# PSP0201 Week 6 Writeup

Group Name: ikun no 1

Members

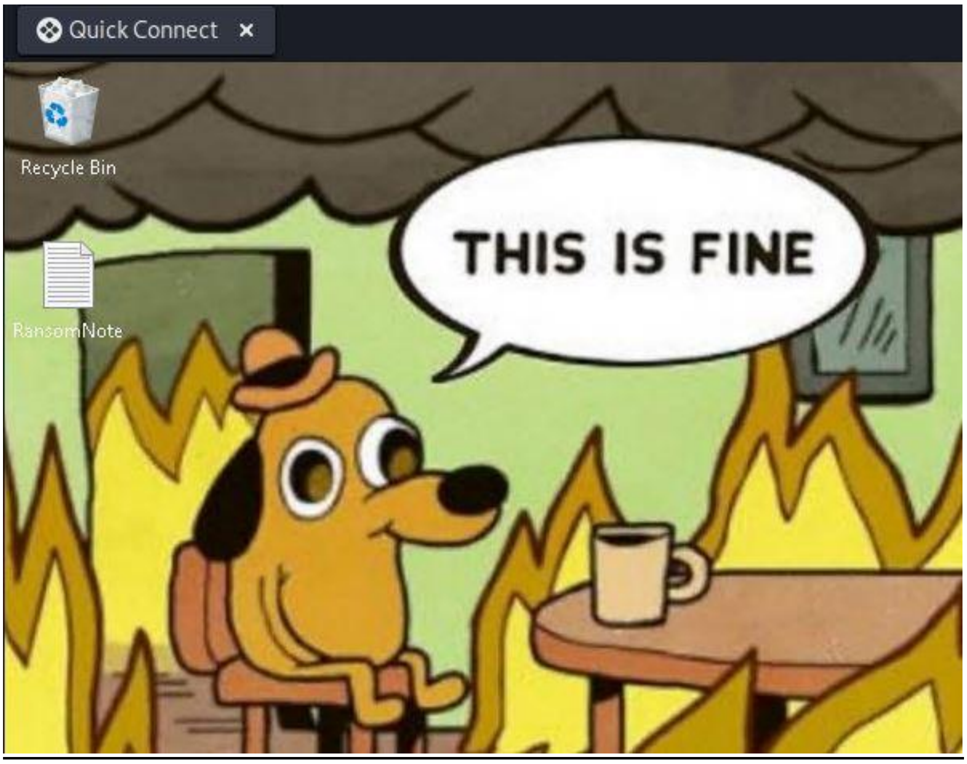
| ID | Name | Role |
|---|---|---|
| 1211102058 | Chu Liang Chern | Leader |
| 1211101401 | Chong Jii Hong | Member |
| 1211103206 | Ng Kai Keat | Member |
| 1211103095 | Siddiq Ferhad Bin Khairil Anual | Member |

