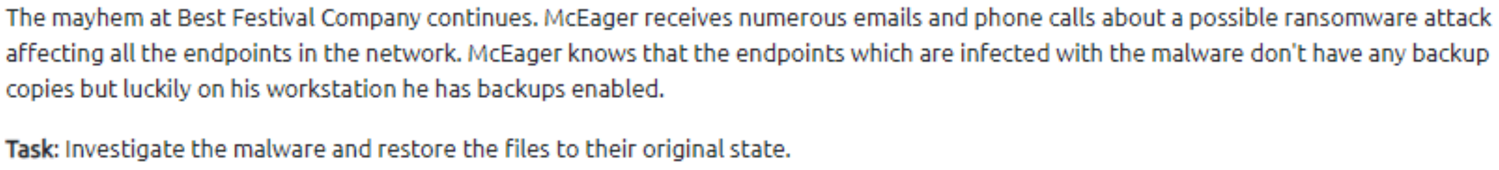
Day 23 - The Grinch strikes again!

scenario

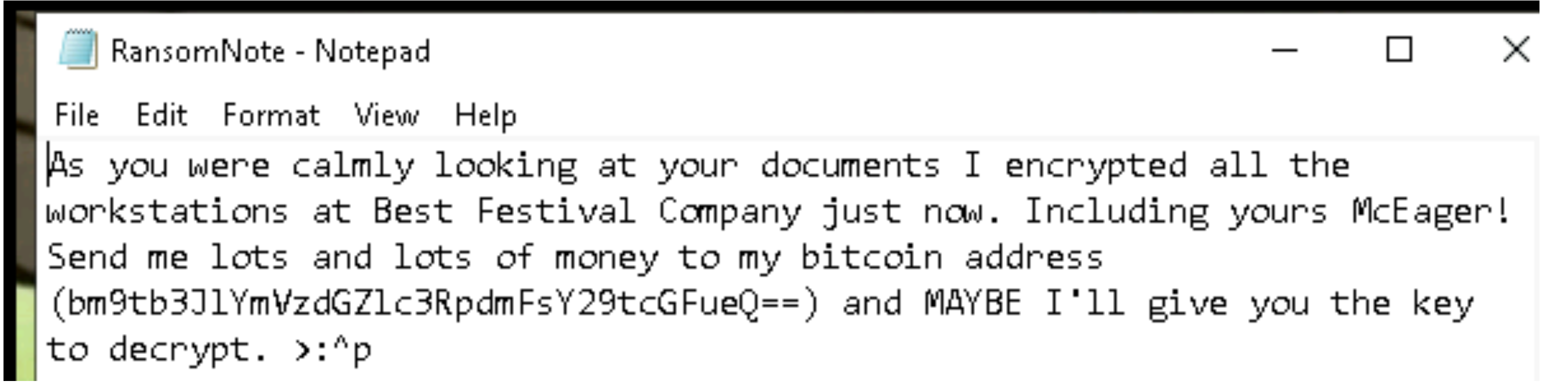


The mayhem at Best Festival Company continues. McEager receives numerous emails and phone calls about a possible ransomware attack affecting all the endpoints in the network. McEager knows that the endpoints which are infected with the malware don't have any backup copies but luckily on his workstation he has backups enabled.

Task: Investigate the malware and restore the files to their original state.

