PSP0201

Week 6

Writeup

Group Name: ikun no 1

Members

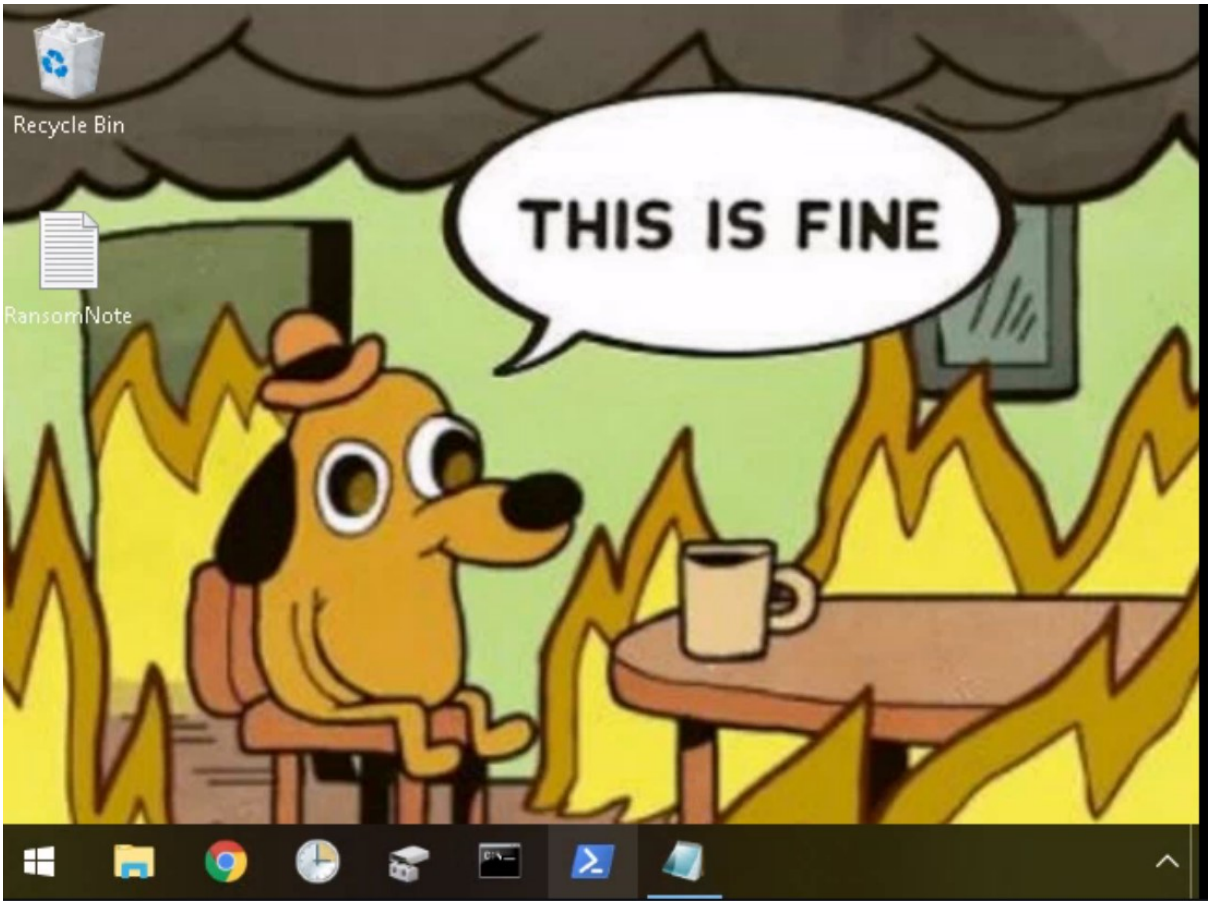
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 23 - [Blue Teaming] The Grinch strikes again!

