EC-Council

codered
FROM EC-COUNCIL

CHAPTER 15

DATA SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Chapter 15:
Data Security

SCENARIO

Data is the heart of any organization. Critical data contains information that is important for business operation. Identification and classification of business-critical data is the first step in securing an organization's data. This is especially important as organizations usually possess abundant amount of data. An organization should identify their critical data or files based on its importance to the business. This requires analyzing and deciding which information is more important for the organization to function properly. Critical data may consist of revenue, emerging trends, marketing plans, database and files including documents, spreadsheet, emails, etc.

Any data-loss lead to a loss of brand loyalty and trust, reduces the number of customers, or affect market share and shareholder value, regulatory fines, legal proceedings, etc. The number of reported data breach and cyberattacks incidents have increased because of the expansion of computer networks; hence, a security professional must have the required knowledge to secure the organization's data to prevent the loss of any critical or sensitive data that can significantly affect the organization.

OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing data security. This includes knowledge of the following tasks:

- Performing disk encryption using BitLocker Drive Encryption and VeraCrypt
- Implementing built-in file system-level encryption on Windows system
- Performing data backup using Genie Backup Manager
- Recovering file using EaseUS Data Recovery Wizard
- Backing Up and Restoring Data in Windows syste1m
- Performing data destruction using DiskPart utility

OVERVIEW OF DATA SECURITY

Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, and data modification.

An organization's data is considered to be secured when they have sufficient provisions for the following:

- Restricting data from intentional or accidental destruction, modification, or disclosure
- Recovering lost or modified data following incidents
- Appropriate data retention and destruction policies

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to implement data security. The recommended labs that will assist you in securing organizational data include the following:

01 **Perform Disk Encryption using BitLocker Drive Encryption**

02 **Perform Disk Encryption using VeraCrypt**

03 **Implement Built-in File System-level Encryption on Windows**

04 **Perform Data Backup using Genie Backup Manager**

05 **File Recovery using EaseUS Data Recovery Wizard**

06 **Back Up and Restore Data in Windows**

07 **Perform Data Destruction using Windows DiskPart Utility**

Note: Turn on PfSense Firewall virtual machine and keep it running throughout the lab exercises

EXERCISE 1: **PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION**

Disk Encryption is an encryption of data stored in a physical or logical disk.

LAB SCENARIO

A security professional must have the required knowledge to implement disk encryption using various techniques and tools to safeguard organization's critical data.

OBJECTIVE

This lab will demonstrate how to perform disk encryption using tools such as BitLocker Drive Encryption.

OVERVIEW OF DISK ENCRYPTION

Full disk encryption is the encryption of all data in a disk except the master boot record (MBR). The data is automatically converted into a form which cannot be easily deciphered by an unauthorized user. In full disk encryption, the data is encrypted while being written on the disk, and decrypted when the user reads the data from the disk. The benefits of full disk encryption are listed below:

- It is a simple encryption method.
- The encryption method is clear and coherent to users, applications, and databases.
- It is a hardware-based encryption with high performance

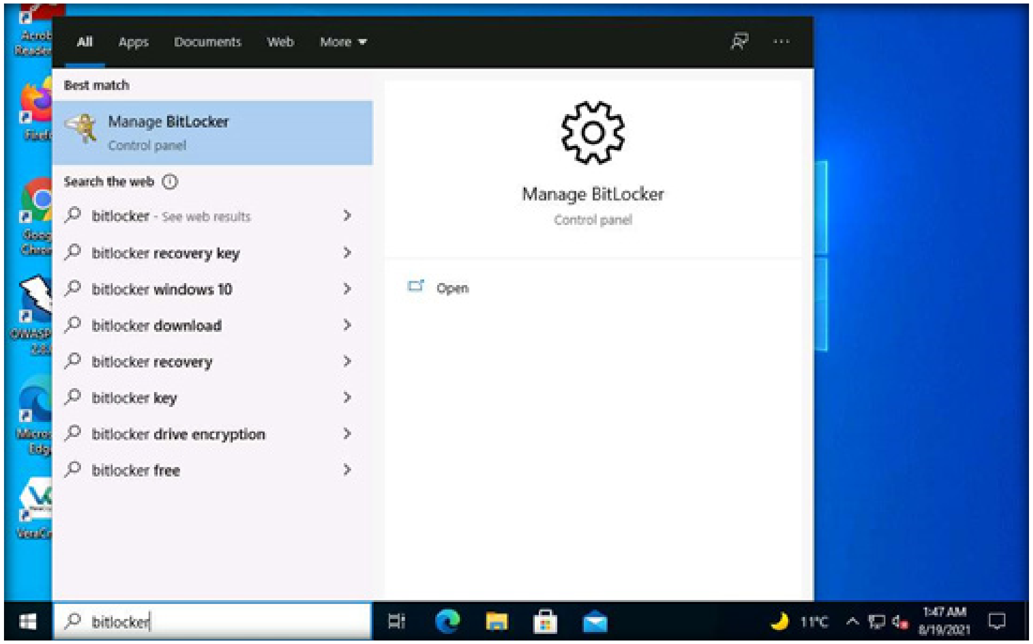
BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

A security professional can use the BitLocker Drive Encryption Tool as a proof of concept to perform disk encryption of organization's data.

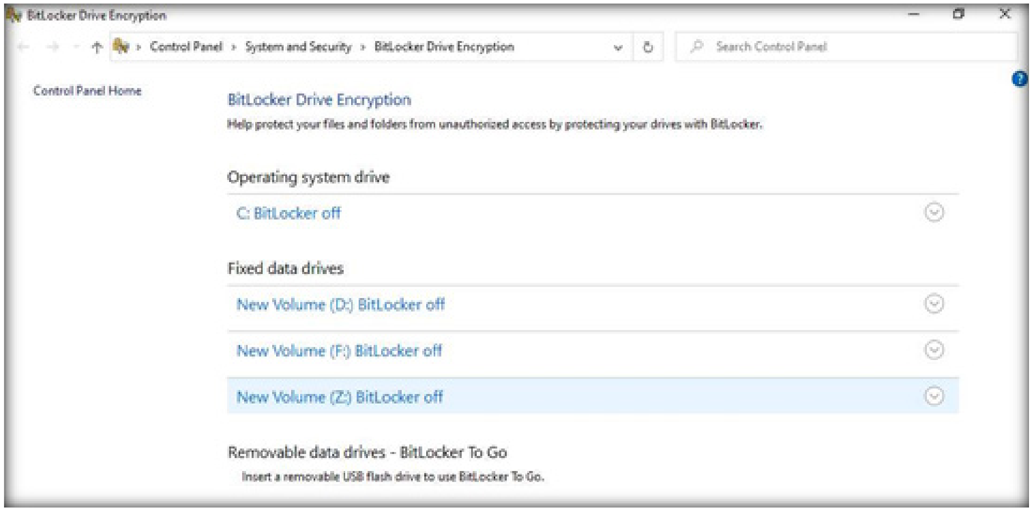
Note: Ensure that the PfSense Firewall virtual machine is running.
1. Turn on the Admin Machine-1 virtual machine.

2. Log in with the credentials Admin and admin@123.
Note: If the network screen appears, click Yes.

3. Click Type here to search field present at the bottom-left corner of Desktop and type bitlocker. Select Manage BitLocker from the search results.



4. The BitLocker Drive Encryption window appears; click the New Volume (Z:) BitLocker off option under the Fixed data drives section.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drives

New Volume (D:) BitLocker off

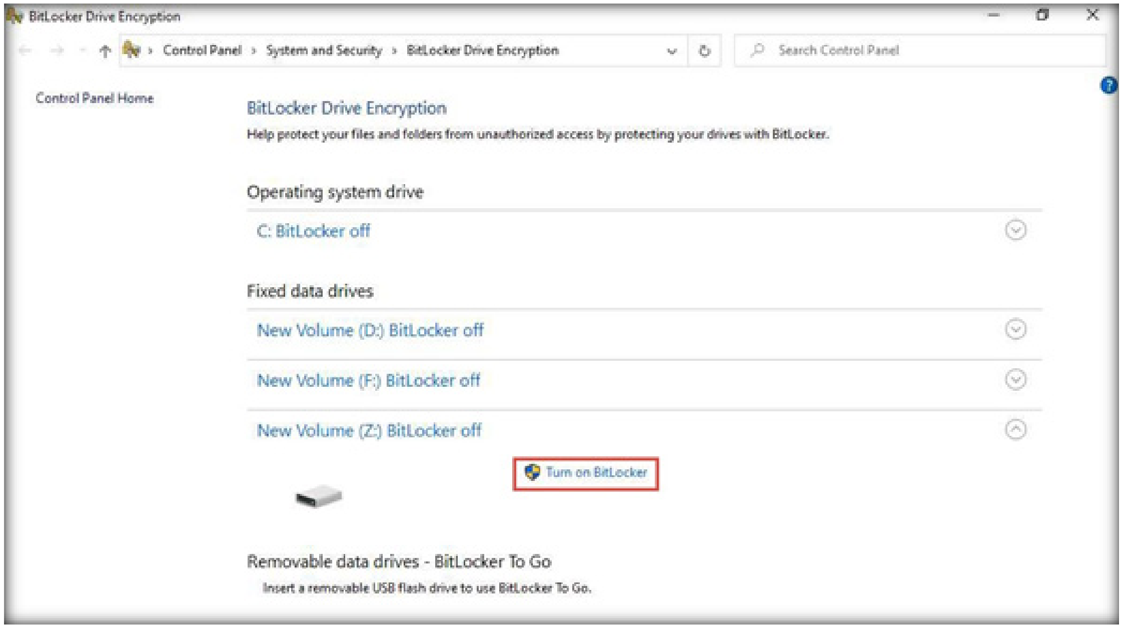
New Volume (F:) BitLocker off

New Volume (Z:) BitLocker off

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

5. Click the Turn on BitLocker option under New Volume (Z:) BitLocker off.



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drives

New Volume (D:) BitLocker off

New Volume (F:) BitLocker off

New Volume (Z:) BitLocker off

Turn on BitLocker

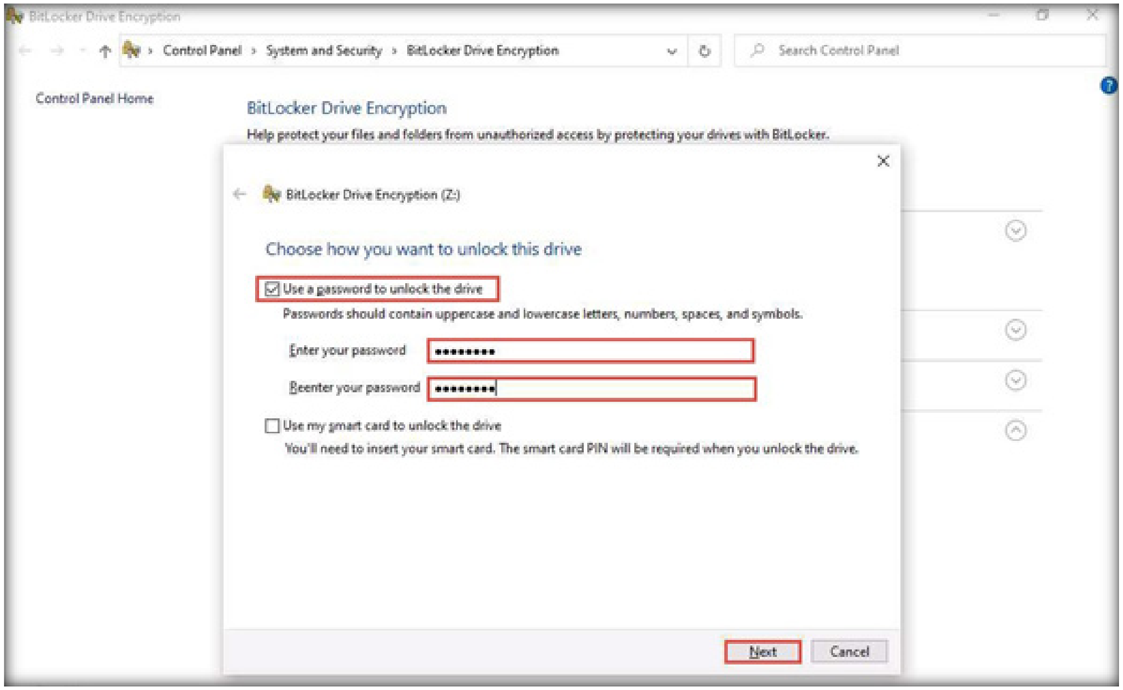
Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

EXERCISE 1: PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION

6. The BitLocker Drive Encryption (Z:) wizard appears; check the Use a password to unlock the drive checkbox.

7. Type the password in the Enter your password field and re-type the password in the Reenter your password field; then, click Next (here, the password entered is test@123).


