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

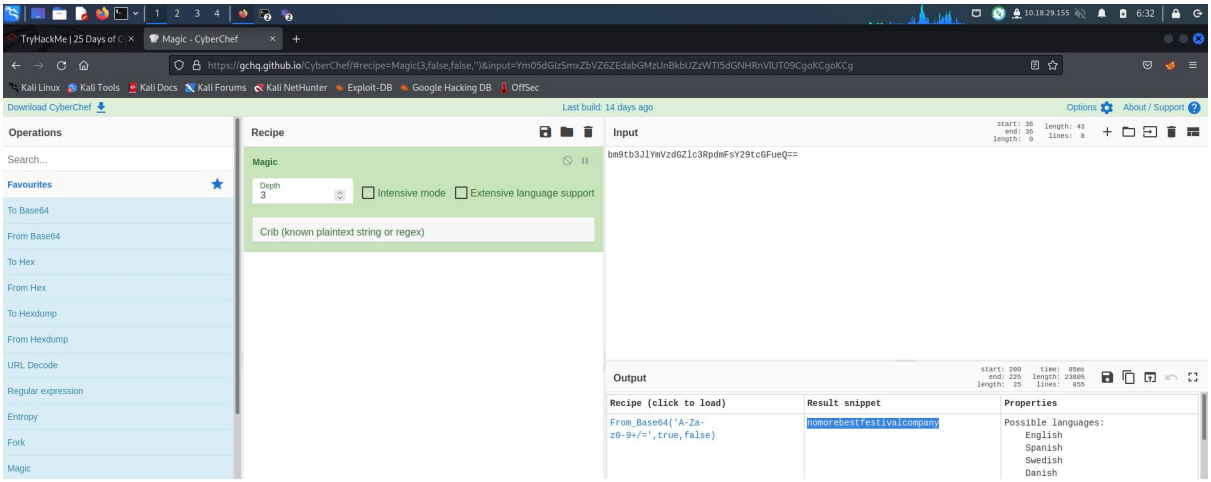
Tool used: kali Linux, Firefox, Remmina, Cyberchef

Solution/Walkthrough:

Q1

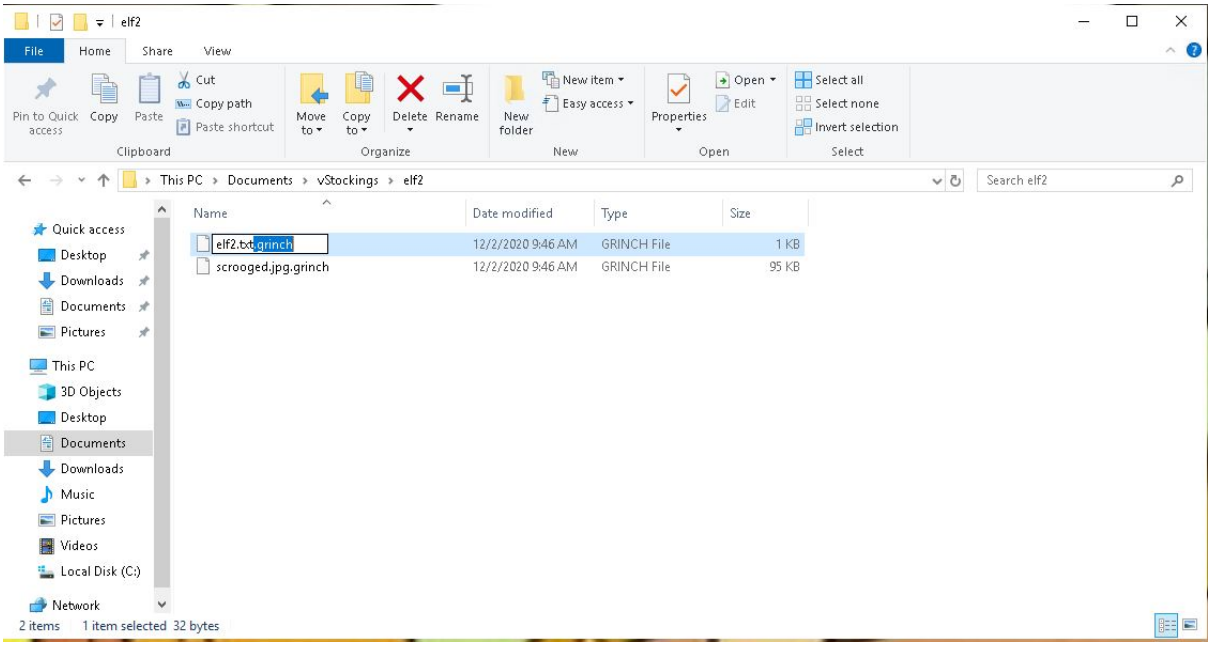
We log into the remote machine. The wallpaper clearly shows us.