Tool used: kali Linux, Remmina, Task Scheduler

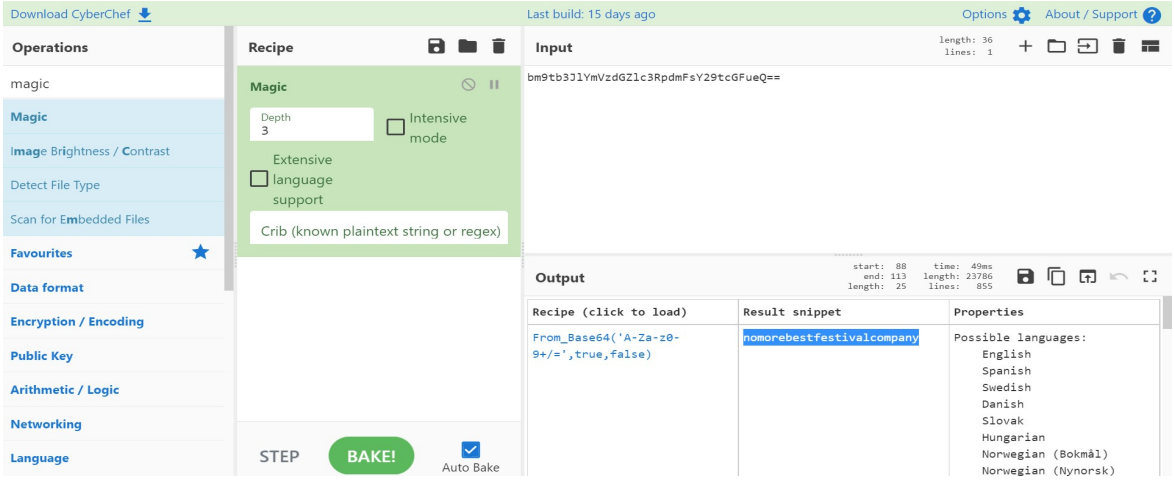
Solution/Walkthrough:

Q1



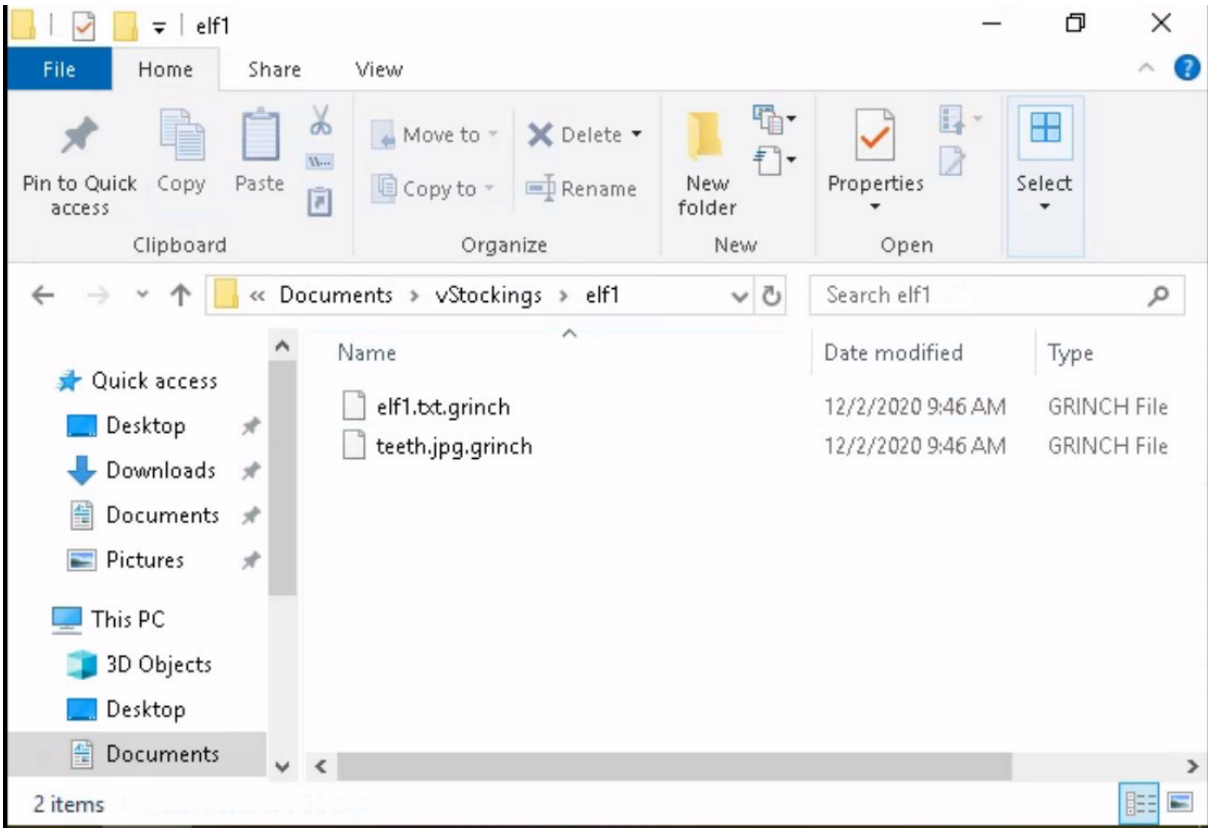
Access into the machine and copy the word in the wallpaper.