## Day 23: Blue Teaming The Grinch strikes again!

**Tool used:** Kali-Linux, Remmina

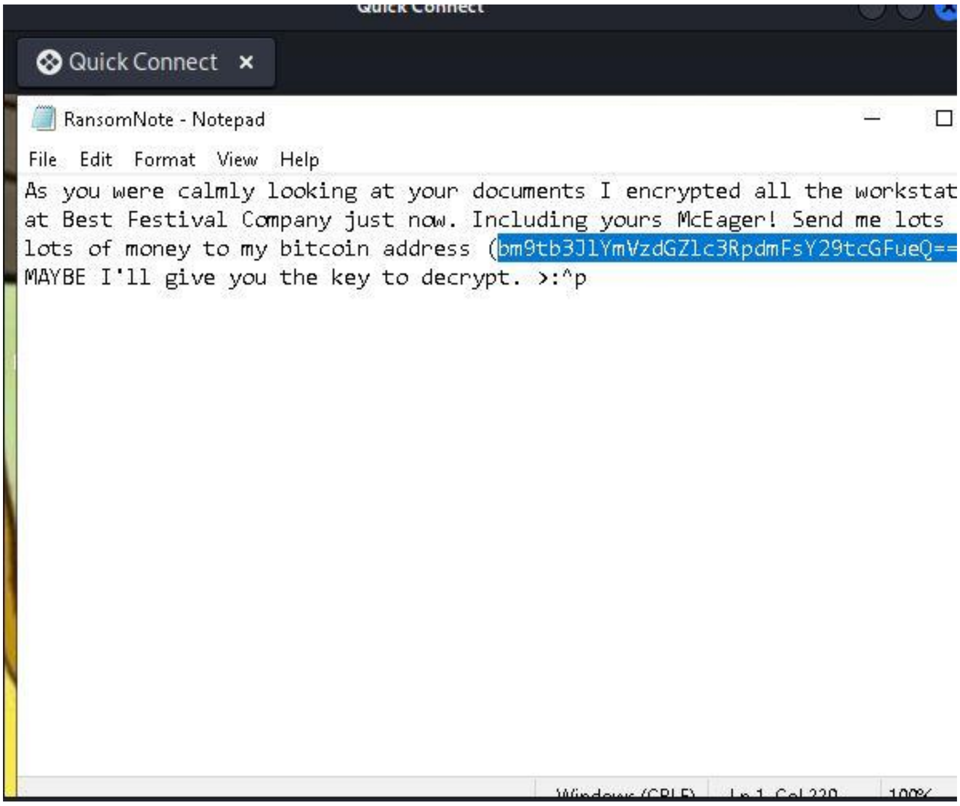
**Solution/walkthrough:**

Question 1



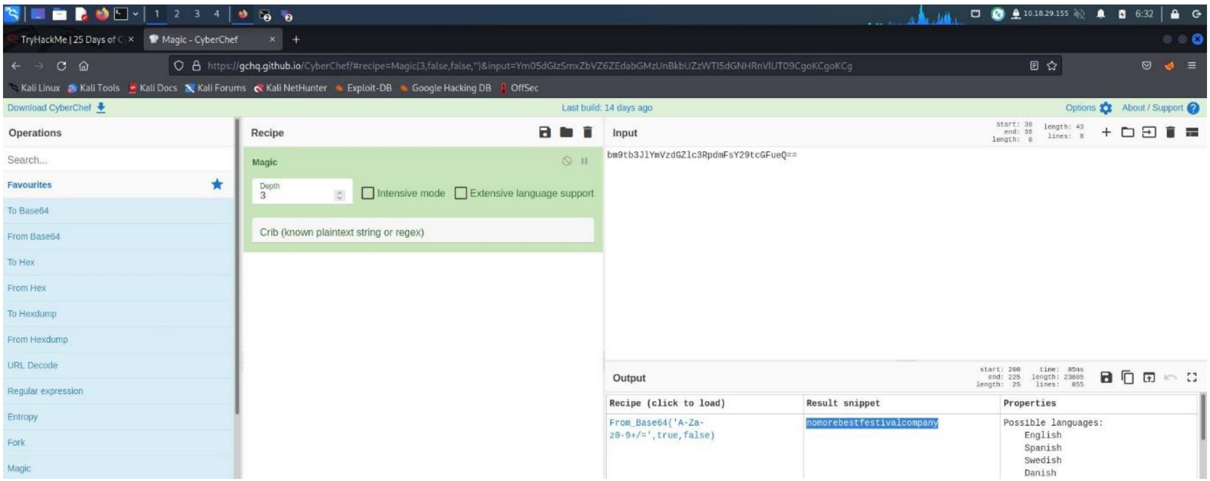
Open the Remmina and the answer shown.

Question 2



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

Open the ransom note and copy the address.



Recipe: Magic

Depth 3 ☐ Intensive mode ☐ Extensive language support

Crib (known plaintext string or regex)