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home
Next
Cancel

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

BitLocker Drive Encryption (Z:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

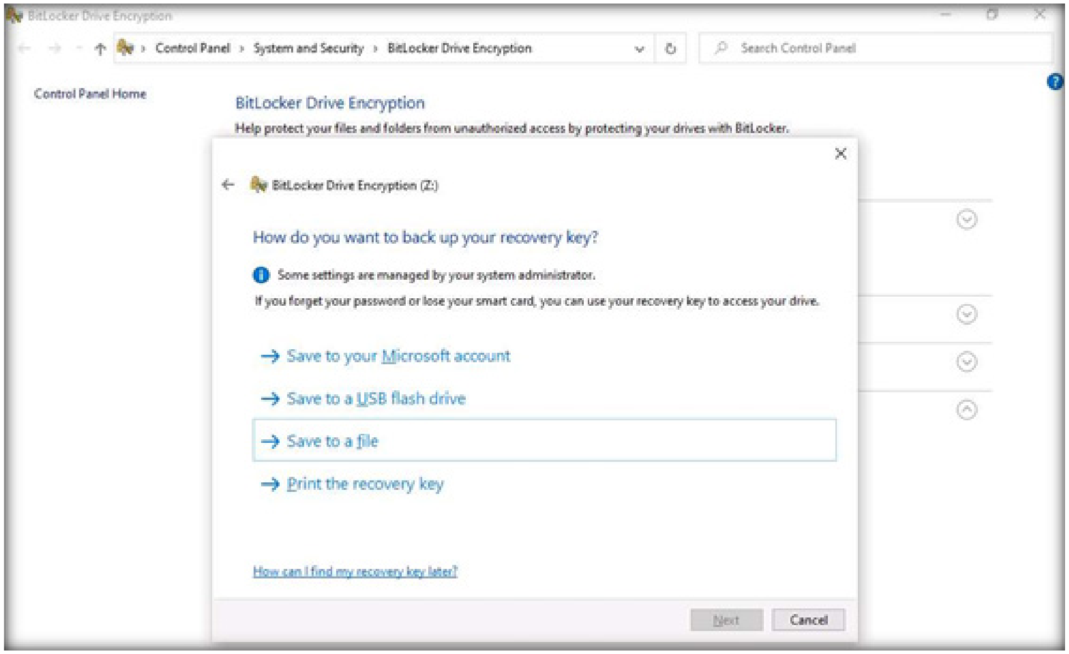
Enter your password: •••••••••

Reenter your password: •••••••••

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

8. The How do you want to back up your recovery key? step appears; click Save to a file from the available options.



BitLocker Drive Encryption

Control Panel > System and Security > BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

BitLocker Drive Encryption (Z:)

How do you want to back up your recovery key?

Some settings are managed by your system administrator.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account

→ Save to a USB flash drive

→ Save to a file

→ Print the recovery key

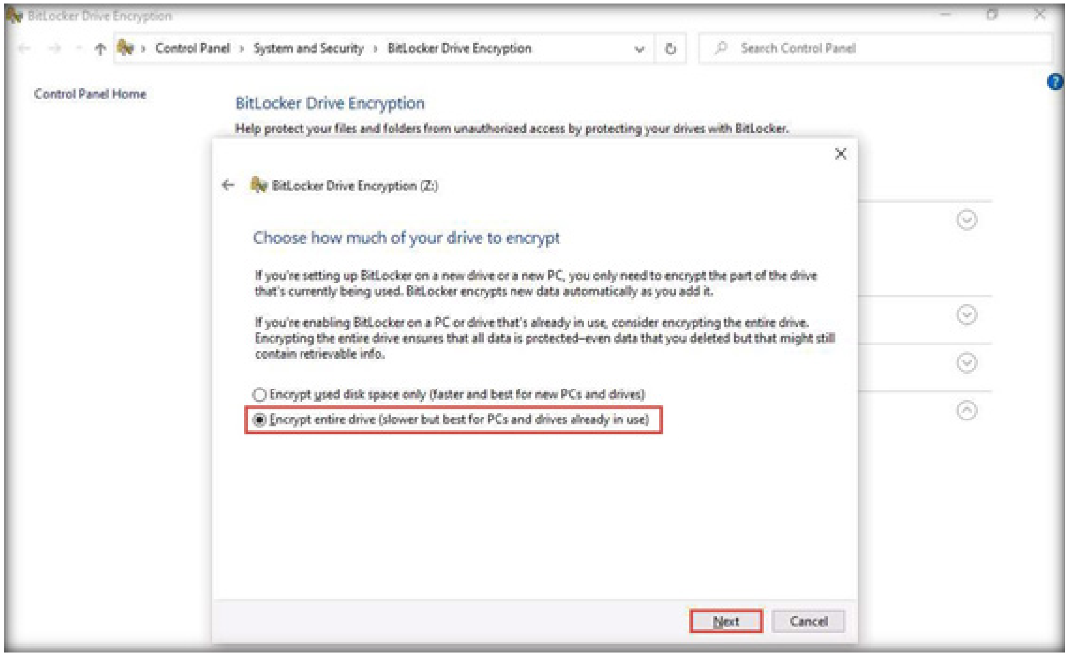
How can I find my recovery key later?

EXERCISE 1: PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION

9. The Save BitLocker recovery key as window appears; keep the save location set to This PC → Documents and click Save.

10. Click Next in the How do you want to back up your recovery key? step.

11. In the Choose how much of your drive to encrypt step, select the Encrypt entire drive (slower but best for PCs and drives already in use) button, and click Next.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

BitLocker Drive Encryption (Z:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

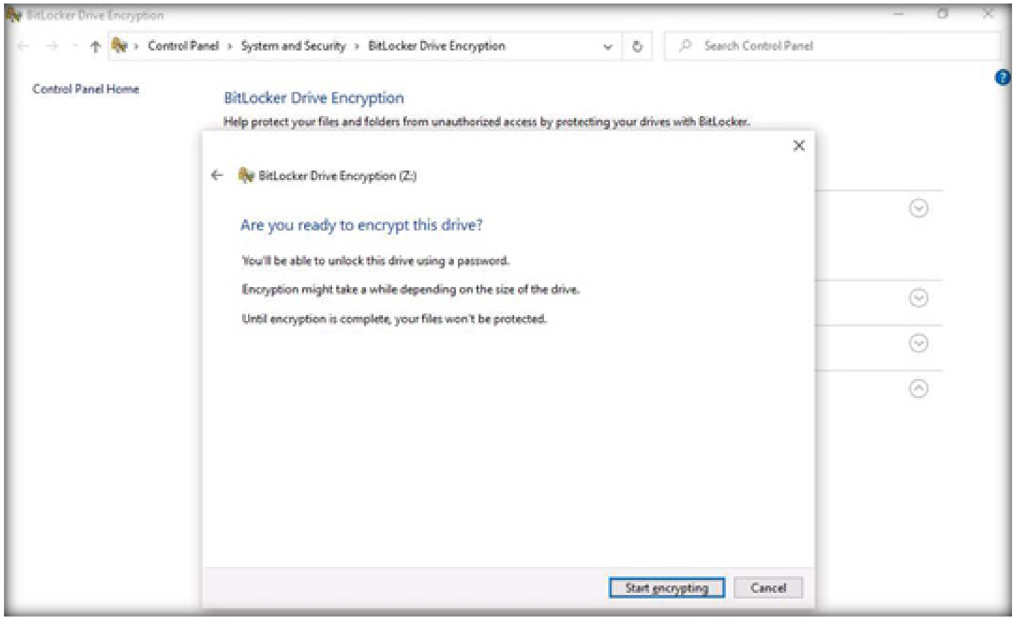
○ Encrypt used disk space only (faster and best for new PCs and drives)

● Encrypt entire drive (slower but best for PCs and drives already in use)

EXERCISE 1: PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION

12. In the Choose which encryption mode to use step, ensure that the Compatible mode (best for drives that can be moved from this device) option is selected, and click Next.

13. In the Are you ready to encrypt this drive? step, click Start encrypting to encrypt the selected drive.


BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

BitLocker Drive Encryption (Z:)

Are you ready to encrypt this drive?

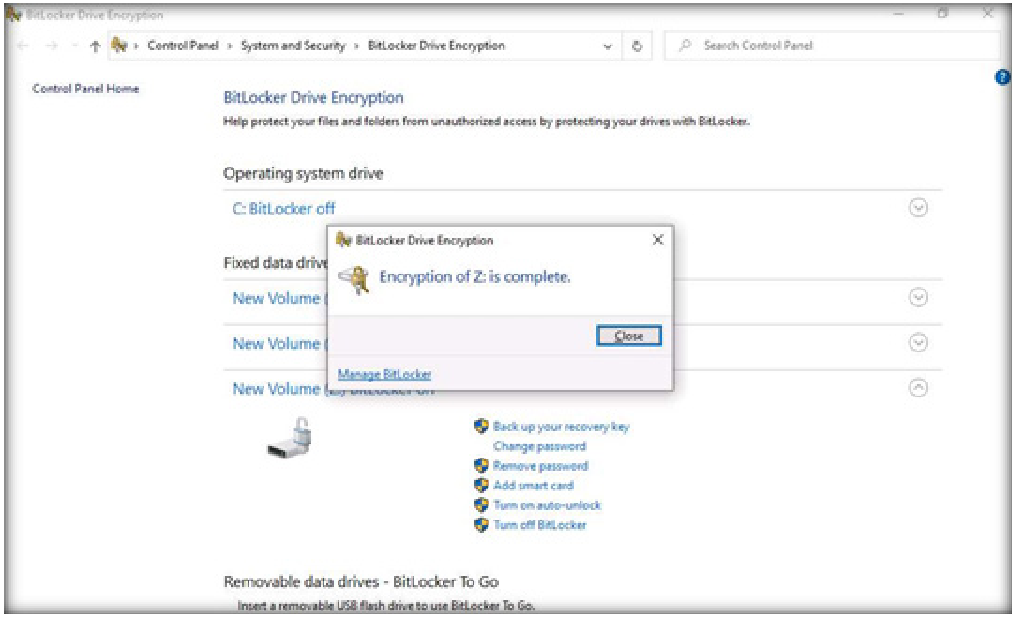
You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

14. The BitLocker Drive Encryption pop-up appears, showing the Encrypting... status.

15. After the completion of the encryption process, the New Volume (Z:) BitLocker off will change to New Volume (Z:) BitLocker on, Restart the machine.
Note: If an Encryption of Z: is complete notification appears; click Close.



BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Fixed data drive

New Volume (

New Volume (

New Volume

BitLocker Drive Encryption

Encryption of Z: is complete.

Close

Manage BitLocker

Removable data drives - BitLocker To Go

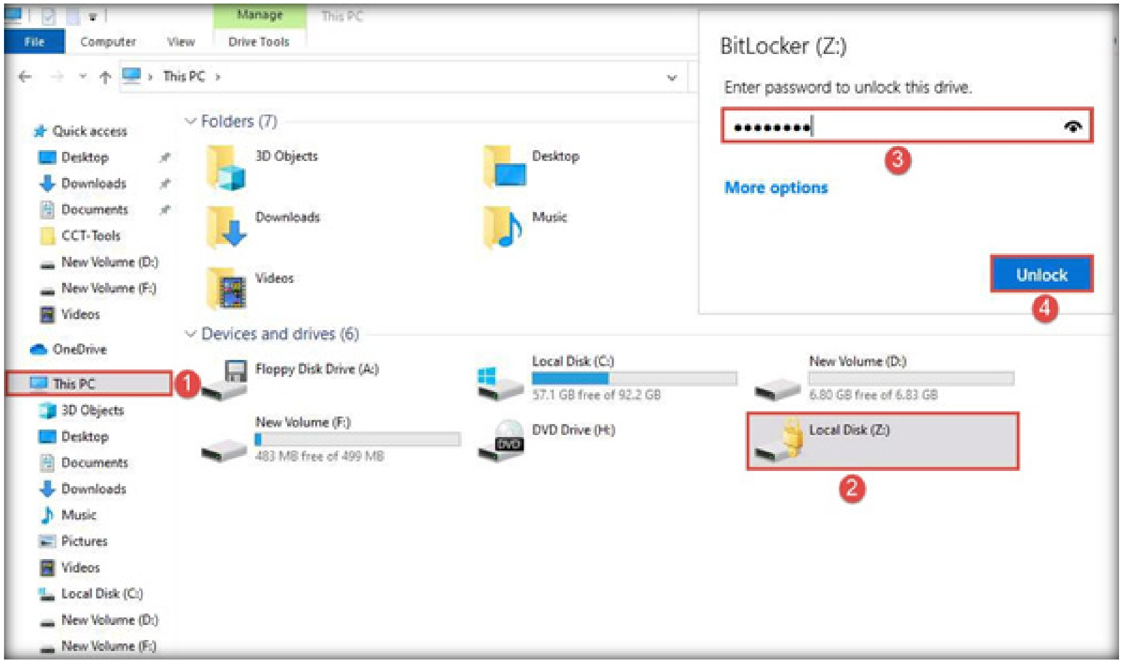
Insert a removable USB flash drive to use BitLocker To Go.

16. After the system reboots, log in with the credentials Admin and admin@123.

17. Open File Explorer and click This PC from the left pane.

18. You can observe that Local Disk (Z:) is now encrypted; double-click and the BitLocker (Z:) security pop-up appears at the top-right corner of Desktop

19. Type the password you provided in Step#7 and click Unlock.
Note: Here, the password is test@123.

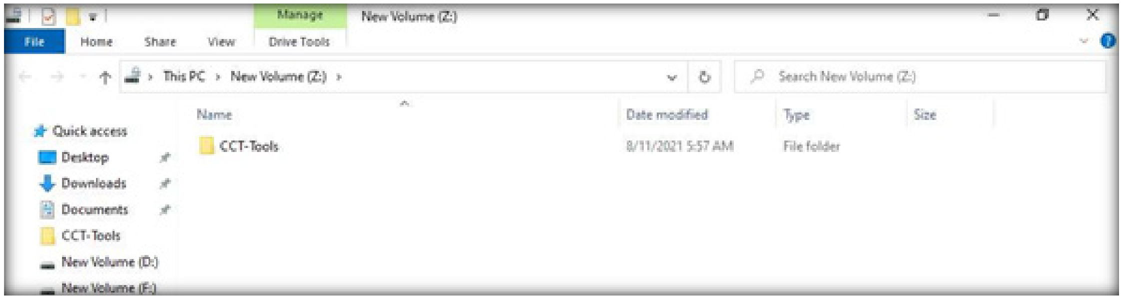


BitLocker (Z:)

Enter password to unlock this drive.

