**Forensics Case**

**X-X-X-X**

Contents

[1. Background 3](#_Toc121682923)

[1.1 Image 3](#_Toc121682924)

[1.2 Tools 3](#_Toc121682925)

[2. Examination Details 3](#_Toc121682926)

[2.1 Email Analysis 6](#_Toc121682927)

[3. Deleted, Encrypted, and Stegnagrahpic Files 8](#_Toc121682928)

[3.1 Stegnagrahpic Files 8](#_Toc121682929)

[3.2 Password-Protected Files 10](#_Toc121682930)

[3.3 XML Files 13](#_Toc121682931)

[3.4 Deleted Files & Mails 13](#_Toc121682932)

[6) Conclusion 15](#_Toc121682933)

[7) References 15](#_Toc121682934)

# Background

The forensics case was given for the analysis to find the Actor behind multiple activities that were done in which the suspect was the harvesting of emails to subscribe to different streaming services. While analyzing the image we saw different steganographic, deleted, encrypted, and many other files that had anti-forensics techniques applied to them. Then the major thing that was kept in the o account was that the timeline was a bit strange. This was because there were activities from 2009, 2015, 2018, and then 2022, and nothing was done in between these years. So initially we analyzed all of the recent activities and materials and saw that the perpetrator accessed and modified a lot of information. Then we applied the forensics techniques to each of the listed files to find strong evidence to prove that the person wants behind some malicious activities. In the report, we will tell and discuss each of the activities that the suspect was doing.

## Image Information

|  |  |
| --- | --- |
| Image | DFFCW2022.E01 |
| MD5 | 7a5d70b5e642b121d92a980efa51074a |
| SHA1 | dc091f7693ddee0eddf02620e62110a0181895d3 |

## Tools

These are the tools that were used during the analysis of the image:

1. Autopsy
2. OSForensics
3. AccessData- FTK Imager
4. ExifTool
5. Aperi’Solve

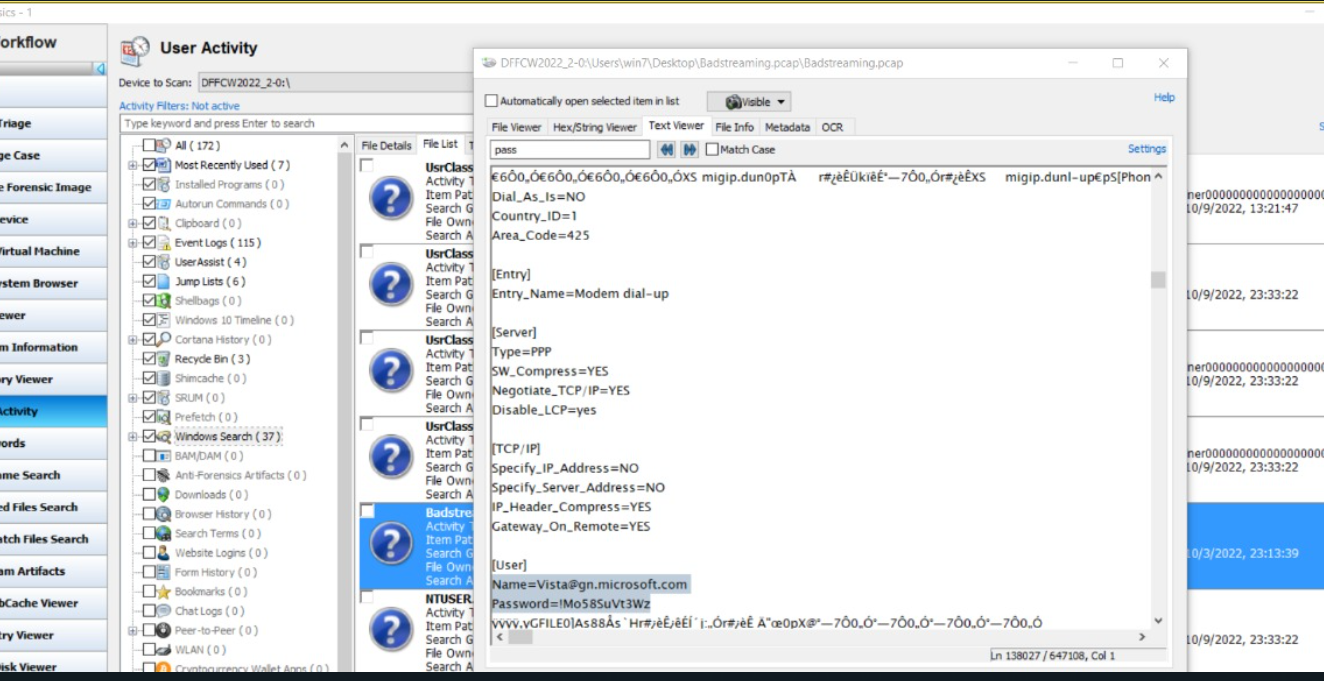
# Examination Details

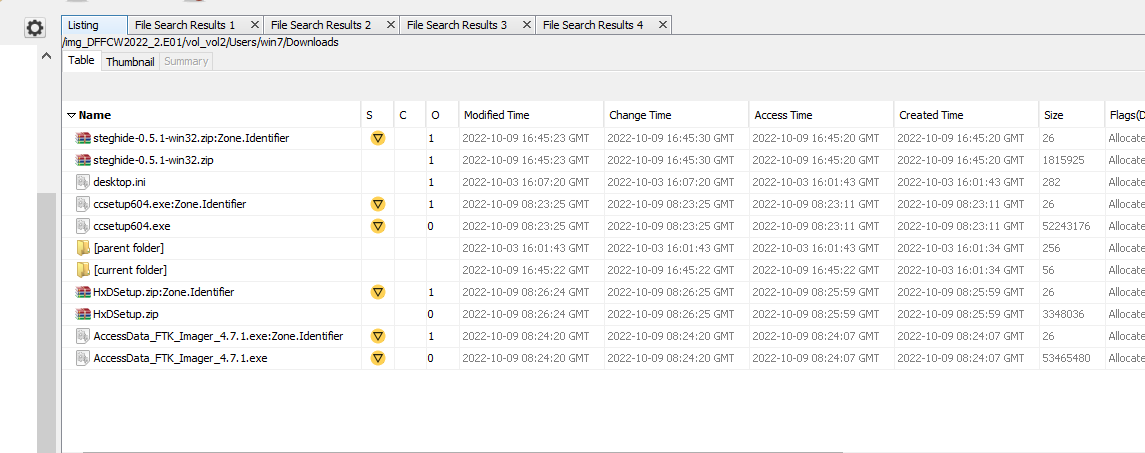
The below image shows the timeline of the activities that happened, and we can see that activities happened in a few of the periods. The red shows the system activities the green shows the web activity and the cyan shows the other activities.

Chart

Description automatically generated

The was a file **Badstreaming. pcap** file and we analyzed it to see what was inside the file then we received the credentials highlighted below, we tried these credentials at many places, but it was not applicable anywhere.

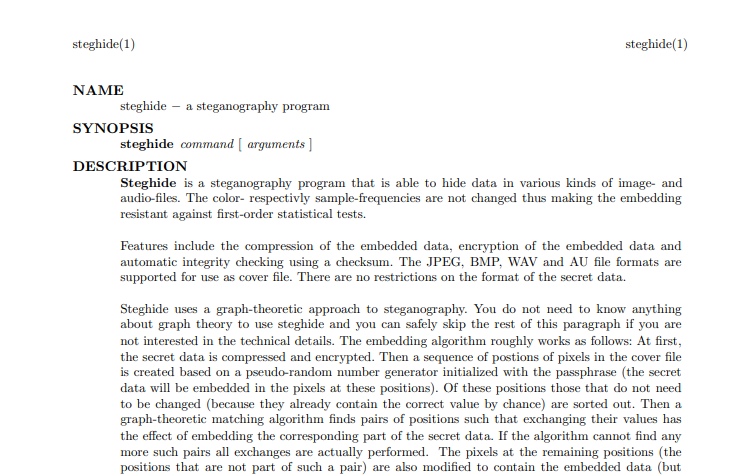




The information that was extracted using Autopsy was that in the download folder we can see many tools were downloaded by the suspect:

1. **Steghide**

We found **steghide-0.5.1-win32.zip** which was used to hide the customer information file in the images.



* Manual to-use steghide was also available in the image which helped extract the information from the image files. The process of extraction of information is in the latter part of the report.



* Emails were sent to Stefan Hetzel the author of steghide regarding the reports that were sent by them to the suspect.

1. **HxD**

We found **HxDSetup.zip** which was used to change the hex of different files which was suspicious.