Input

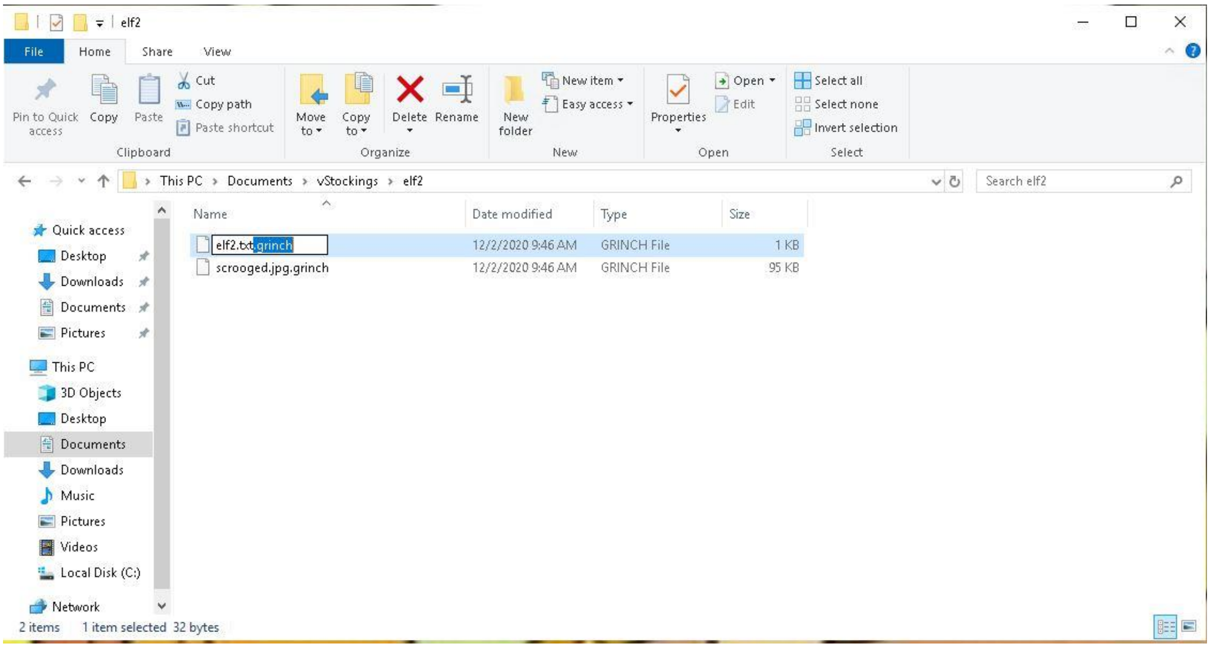
```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

Output

| Recipe (click to load) | Result snippet | Properties |
|---|---|---|
| From_Base64('A-Za-z0-9+/=',true,false) | nomorebestfestivalcompany | Possible languages:<br>English<br>Spanish<br>Swedish<br>Danish |

Use cyberchef and magic operations to bake the address. The answer shown.

Question 3



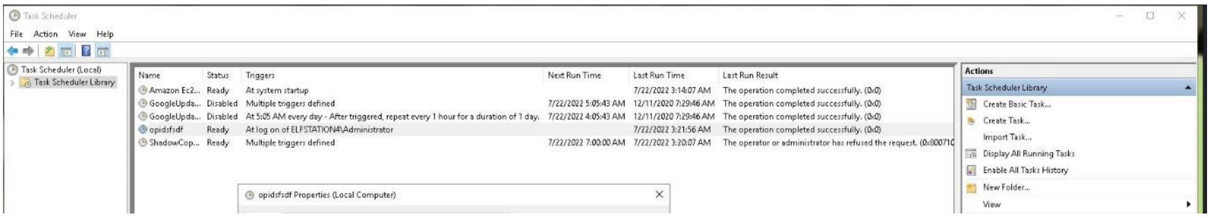
This PC › Documents › vStockings › elf2

| Name | Date modified | Type | Size |
|---|---|---|---|
| elf2.txt.grinch | 12/2/2020 9:46 AM | GRINCH File | 1 KB |
| scrooged.jpg.grinch | 12/2/2020 9:46 AM | GRINCH File | 95 KB |

2 items 1 item selected 32 bytes

Search in the Documents and random choose one folder. The answer shown.

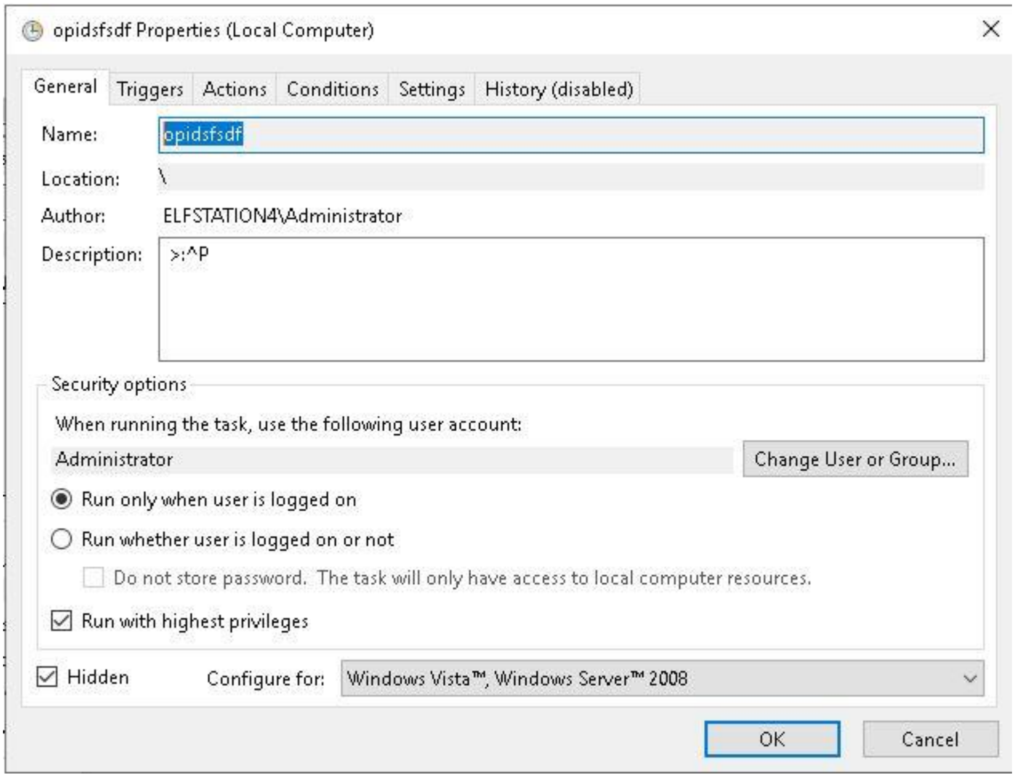
## Question 4



| Name | Status | Triggers | Next Run Time | Last Run Time | Last Run Result |
|---|---|---|---|---|---|
