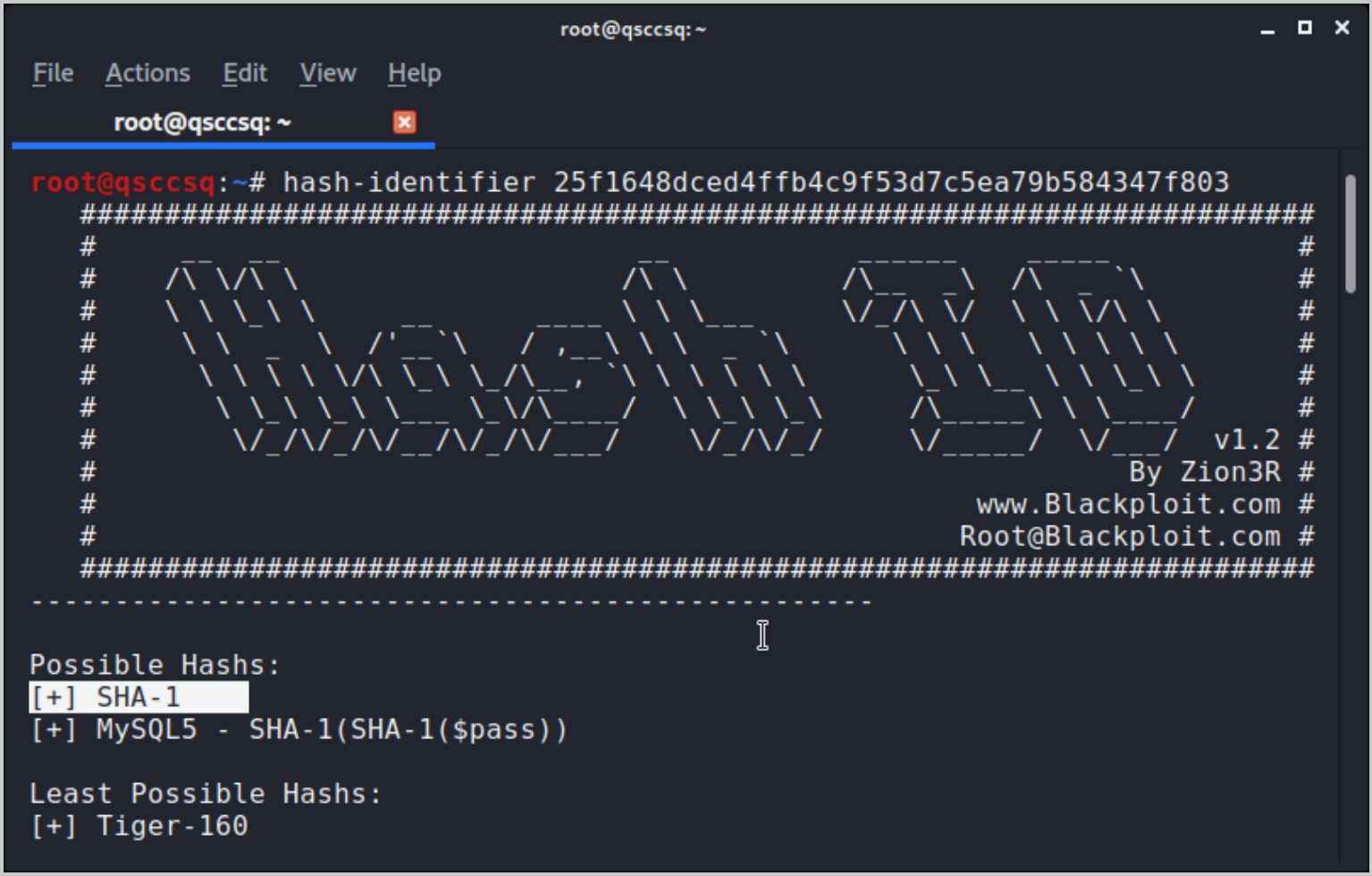
Content Hiding

Content hiding has always brought great advantages. Encryption - hiding methods dating back to 4,000 years are still used today. File encryption - hiding processes in technological devices are used from standard users to high level users. While hashing methods such as SHA, MD5, X11 are sometimes used by programmers to protect user data, simple ways such as file hiding or operating system login password are followed by standard users. Despite the fact that the methods such as SHA, X11, and MD5 are abused by hackers, it is getting easier day by day because every detected password will cause conflicts that will be caught in the future. That is, if we consider that the data with "Admin" content hashed with MD5, the "Admin" content will give the same MD5 output again by another user. Thanks to the application named "hash-identifier" in Kali Linux, unknown hash outputs can be checked;