Q2



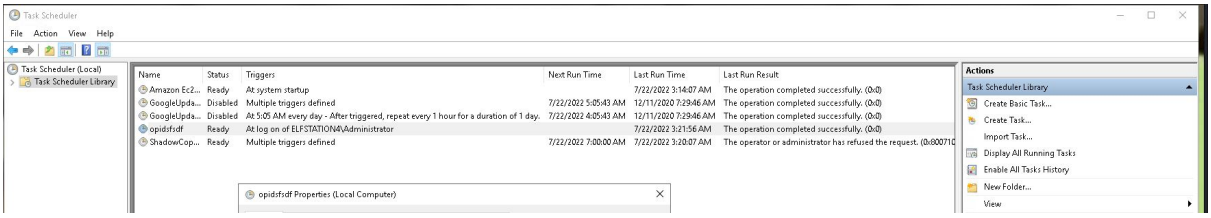
With the help of ‘magic’ operation in Cyberchef, we decrypt the fake 'bitcoin address' and get the text.

Q3

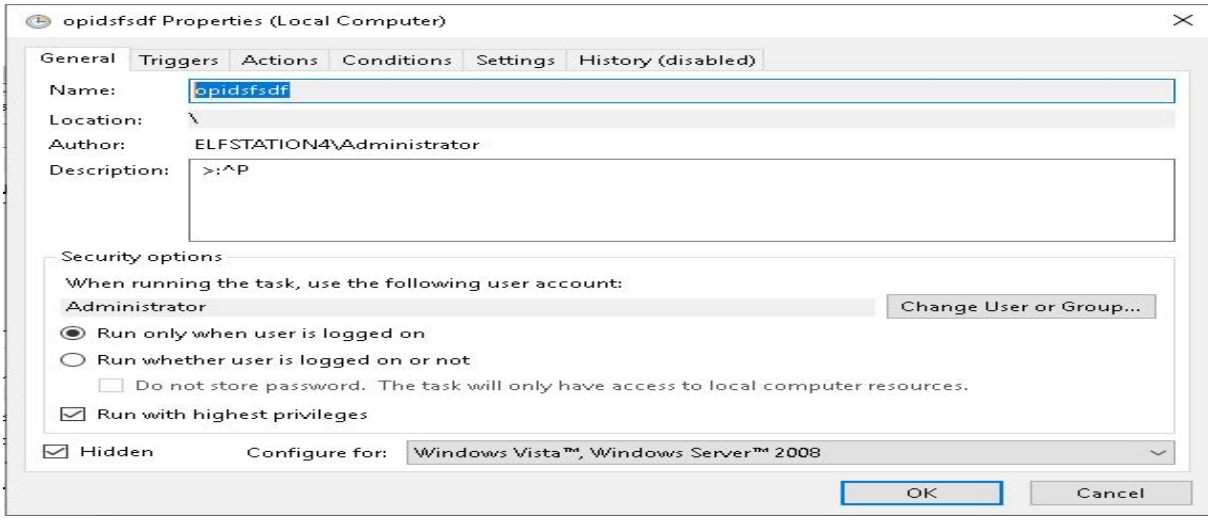


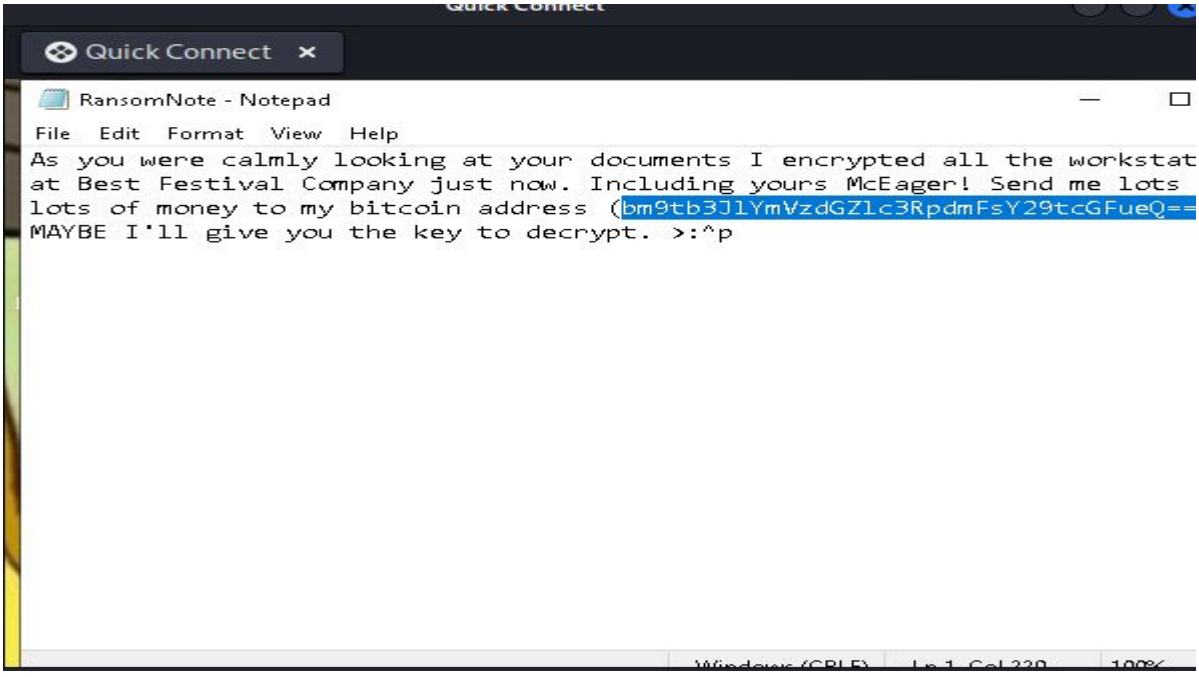
We look through the file in the machine. In a file named ‘elf2’, we can identify the extension precisely.