| Amazon Ec2... | Ready | At system startup | | 7/22/2022 3:14:07 AM | The operation completed successfully. (0x0) |
| GoogleUpda... | Disabled | Multiple triggers defined | 7/22/2022 5:05:43 AM | 12/11/2020 7:29:46 AM | The operation completed successfully. (0x0) |
| GoogleUpda... | Disabled | At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day. | 7/22/2022 4:05:43 AM | 12/11/2020 7:29:46 AM | The operation completed successfully. (0x0) |
| opidsfsdf | Ready | At log on of ELFSTATION4\Administrator | | 7/22/2022 3:21:56 AM | The operation completed successfully. (0x0) |
| ShadowCop... | Ready | Multiple triggers defined | 7/22/2022 7:00:00 AM | 7/22/2022 3:20:07 AM | The operator or administrator has refused the request. (0x80071 |

opidsfsdf Properties (Local Computer)

Open Task Schedular to find the name



opidsfsdf Properties (Local Computer)

Name: opidsfsdf

Location: \

Author: ELFSTATION4\Administrator

Description: >:^P

Security options

When running the task, use the following user account:

Administrator

● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

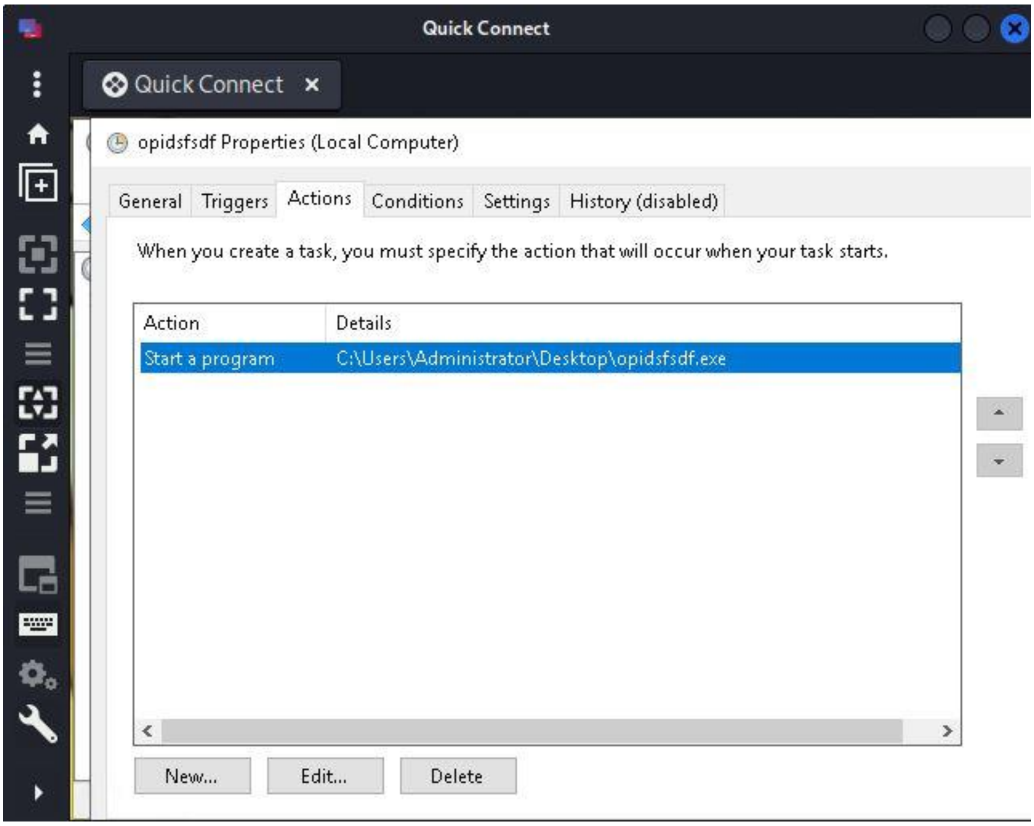
☑ Run with highest privileges

☑ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

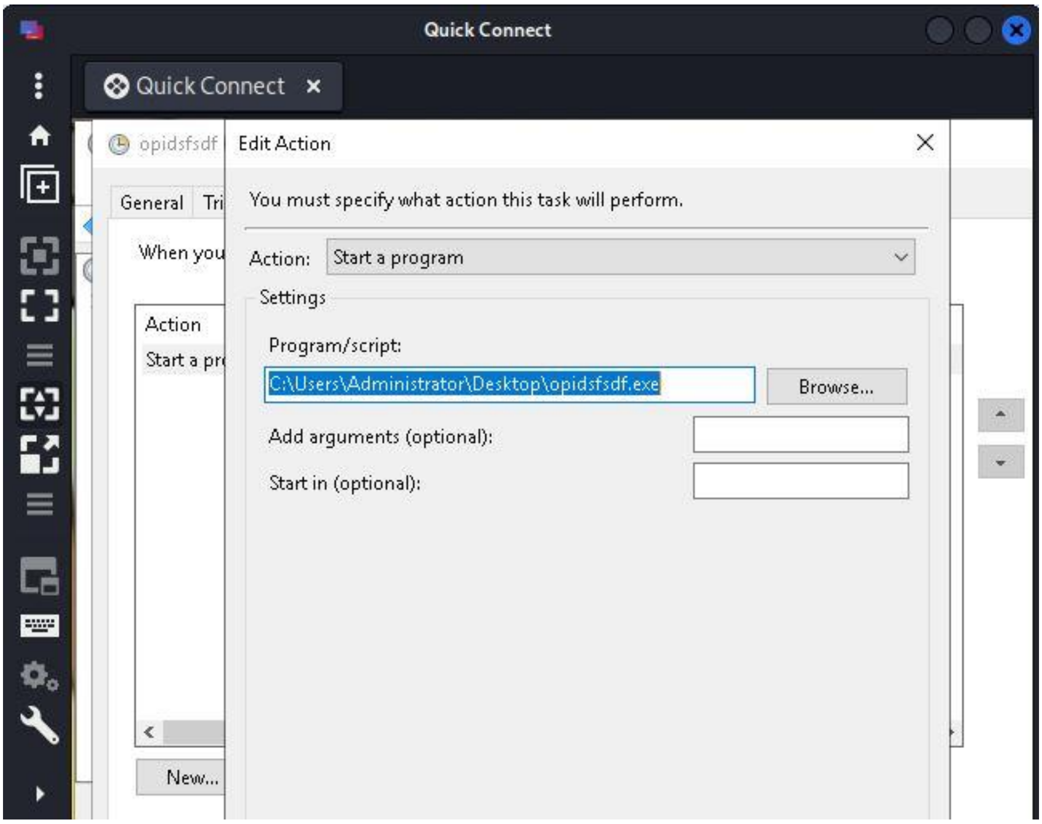
Click on the suspicious file and the name shown.

Question 5



When you create a task, you must specify the action that will occur when your task starts.

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



You must specify what action this task will perform.

Action: Start a program

Settings

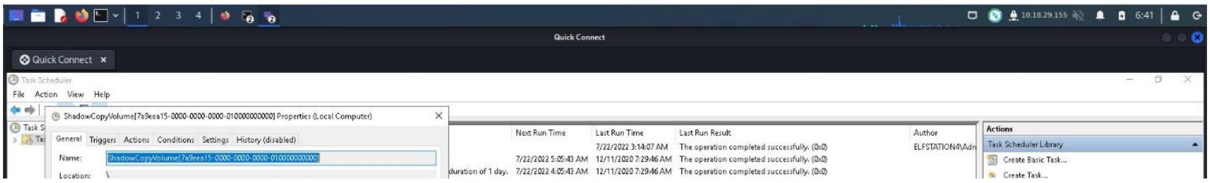
Program/script: C:\Users\Administrator\Desktop\opidsfsdf.exe

Add arguments (optional):

Start in (optional):

Inspect and copy the location.

## Question 6



Quick Connect
Task Scheduler
File Action View Help

ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Computer)

General Triggers Actions Conditions Settings History (disabled)