Hash: 25f1648dced4ffb4c9f53d7c5ea79b584347f803



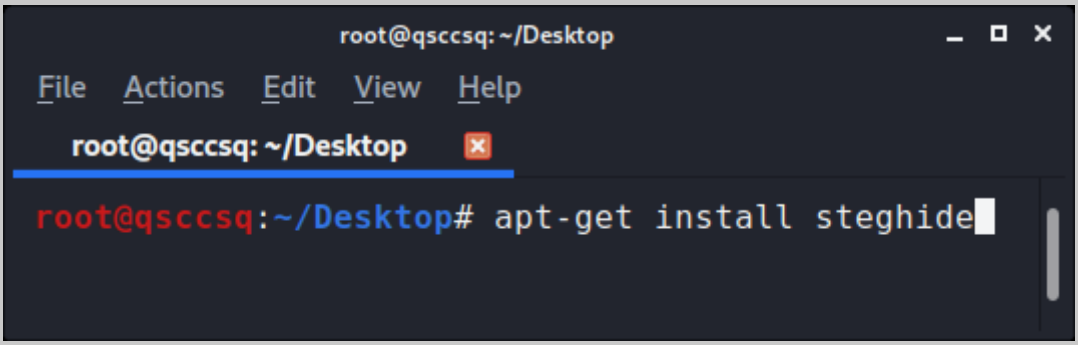
There are complex and safe ways for high-end users. For example, Host Protected Area (HPA) is a hidden hard disk space that is not normally seen by the operating system. It is often used by hardware manufacturers to store installation and driver files for the respective device. However, HPA has become a highly abused method by hackers solely due to access restrictions. The data of the suspect may be

overlooked during a digital forensic investigation as a result of transferring the data contained in HPA and transferring the files to be hidden.

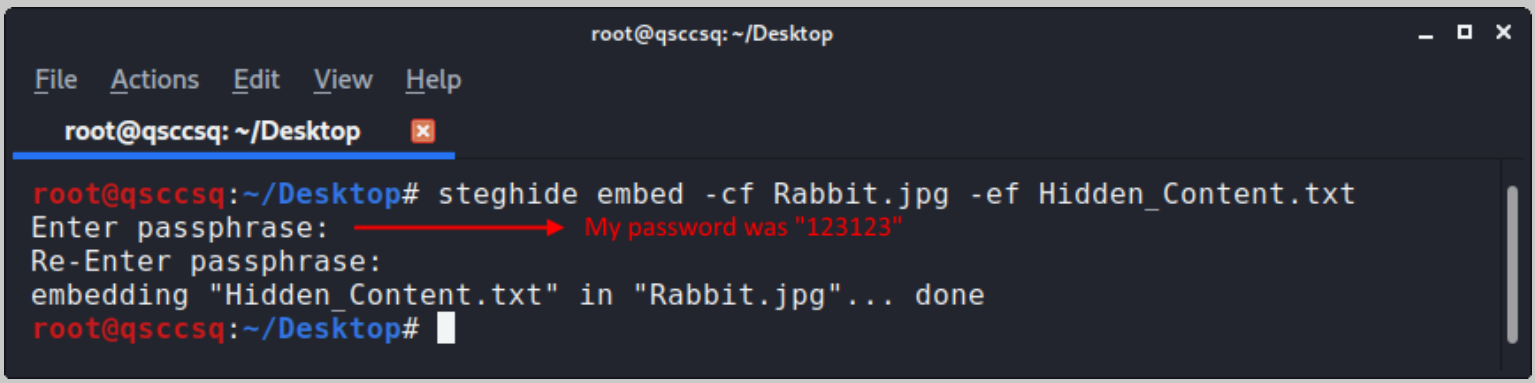
Checking the presence of HPA content on the hard disk using the Kali Linux terminal;

Today, the most preferred methods are encrypting ZIP - RAR files or hiding a content inside the image file. With the application named "Steghide" in Kali Linux, a desired file can be embedded in a standard image file and recovered for future use. The example below will show you how to place a .txt file into the image and how to get it again;

