Writeup - Ghosts in the Profiles

There will be a **C.img** which when mounted will give a C drive, similar to windows

Mounting the disk

```
losetup –show -fP C.img
lsblk # Just to check if any partitions are there or not
mkdir /mnt/ntfs
mount -o rw /dev/loop0 /mnt/ntfs
```

Part 1 -

Users need to first analyse all the folders, they will see a **todo.txt** in **Documents** folder, now it is given a hint of "**Saving a copy of an email**", now users will go and analyze all chrome, brave, mozilla profiles if they exists, there is a **History** file in each profile, they can open it using **online sql viewer** or **sqlite3** in terminal, then after doing "**SELECT * FROM urls;**" they can see the history for that profile

There is a **drive link** in **History file** of **Profile 3** in the Chrome browser, which will lead them to download a **copy of the email**, it is a **.eml** file, so they can just open the file in an email application and download the **secret.7z** file or decode the base64 from the **.eml** file and save the **secret.7z** file, which is password protected.

Now users have been given a hint in description about a **saved credential**, so now a user needs to find that saved credential, now there are saved credentials in **Chrome, Brave and Mozilla** folder, since **Chrome** and **Brave** use **DPAPI Encryption** so **localstate** and **login data** are of no use as we would not be able **decrypt** them as actual host machines environment will be required, now **Mozilla Firefox** uses **NSS Encryption** which is not like **DPAPI**, so now a user needs to copy that **Mozilla** folder and replace it with their actual PC's **Mozilla** folder,

Copy C:\Users\Manya\AppData\Roaming\Mozilla folder and paste it on your C:\Users\%USERNAME%\AppData\Roaming\Mozilla, then open **Firefox**, on your PC.

and when they open firefox, they will be able to see a **saved credential**, so a user needs to use that saved **password**, and open the **secret.7z**, after which they will get a pdf, which on opening will give them the first half of the flag.

Part 2 -

Now when users were analyzing the **History** files, they will see something related to “**Cache**”, in **Profile 5**, which will hint them to see **Cache folder**, after when seeing the folder they will see many files, out of which they can use **file** command to see all the files, and filter out which they think has some data, then they can use **cat** command to see contents of the file, they will see many base64 encoded strings, out of which one is the part 2 of the flag