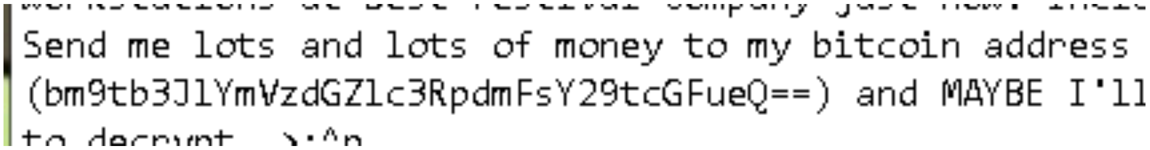
access the remote host RDP

found a ransomNote on the desktop



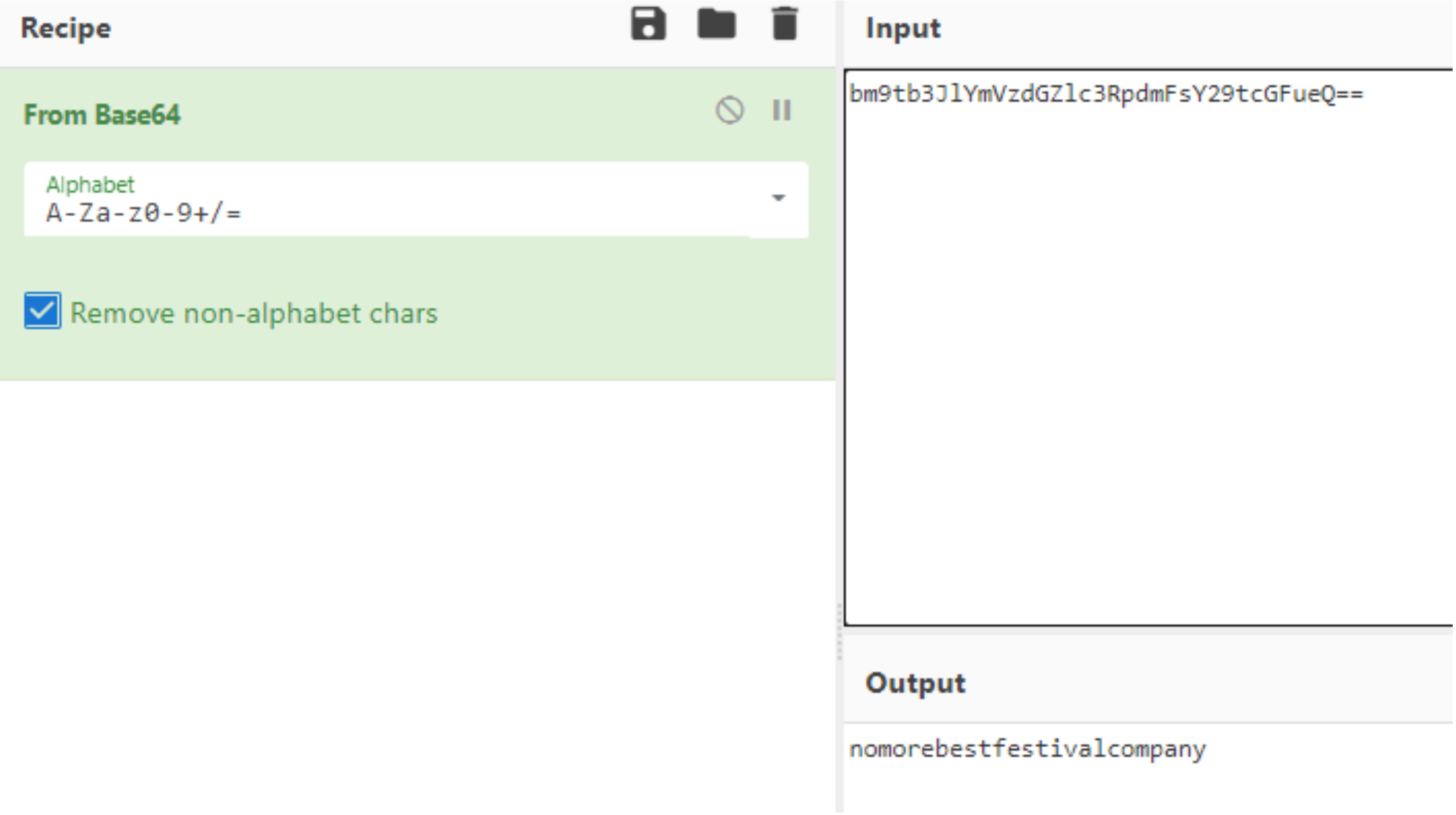
As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots and lots of money to my bitcoin address (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p

bitcoin address in base64 encoded format?



```
workstations at best festival company just now. Their
Send me lots and lots of money to my bitcoin address
(bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll
to decrypt. >:^p
```

after decode it, we got the fake bitcoin address in plaintext



From Base64

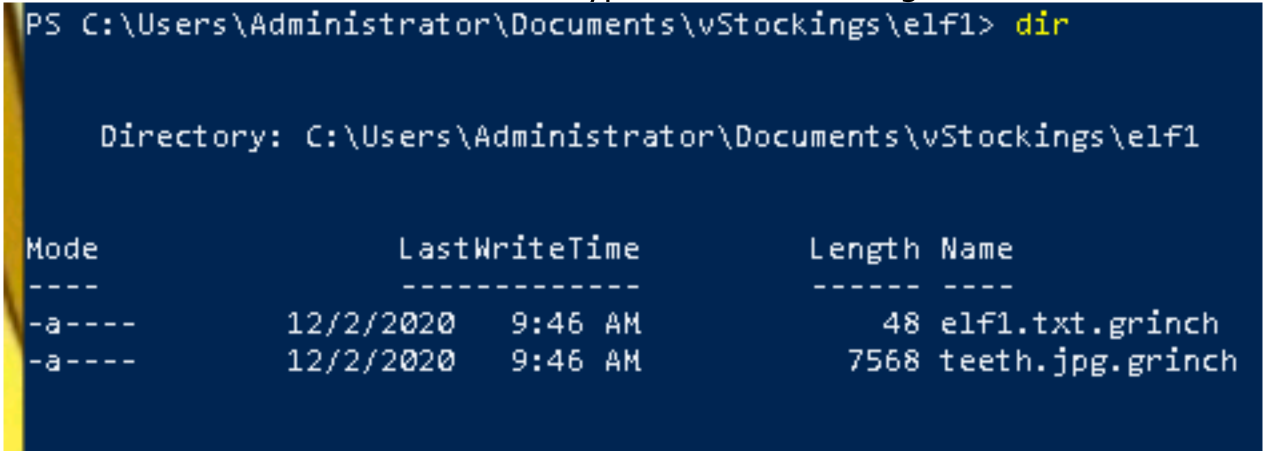
Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

```
nomorebestfestivalcompany
```

