

# ASSIGNMENT 2: FILE SYSTEM

## Digital Forensics

Elisa Pioldi  
ID 12305812

November 28, 2023

## 1 Factual part

### 1.1 Background

The company Indiga has developed a video game called Sniper, but the designer Sabrina found that the main character of the brand new game presented by competing company was suspiciously similar to her own concept. The investigators have confiscated the home computer of Peter (who is a developer at Indiga) and have acquired a forensic image. Hash (SHA-1) of the image is `b4c3ae80f840bb612f982ba5081872b8a6a19e83`.

The goal is to find evidence that Peter has leaked information about the game to the competing company.

The Indiga employees involved in the case are the following:

- **Anna:** director and founder of Indiga, mainly responsible for business challenges
- **John:** co-director, founder and lead developer
- **Iris:** developer
- **Peter:** developer and primary suspect
- **Sabrina:** designer

### 1.2 Software and hardware specifications

For this analysis, I utilized the following software:

- **Autopsy** [1] – version 1.24 (update 7); to perform container mounting and access.
- **Qemu** [2]; to convert the image from qcow format to raw format.
- **PhotoRec** [3] – version 6.2.6; to perform file carving.
- **TeslaDecrypter** [4]; to decrypt the files encrypted by the ransomware TeslaCrypt.



(a) Autopsy logo.



(b) PhotoRec logo.

### 1.3 Initial setup

First, I had to convert the image from qcow format to raw format, which is supported by the utilized tool, using Qemu.

Then, I analyzed the image using Autopsy. After a first analysis, I performed file carving using PhotoRec on the unallocated space of the image.

### 1.4 System specifications

The image analyzed is a desktop computer, with a 64-bit architecture, running Windows 7 Professional Service Pack 1. You can find more details in Table 1.

System specifications	
<b>Operating system</b>	Windows 7 Professional Service Pack 1
<b>Computer name</b>	HYRULE
<b>Installing date of the OS</b>	2016-07-06 23:27:42 GMT+0000
<b>Last usage time</b>	2016-09-05 15:28:53
<b>SID</b>	S-1-5-21-3032217210-630098460-752710606

Table 1: Statistics of some cracked containers.

### 1.5 Suspicious activity

After a deep analysis of the file system, I found numerous files linked to tutorials about games and game design, with a lot of examples of concept arts.

Moreover, analyzing web history, I found out that Peter has visited numerous websites to find a way to hide files on his computer.

### 1.6 Notable files

In this analysis I will focus on the files that I found more relevant to the case, which are two e-mail exchanges and a photo of a concept art.

To verify the integrity of files found, I computed the SHA-1 checksum of some of them. The results are shown in Table 2.

The major evidence that I found is the following e-mail exchanges between Peter and Iris.

### 1.6.1 Email exchanges

**First email exchange** The following e-mail exchange is the first one in time between Peter and Iris, where they are planning a date.

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

On 2016-08-24 01:28, Peter wrote:
> Hey,
>
> nice! Puh the traffic today was terrible...
> Hope you had a nice ride. :)
>
> Am Wed, 24 Aug 2016 00:48:30 +0200
> schrieb briennefan@openmailbox.org:

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

**Second email exchange** The following e-mail exchange is the second one in time between Peter and Iris, where they are talking about a date they had.

```
On 2016-08-24 01:36, Peter wrote:
> Hey,
>
> it felt like one, hope do not take it wrong, that I call our meeting a
> date.

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. ;)
```

**Third email exchange** The following e-mail exchange is the third one in time between Peter and Iris, where Iris is asking Peter about some design concepts of Sabrina.

```
> >> > On 2016-08-24 01:43:05 +0200
> >> > schrieb briennefan@openmailbox.org:
```

```
> > > Hey, can you do me a favor?
> > > you seen some design concepts of Sabrina?

> > On 2016-08-24 01:45, Peter wrote:
> > > Nope, not really. She only shows it to Anna and John, but I know
> > > that she keeps it in her desk. Why?

> > On 2016-08-24 01:46:58 +0200
> > schrieb briennefan@openmailbox.org:
> > Can you get a copy for me? I'm very interested in it :)

> On 2016-08-24 01:49, Peter wrote:
> > Hehe why don't you just wait until she presents the first 3D model?
> > Sometimes she lets her drawings unlocked on her table, but I don't
> > think that I should copy them :/

On 2016-08-24 01:51:15 +0200
schrieb briennefan@openmailbox.org:
> I'm very impatient. Please do it for me, maybe I will reward you with
> another date? ;)
```

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

**Fourth email exchange** This is the last e-mail exchange between Peter and Iris, where Peter is asking Iris about the leak of information.

```
Date: Wed, 24 Aug 2016 02:01:36 +0200
From: Peter <peter1983@openmailbox.org>
To: briennefan@openmailbox.org
Subject: Question
```

Hey Iris!