Q4



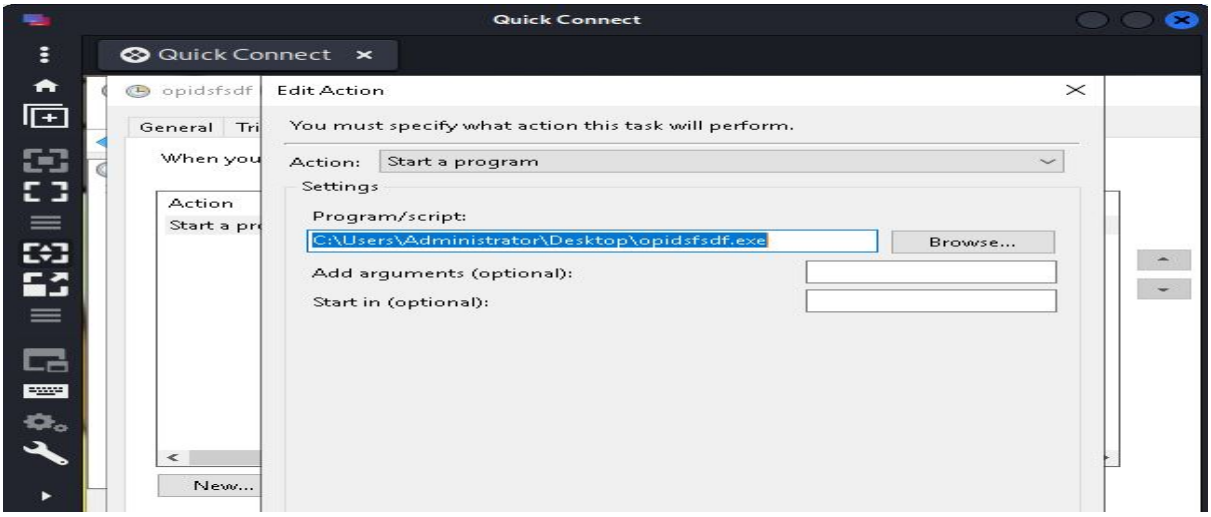
We opened the Task Scheduler Library to find something suspicious. In the 5 tasks, we observe that one of them is named in random order.





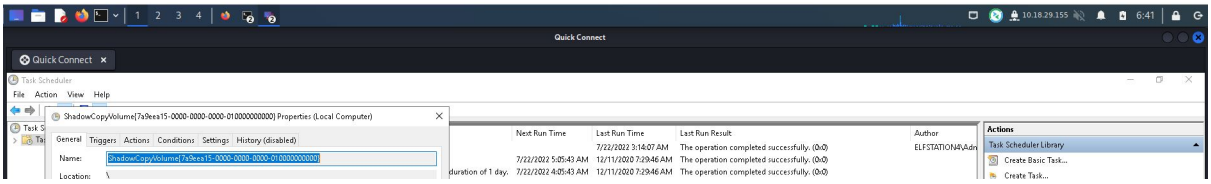
We open it, and we can see similarities between description and the note.

