INTRODUCTION

This investigation supports Indiga, a video game developer, in examining potential intellectual property theft related to their game "Snipper." A competitor recently showcased a game with a main character closely resembling Sabrina's design, prompting legal scrutiny. As part of a Digital Forensics course, students assumed the role of analysts to conduct this simulated investigation.

The analysis centered on a qcow image of Peter's Windows 7 home computer, with Peter being a developer at Indiga and the main suspect. Key individuals include Anna (founder and director), John (co-founder and lead developer), Iris (developer), Sabrina (designer), and Peter.

The project's core objective was to master forensic techniques for data retrieval, analysis, and documentation. Tasks included file carving and recovering deleted files, with Autopsy recommended for hands-on forensic practice.

1 FINDINGS (BEFUND)

Upon receiving the disk image, the first step was to ensure its integrity by generating SHA-1 hashes for both the original and cloned files. This precautionary measure allowed for verification throughout the investigation.

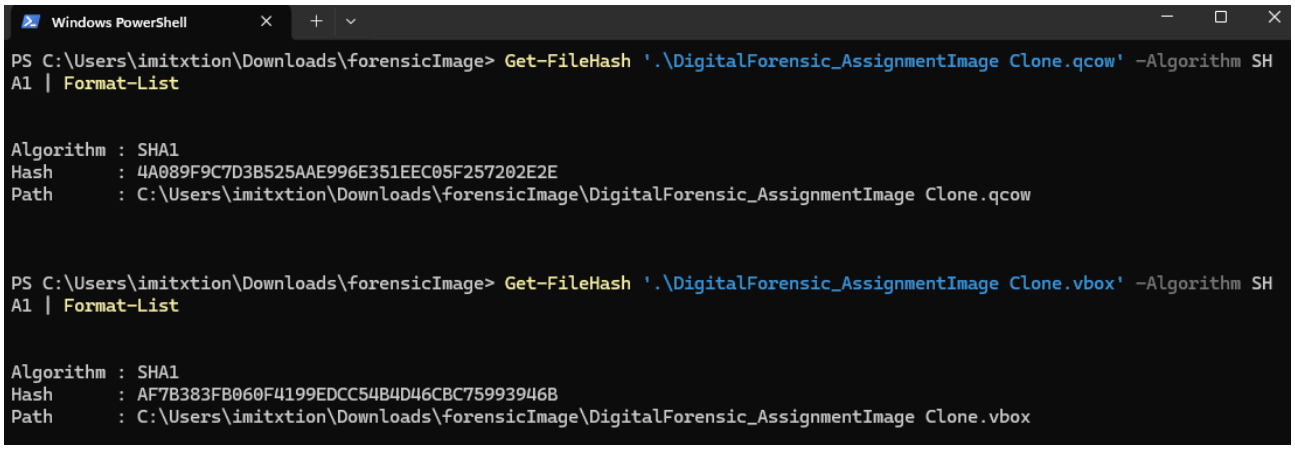


Image 1: Hashes of initial files

DigitalForensic_AssignmentImage Clone.qcow:

SHA-1: 4A089F9C7D3B525AAE996E351EEC05F257202E2E

DigitalForensic_AssignmentImage Clone.vbox:

SHA-1: AF7B383FB060F4199EDCC54B4D46CBC75993946B

Using VirtualBox (v6.1.38), a copy of the system was booted, revealing a Windows 7 environment with three user accounts: Gary, Peter, and StuffAccount. Peter's account was password-protected, indicating its significance. Initial exploration of public directories uncovered files related to character designs, including a notable image signed by Sabrina (Image 2), stored in *C:\Private\Work\Info*. This image, dated August 24, 2016, included references to discussions with Anna and John, suggesting its relevance to the case.