1. **CCleaner**

CCleaner was also used to delete some of the information so that the suspect didn’t want the investigator to find it. It was also used to delete the **must\_be\_careful.eml** file which was sent to maybeto warn the other person. This tool uses anti-forensics techniques to delete files permanently.

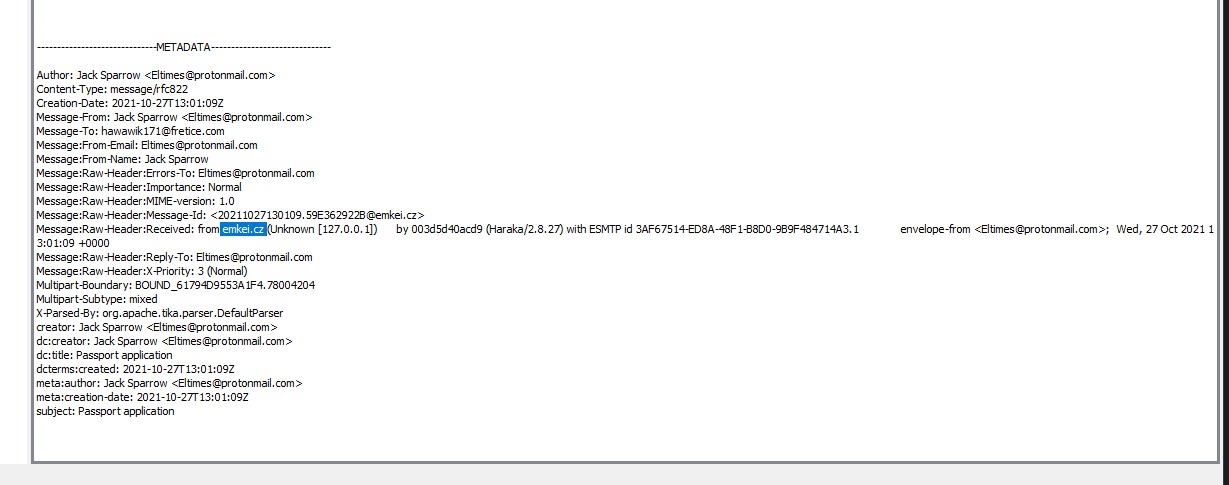
## Email Analysis

As the information extracted from the protect doc file “**How to Steal Credit Numbers.doc**” we found the method to extract credit information using emails. Then I searched the word “aol” which was used to send the email and was also mentioned in the doc file. The email was in French and other languages. I translated it and below is the image of the sample file translation.

Text

Description automatically generated

The above text in the image is very suspicious and doesn’t make proper sense so this may be the hidden conversion of the suspect and his compliance.

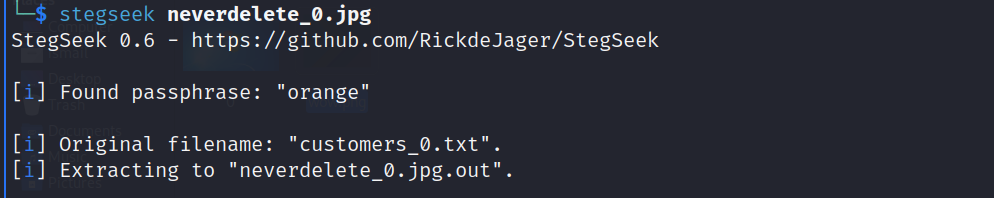


Emkei.cz is an email spoof/hijack/spam web site to send anonymous emails to anyone. The above screenshot shows that the suspect was using this website for sending spam mail.

# Deleted, Encrypted, and Stegnagrahpic Files

## Stegnagrahpic Files

The analysis of the Steganographic files:



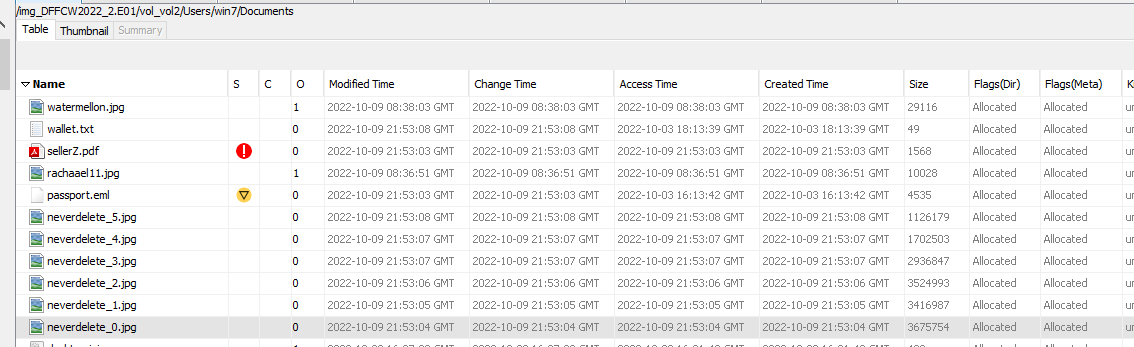
* The password was **“orange”**.