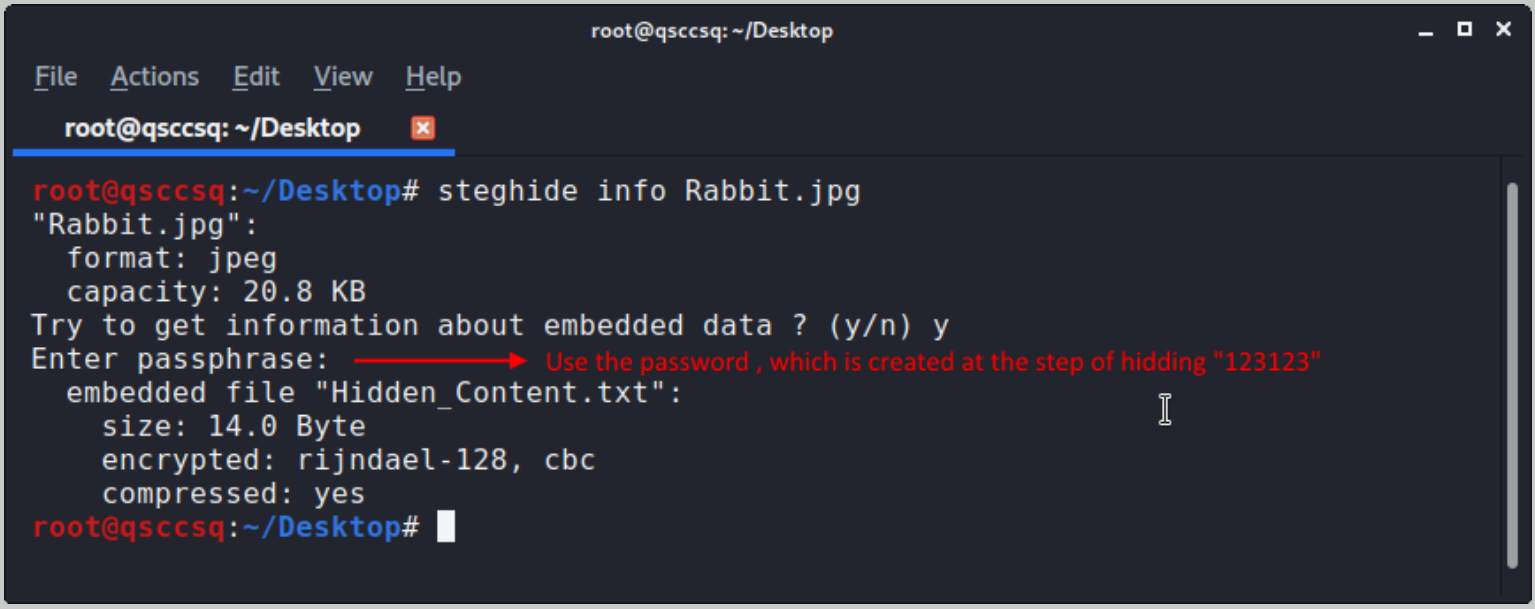
Step 1: Install Steghide;



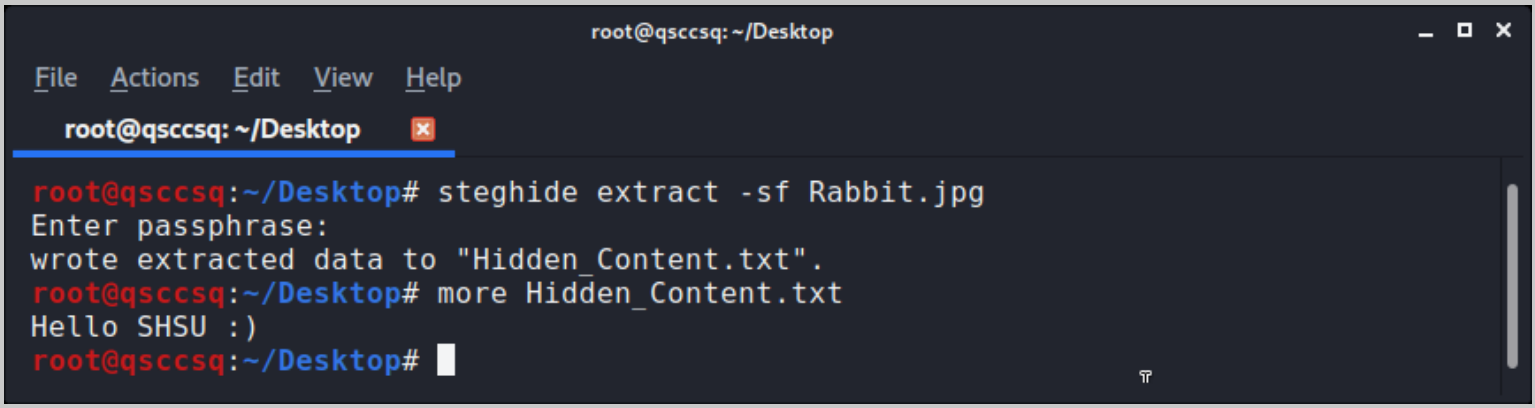
Step 2: Merge .txt and .jpg file;