if we notice that the ransomware encrypted the files with .grinch extension

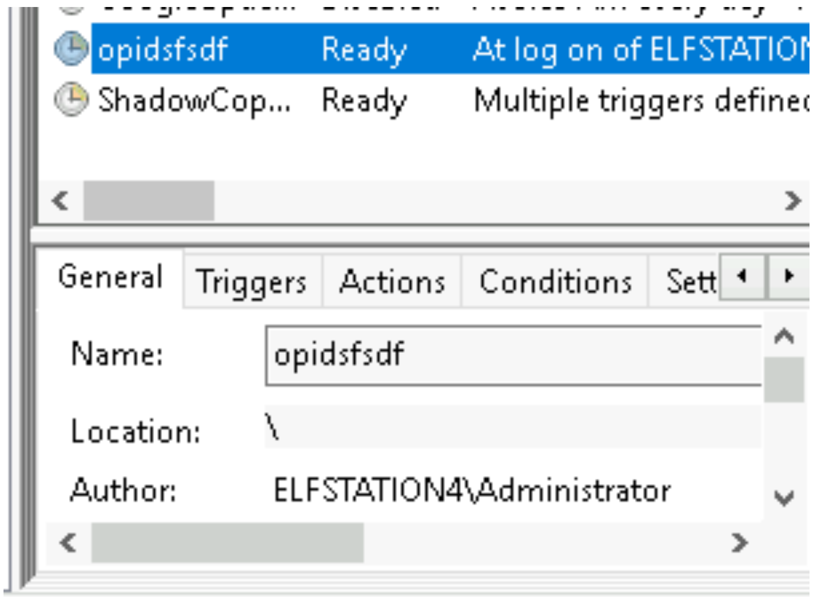


```
PS C:\Users\Administrator\Documents\vStockings\elf1> dir


    Directory: C:\Users\Administrator\Documents\vStockings\elf1


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/2/2020   9:46 AM             48 elf1.txt.grinch
-a----         12/2/2020   9:46 AM           7568 teeth.jpg.grinch
```

in the task scheduler found a suspicious scheduled task



opidsfsdf Ready At log on of ELFSTATION

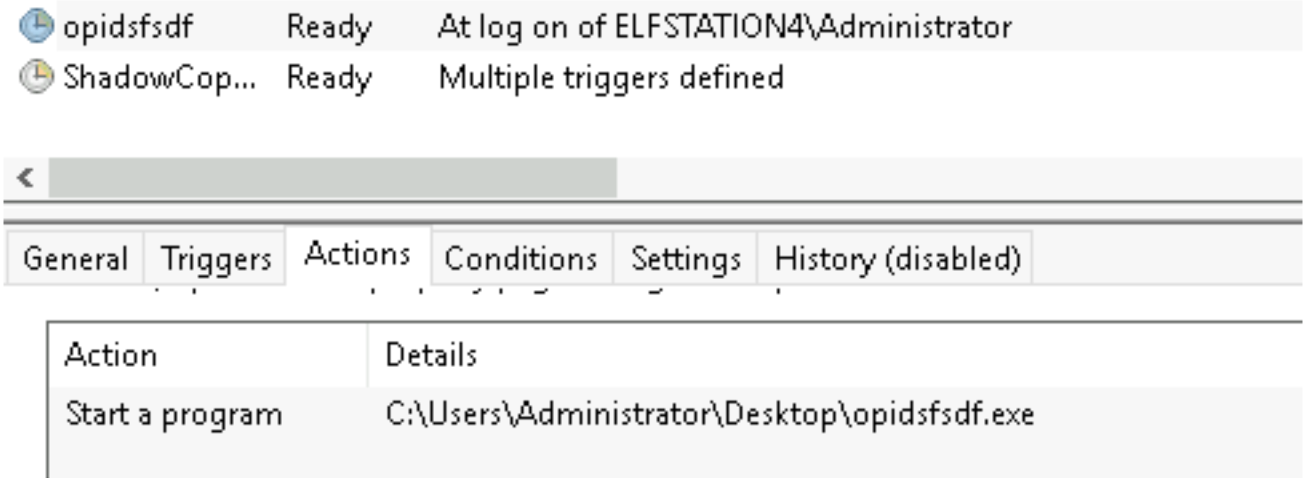
ShadowCop... Ready Multiple triggers define

Name: opidsfsdf

Location: \

Author: ELFSTATION4\Administrator

under the action panel, we found where's the suspicious executable binary that this suspicious scheduled task execute