Q2



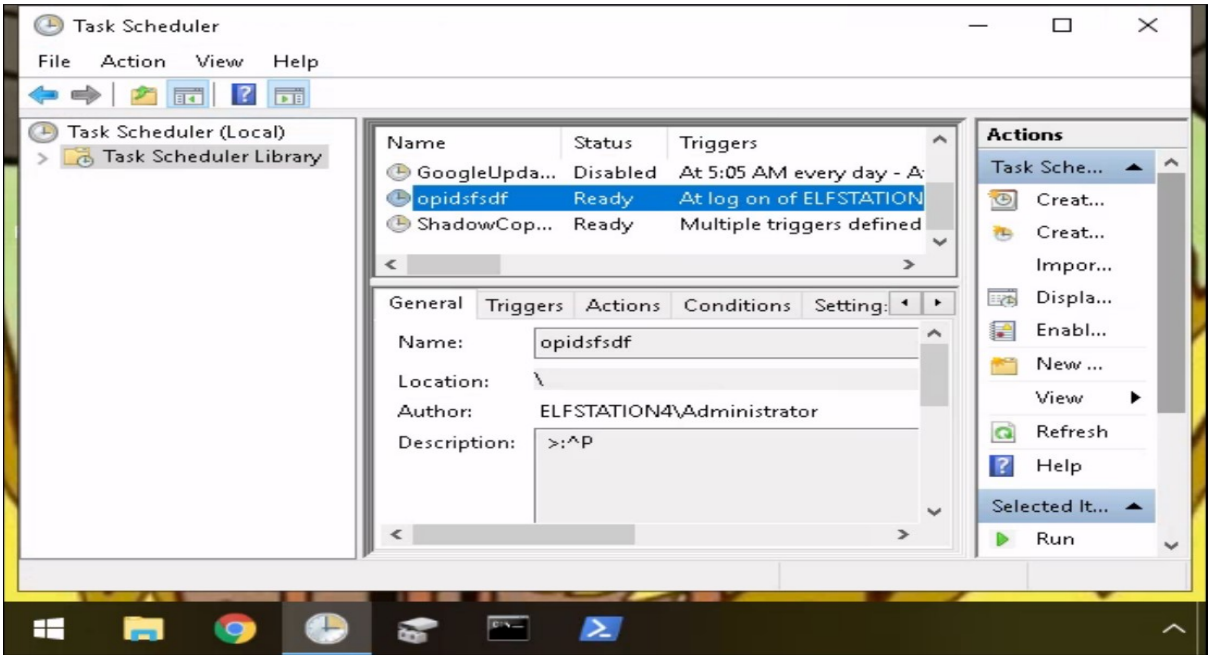
Open the RansomNote file and copy the address. Paste it into cyberchef and decode it.