Q5



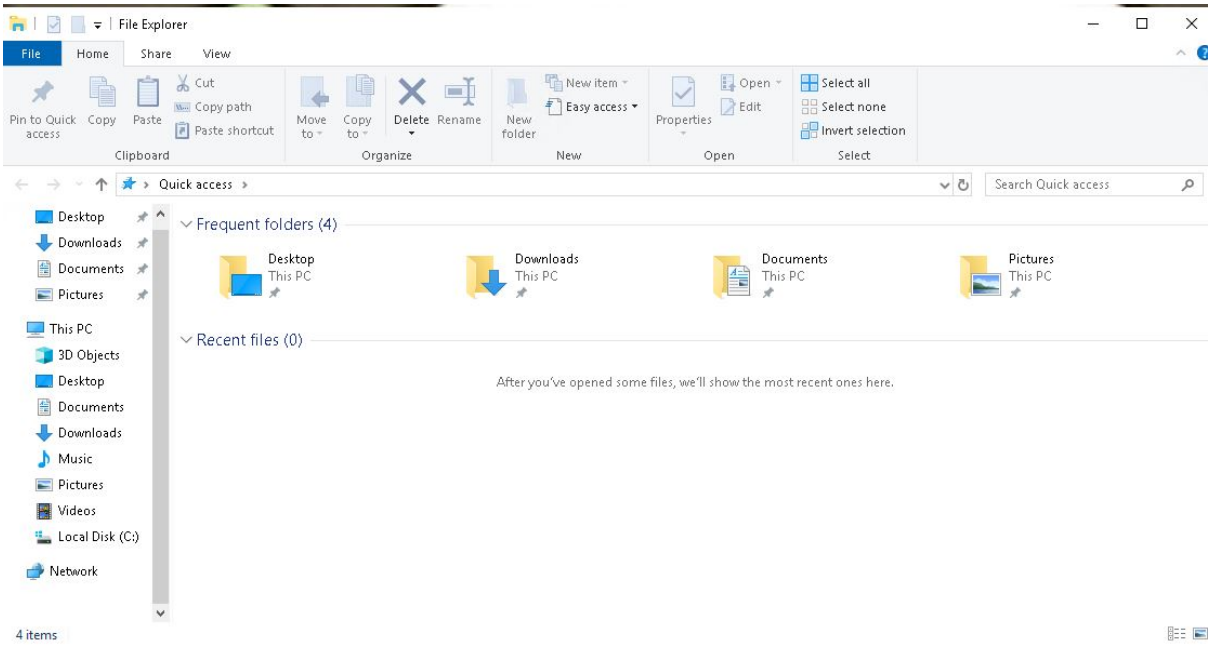
We inspect the file at action. The location of the program is found.