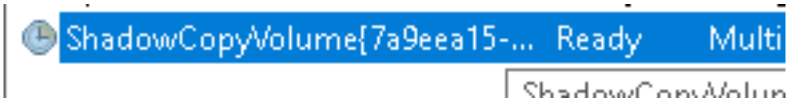


opidsfsdf Ready At log on of ELFSTATION4\Administrator

ShadowCop... Ready Multiple triggers defined

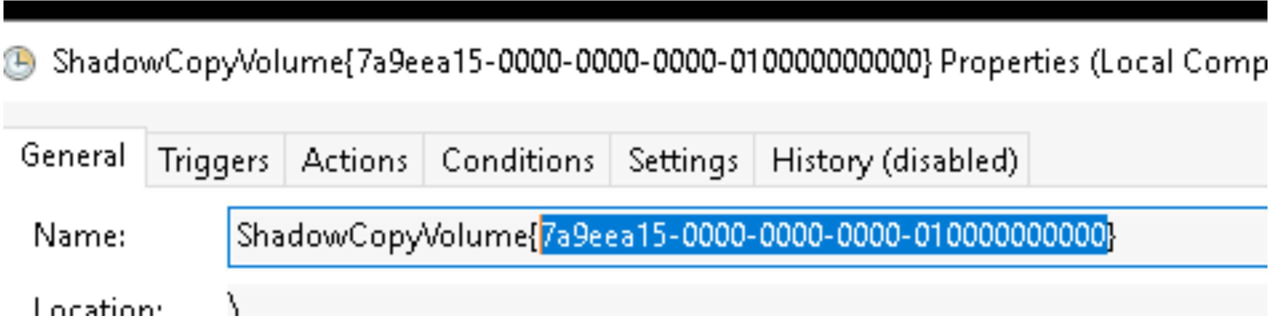
Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

there's another scheduled task we found here too about the VSS



ShadowCopyVolume{7a9eea15-... Ready Multi

over here we can find the shadowCopyVolume id

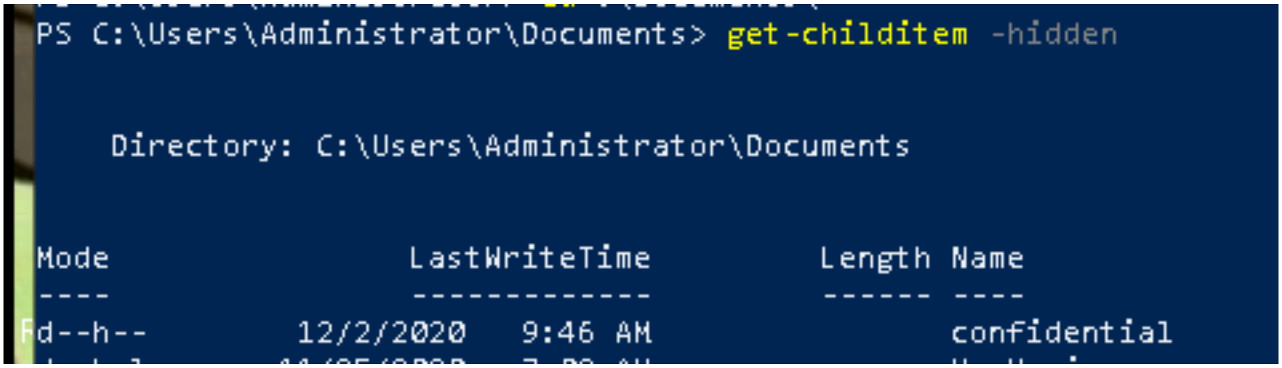


ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Comp

Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location: \

found a hidden directory in the documents directory

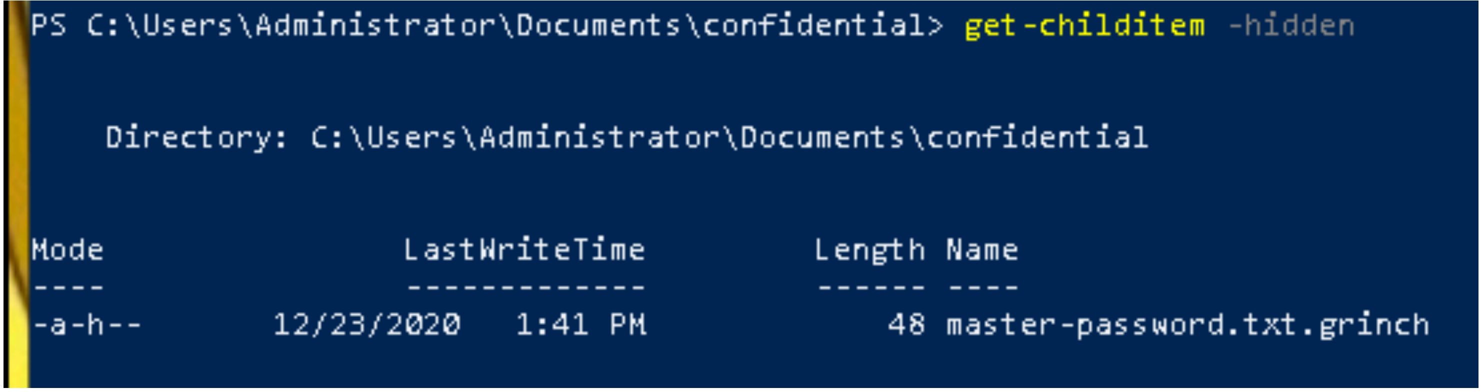


```
PS C:\Users\Administrator\Documents> get-childitem -hidden


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        12/2/2020   9:46 AM                confidential
```

master pw encrypted?