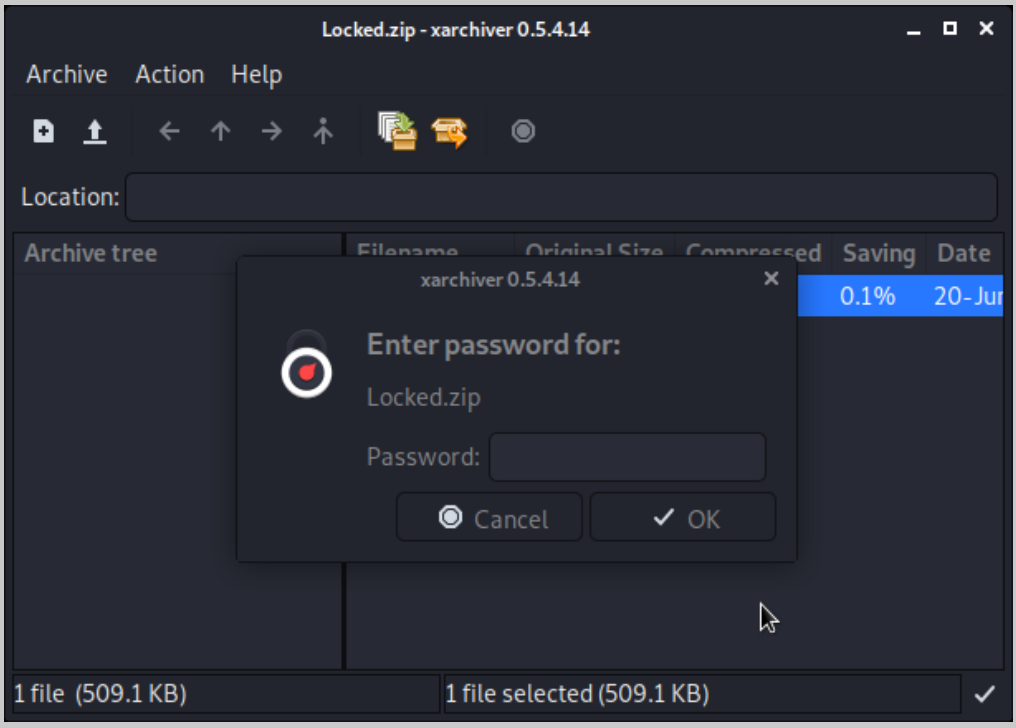
Step 3: Get info about .jpg file, which include a hidden content;



Step 4: Carve Hidden Content from .JPG file;