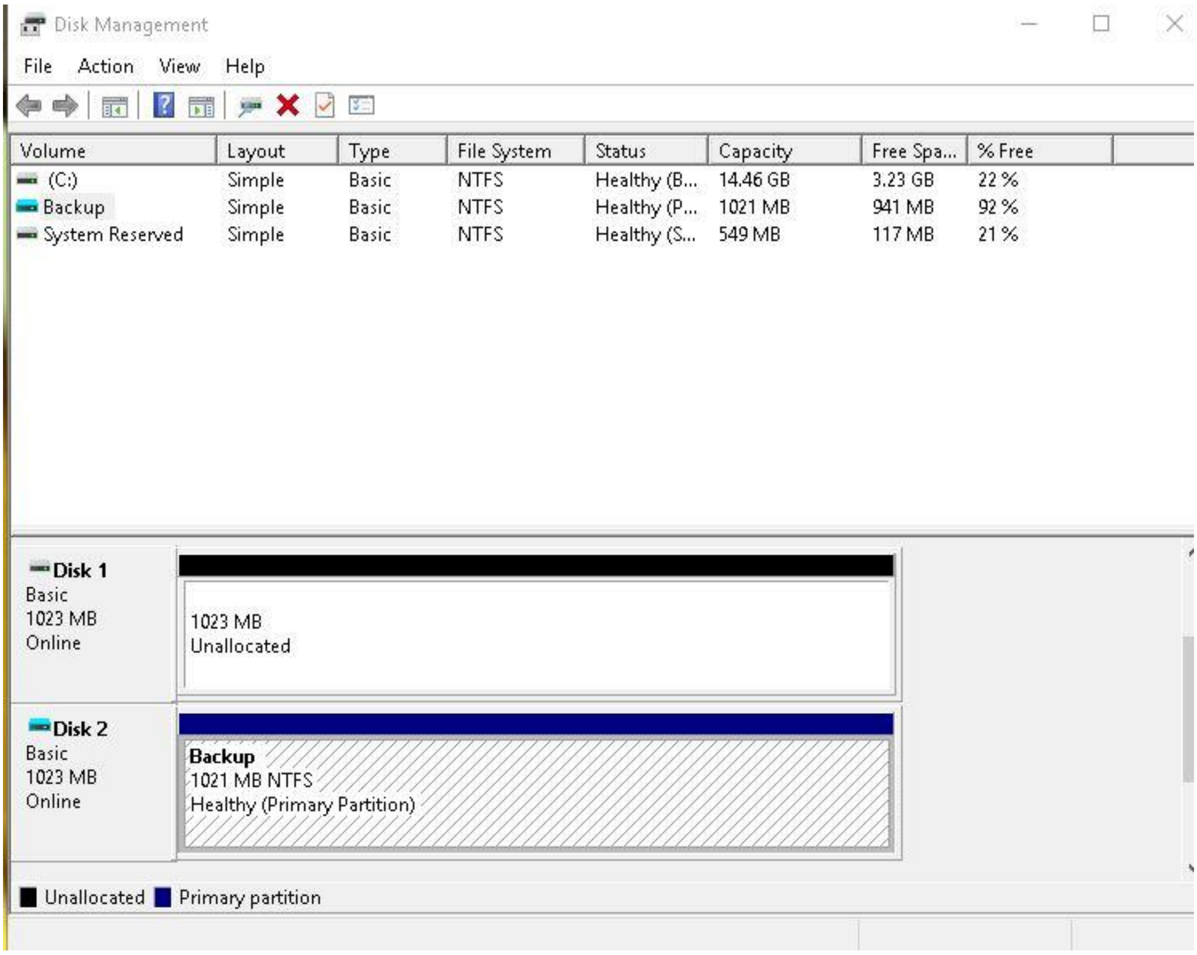
Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location: \

| | Next Run Time | Last Run Time | Last Run Result | Author |
|---|---|---|---|---|
| | | 7/22/2022 3:14:07 AM | The operation completed successfully. (0x0) | ELFSTATION4\Adn |
| | 7/22/2022 5:05:43 AM | 12/11/2020 7:29:46 AM | The operation completed successfully. (0x0) | |
| duration of 1 day. | 7/22/2022 4:05:43 AM | 12/11/2020 7:29:46 AM | The operation completed successfully. (0x0) | |

Go back to the general to check the ShadowCopyVolume ID.

## Question 7



| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 14.46 GB | 3.23 GB | 22 % |
| Backup | Simple | Basic | NTFS | Healthy (P... | 1021 MB | 941 MB | 92 % |
| System Reserved | Simple | Basic | NTFS | Healthy (S... | 549 MB | 117 MB | 21 % |

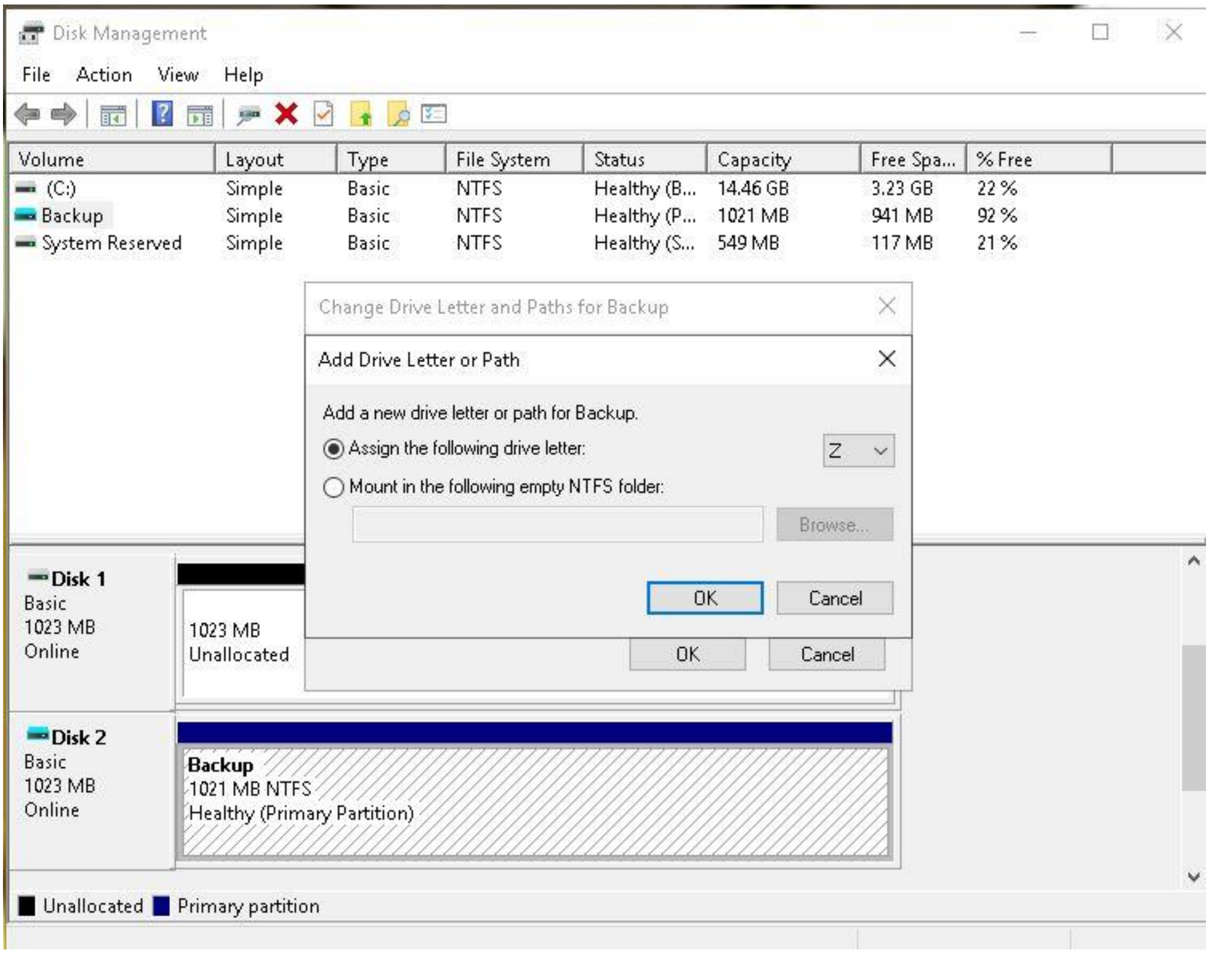
**Disk 1**
Basic
1023 MB
Online

1023 MB
Unallocated

**Disk 2**
Basic
1023 MB
Online

**Backup**
1021 MB NTFS