Q3



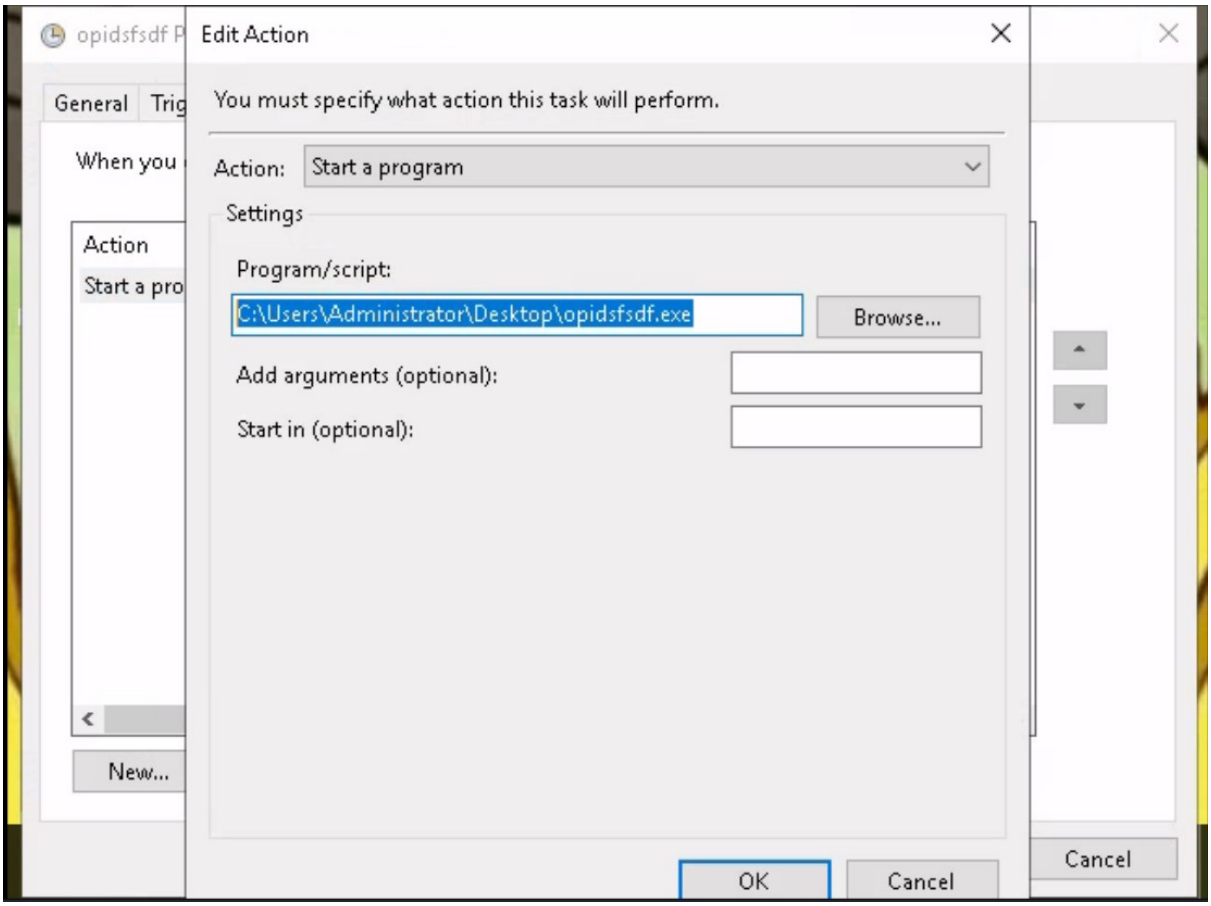
Open a folder in Documents. Look at the file extensions behind the encrypted files and the file extensions can be found.

Q4.



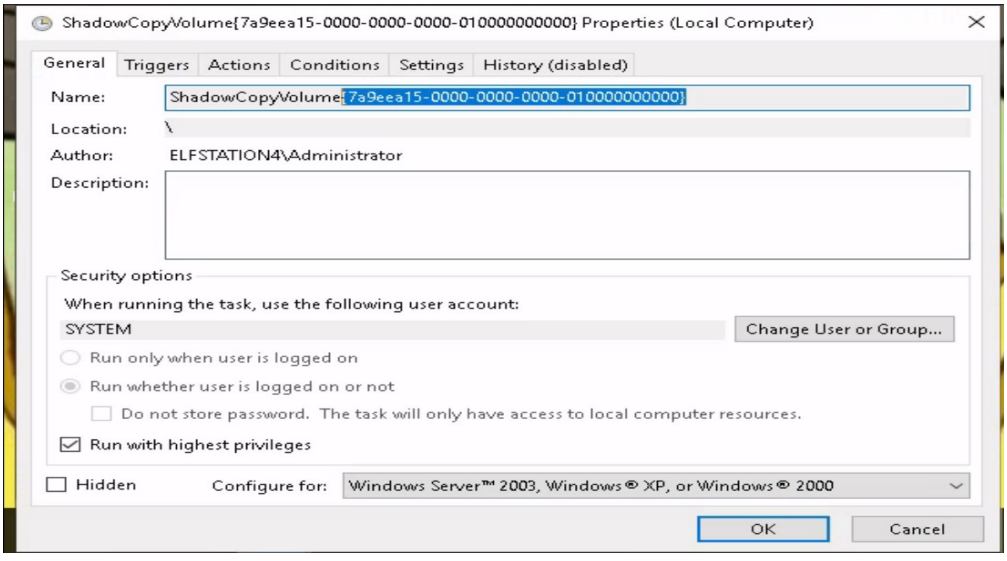
Open the task scheduler. Find out the task that has unusual names.