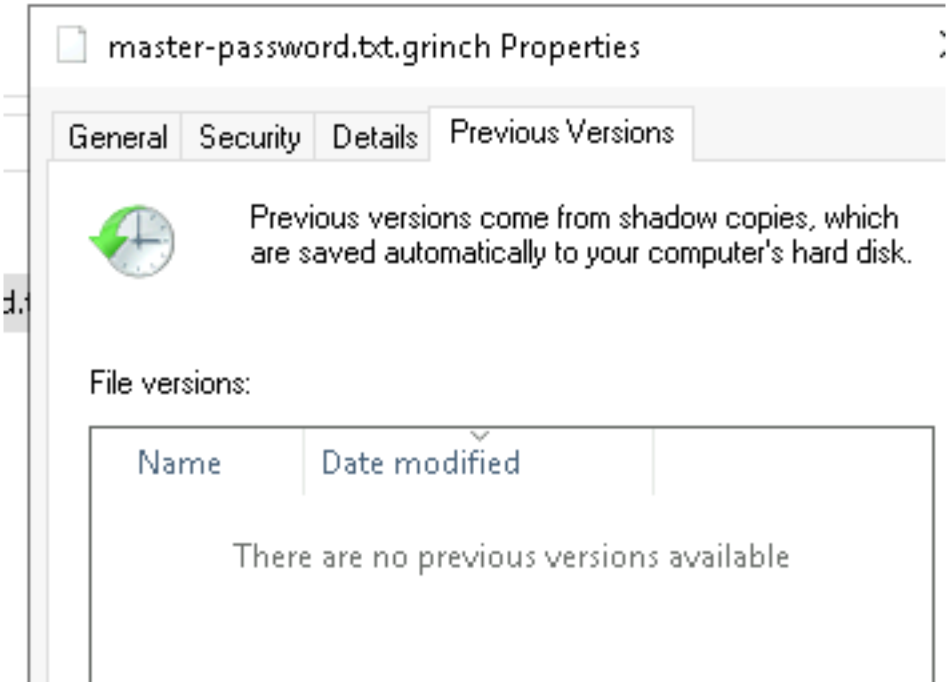


```
PS C:\Users\Administrator\Documents\confidential> get-childitem -hidden


    Directory: C:\Users\Administrator\Documents\confidential


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-h--       12/23/2020   1:41 PM             48 master-password.txt.grinch
```