Healthy (Primary Partition)

First, open disk management and make Disk 2 online.



| Volume | Layout | Type | File System | Status | Capacity | Free Spa... | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 14.46 GB | 3.23 GB | 22 % |
| Backup | Simple | Basic | NTFS | Healthy (P... | 1021 MB | 941 MB | 92 % |
| System Reserved | Simple | Basic | NTFS | Healthy (S... | 549 MB | 117 MB | 21 % |

Change Drive Letter and Paths for Backup

Add Drive Letter or Path

Add a new drive letter or path for Backup.

● Assign the following drive letter: Z

○ Mount in the following empty NTFS folder:

Disk 1
Basic
1023 MB
Online

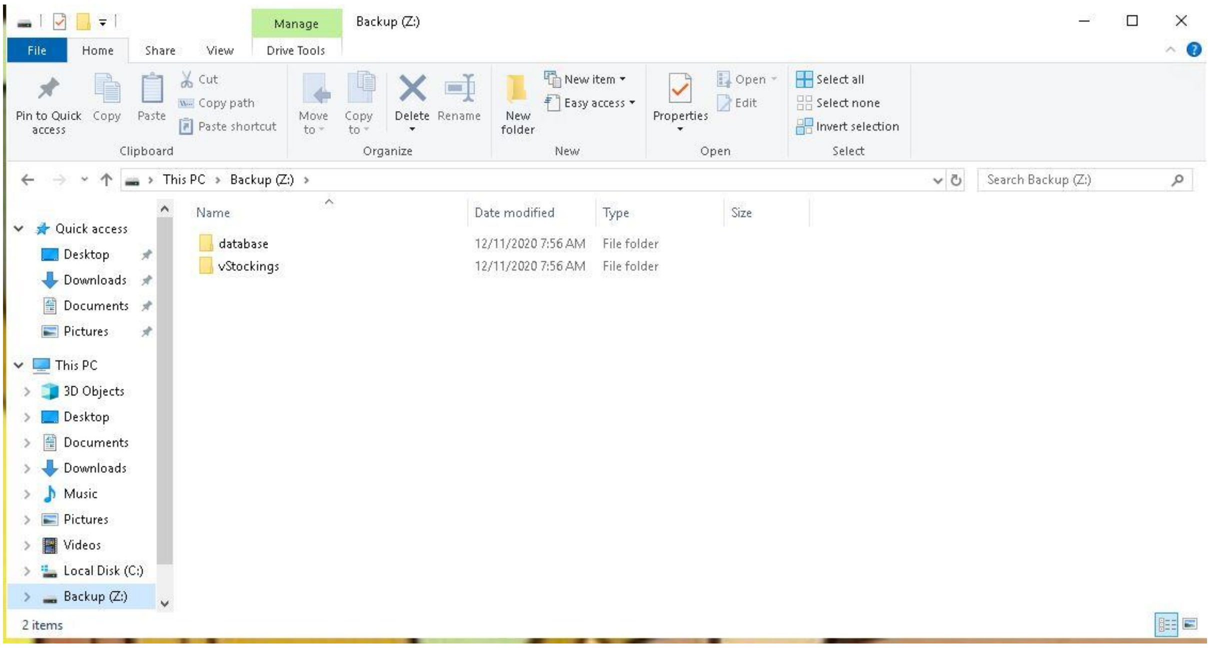
1023 MB
Unallocated

Disk 2
Basic
1023 MB
Online

Backup
1021 MB NTFS
Healthy (Primary Partition)

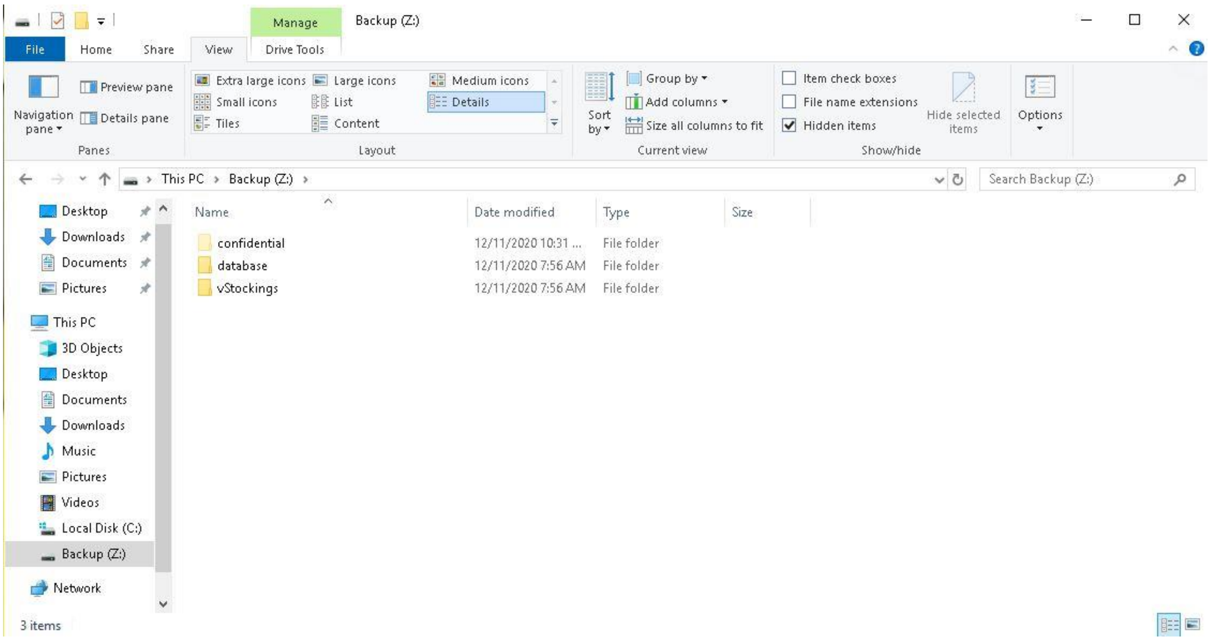
■ Unallocated ■ Primary partition

Then, right click the backup drive to change drive letter and a new letter to represent it.