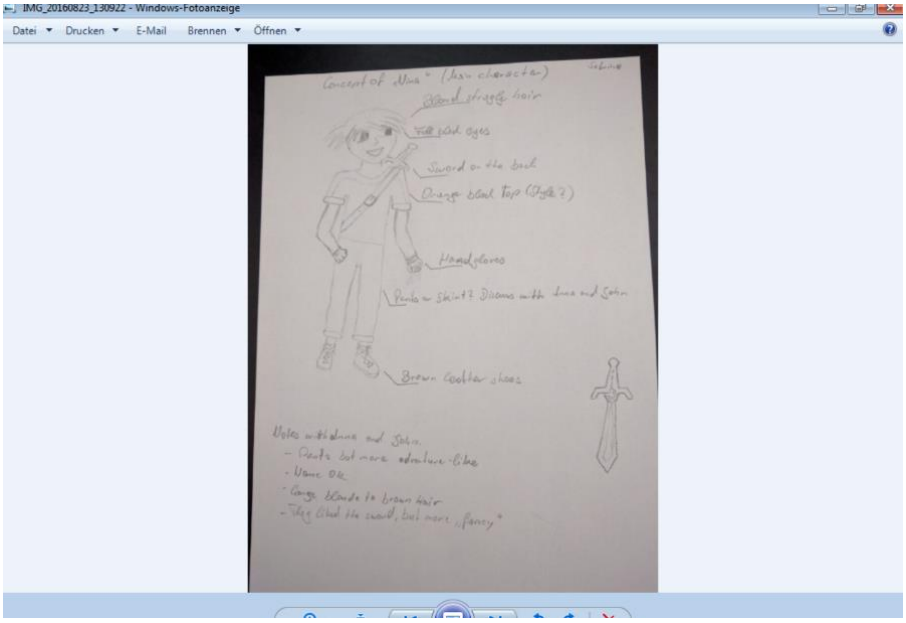


Image 2 – Character design

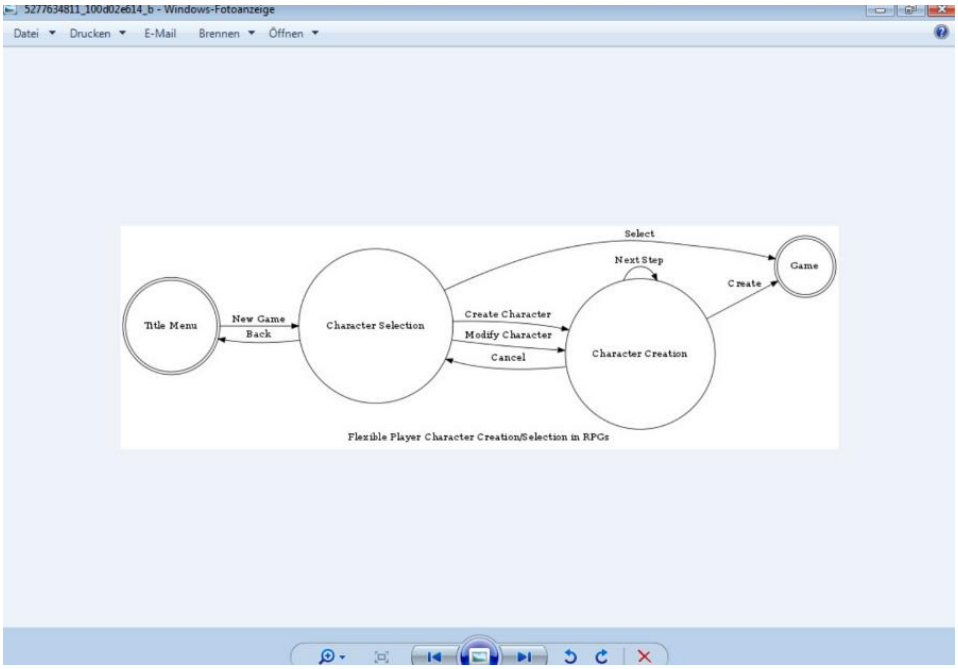


Image 3 – Character creation flowchart

Autopsy (v4.22.1) was then employed for in-depth analysis, including file carving and recovery of deleted data. The process, though time-intensive, yielded critical artifacts such as user profiles, browser history, and email communications. Among these, Peter's emails with *briennefan@openmailbox.org* (Iris) were pivotal, detailing their personal relationship and Iris's request for Sabrina's design. Peter's compliance, driven by emotional incentives, was evident in his August 24 email.

Conversation:

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.

Additionally, an email to *techsupportguy@mailinator.com* highlighted Peter’s encounter with ransomware, marked by files converted to MP3s and a ransom note. Web history analysis linked this to a "Clash of Clans" cheat download, confirming the malware as *TeslaCrypt*.

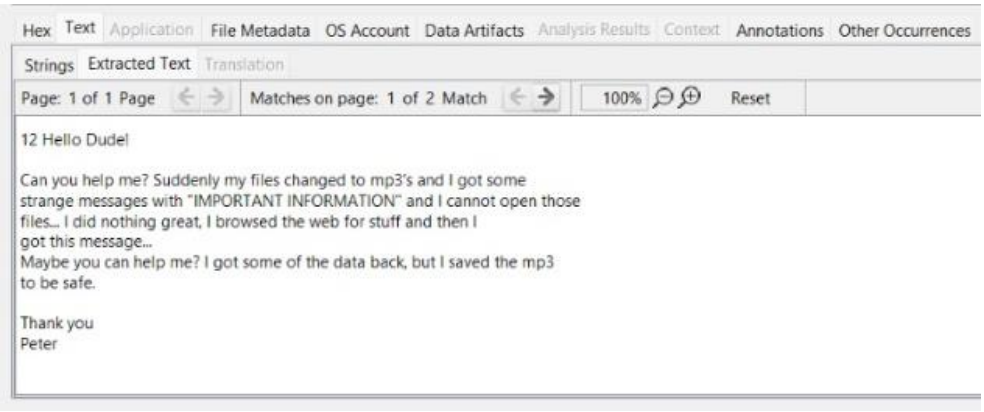


Image 4 - Email of Peter

Image 5 – Ransom note

2 ANALYSIS (GUTACHTEN)

This section addresses the specific questions posed in the assignment, providing detailed responses based on the investigation's findings.