Note: If the New Volume (Z:) pop-up appears at the top-right corner of the window. Click the Open folder to view files option to view the disk content.

20. The New Volume (Z:) window appears displaying the disk content, as shown in the screenshot below.
Note: The disk will remain unlocked until the next time you restart the system.

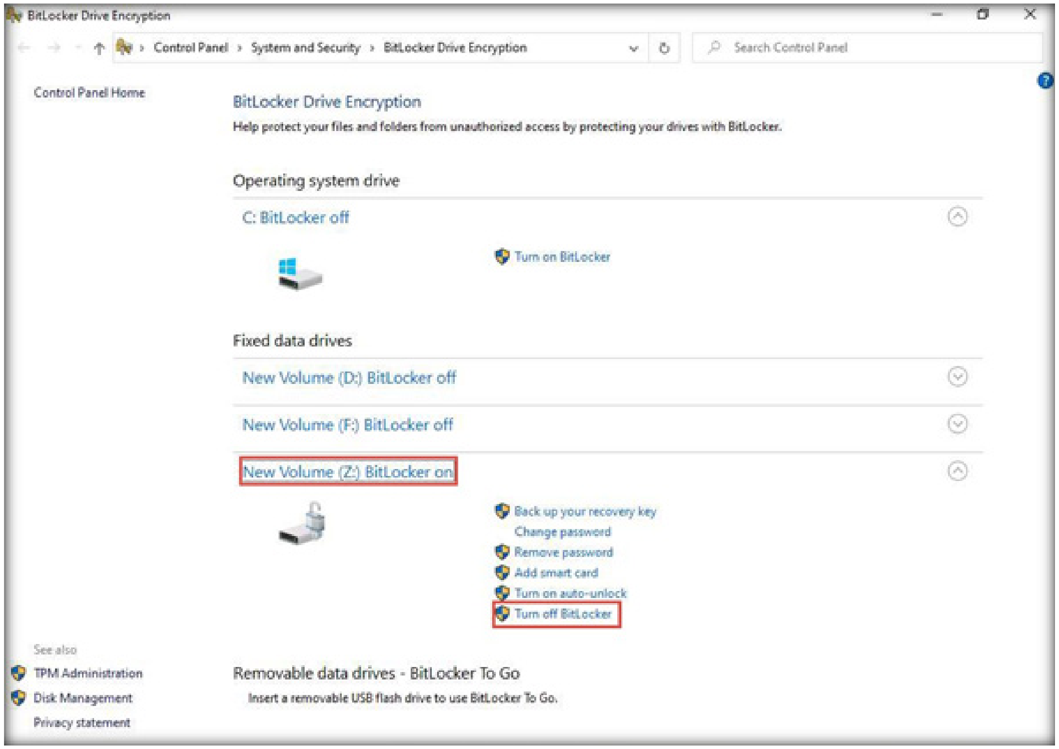


21. This concludes the demonstration showing how to perform disk encryption using BitLocker Drive Encryption.

22. Once, you are done with this task; you must turn off BitLocker to decrypt the New Volume (Z:) disk.

23. To do so, open the BitLocker Drive Encryption window, click New Volume (Z:) BitLocker on; from the options click Turn off BitLocker.
Note: To open BitLocker Drive Encryption window, follow Step#3.

EXERCISE 1: PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION



BitLocker Drive Encryption

Control Panel › System and Security › BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

New Volume (D:) BitLocker off

New Volume (F:) BitLocker off

New Volume (Z:) BitLocker on

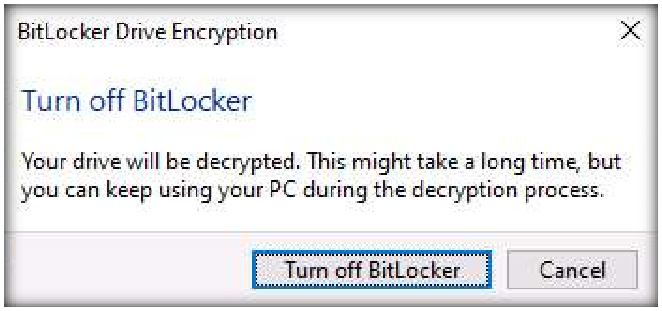
Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker

See also
TPM Administration
Disk Management
Privacy statement

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

24. The BitLocker Drive Encryption pop-up appears; click Turn off BitLocker.


BitLocker Drive Encryption

Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

25. BitLocker initiates the decryption process. Wait for it to complete.
Note: If after the completion of decryption process, the Decryption of Z: is complete pop-up appears; click Close.

26. The New Volume (Z:) decrypts successfully.

27. Close all open windows and document all the acquired information.

EXERCISE 1: PERFORM DISK ENCRYPTION USING BITLOCKER DRIVE ENCRYPTION

EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device).

LAB SCENARIO

A security professional should know how to encrypt volume/disk to safeguard organization data.

OBJECTIVE

This lab will demonstrate how to perform disk encryption using tools such as VeraCrypt.

OVERVIEW OF DISK ENCRYPTION

It is prevalent to encrypt data as it prevents the data from unauthorized access. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

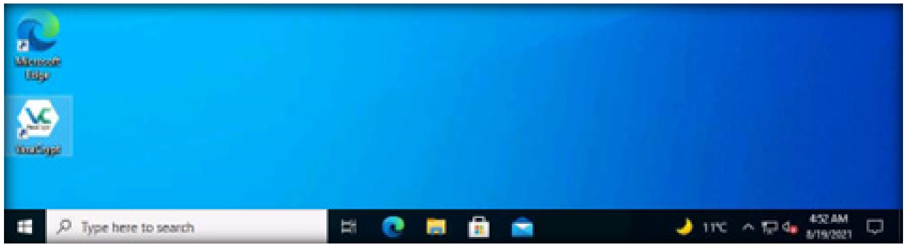
VeraCrypt offers on-the-fly encryption which means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention.

A security professional can use the VeraCrypt Tool as a proof of concept to perform disk encryption of organization's data.

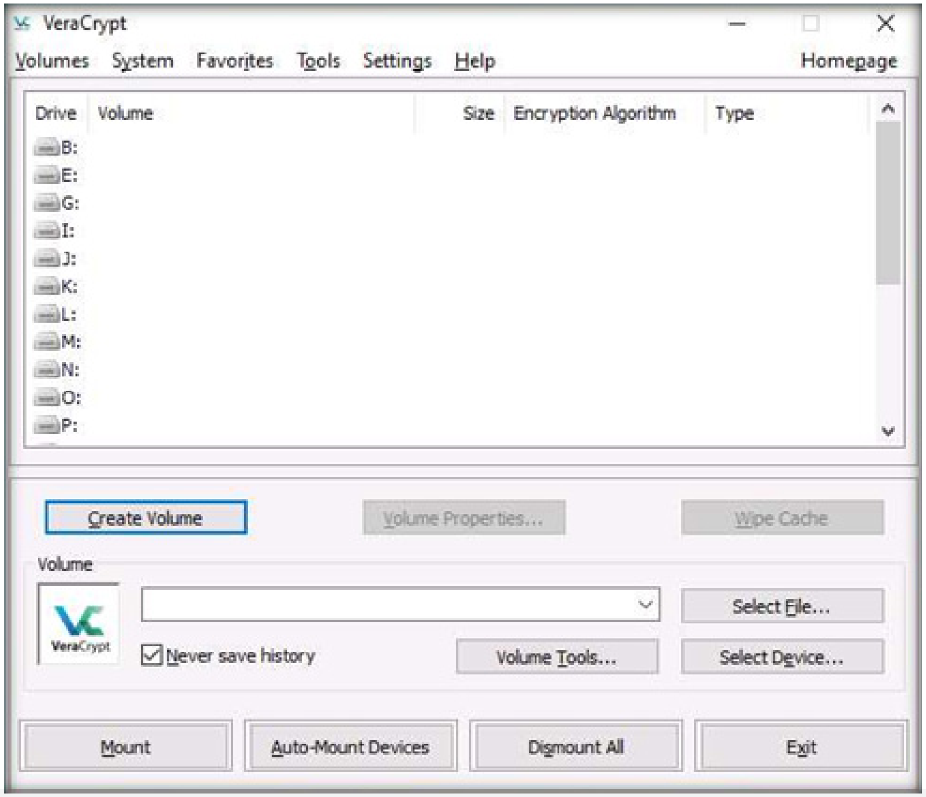
EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, navigate to the Desktop, double-click VeraCrypt shortcut.



2. The VeraCrypt main window appears; click the Create Volume button.

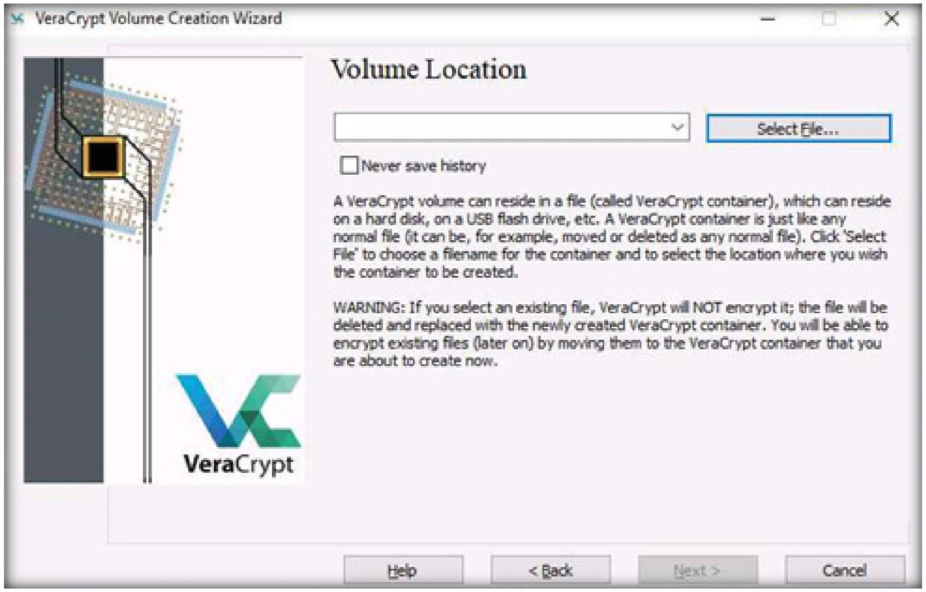


EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

3. The VeraCrypt Volume Creation Wizard window appears. Ensure that the Create an encrypted file container radio-button is selected and click Next to proceed.

4. In the Volume Type wizard, keep the default settings and click Next.

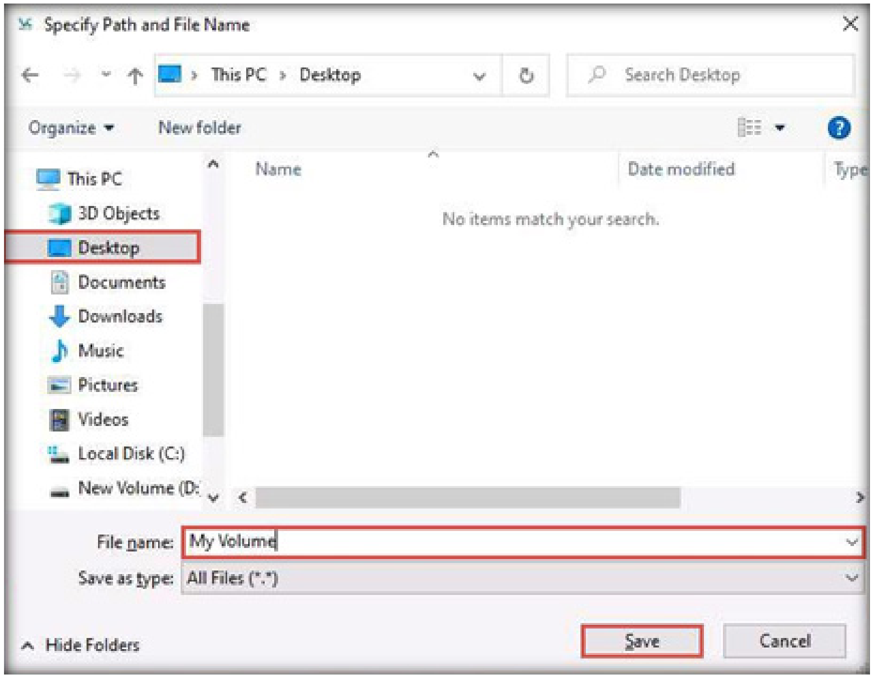
5. In the Volume Location wizard, click Select File....



A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

6. The Specify Path and File Name window appears; navigate to the desired location (here, Desktop), provide the File name as My Volume, and click Save.



File name: My Volume

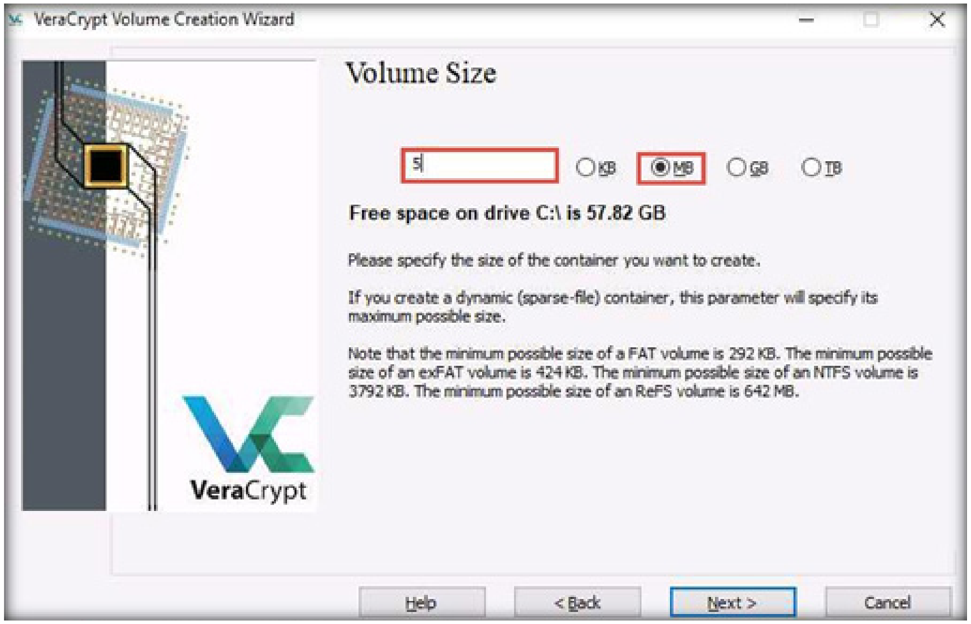
Save as type: All Files (*.*)

EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

7. After saving the file, the location of the file containing the VeraCrypt volume appears under the Volume Location field; then, click Next.