Q6

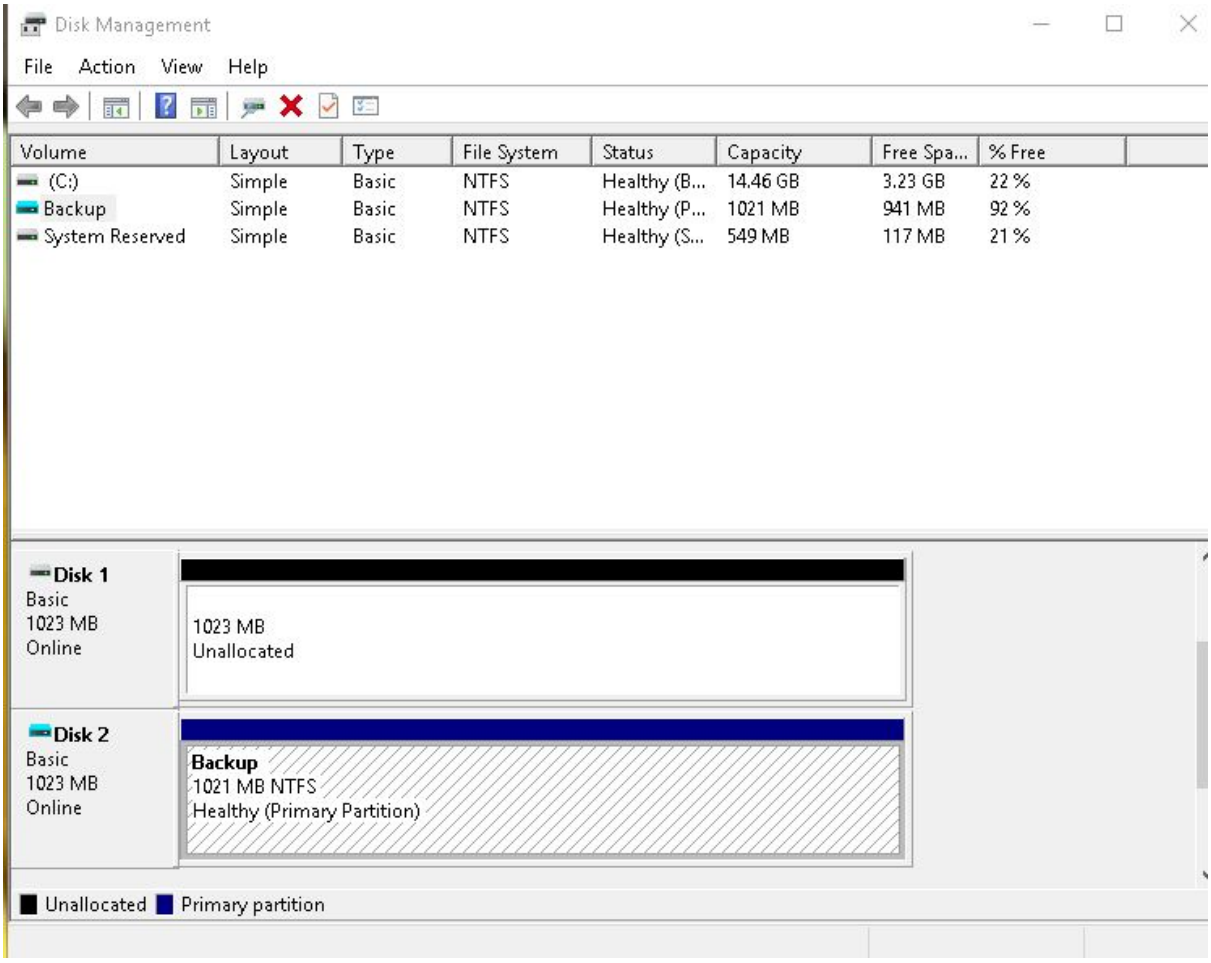


We open the ‘shadow’ program. The ShadowCopyVolume ID is the value after the name.