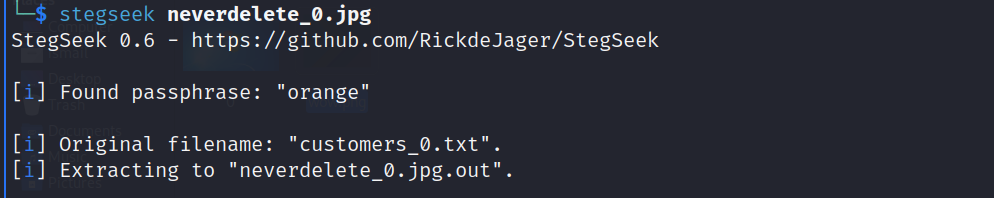
As discussed in the previous section, the suspect used **steghide** to hide the information in the pictures and then applied different passwords to protect them.

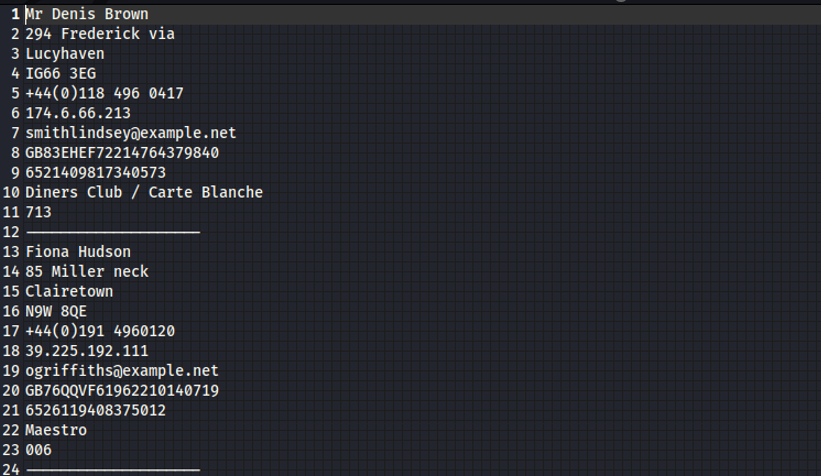
Graphical user interface, text, application, email

Description automatically generated

* There was this hint in one of the files that the password of the steganographic files is “Your friend’s favorite color”. Then, I generated a text file with all of the color names and then we applied the passwords on all of the images and text files and I was successful in that.



* So, after further analysis I came to know that some information is hidden in the images. The information was hidden with the password. On Brute Forcing the password I analyze that the password to hidden content is “**orange**”. I used **stegseek** to brute force the password and **steghide** to fetch the information from the image.
* On further Analysis of the txt files, I came to know that the .txt files contain the sensitive information of different people.



* The information includes the name, address, phone number, email, and credit card number with some other confidential information. Similarly, other images also had **Personal Identification Information**, which can be used for **data triangulation.**