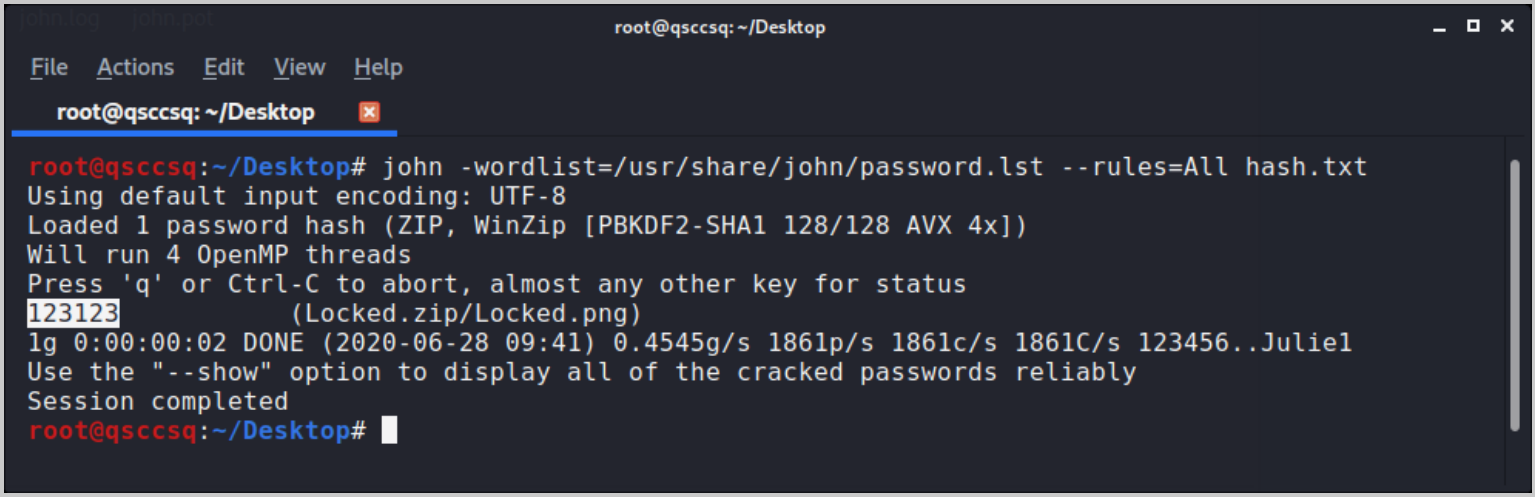


In the following stages, an example of obtaining the password of an encrypted .ZIP file will be shown with the application named "John the Ripper";



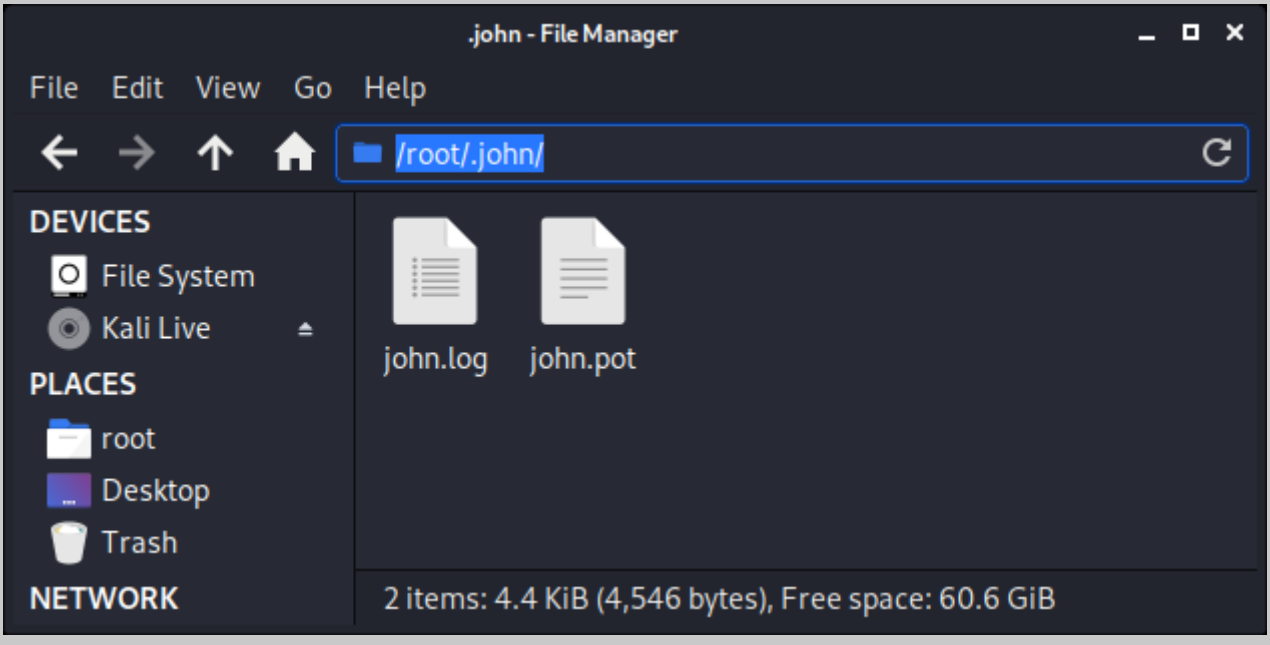
Step 1: Dumping of Locked.zip file's hash values;

Step 2: Cracking hash file;



Password: 123123

IMPORTANT: IF YOU HAVE SOME TROUBLE WITH JOHN THE RIPPER STEP 2, PLEASE GO TO "/root/.john/" AND DELETE ALL DOCUMENT FILES ON IT.



Homework:

1) Download ZIP file from: https://filebin.net/giiqmzuti79wny2y

2) Unzip downloaded file and reach out to Homework.JPG.

For unzip, open the terminal and type: unzip Homework.zip

3) Investigate the Homework.JPG with Steghide.

Steghide password hash is: **482c811da5d5b4bc6d497ffa98491e38**

Hint: Try to find an online cracker to crack hash value. However, you have to know the hashing algorithm name. May you can use Hash-ID for it ☺

4) Extract the Locked.ZIP file from Homework.JPG with Steghide.

5) Crack the password of Locked.ZIP.

6) Open the Locked.ZIP with password. You'll see a Flag.txt on it. Open Flag.txt and get Screenshot of it.

Please provide Screenshots of each steps of homework.