no previous version to restore this master-password in the Documents directory



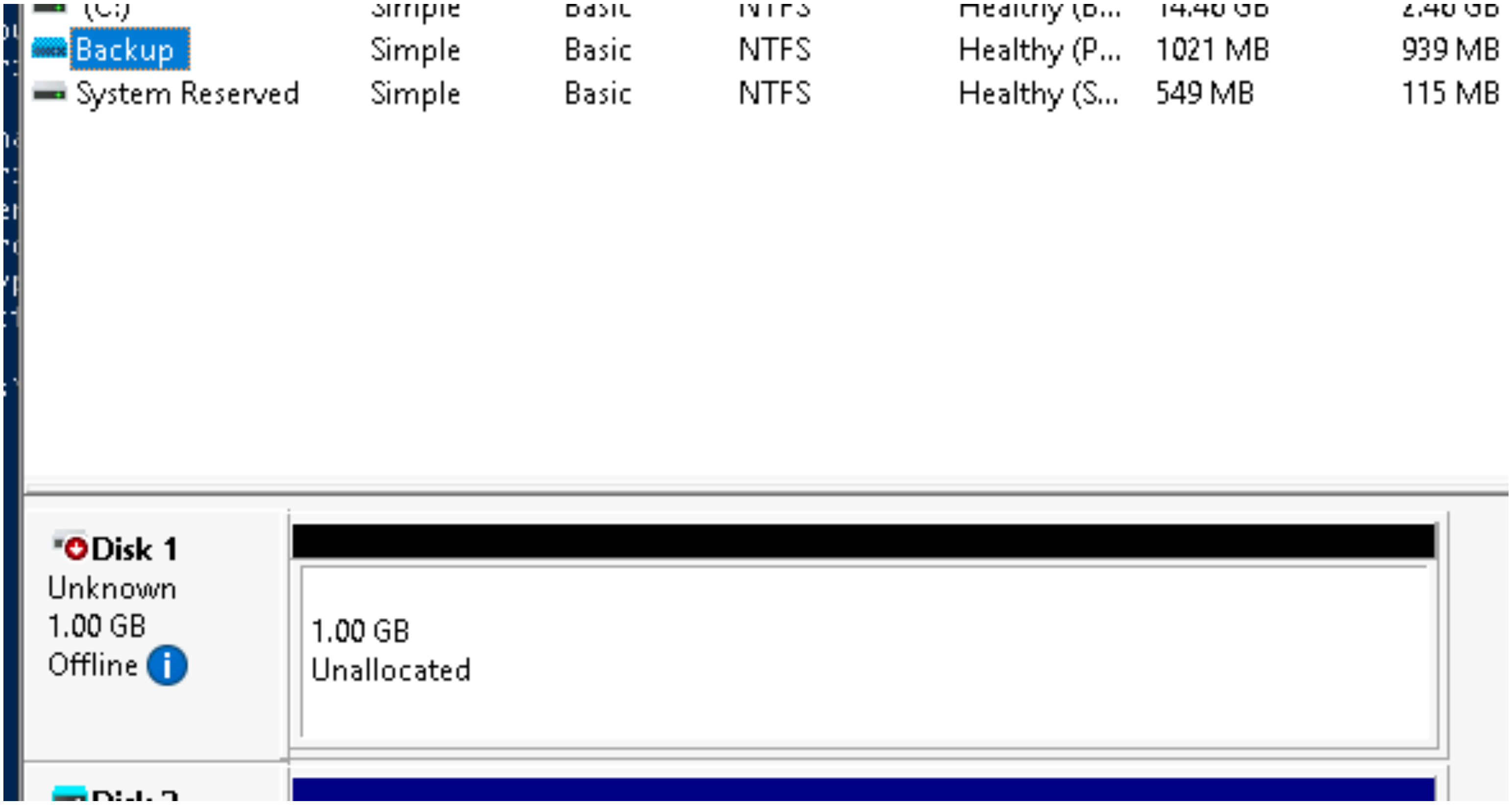
master-password.txt.grinch Properties

Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

File versions:

There are no previous versions available

checking partitions & found Backup doesnt have letter assigned



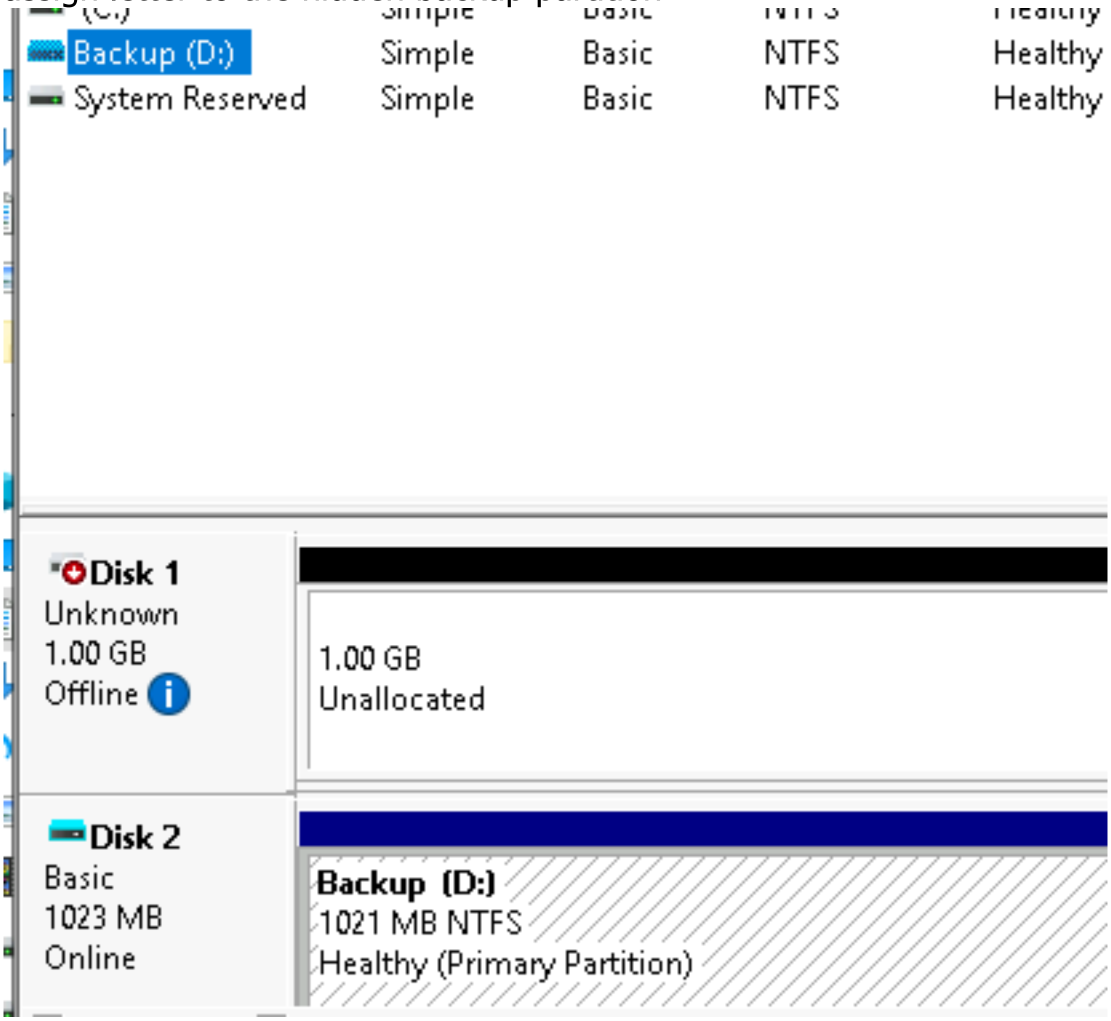
(C:)	Simple	Basic	NTFS	Healthy (B...	14.46 GB	2.46 GB
Backup	Simple	Basic	NTFS	Healthy (P...	1021 MB	939 MB
System Reserved	Simple	Basic	NTFS	Healthy (S...	549 MB	115 MB