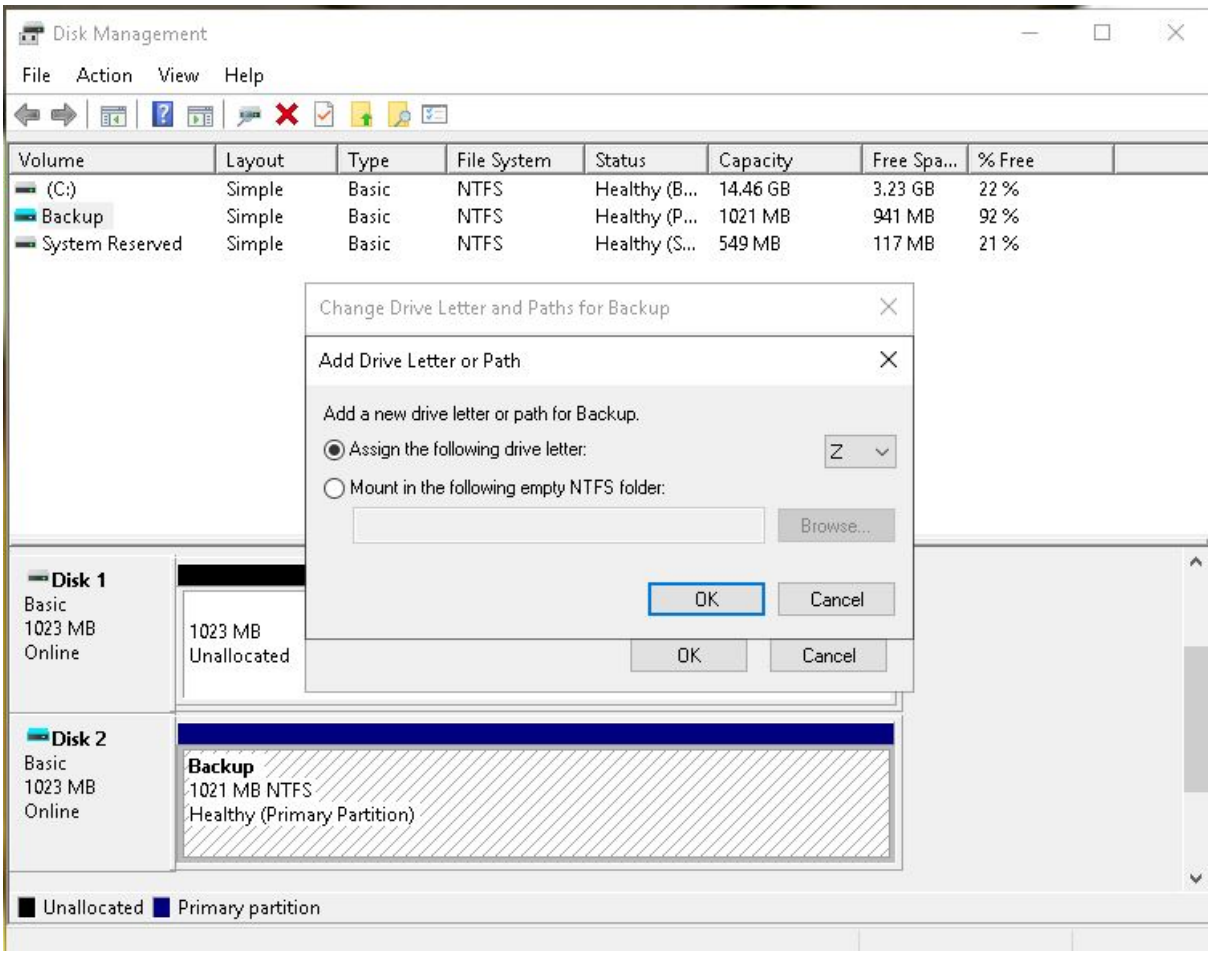
Q7



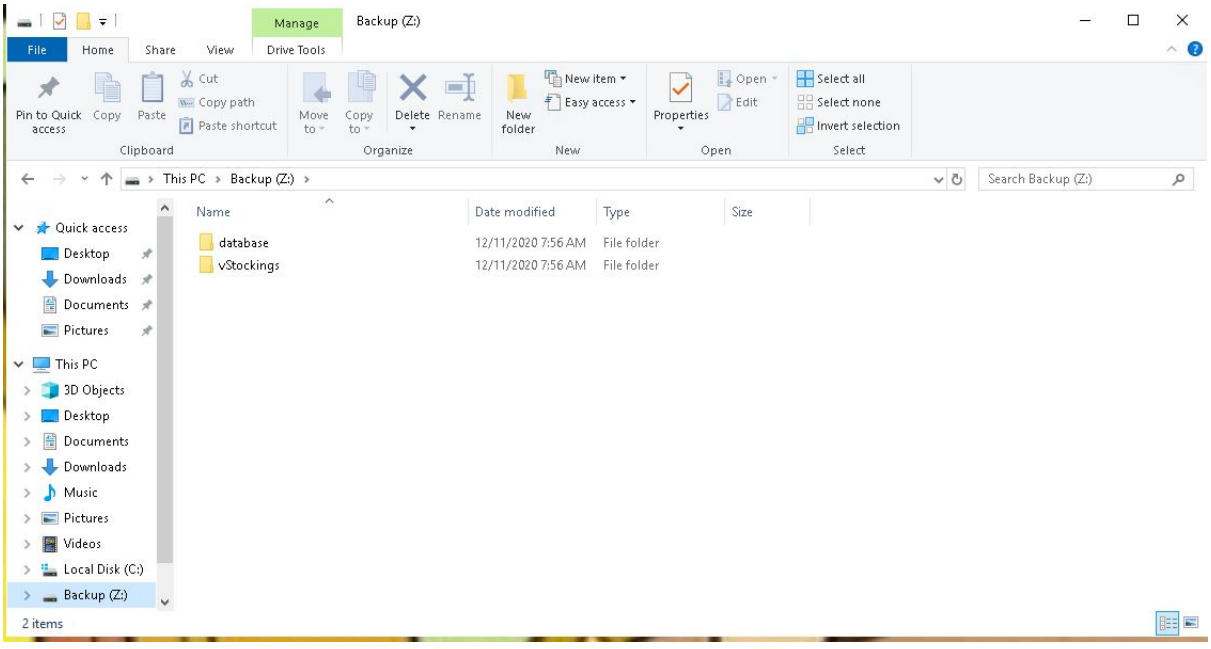
At first, we cannot view the hidden folder in any way.