Q5.



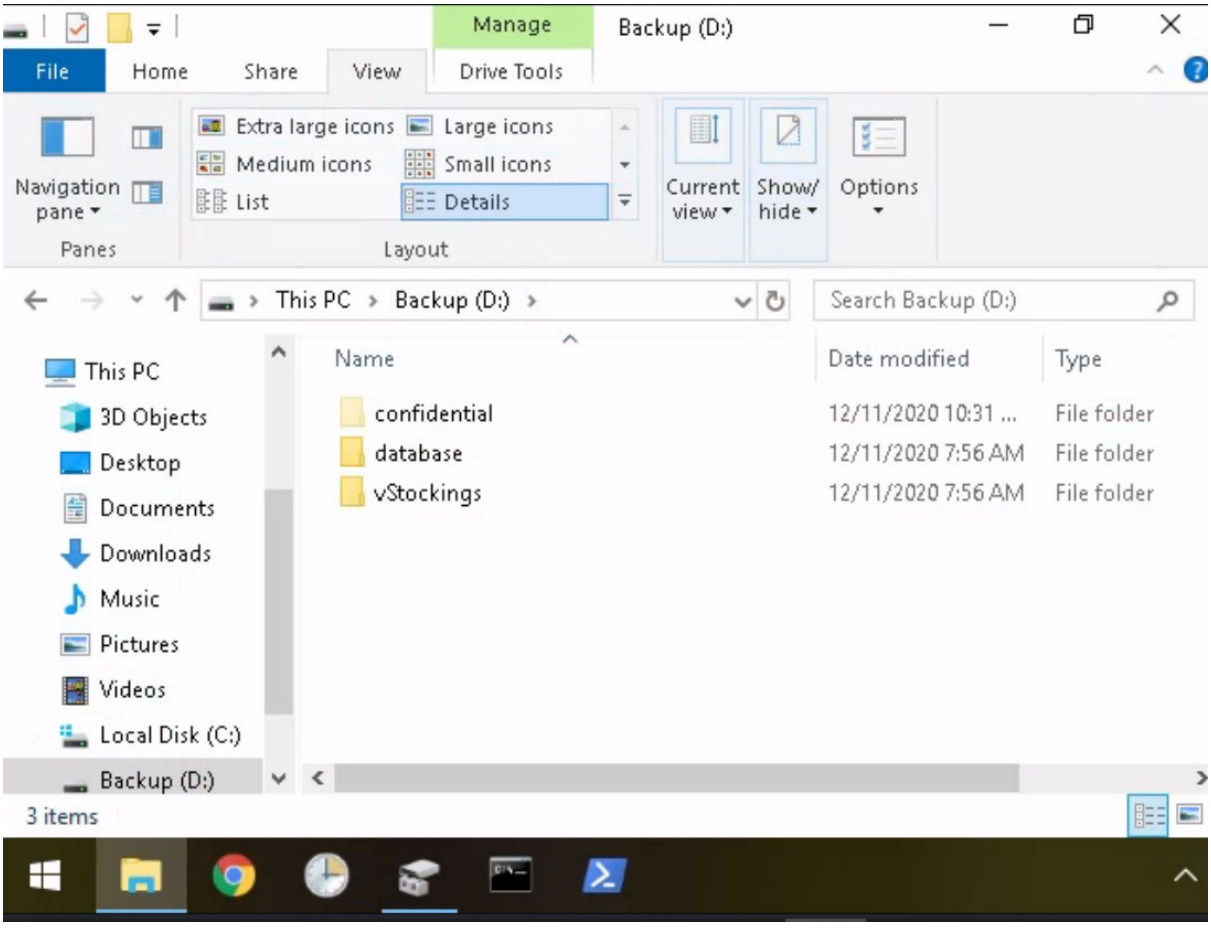
Look at the properties of the task. Inspect it and the location can be found.

Q6.