**The hashes of the images and the hidden text files fetched from them are given below:**

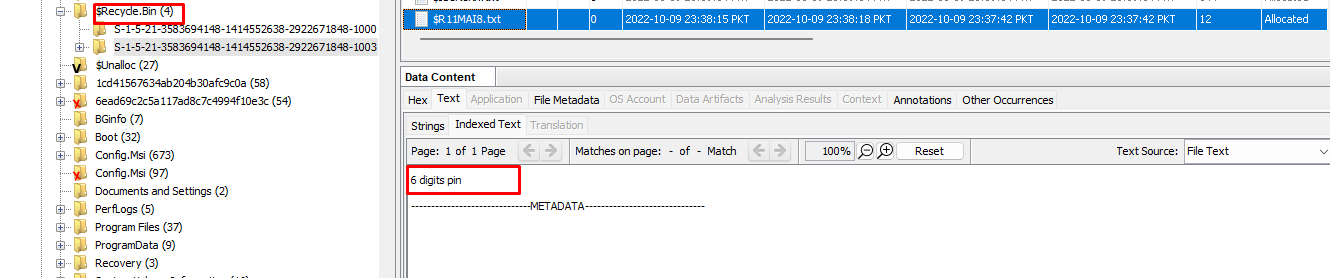
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  | | --- | | 57260a5894a0ab96a2bec51769534dfa |   f2e395c0d4052b2886302826a4e75022 | |  | | --- | | neverdelete\_0.jpg | | customers\_0.txt | |
| |  | | --- | | 3c82e680b3ccc429e7d11562ca0105ca |   d6d4b82c0b3d10b50c20673c4144109b | |  | | --- | | neverdelete\_1.jpg | | customers\_1.txt | |
| |  | | --- | | b0b5194653ddaa8715bf1da84437c3c3 |   80bf9437b2538890c29455c24bf665b1 | |  | | --- | | neverdelete\_2.jpg | | customers\_2.txt | |
| |  | | --- | | b458c64b13d1b9ae40b5821cf68a8be0 |   205df9f8c0a98adf774f60923add1e32 | neverdelete\_3.jpg  customers\_3.txt |

## Password-Protected Files

Many of the files had passwords:

1. Word
2. Pdf
3. Pdf
4. XML

All the above files had a password, the steganography password was detected using the hint given for the file password we looked for the hint and we received a hint.



* The hint was found in the Recycle Bin folder and that was a 6-digit pin.

While Analysis the file system, I saw the encrypted files. These encrypted files were very suspicious because of their title “**SellerZ.pdf**”, **“f0191736.pdf”** and “**How to Steal Credit Numbers.doc**”. The password of “SellerZ.pdf” was Brute forced and it was “**121212**”.

Text

Description automatically generated

On Opening the File, I found the seller’s information. These are the people to whom the suspect was selling the information. The same happened when I cracked the password of **f0191736.pdf** I got more information on the seller. This was suspicious why would a person have the information of sellers and encrypt those files?

Graphical user interface, application

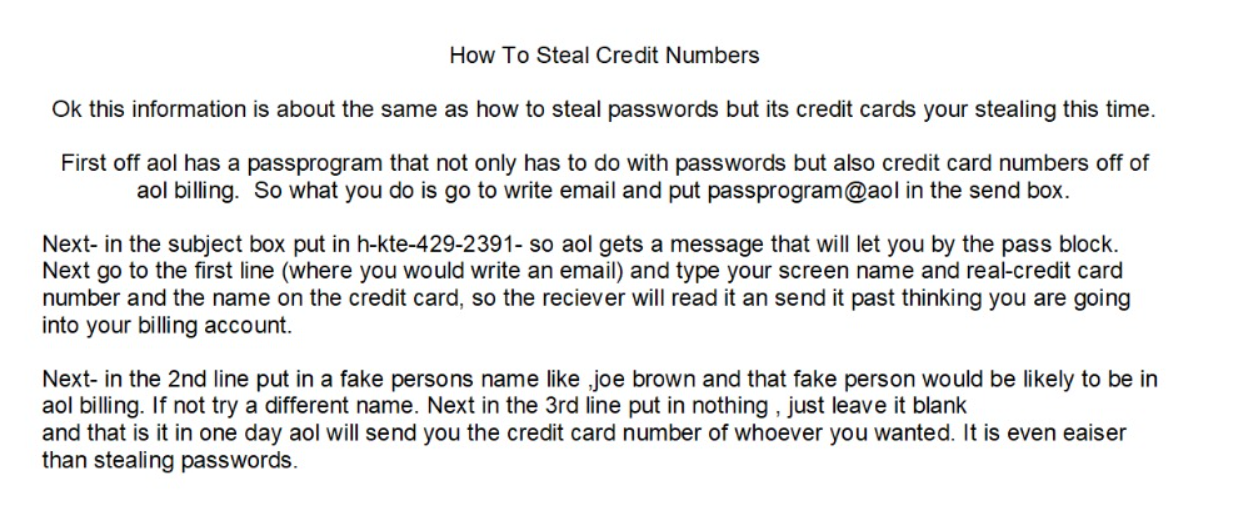
Description automatically generated with medium confidenceGraphical user interface, text, application