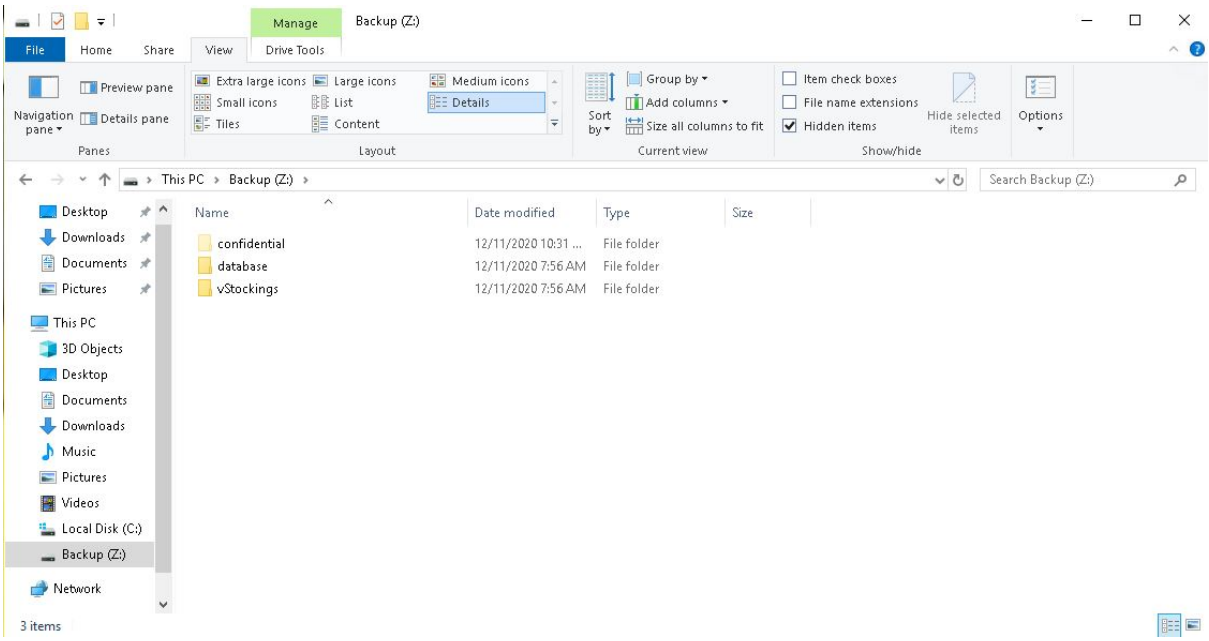
However, in disk management, we find out there is a backup volume. We can use it to restore back the files we needed.



To make it work, we are going to assign it a drive letter.