| Name | Date modified | Type | Size |
|---|---|---|---|
| database | 12/11/2020 7:56 AM | File folder | |
| vStockings | 12/11/2020 7:56 AM | File folder | |

Next, open file explorer and the backup(z) is shown.

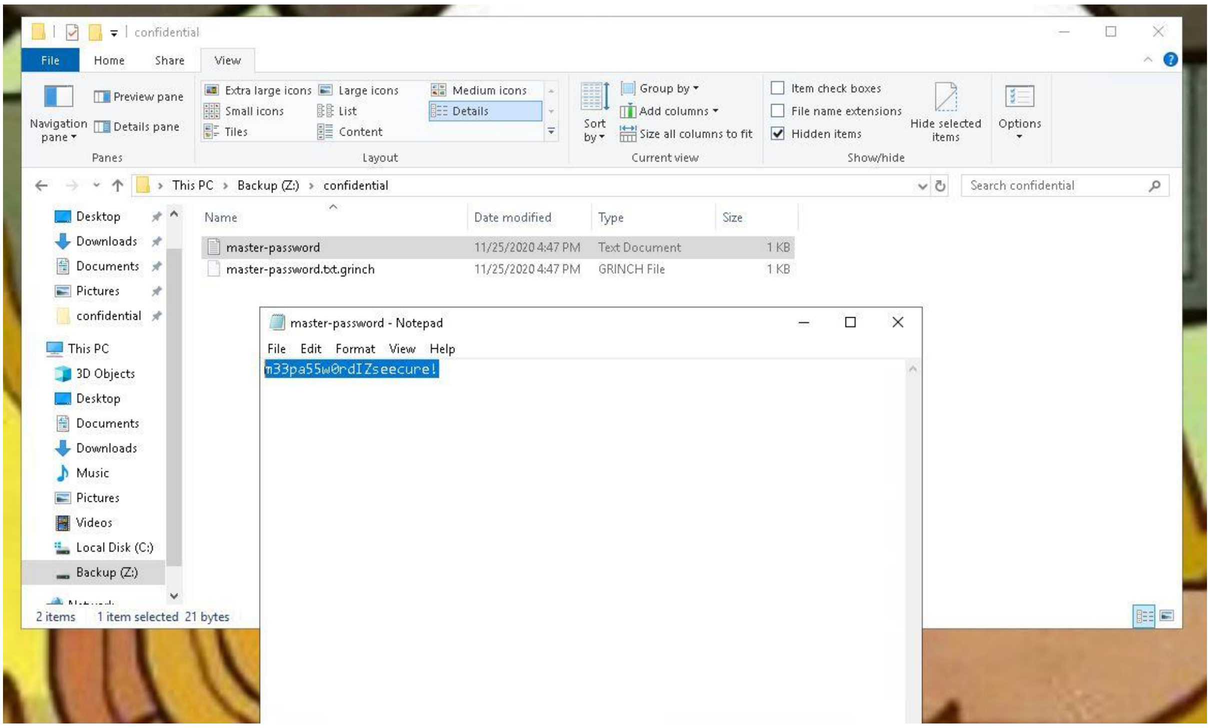


☐ Item check boxes
☐ File name extensions
☑ Hidden items

| Name | Date modified | Type | Size |
|---|---|---|---|
| confidential | 12/11/2020 10:31 ... | File folder | |
| database | 12/11/2020 7:56 AM | File folder | |
| vStockings | 12/11/2020 7:56 AM | File folder | |

Click view and tick to see the hidden items. The hidden folder shown.

## <u>Question 8</u>



☐ Item check boxes
☐ File name extensions
☑ Hidden items

| Name | Date modified | Type | Size |
|---|---|---|---|
| master-password | 11/25/2020 4:47 PM | Text Document | 1 KB |
| master-password.txt.grinch | 11/25/2020 4:47 PM | GRINCH File | 1 KB |

```
m33pa55w0rdIZseecure!
```

Click on the hidden file and open the master-password. The answer shown.