Disk 1
Unknown
1.00 GB
Offline

1.00 GB
Unallocated

Disk 2

assign letter to the hidden backup partition



(C:)	Simple	Basic	NTFS	Healthy
Backup (D:)	Simple	Basic	NTFS	Healthy
System Reserved	Simple	Basic	NTFS	Healthy

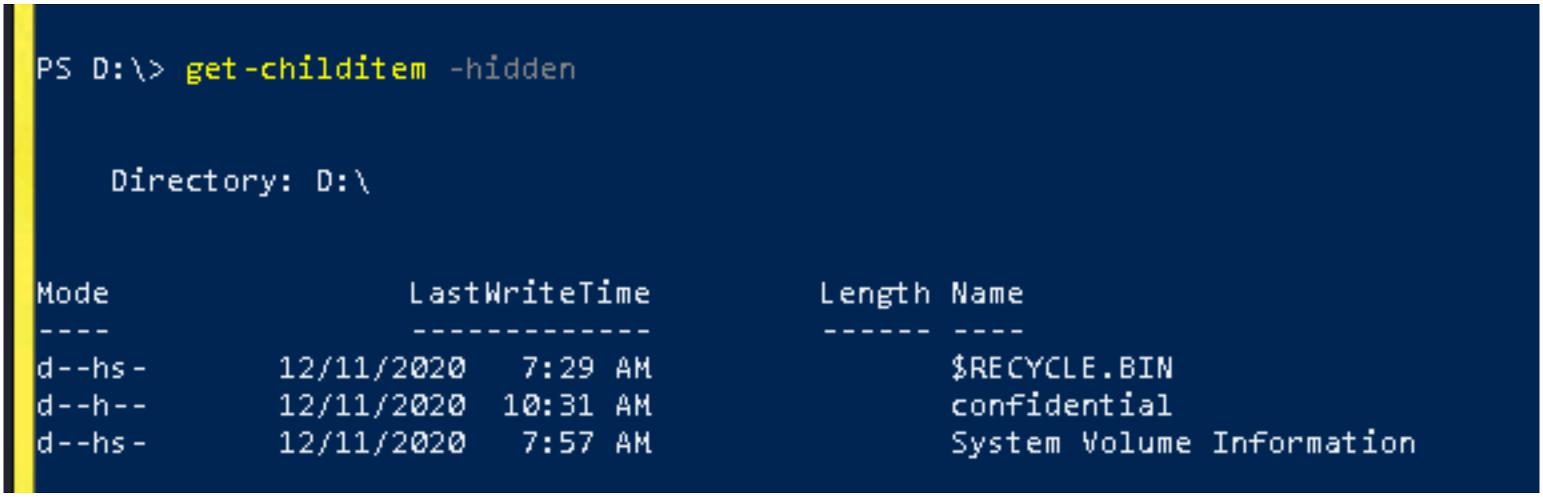
Disk 1
Unknown
1.00 GB
Offline

1.00 GB
Unallocated

Disk 2
Basic
1023 MB
Online

Backup (D:)
1021 MB NTFS
Healthy (Primary Partition)

accessing it & we notice that the content in the backup partition was the same as the one in the Documents