Description automatically generated with medium confidence

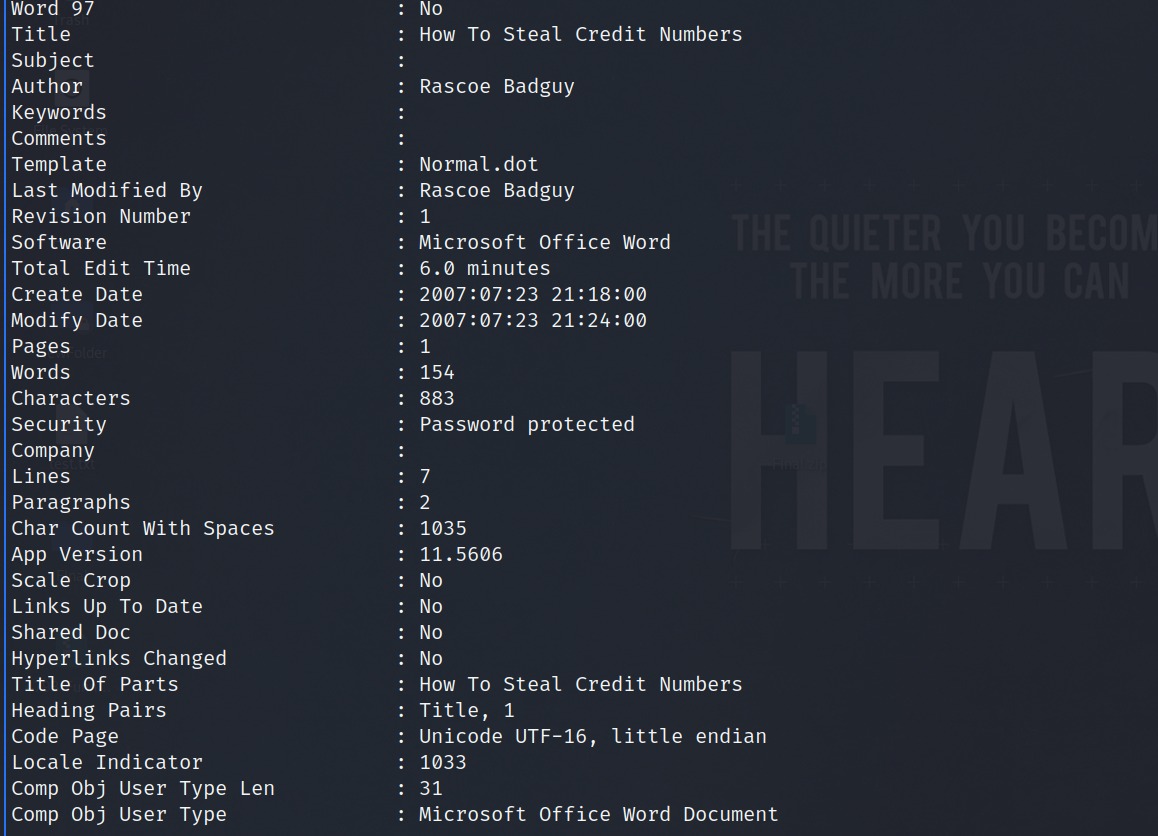
These were the names and contact information of the sellers.

On Further analysis, I was unable to find the password of the **“How to Steal Credit Numbers.doc”** file. As the word file was very old, so I applied the forensics techniques and used the vulnerability in Microsoft to decrypt the file using this website: <https://www.password-find.com/crack_office_password.htm?js=on>

On viewing this file, I find a clear method of stealing information. Below is the text in the file.



This information is very important for us as this file was hard to decrypt and shows us the method the suspect was using to get the credit card information. The suspect was using this process to get the information of different people and then saved this information in the images using the steganography tool **steghide**. This indicates that the suspect was involved in stealing the credit card information of the people.