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.

Peter

For further analysis on the mail exchange, see Section 2.1.

### 1.6.2 Concept art

I found a photo of a concept art, which is shown in Figure 2. This file was found in 3 different situations: one as deleted file, one as encrypted file (see Section 2.3) and only the last one as a normal file which could be opened.

Analysis of the picture is shown in Section 2.2.

Content	SHA-1
Nina concept art	98296EF2B0A297A323EA36CA7E5C31399D412D91
1st email exchange with Iris	7CCB4BF11E4601E9DCFC1821F286CF673DA4142E
2nd email exchange with Iris	74D1A62DCB6332BD1215083B99FB0A92F95CDDE4
3rd email exchange with Iris	3486BE7A44BA05D0EED985881C38C2DC226CC4E5
4th email exchange with Iris	E08A6FCED0D464E55C4C4357164B4258E9F634B9

Table 2: Checksums of the most important files for evidence.

### 1.7 Malware traces

In addition of the files mentioned above, I found a great amount of files with the extension .mp3, which were all encrypted. They were in different location, but all of them were in private folders of Peter and looked like personal files. The files mentioned are the following (see Table 3 for the checksums):

- Fallen\_Champions\_concept\_art\_3.jpg.mp3
- Fungus-Documentation.pdf.mp3
- IMG\_20160823\_130922.jpg.mp3
- Leonard\_Nimoy\_William\_Shatner\_Star\_Trek\_1968.JPG.mp3
- monster\_concept\_art\_vii\_by\_d\_faultx.jpg.mp3
- myrating.csv.mp3
- passwords.docx.mp3
- unityassetstoreguide.pdf.mp3
- contactdata.csv.mp3

Content	SHA-1
Fallen_Champions_concept_art_3	457598C7417C909EEA12756E8DA5775311627B36
Fungus-Documentation	DE51A21FBF86F8A840F9E44FB9CCB1986B31ECFD
IMG_20160823_130922	98296EF2B0A297A323EA36CA7E5C31399D412D91
Leonard_Nimoy_William[...]	E02A76764D9DF6EACA8A237A74E1A5E6EC35C356
monster_concept_art_vii[...]	6BB17DAF3AF58C660D50C47D2CA0CB0A0F32BD96
myrating	8C08911E7C740AC2A4E15F876DACFE7C4846D2DE
passwords	11473175A82EF96BF0588BFC5308FD787A7FC17F
unityassetstoreguide	A6BDBA728EBC450CE7353596C460543094DC5196
contactdata3	AD862FCC026E81639E15033DD886EC09CB46CB14

Table 3: Checksums of the files encrypted by the malware.

As confirmation of this anomaly, I found an e-mail from Peter to tech support, signaling this weird behavior of the computer:

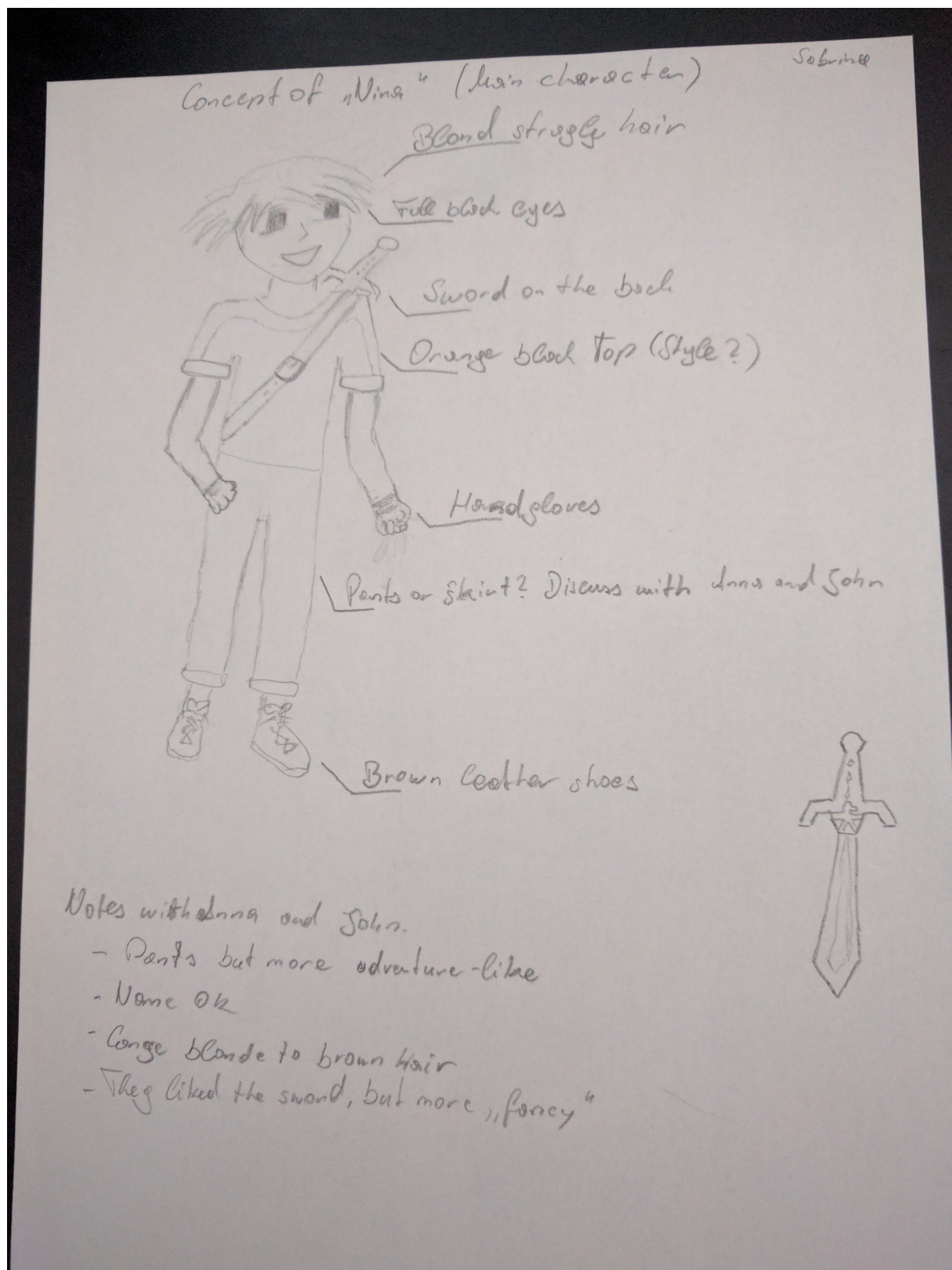


Figure 2: Nina concept art.

Hello Dude!

Can you help me? Suddenly my files changed to mp3's and I got some strange messages with "IMPORTANT INFORMATION" and I cannot open those files... I did nothing great, I browsed the web for stuff and then I got this message...  
Maybe you can help me? I got some of the data back, but I saved the mp3 to be safe.

Thank you  
Peter

I also found three files called \_RECoVERY\_+wdbic of different types (PNG, HTML, TXT) in the Roaming directory (see Table 4 for the checksums). You can see the content of the HTML file in Figure 3

Further analysis on these files is shown in Section 2.3.

Content	SHA-1
Email exchange with the tech support	A9E2290731742703465F183C5F4E52CD640E65C6
_RECoVERY_+wdbic.html	FD47F9BC079230331F239A6DE549FB60F625E124
_RECoVERY_+wdbic.png	8BDAF44B3454C4DE35B13F66AB04F8092DCAFB5

Table 4: Checksums of the ransomware notes and the e-mail to tech support.

## 2 Expert testimony

### 2.1 Mail exchange

Reading the e-mails, I found out that Iris has asked Peter to steal the concept art from Sabrina's desk (since sometimes she leaves drawings unlocked on the table), getting advantage of the fact that Peter seems to like her: from previous e-mails (first and second exchange), I understood that they have been already on a date.

From the fourth e-mail exchange, I found out that Peter has been accused of leaking information about the game, and he is asking Iris to talk about it in private.