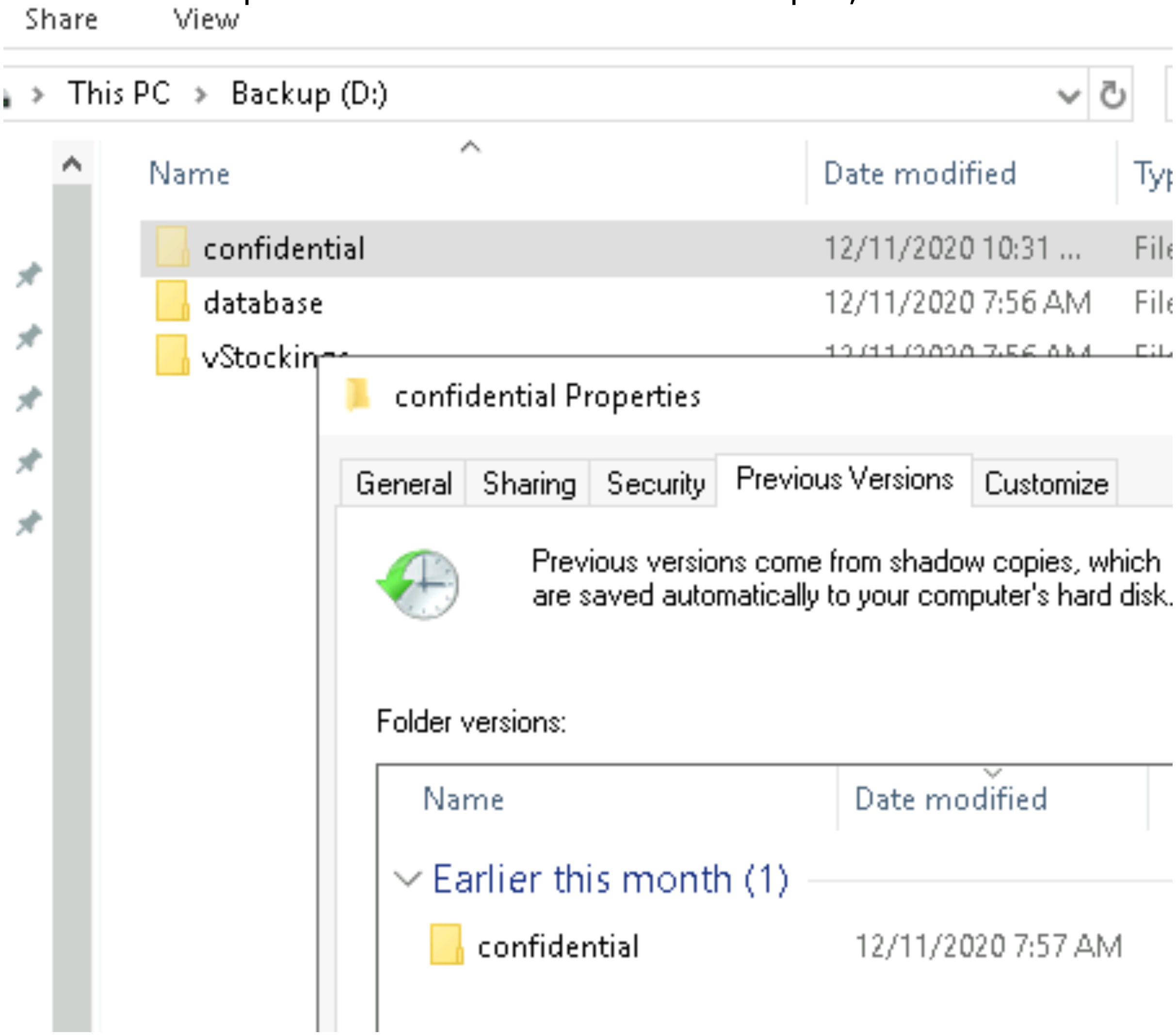


```
PS D:\> get-childitem -hidden


    Directory: D:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-        12/11/2020   7:29 AM                $RECYCLE.BIN
d--h--        12/11/2020  10:31 AM                confidential
d--hs-        12/11/2020   7:57 AM                System Volume Information
```

& we found the previous version from the shadow copies, let's restore it



confidential 12/11/2020 10:31 ... File
database 12/11/2020 7:56 AM File
vStockin

confidential Properties

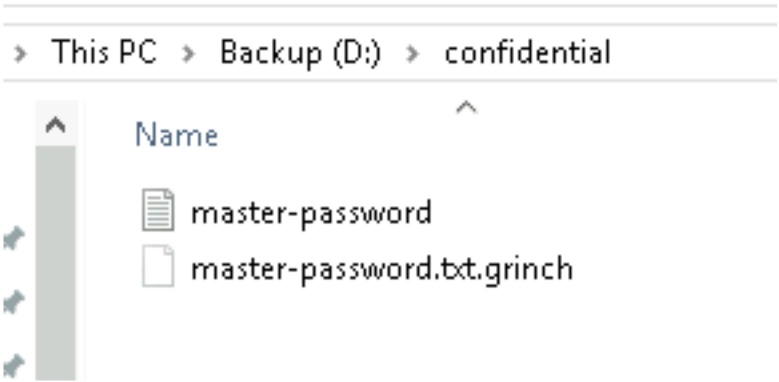
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

Earlier this month (1)

confidential 12/11/2020 7:57 AM

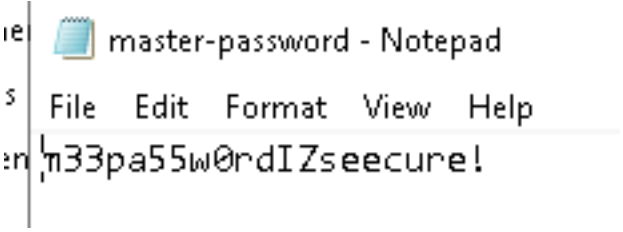
& voila we've restore the master-password back to the unencrypted version



master-password

master-password.txt.grinch

here's the master-password



```
m33pa55w0rdIZseecure!
```