This is the metadata of the word file, and we can see that the last modification was done by **“Rascoe Badguy”.**

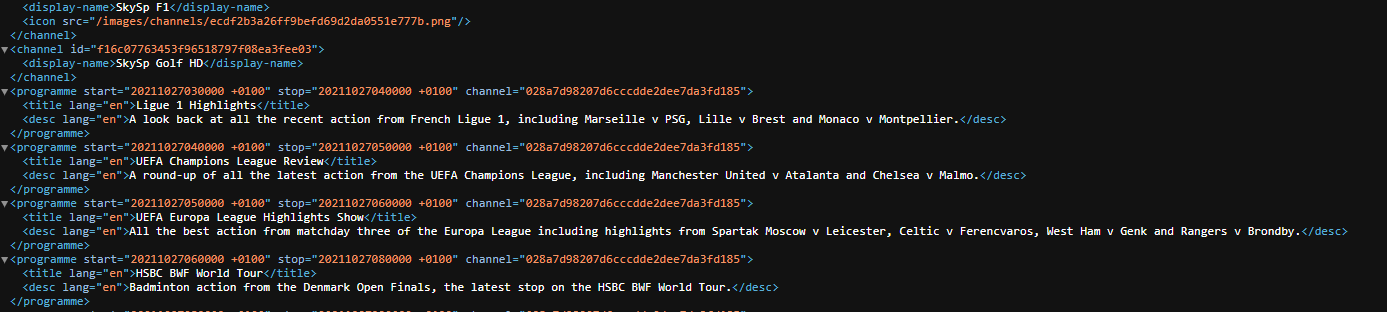
The hashes of the above files are given below:

|  |  |  |  |
| --- | --- | --- | --- |
| |  |  | | --- | --- | |  | d263db2a55516e67332ba6601236109f | | SellerZ.pdf |
| |  | | --- | | 018d1f4a74fd8f026c1f796c861b3611 | | |  | | --- | | How To Steal Credit Numbers.doc | |

## XML Files

When looking for the streaming services evidence, I came across a file named “**config.zip**” which was also encrypted with the password. By applying Forensics Password Recovery techniques, I was able to decrypt these files. The password of this file was also found to be “**121212**”.

On Analyzing this zip file, it had three different files inside of it. These three different files had the Streaming information. Below is the screenshot of the sample streaming service data



On viewing it on XML Editor, I analyzed that the information contains the XML Objects about each channel and a description of the program below are the hashes provided of the documents containing the Streaming Service information.

|  |  |
| --- | --- |
| 7fb620bad6029f7eb3a7687d597fbf65 | configs.zip |
| d40b9129b1a44f219dddce97872ae380 | 4378.xml |
| 5cd032d920551513f20599086c1403ac | 7365.xml |
| 79b173fc94d33f6e282d62a668e03159 | 9437.xml |

## Deleted Files & Mails

When analyzing the image file, I find some emails that were deleted. These emails look suspicious based on their titles. Following are some emails that were detected.

Graphical user interface, text, application, email

Description automatically generated

I was able to investigate “**passport.eml**” but I was unable to investigate “**customer\_complaint.eml**” and “**must\_be\_careful.eml**”. It is suspicious because the email was deleted with an anti-forensic tool such as CCleaner which was installed on the system. This gives me a clue that something suspicious was present in these emails that were deleted.

There were some deleted files as well. One of them gave clue about the zip passwords. The other important deleted file “**$RU3R5KX.txt**” has the Personal Identification information of different people including the credit card number which is very suspicious.

Text, letter

Description automatically generated

* The suspect tried to delete the file that contained all the information on different persons.

The hash of the file is given Below

|  |  |  |
| --- | --- | --- |
| |  | | --- | | 0772fca97c90869ed84d2f6b0321e084 | | $RU3R5KX.txt |

# Conclusion

There was multiple finding in this case which included:

1. Anti-forensics techniques:
2. Steganography
3. Encryption
4. Data wiping
5. Suspicious Emails and documents
6. Hidden Confidential Information (PII- Personal Identification Information)

With all this information and evidence we can conclude that the person must be persecuted further because the suspect used spamming websites to store personal and confidential information and also shared it with his/her compliance. Then the information that he received was inserted into the image files using steghide. The suspect also had communication with the steghide company the steghide manual was extracted which was used by the suspect to do steganography. The suspect also protected files with passwords that had information regarding the sellers and victims. One of the files also contained the process the suspect used to extract credit card information using spam mail. This credit card information was used by the suspect to do illegal activities.

\* All the screen shots have been taken by the Lightshot app (version: 5.5.0.4)

# References

1. <https://www.password-find.com/crack_office_password.htm?js=on>
2. <https://www.openwall.com/john/>
3. <https://github.com/RickdeJager/stegseek>
4. <https://github.com/StefanoDeVuono/steghide>
5. <https://github.com/ReFirmLabs/binwalk>
6. <https://accessdata.com/product-download/ftk-imager-version-4-5>
7. <https://www.aperisolve.com/>
8. <https://www.autopsy.com/>