8. In the Encryption Options wizard, keep the default settings and click Next.

9. In the Volume Size wizard, ensure that the MB radio-button is selected and specify the size of the VeraCrypt container as 5; then, click Next.



VeraCrypt Volume Creation Wizard

Volume Size

5 ○ KB ● MB ○ GB ○ TB

Free space on drive C:\ is 57.82 GB

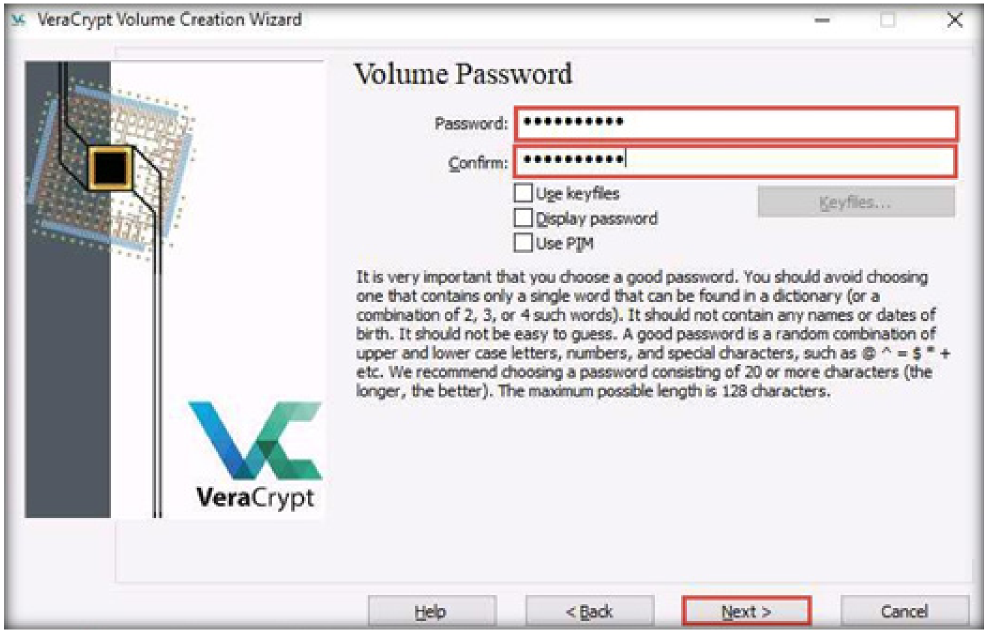
Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an exFAT volume is 424 KB. The minimum possible size of an NTFS volume is 3792 KB. The minimum possible size of an ReFS volume is 642 MB.

10. The Volume Password wizard appears; provide a strong password in the Password field, re-type in the Confirm field, and click Next. The password provided in this lab is qwerty@123.

Note: If VeraCrypt Volume Creation Wizard warning pop-up appears; click Yes.



Volume Password

Password: •••••••••••

Confirm: •••••••••••

□ Use keyfiles
□ Display password
□ Use PIM

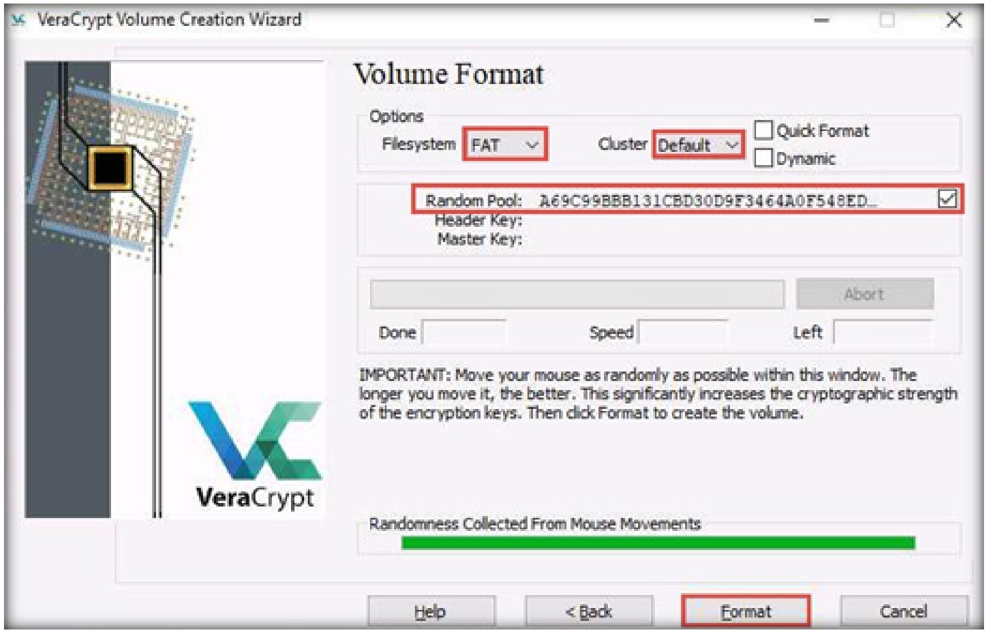
It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

11. The Volume Format wizard appears; ensure that FAT is selected in the Filesystem option and Default is selected in Cluster option.

12. Check the checkbox under the Random Pool, Header Key, and Master Key section.

13. Move your mouse as randomly as possible within the Volume Creation Wizard window for at least 30 seconds and click the Format button.



VeraCrypt Volume Creation Wizard

Volume Format

Options

Filesystem: FAT

Cluster: Default

□ Quick Format

□ Dynamic

Random Pool: A69C99BBB131CBD30D9F3464A0F548ED... ☑

Header Key:

Master Key:

Done

Speed

Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Randomness Collected From Mouse Movements

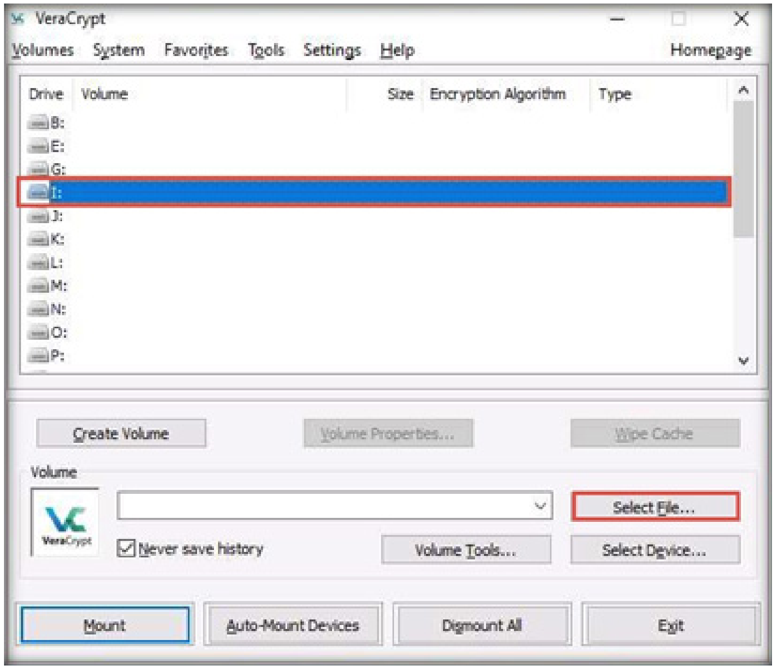
14. After clicking Format, VeraCrypt will create a file called My Volume in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).

15. Depending on the size of the volume, volume creation may take some time.

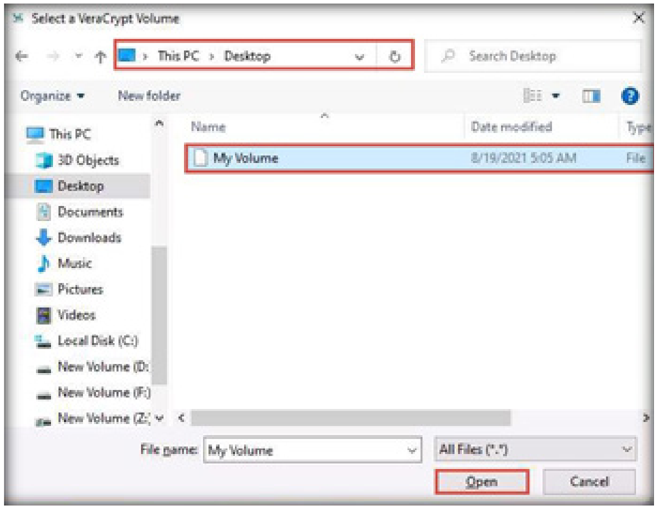
16. Once the volume is created, a VeraCrypt Volume Creation Wizard dialog-box appears; click OK.

17. In the VeraCrypt Volume Creation Wizard window, a Volume Created message appears; click Exit.

18. The VeraCrypt main window appears; select a drive (here, I:) and click Select File....



19. The Select a VeraCrypt Volume window appears; navigate to Desktop, click My Volume, and click Open.

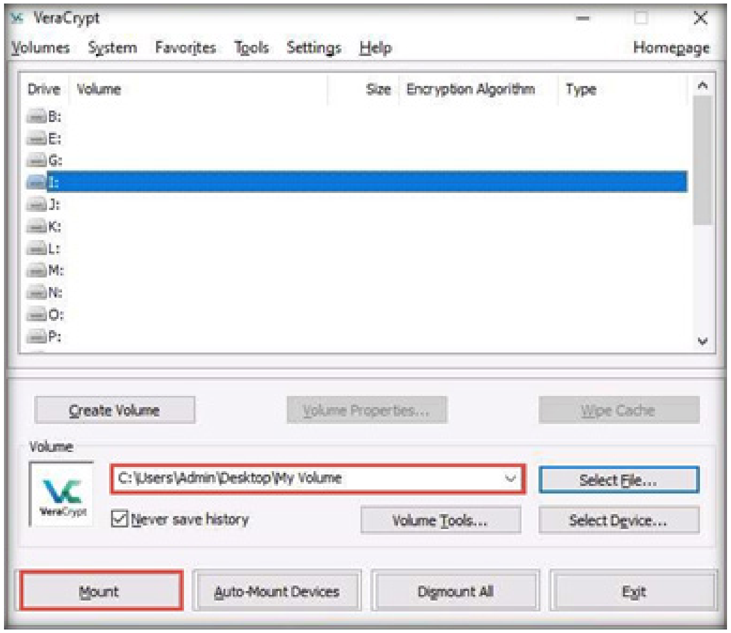


My Volume 8/19/2021 5:05 AM File

File name: My Volume

EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

20. The window closes, and the VeraCrypt window appears displaying the location of selected volume under the Volume field; then, click Mount.

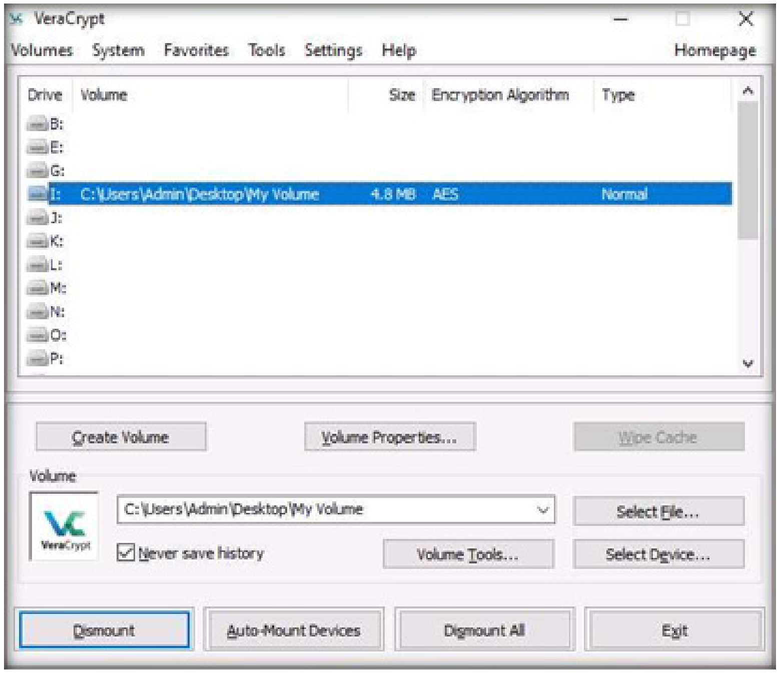


Volume: C:\Users\Admin\Desktop\My Volume

☑ Never save history

21. The Enter password dialog-box appears; type the password you specified in Step#10 into the Password field and click OK.
Note: The password specified in this task is qwerty@123.