3.1 What information was stolen?

The leaked data was a digital image of Sabrina's character design, originally displayed on her desk. Iris's emotional manipulation coerced Peter into sharing this restricted asset, intended only for Anna and John.

Evidence:

- Emails between Peter and Iris confirming the request and transfer.
- Browser history reflecting Peter's personal interest in Iris.

3.2 Which persons were involved in the case?

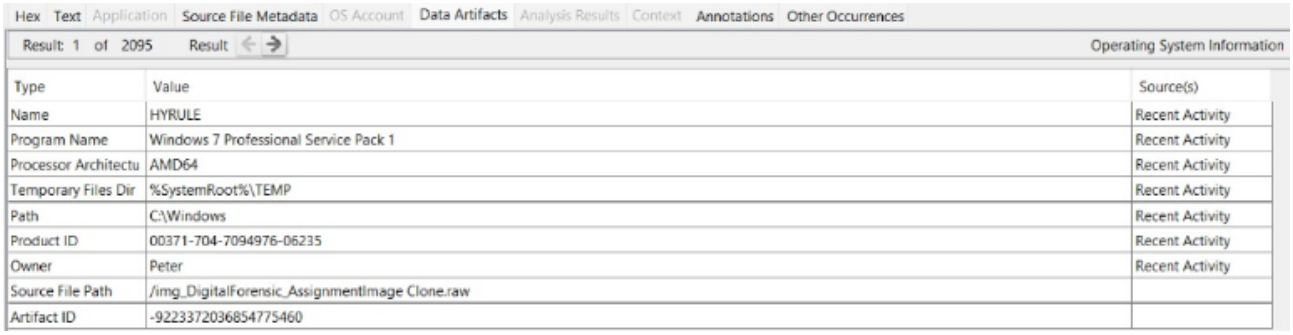
Peter and Iris were the primary actors in the breach, with Peter illicitly obtaining and sharing the design at Iris's behest. Sabrina, as the designer, is indirectly implicated, while Anna and John, though informed of the design, played no active role in the incident.

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

Further investigation should focus on Iris's communications and devices to trace the design's external dissemination. The TeslaCrypt infection, while notable, is unrelated to the breach. Peter's use of encryption tools, including a TrueCrypt container, suggests potential hidden information warranting examination.

3.4 What operating system was used?

The system runs Microsoft Windows 7 Professional with Service Pack 1 on an AMD64 architecture, registered to Peter with product ID 00371-704-7094976-06235.


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	

Image 6 – Operating system artifact

3.5 What is the computer's name?

The machine is named "HYRULE," as confirmed by system settings and forensic artifacts.

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

The OS was installed on July 7, 2016, approximately at 01:04, based on the client-side cache's last write time. The system was last booted on September 5, 2016, at 15:26:40, as per Event Viewer logs.

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

Peter's Security Identifier is S-1-5-21-3032217210-630098460-752710606-1001, retrieved via PowerShell.

3.8 Can you find traces of malware on the system?

Indeed, the system was compromised by TeslaCrypt ransomware.

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

The malware is TeslaCrypt, detected via Peter's correspondence with tech support and the "IMPORTANT INFORMATION" ransom note. Verification was achieved by cross-referencing the note's content with documented TeslaCrypt indicators.

3.8.2 Which data is affected?

Affected files, primarily those with altered extensions (e.g., .mp3) or corruption, include *contactdata.csv*, various images, and documents, all modified post-infection.

3.8.3 Is it possible to restore the affected data?

Restoration is feasible via the publicly available TeslaCrypt master key. Tools such as TeslaDecrypt can recover most files, though passwords.docx remains inaccessible, possibly due to separate encryption.

CONCLUSION

This investigation confirms that Peter, under Iris's influence, leaked Sabrina's character design, compromising Indiga's intellectual property. The unrelated

TeslaCrypt infection underscores broader security concerns. To mitigate future risks, Indiga should:

- Investigate Iris’s activities for potential external leaks.
- Implement stricter access controls and employee training on data security.
- Enhance malware protection measures.

These actions will help safeguard Indiga’s assets and prevent similar incidents.