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 Snipper, 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.
- **PhotoRec** [2] – version 6.2.6; to perform file carving.
- **TeslaDecrypter** [3]; to decrypt the files encrypted by the ransomware TeslaCrypt.

1.3 Initial setup

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

(a) Autopsy logo.

(b) PhotoRec logo.

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	
Operating system	Windows 7 Professional Service Pack 1
Computer name	HYRULE
Installing date of the OS	2016-07-07 01:27:42
Last usage time	2016-09-05 15:28:53
SID	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 website 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

```
>> 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

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

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

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

> >> > 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 01:45, Peter wrote:

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

> > On 2016-08-24 01:46:58 +0200
> > schrieb briennefan@openmailbox.org:

> > 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 01:49, Peter wrote:

> I'm very impatient. Please do it for me, maybe I will reward you with
> another date? ;)

On 2016-08-24 01:51:15 +0200
schrieb briennefan@openmailbox.org:

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

Fourth email exchange

```
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. Analysis of the picture is shown in Section 2.2.

1.7 Malware traces

In addition of the files mentioned above, I found a lot of files with the extension `.mp3`, which were all encrypted. As confirmation of this, I found the following e-mail exchange between Peter and the tech support:

```
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
```

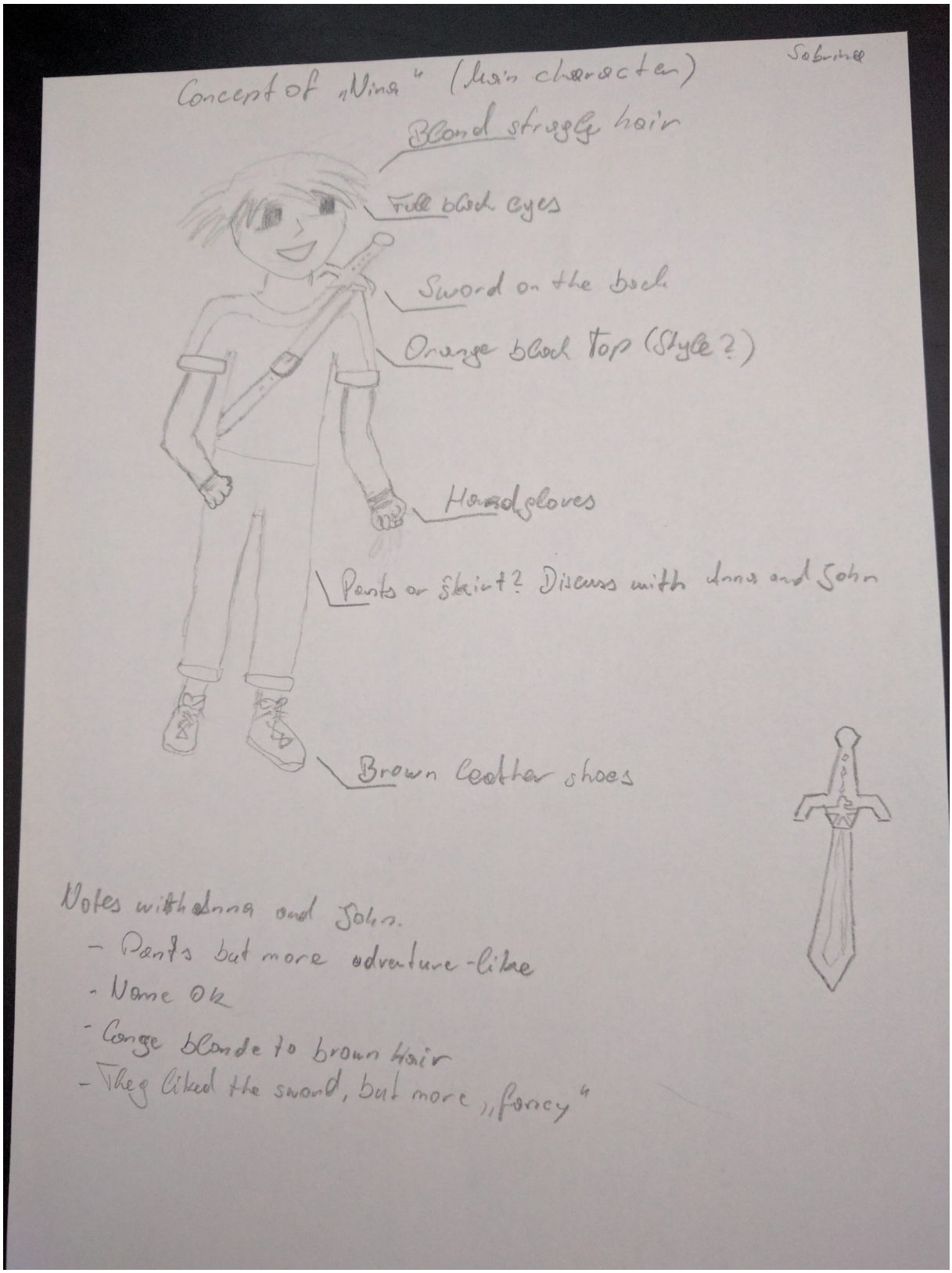

Figure 2: Nina concept art.

I also found a file called `_RECoVERY_+wdbic.html` (see Figure 3).
Further analysis on these files is shown in Section 2.3.