22. After the password is verified, VeraCrypt will mount the volume in I: drive, as shown in the screenshot below.



Drive	Volume	Size	Encryption Algorithm	Type
B:				
E:				
G:				
I:	C:\Users\Admin\Desktop\My Volume	4.8 MB	AES	Normal
J:				
K:				
L:				
M:				
N:				
O:				
P:				

Volume: C:\Users\Admin\Desktop\My Volume

☑ Never save history

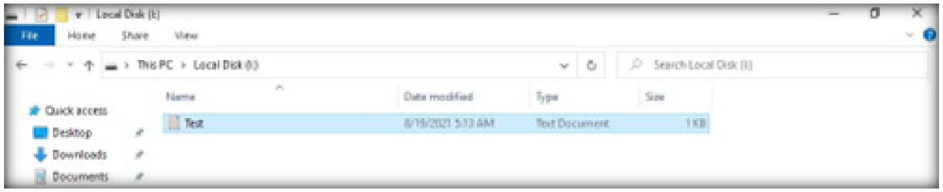
EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

23. My Volume has successfully mounted the container as a virtual disk (I:). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similar to a real disk. You can copy or move files to this virtual disk to encrypt them.

24. Create a text file on Desktop and name it Test. Open the text file and insert text.

25. Click File in the menu bar and click Save.

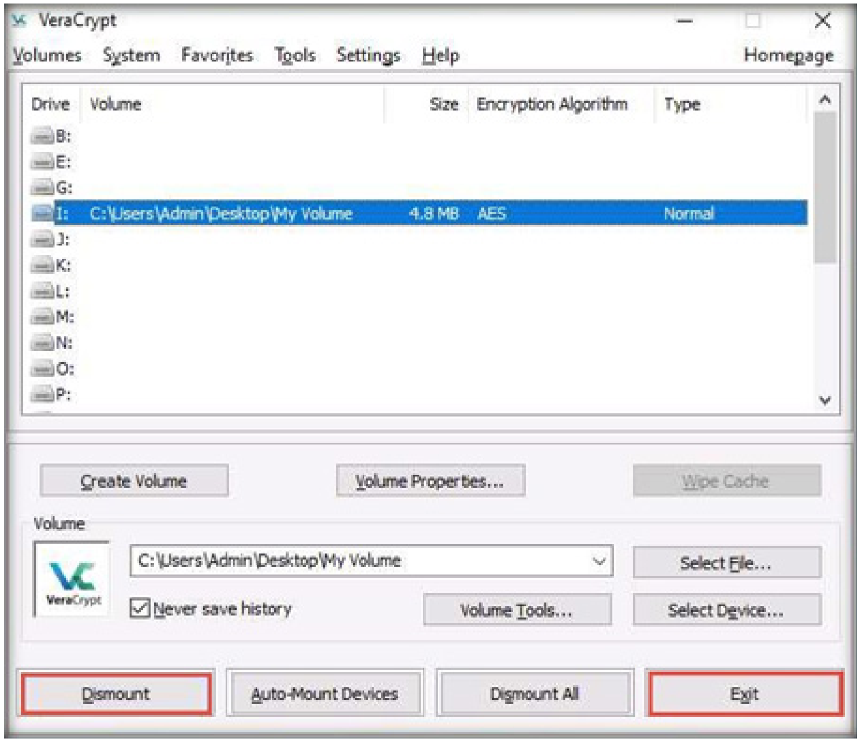
26. Copy the file from Desktop and paste it into Local Disk (I:). Close the window.



Name	Date modified	Type	Size
Test	8/19/2021 5:13 AM	Text Document	1 KB

EXERCISE 2: PERFORM DISK ENCRYPTION USING VERACRYPT

27. Switch to the VeraCrypt window, click Dismount, and then click Exit.



Drive	Volume	Size	Encryption Algorithm	Type
B:				
E:				
G:				
I:	C:\Users\Admin\Desktop\My Volume	4.8 MB	AES	Normal
J:				
K:				
L:				
M:				
N:				
O:				
P:				

Volume: C:\Users\Admin\Desktop\My Volume

☑ Never save history

28. The I: drive located in This PC disappears.
Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

29. This concludes the demonstration showing how to perform disk encryption using VeraCrypt.

30. Close all open windows and document all the acquired information.

EXERCISE 3: IMPLEMENT BUILT-IN FILE SYSTEM-LEVEL ENCRYPTION ON WINDOWS

The Encrypting File System (EFS) provides file system-level encryption in Windows (starting from Windows 2000), except the home version.

LAB SCENARIO

Windows 10 has built-in disk encryption methods to encrypt hard drives and safeguard user data. By default, disk encryption is enabled in all devices using Windows 10.
A security professional must have a required knowledge to implement disk encryption using Windows built-in encryption techniques to safeguard important data.

OBJECTIVE

This lab will demonstrate how to perform system-level encryption on Windows using the following:

- File encryption with EFS using Command Prompt
- Enable EFS using advanced attributes in a selected file/folder

OVERVIEW OF ENCRYPTING FILE SYSTEM (EFS)

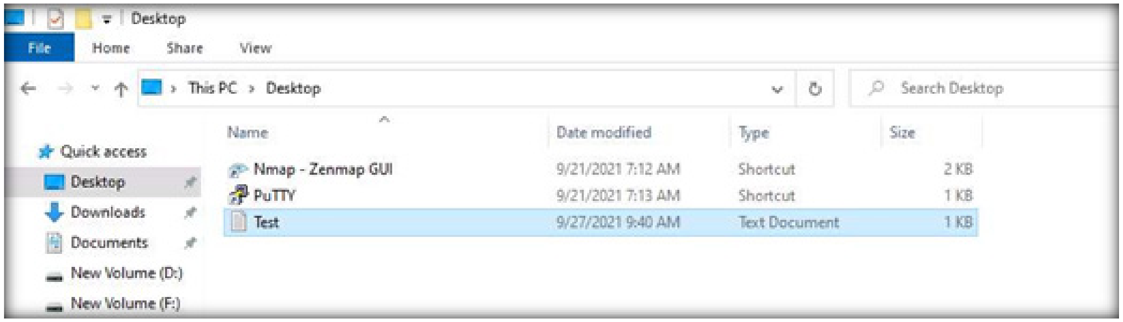
The user needs to enable EFS on a specific file, directory, or drive. This feature protects the confidential information from unauthorized users who have physical access to a computer.

EXERCISE 3: IMPLEMENT BUILT-IN FILE SYSTEM-LEVEL ENCRYPTION ON WINDOWS

Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, we will firstly create a sample text file named as Test at the location C:\Users\Admin\Desktop. After creating a Test.txt file, enter some random text inside the file.

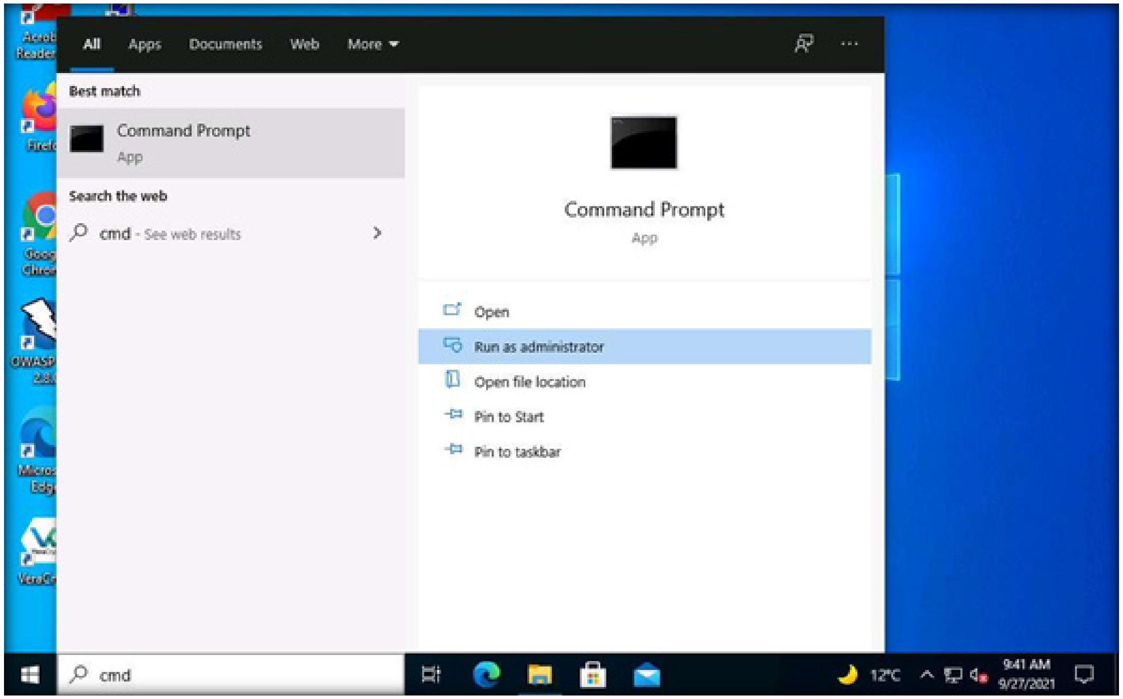
2. The created Test.txt file at location C:\Users\Admin\Desktop is shown in the screenshot below.



Name	Date modified	Type	Size
Nmap - Zenmap GUI	9/21/2021 7:12 AM	Shortcut	2 KB
PuTTY	9/21/2021 7:13 AM	Shortcut	1 KB
Test	9/27/2021 9:40 AM	Text Document	1 KB

3. Minimize the File Explorer window.

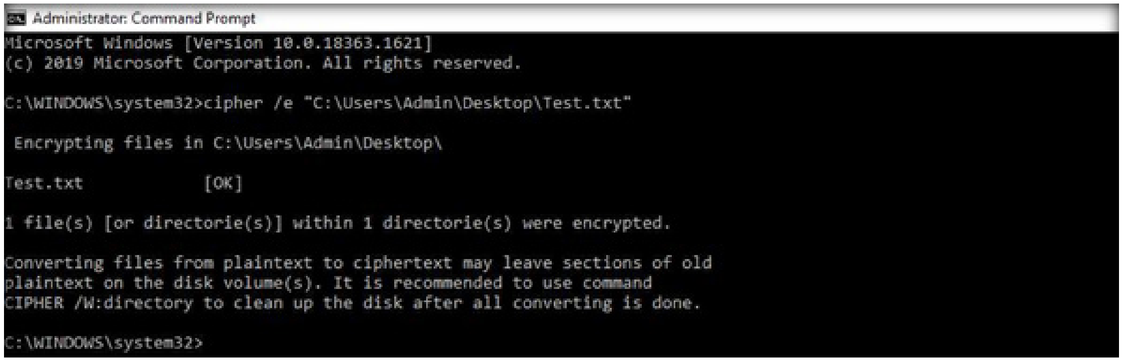
4. Now, click the Type here to search field present at the bottom-left corner of Desktop and type cmd. Command Prompt appears in the search results, from the right-pane, select Run as administrator option.



5. User Account Control window appears, click Yes to proceed.

6. Switch to the Command Prompt window. In the Command Prompt, type cipher /e “C:\Users\Admin\Desktop\Test.txt” and press Enter.
Note: /e: Specifies encryption of a file or a directory.
Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

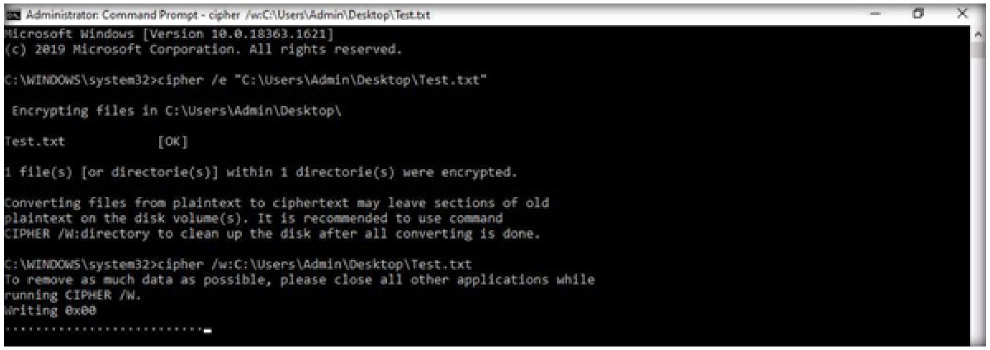
7. The text file has been encrypted successfully, as shown in the screenshot below.



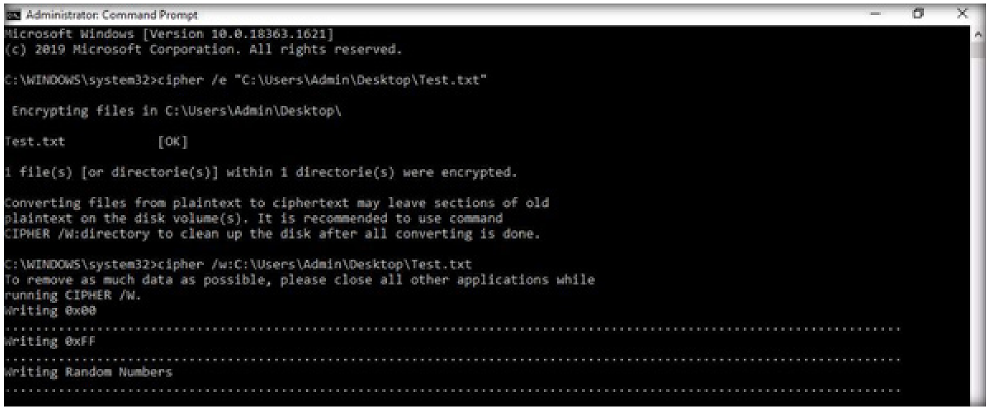
```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt"

 Encrypting files in C:\Users\Admin\Desktop\

Test.txt            [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\WINDOWS\system32>
```

8. Type cipher /w:C:\Users\Admin\Desktop\Test.txt and press Enter.
Note: As stated in the result of previous command, encrypting plaintext files might leave certain portions of old plaintext on the disk volume(s). Therefore, it is recommended to use cipher /w:directory command to clean up the disk after conversion is complete.

