.jpg	912260ae85f63c49e64bfcbf5c4cbdfa
myrating.csv	d49db59ff31bb0149f4a84d1dd27adc9
passwords.docx	6d65e612a09e12c636e0e1b552bbda33
unityassetstoreguide.pdf	19fe9b8f6878bed8b7f58be46e731ffb
IMG_20160823_130922.jpg	3ec7e648ea97e41a192d5c1453087699
Fallen_Champions_concept_art_3.jpg	d21158a66ca1fa9d73146043d8b93164
Fungus-Documentation.pdf	80d3528a9d94cc96b3f3436eb5414b87
companydata.csv	601eecf6163c9fd8c432c70bafe94e35
Computing_short19.pdf	8778591a432c4d03dc3738eae1075f9e

3.8.3 Is it possible to restore the affected data?

TeslaCrypt was terminated in 2016, and its master decryption key was publicly released through their former payment website (Figure 15) [5]. Consequently, the key or tools like TeslaDecrypt can now be employed to restore all affected files. By utilizing this software, I successfully recovered nearly all of Peter's files, with the exception of *passwords.docx*. It appears that Peter may have encrypted this file himself, possibly using the encryption program installed on his computer. To illustrate, consider the decrypted file *monster_concept_art_vii_by_d_faultx.jpg* shown in Figure 16. Also note that the leaked photograph is included in the list of encrypted files.

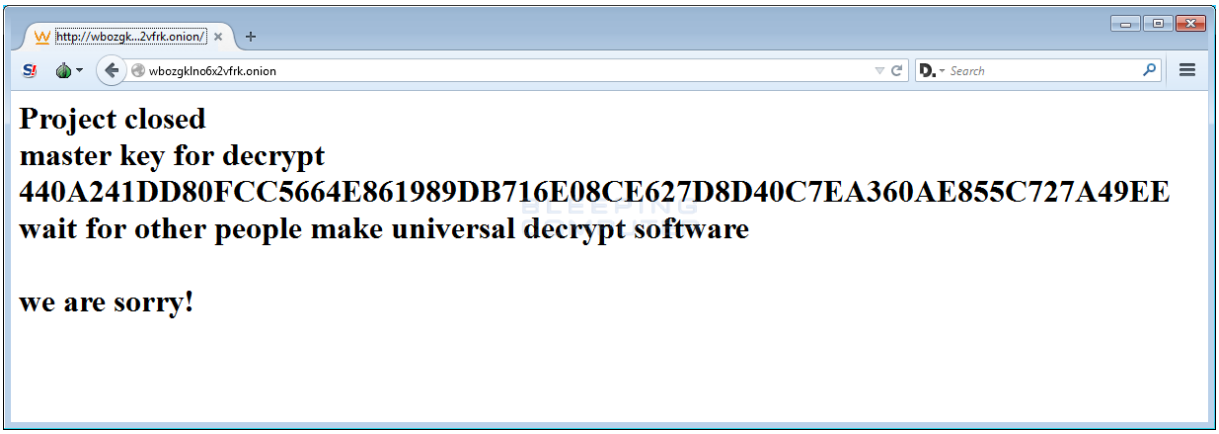


Figure 15: TeslaCrypt's payment site displaying the master decryption key

Figure 16: One of the pictures present amonght Peter's encrypted files

4 Literature Cited

References

[1] Forensics Matters. Find out windows installation date, 2018. URL https://www.forensics-matters.com/2018/09/15/find-out-windows-installation-date/.

[2] Spiceworks. How to find windows 10 original install date? (not the last updated date), 2017. URL https://community.spiceworks.com/topic/2076966-how-to-find-windows-10-original-install-date-not-the-last-updated-date.

[3] Zainab Falak. How to check your startup and shutdown history in windows, 2022. URL https://www.makeuseof.com/windows-check-startup-shutdown-history/.

[4] Abhishek Kumar Mishra. How to find the sid of any user in windows 11, 2023. URL https://www.makeuseof.com/find-sid-of-any-user-in-windows/.

[5] Lawrence Abrams. Teslacrypt shuts down and releases master decryption key, 2016. URL https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/.