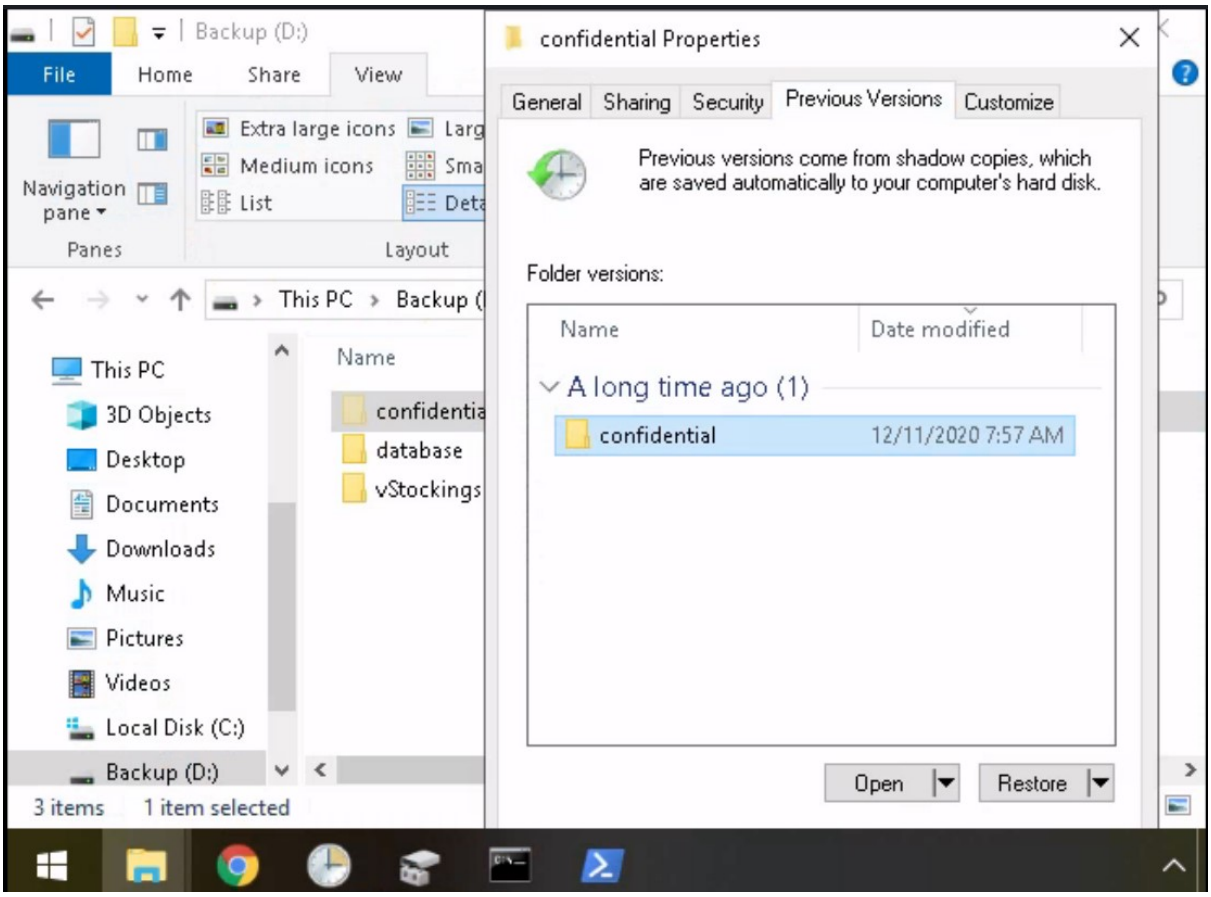
Look at the properties of ShadowCopyVolume. The ID can be found behind the name of the file.

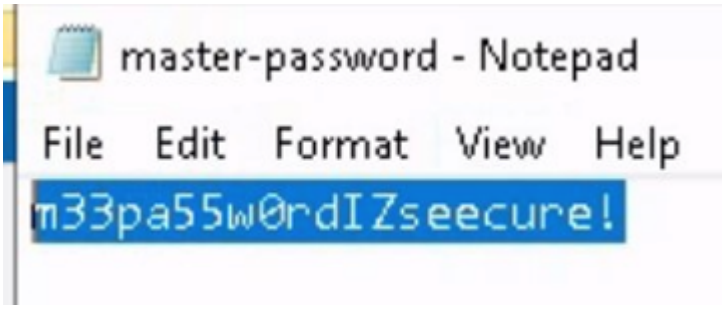
Q7.



Tick the hidden files options on top of the File Explorer. The hidden file can be found.

Q8.





Restore the file to the previous version. A new file called master-password will appear. Open the file and copy the notes inside of it.