9. The Cipher.exe utility starts overwriting the files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot below.
Note: It takes approximately 5 minutes for the encryption to finish.

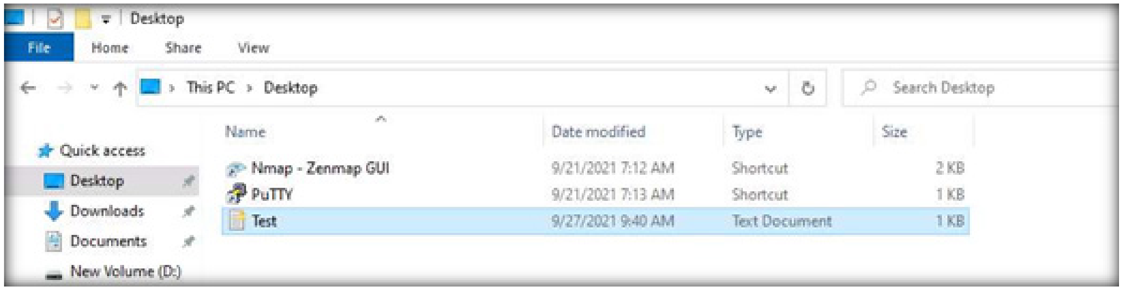

Administrator: Command Prompt - cipher /w:C:\Users\Admin\Desktop\Test.txt

```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt"

 Encrypting files in C:\Users\Admin\Desktop\

Test.txt            [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\WINDOWS\system32>cipher /w:C:\Users\Admin\Desktop\Test.txt
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
..........................
```



```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher /e "C:\Users\Admin\Desktop\Test.txt"

 Encrypting files in C:\Users\Admin\Desktop\

Test.txt            [OK]

1 file(s) [or directorie(s)] within 1 directorie(s) were encrypted.

Converting files from plaintext to ciphertext may leave sections of old
plaintext on the disk volume(s). It is recommended to use command
CIPHER /W:directory to clean up the disk after all converting is done.

C:\WINDOWS\system32>cipher /w:C:\Users\Admin\Desktop\Test.txt
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
.........................................................................................................................
Writing 0xFF
.........................................................................................................................
Writing Random Numbers
.........................................................................................................................
```

10. You can navigate back to the location C:\Users\Admin\Desktop to observe that the text file has been encrypted.

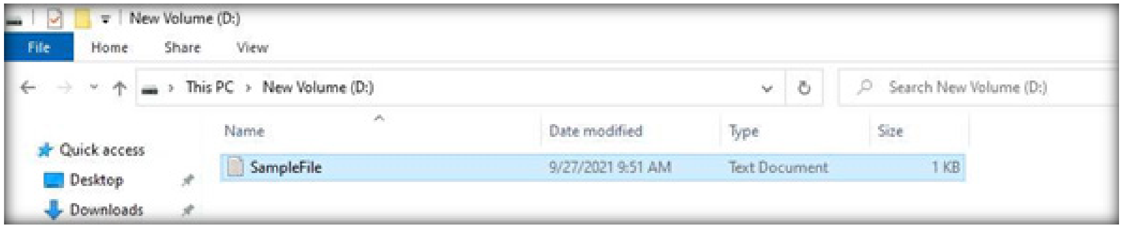


Name	Date modified	Type	Size
Nmap - Zenmap GUI	9/21/2021 7:12 AM	Shortcut	2 KB
PuTTY	9/21/2021 7:13 AM	Shortcut	1 KB
Test	9/27/2021 9:40 AM	Text Document	1 KB

11. Close the Command Prompt window.

12. Now, we will enable EFS using advanced attributes in a selected file/folder. To do so, we will create another text file named as SampleFile in D:\ directory. After creating a SampleFile.txt file, enter some random text inside the file.

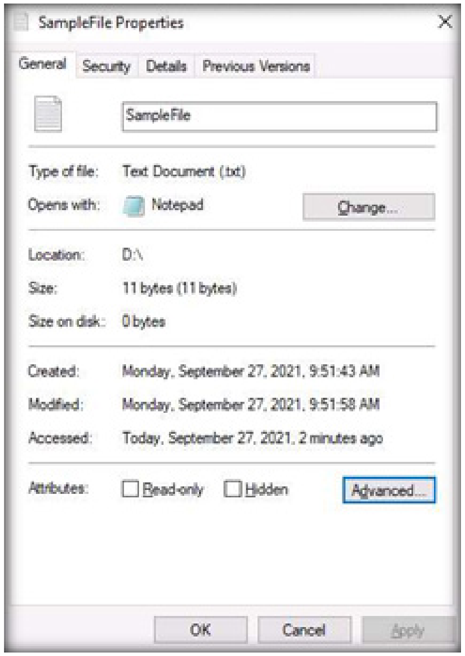
13. The created SampleFile.txt file at location D:\ is shown in the screenshot below.



Name	Date modified	Type	Size
SampleFile	9/27/2021 9:51 AM	Text Document	1 KB

14. Click to select the text file (SampleFile), right-click on it and select Properties from the options.

15. SampleFile Properties window appears, click Advanced button.



SampleFile Properties

SampleFile

Type of file: Text Document (.txt)

Opens with: Notepad

Location: D:\

Size: 11 bytes (11 bytes)

Size on disk: 0 bytes

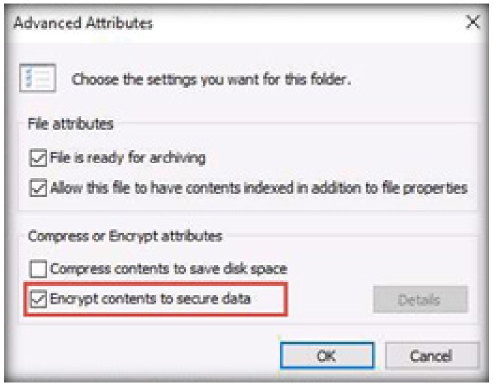
Created: Monday, September 27, 2021, 9:51:43 AM

Modified: Monday, September 27, 2021, 9:51:58 AM

Accessed: Today, September 27, 2021, 2 minutes ago

Attributes: □ Read-only □ Hidden

16. Advanced Attributes window appears, select Encrypt contents to secure data checkbox under Compress or Encrypt attributes section and click OK.



Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

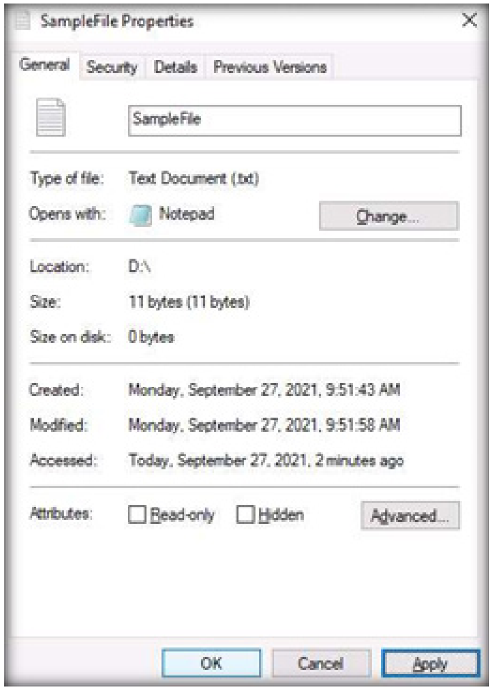
☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

17. In the SampleFile Properties window, click Apply and OK.



SampleFile Properties

General | Security | Details | Previous Versions

SampleFile

Type of file: Text Document (.txt)

Opens with: Notepad

Location: D:\

Size: 11 bytes (11 bytes)

Size on disk: 0 bytes

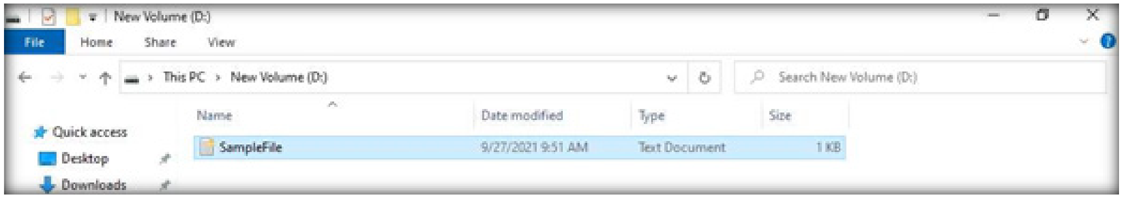
Created: Monday, September 27, 2021, 9:51:43 AM

Modified: Monday, September 27, 2021, 9:51:58 AM

Accessed: Today, September 27, 2021, 2 minutes ago

Attributes: □ Read-only □ Hidden

18. You can observe that the selected file has been encrypted, as shown in the screenshot below.



Name	Date modified	Type	Size
SampleFile	9/27/2021 9:51 AM	Text Document	1 KB

EXERCISE 3: IMPLEMENT BUILT-IN FILE SYSTEM-LEVEL ENCRYPTION ON WINDOWS

19. This concludes the demonstration showing how to encrypt files using built-in file system-level encryption in Windows.

20. Close all open windows.

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

Data backup is the process of copying or storing important data.

LAB SCENARIO

Data loss is a major risk that organizations face today. Loss of critical data can result in considerable damage to the organization. Any organization that encounters a critical data loss has a higher probability of facing serious issues later. Therefore, a strong data backup and retention plan is a must to deal with such incidents.

A security professional must have a required knowledge to perform a data backup on a regular schedule to avoid severe damage to an organization's assets and to run their business successfully and efficiently.

OBJECTIVE

This lab will demonstrate how to perform data backup using tools such as Genie Backup Manager.

OVERVIEW OF DATA BACKUP

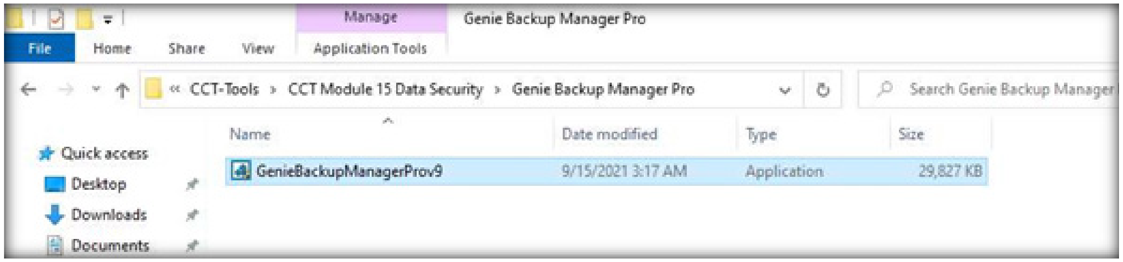
A data backup helps restore the original data when data is lost or corrupted. Backup is a mandatory process for all organizations. The process of retrieving lost files from a backup is known as restoring or recovery of files.

The main idea behind data backup is to protect data and information and recover the same after data loss. Data backup is mainly used for two purposes: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption.

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, open File Explorer and navigate to Z:\CCT-Tools\CCT Module 15 Data Security\Genie Backup Manager Pro. Double-click GenieBackupManagerProv9.exe.

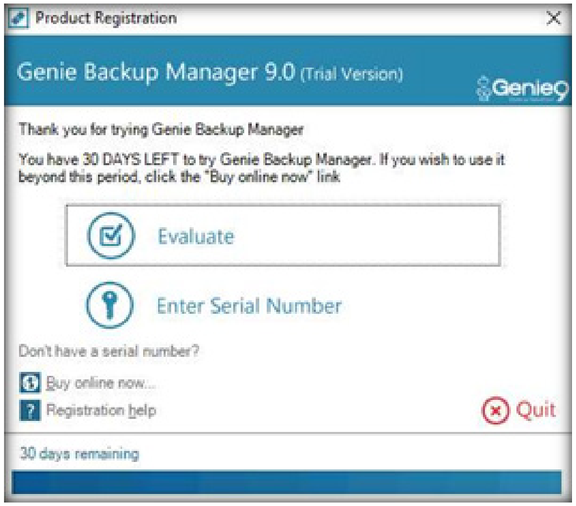


2. The User Account Control pop-up appears. Click Yes.

3. Installer Language pop-up appears, leave the language set to default (English) and click OK.

4. In the next window, click Next and follow the wizard driven installation to install the tool using default settings.

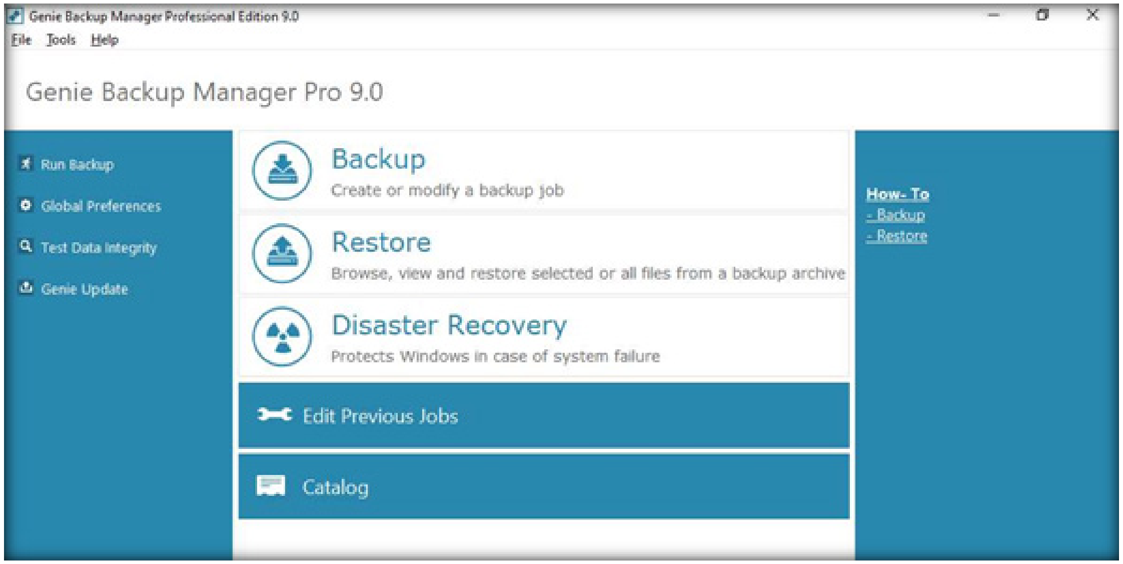
5. After the installation completes, Product Registration window appears. Select Evaluate.