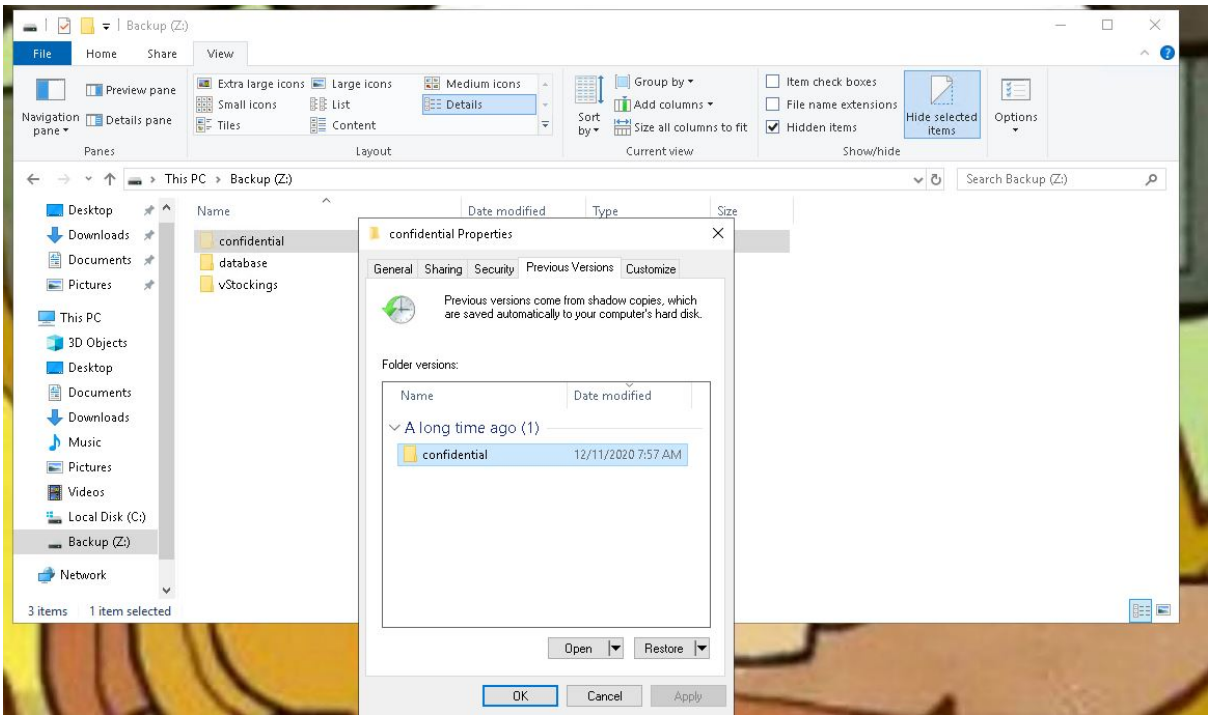


Now we can have a look at this backup volume.

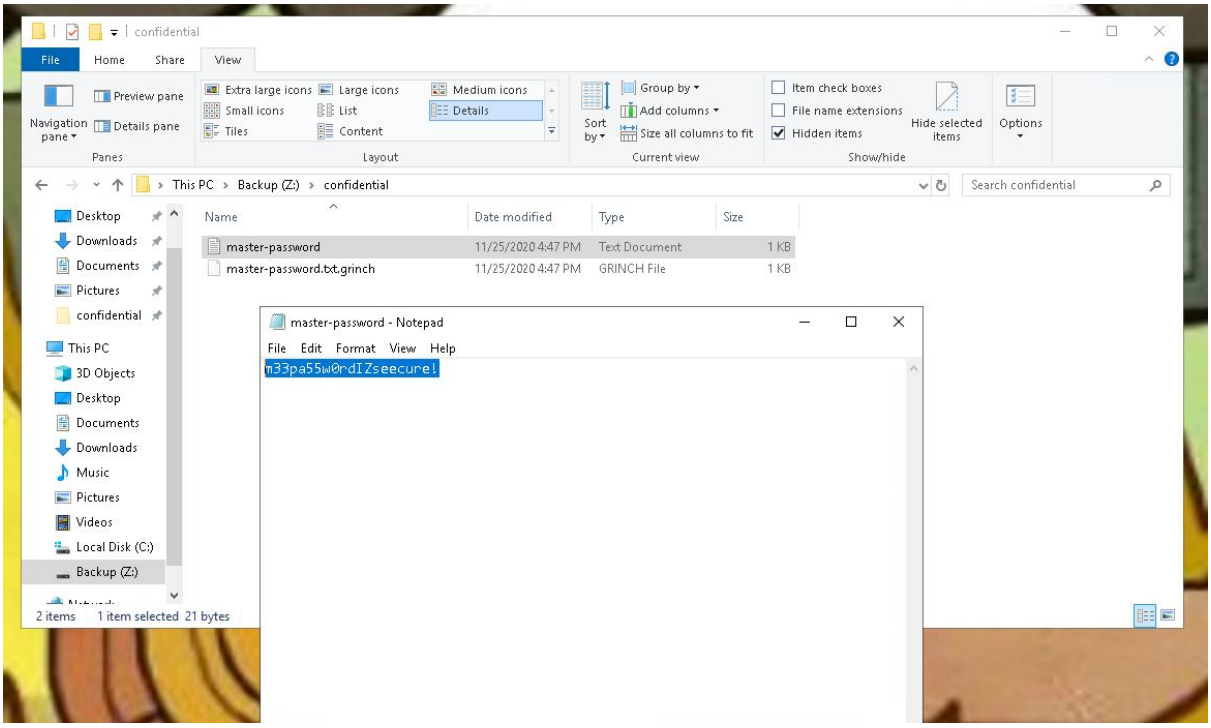


As we want to see the hidden files and folders, we select [view] in the menu, then check mark the [hidden items]. We have our hidden folder back, with its name.

Q8



We restore the hidden folder.



After that, we examine the file inside, and we get back our master-password without any encryption.