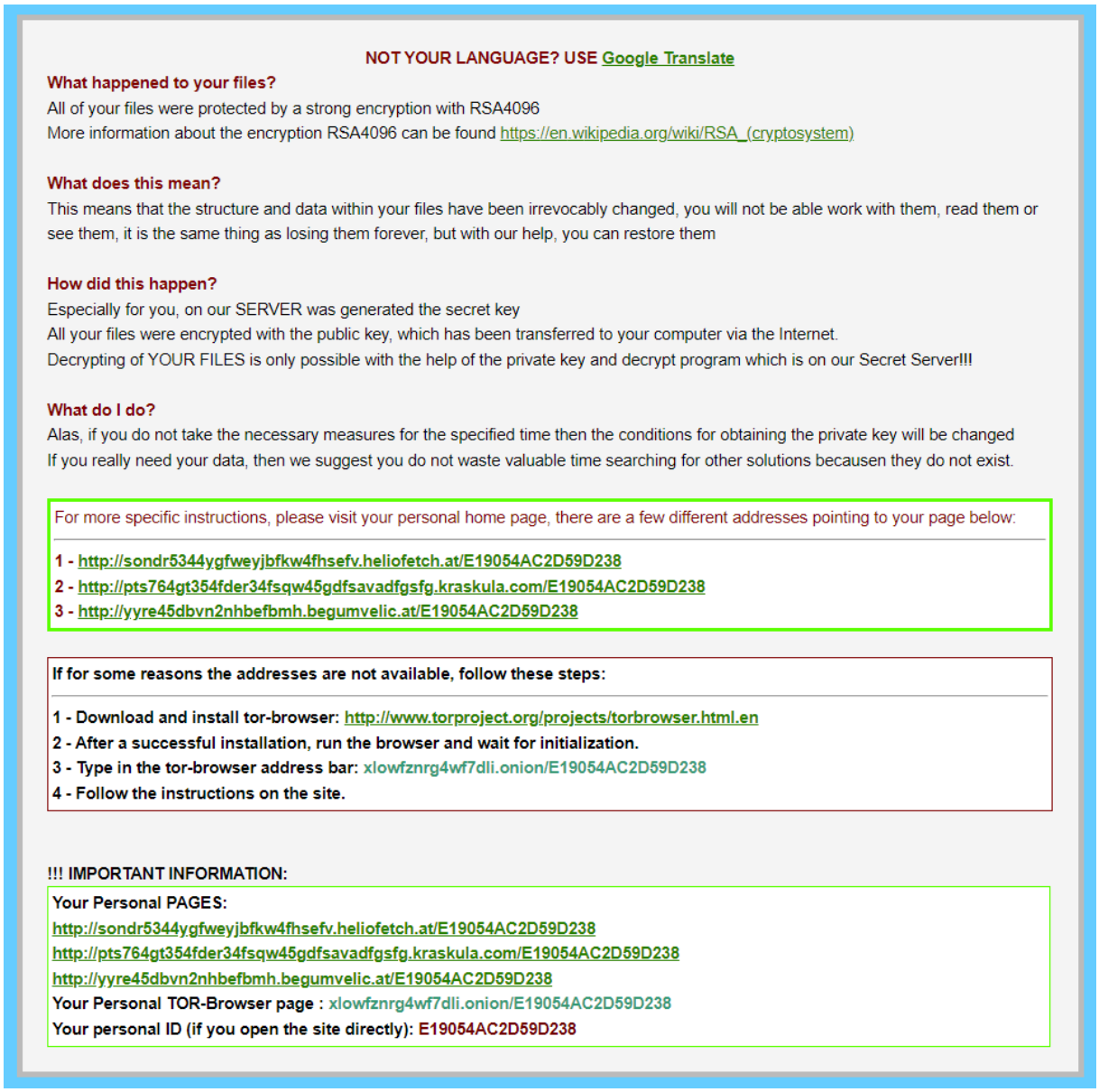

Figure 3: Ransomware note.

Content	SHA-1
Nina concept art	98296EF2B0A297A323EA36CA7E5C31399D412D91
Ransomware note	FD47F9BC079230331F239A6DE549FB60F625E124
1st email exchange with Iris	7CCB4BF11E4601E9DCFC1821F286CF673DA4142E
2nd email exchange with Iris	74D1A62DCB6332BD1215083B99FB0A92F95CDDE4
3rd email exchange with Iris	3486BE7A44BA05D0EED985881C38C2DC226CC4E5
4th email exchange with Iris	E08A6FCED0D464E55C4C4357164B4258E9F634B9
Email exchange with the tech support	A9E2290731742703465F183C5F4E52CD640E65C6

Table 2: Checksums of some files.

2 Expert testimony

2.1 Mail exchange

Reading the e-mails, I found out that Peter has asked Iris to steal the concept art from Sabrina's desk (since sometimes she leaves drawings unlocked on the table), getting advantage of the fact that Iris seems to like him: 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 understood 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 Peter has leaked information about the game to the competing company with high probability.

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 Peter asked Iris to steal.

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. 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, and there are some tools to decrypt the files. I used the tool TeslaDecrypter [3] 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 reccomend to the investigators to analyze the computer of Iris, to find out if she has leaked other information about the game. Moreover, since Peter tried to hide the files, I would suggest to find the password to the TrueCrypt container, to see if there are other files that he tried to hide, like any contact with the competing company, and a concrete proof of the leak.

Do we have to list all the files affected by malware? Do we need to find the password to TrueCrypt container? Weird installation date

Sources

[1] SLEUTH KIT LABS. *Autopsy*. URL: https://www.autopsy.com/ (visited on 10/2023).

[2] Christophe Grenier. *PhotoRec*. URL: https://www.cgsecurity.org/wiki/PhotoRec (visited on 10/2023).

[3] Talos. *TeslaCrypt Decryption Tool*. URL: https://www.talosintelligence.com/teslacrypt_tool (visited on 10/2023).