Thank you for trying Genie Backup Manager

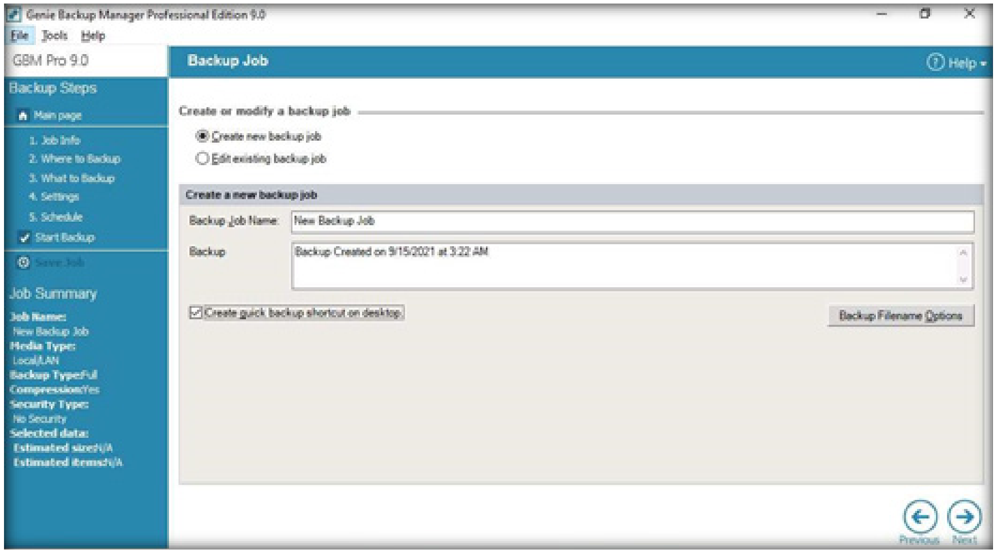
You have 30 DAYS LEFT to try Genie Backup Manager. If you wish to use it beyond this period, click the "Buy online now" link

6. Genie Backup Manager main window appears, select Backup option.


Genie Backup Manager Professional Edition 9.0
File Tools Help
Genie Backup Manager Pro 9.0
Run Backup
Global Preferences
Test Data Integrity
Genie Update
Backup
Create or modify a backup job
Restore
Browse, view and restore selected or all files from a backup archive
Disaster Recovery
Protects Windows in case of system failure
Edit Previous Jobs
Catalog
How- To
- Backup
- Restore

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

7. Backup Job wizard appears, leave all the settings as default, and select Create quick backup shortcut on desktop checkbox. Click Next.



Create or modify a backup job

● Create new backup job

○ Edit existing backup job

Create a new backup job

Backup Job Name: New Backup Job

Backup: Backup Created on 9/15/2021 at 3:22 AM

☑ Create quick backup shortcut on desktop

Job Summary

Job Name: New Backup Job

Media Type: Local/LAN

Backup Type:Full

Compression:Yes

Security Type: No Security

Selected data:

Estimated size:N/A

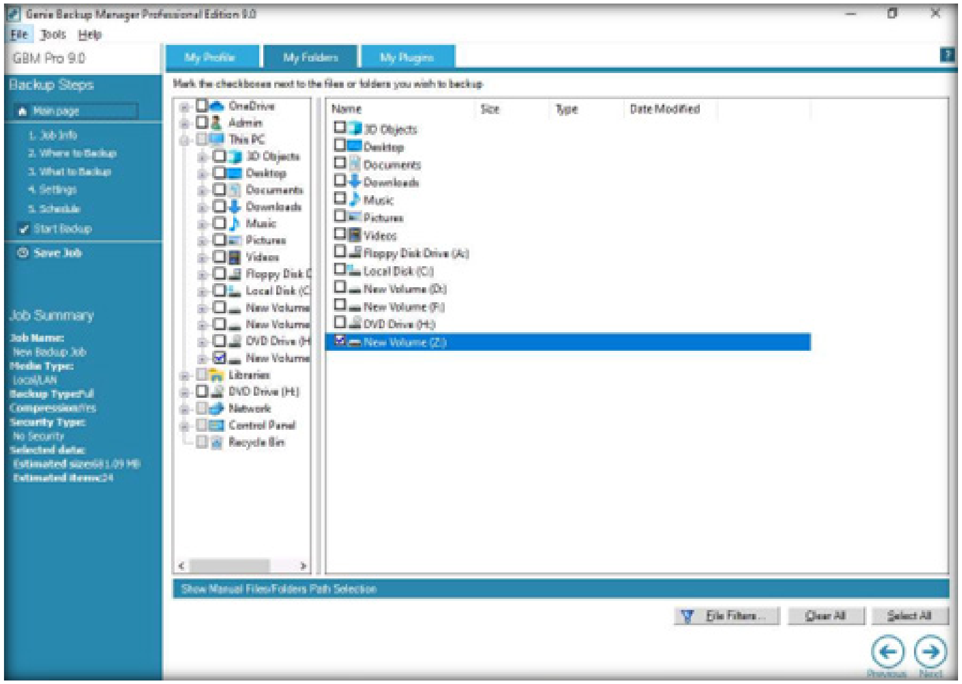
Estimated items:N/A

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

8. Where to backup wizard appears, leave all the settings as default, and click Next.

9. Here, you can select different backup media such as Local/LAN location, Removable media devices, Remote location using FTP/FTPS, CD/DVD/Blu-ray media and Amazon S3. In this lab task, we select Local/LAN location as default option for backup media.

10. Backup item selection wizard appears, navigate to My Folders tab and from the list, select New Volume (Z:) checkbox from the left-pane. Click Next.
Note: You can select an item or a folder of your choice for a data backup.

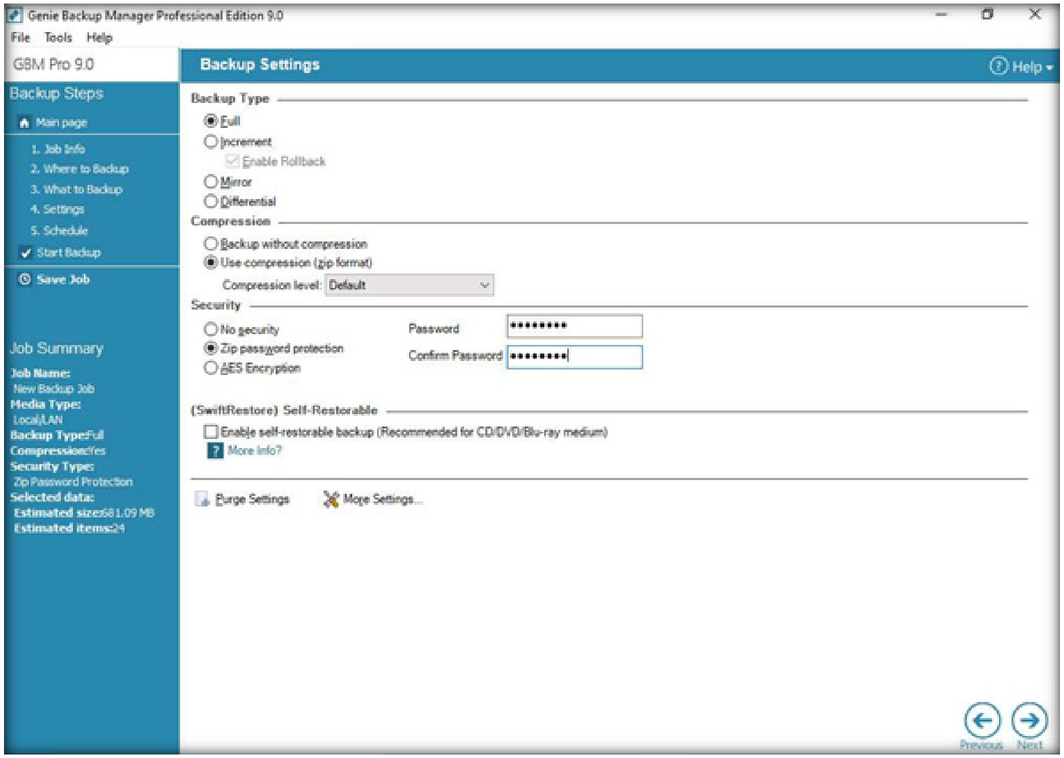


Mark the checkboxes next to the files or folders you wish to backup

Job Summary
Job Name:
New Backup Job
Media Type:
Local/LAN
Backup Type:Full
Compression:Yes
Security Type:
No Security
Selected data:
Estimated size:681.09 MB
Estimated items:24

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

11. Backup Settings wizard appears, leave all the settings as default. Under the Security section, select Zip password protection radio-button and enter test@123 in both Password and Confirm Password field. Click Next.



Backup Settings

Backup Type
● Full
○ Increment
☑ Enable Rollback
○ Mirror
○ Differential

Compression
○ Backup without compression
● Use compression (zip format)
Compression level: Default

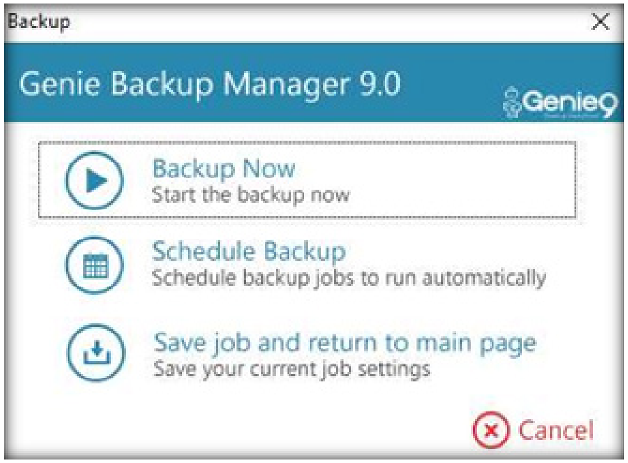
Security
○ No security
● Zip password protection
○ AES Encryption
Password: •••••••••
Confirm Password: •••••••••

(SwiftRestore) Self-Restorable
□ Enable self-restorable backup (Recommended for CD/DVD/Blu-ray medium)

Job Summary
Job Name:
New Backup Job
Media Type:
Local/LAN
Backup Type:Full
Compression:Yes
Security Type:
Zip Password Protection
Selected data:
Estimated size:681.09 MB
Estimated items:24

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

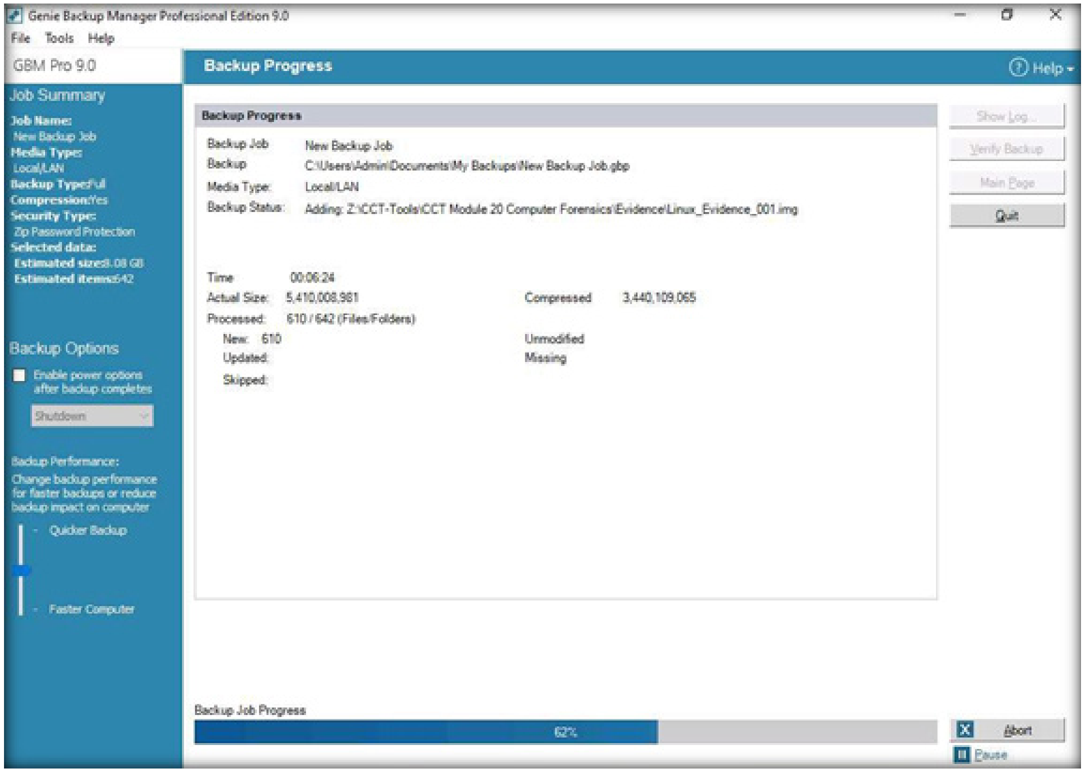
12. Backup pop-up appears, select Backup Now option.