These two emails are the evidence that Iris has leaked information about the game to the competing company with high probability, getting advantage of the fact that Peter likes her.

### 2.2 Concept art

The concept art found is a drawing of the main character of the game, Nina. We can spot the name of the designer, Sabrina, on the top right corner of the image and the mentions to Anna and John, who suggested some changes to the design. This is probably the file that Iris asked Peter to steal.



**NOT YOUR LANGUAGE? USE [Google Translate](#)**

**What happened to your files?**  
All of your files were protected by a strong encryption with RSA4096  
More information about the encryption RSA4096 can be found [https://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

**What does this mean?**  
This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them

**How did this happen?**  
Especially for you, on our SERVER was generated the secret key  
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.  
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!

**What do I do?**  
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed  
If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- 1 - <http://sondr5344ygfweyjbfbkw4fhsefv.heliofetch.at/E19054AC2D59D238>
- 2 - <http://pts764gt354fder34fsqw45gdfsavadfgsfk.kraskula.com/E19054AC2D59D238>
- 3 - <http://yyre45dbvn2nhbefbmh.begumvelic.at/E19054AC2D59D238>

If for some reasons the addresses are not available, follow these steps:

- 1 - Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- 2 - After a successful installation, run the browser and wait for initialization.
- 3 - Type in the tor-browser address bar: [xlowfznrg4wf7dli.onion/E19054AC2D59D238](http://xlowfznrg4wf7dli.onion/E19054AC2D59D238)
- 4 - Follow the instructions on the site.

**!!! IMPORTANT INFORMATION:**

Your Personal PAGES:  
<http://sondr5344ygfweyjbfbkw4fhsefv.heliofetch.at/E19054AC2D59D238>  
<http://pts764gt354fder34fsqw45gdfsavadfgsfk.kraskula.com/E19054AC2D59D238>  
<http://yyre45dbvn2nhbefbmh.begumvelic.at/E19054AC2D59D238>  
Your Personal TOR-Browser page : [xlowfznrg4wf7dli.onion/E19054AC2D59D238](http://xlowfznrg4wf7dli.onion/E19054AC2D59D238)  
Your personal ID (if you open the site directly): **E19054AC2D59D238**

Figure 3: Ransomware note.

## 2.3 Malware

### 2.3.1 Discovery

I found traces on the device of the malware TeslaCrypt, which is a ransomware that encrypts files on the victim's computer and asks for a ransom to decrypt them [5]. The first thing I noticed was the great amount of files with the extension .mp3, and the fact that they were all encrypted. Moreover, I found an e-mail from Peter to tech support, signaling this weird behavior of the computer.

Conducting a search on the Internet, I found out that the malware TeslaCrypt is responsible for this kind of encryption. This malware is common downloading games: this is compatible with the fact that Peter is close to the gaming industry.

I started looking for the ransom note, which is usually a file with the recovery instructions: indeed I found the file \_RECOVERY\_+wdbic.html (see Figure 3).



### 2.3.2 Decryption

Conducting some researches, I found out that the author of the ransomware have released the master key [6]:

440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE

There are some tools to decrypt the files: I used the tool TeslaDecrypter [4] to decrypt the files with the extension .mp3.

One of the file affected was the concept art of the game.

## 2.4 Future work

After this analysis, I would recommend to the investigators to analyze the computer of Iris, to find out if she has leaked the concept art sent by Peter. It would be significant to analyze her e-mails and her web history, to find out if she has any contact with the competing company.

## References

- [1] SLEUTH KIT LABS. *Autopsy*. URL: <https://www.autopsy.com/> (visited on 10/2023).
- [2] Fabrice Bellard. *QEMU*. URL: <https://www.qemu.org/> (visited on 10/2023).
- [3] Christophe Grenier. *PhotoRec*. URL: <https://www.cgsecurity.org/wiki/PhotoRec> (visited on 10/2023).
- [4] Talos. *TeslaCrypt Decryption Tool*. URL: [https://www.talosintelligence.com/teslacrypt\\_tool](https://www.talosintelligence.com/teslacrypt_tool) (visited on 10/2023).
- [5] *TeslaCrypt*. URL: <https://en.wikipedia.org/wiki/TeslaCrypt> (visited on 10/2023).
- [6] Lawrence Abrams. *TeslaCrypt Shuts Down and Releases Master Decryption Key*. May 18, 2016. URL: <https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/> (visited on 10/2023).