Backup
Genie Backup Manager 9.0
Genie9
Backup Now
Start the backup now
Schedule Backup
Schedule backup jobs to run automatically
Save job and return to main page
Save your current job settings
Cancel

13. Confirming Data Selections pop-up appears after which the countdown backup process begins.

14. Backup Progress wizard appears, observe the status bar at the lower section of the window. Wait for it to finish.

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER



Job Summary
Job Name:
New Backup Job
Media Type:
Local/LAN
Backup Type:Full
Compression:Yes
Security Type:
Zip Password Protection
Selected data:
Estimated size:8.08 GB
Estimated items:642

Backup Options
□ Enable power options after backup completes
Shutdown

Backup Performance:
Change backup performance for faster backups or reduce backup impact on computer
Quicker Backup
Faster Computer

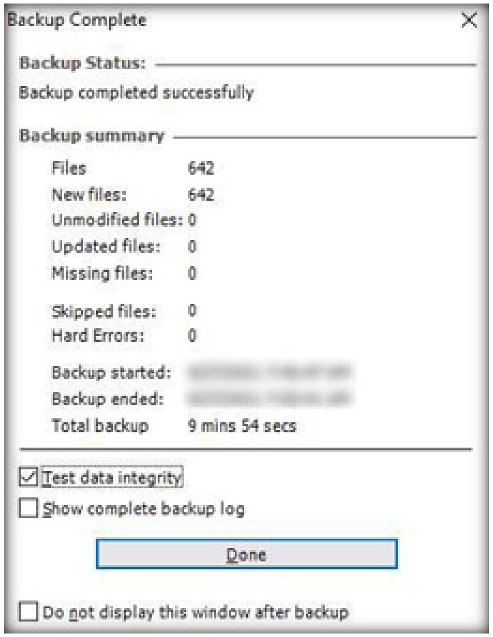
Backup Progress

Backup Job New Backup Job
Backup C:\Users\Admin\Documents\My Backups\New Backup Job.gbp
Media Type: Local/LAN
Backup Status: Adding: Z:\CCT-Tools\CCT Module 20 Computer Forensics\Evidence\Linux_Evidence_001.img

Time 00:06:24
Actual Size: 5,410,008,981 Compressed 3,440,109,065
Processed: 610 / 642 (Files/Folders)
New: 610 Unmodified
Updated: Missing
Skipped:

Backup Job Progress
62%

15. After the backup process is finished, Backup Complete notification appears, displaying Backup Status and Backup summary. Ensure that Test data integrity checkbox is selected and click Done button.



Backup Complete

Backup Status:

Backup completed successfully

Backup summary

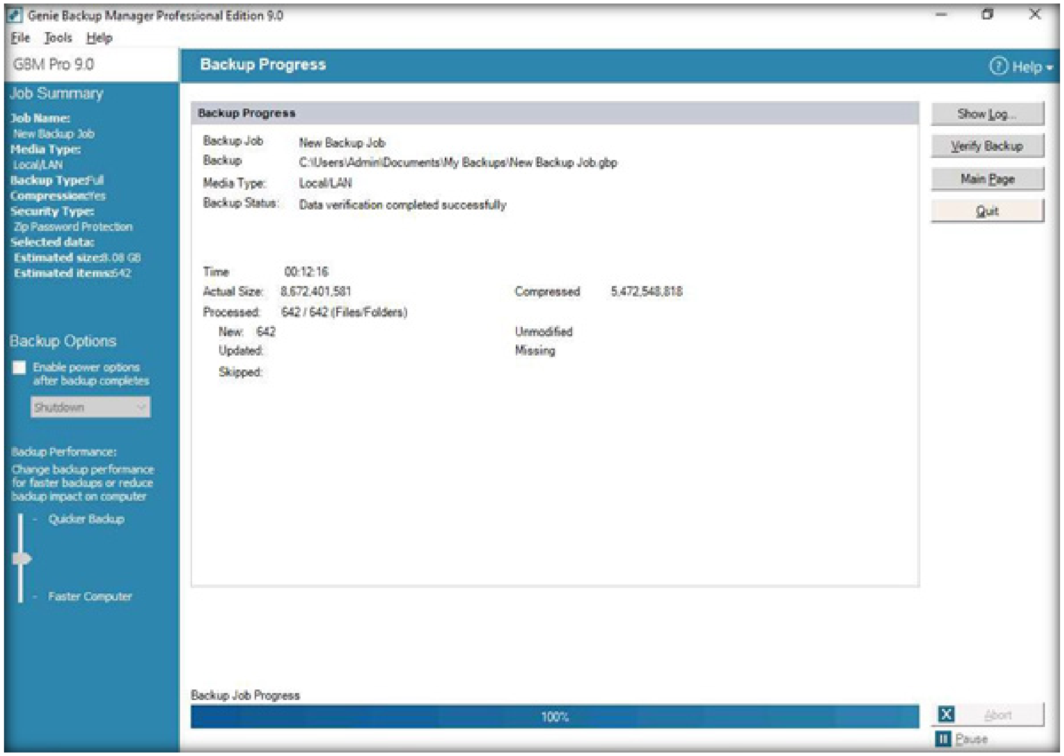
Files	642
New files:	642
Unmodified files:	0
Updated files:	0
Missing files:	0
Skipped files:	0
Hard Errors:	0
Backup started:	[redacted]
Backup ended:	[redacted]
Total backup	9 mins 54 secs

☑ Test data integrity

☐ Show complete backup log

☐ Do not display this window after backup

16. Data verification process initializes. After the completion of data verification process, click Quit button from the right-pane.



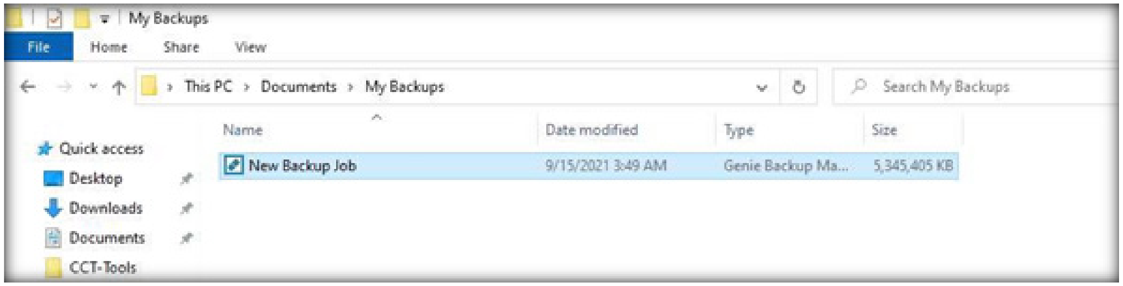
```
Job Summary
Job Name:
 New Backup Job
Media Type:
 Local/LAN
Backup Type:Full
Compression:Yes
Security Type:
 Zip Password Protection
Selected data:
 Estimated size:8.08 GB
 Estimated items:642

Backup Options
□ Enable power options
  after backup completes
  Shutdown

Backup Performance:
Change backup performance
for faster backups or reduce
backup impact on computer
 - Quicker Backup
 - Faster Computer
```

```
Backup Progress
Backup Job      New Backup Job
Backup          C:\Users\Admin\Documents\My Backups\New Backup Job.gbp
Media Type:     Local/LAN
Backup Status:  Data verification completed successfully

Time         00:12:16
Actual Size: 8,672,401,581                      Compressed     5,472,548,818
Processed:   642 / 642 (Files/Folders)
   New:   642                                   Unmodified
   Updated:                                     Missing
   Skipped:

Backup Job Progress
100%
```

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

17. In Quit GBM window, click Quit button.

18. Switch to the File Explorer window and navigate to the location C:\Users\Admin\Documents\My Backups. You can observe that a backup file named as New Backup Job, has been created.
Note: A shortcut file of the backup has also been created on the Desktop.

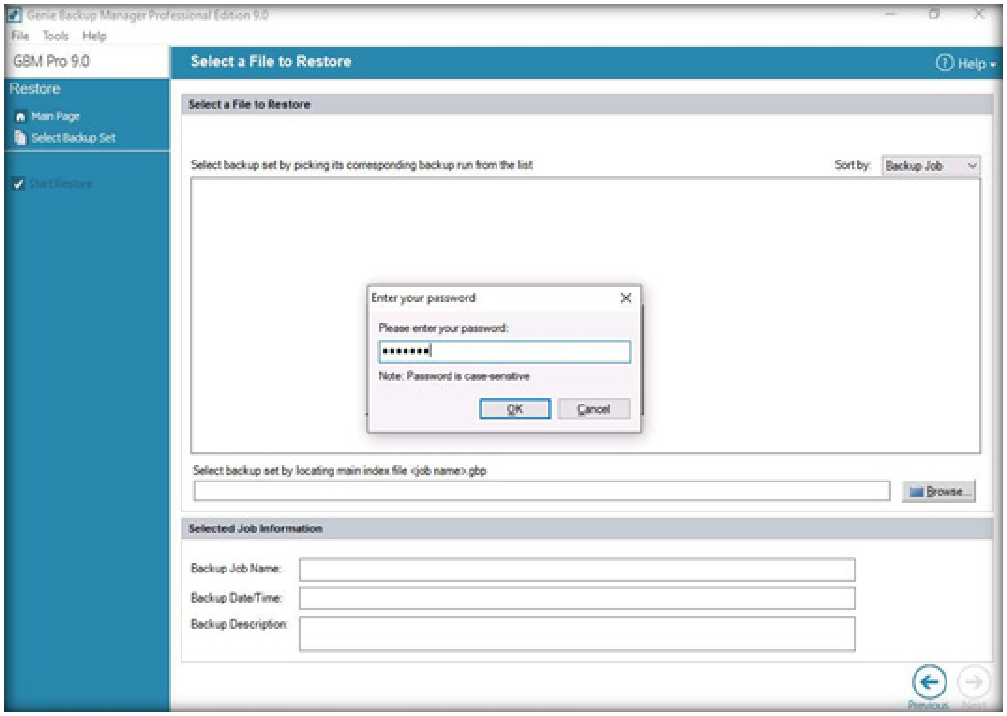


Name	Date modified	Type	Size
New Backup Job	9/15/2021 3:49 AM	Genie Backup Ma...	5,345,405 KB

19. Now, we will learn how to restore a deleted folder from the backup media file.

20. Double-click on the file New Backup Job. In the User Account Control pop-up, click Yes.

21. Genie Backup Manager window appears, along with Enter your password pop-up. Enter test@123 as the password and click OK.



Select a File to Restore

Select backup set by picking its corresponding backup run from the list

Sort by: Backup Job

Enter your password

Please enter your password:

••••••••

Note: Password is case-sensitive

OK Cancel

Select backup set by locating main index file <job name>.gbp

Selected Job Information

Backup Job Name:

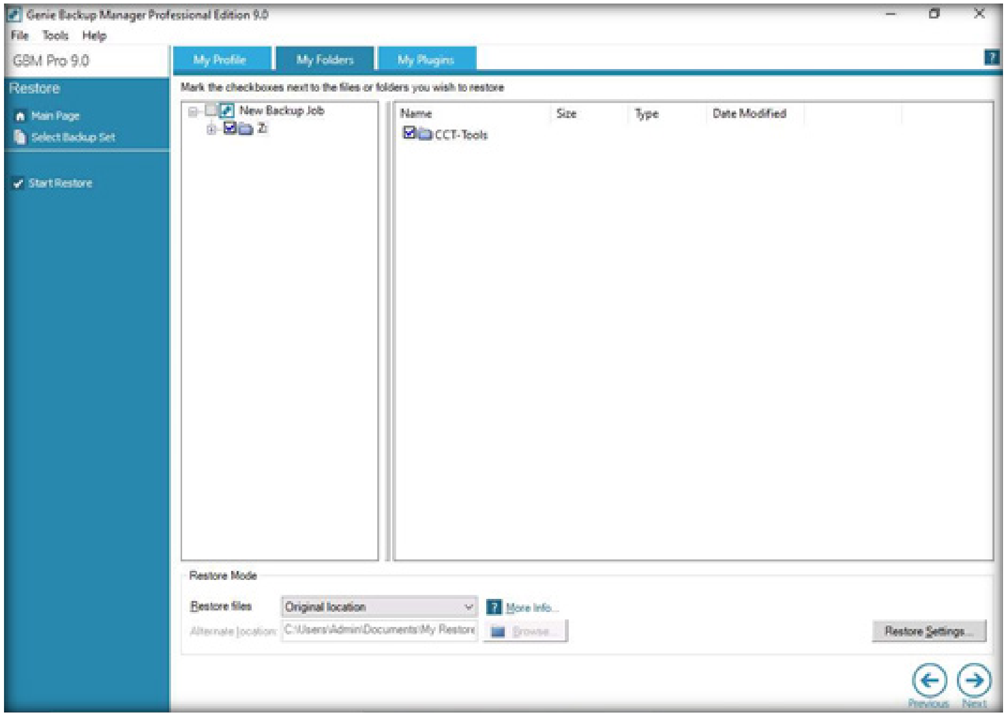
Backup Date/Time:

Backup Description:

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER

22. In the Select a File to Restore wizard, click Next.

23. My Folders tab appears, select Z: drive checkbox from the left-pane and click Next.



Mark the checkboxes next to the files or folders you wish to restore

- ☐ New Backup Job
  - ☑ Z:

☑ CCT-Tools

Restore Mode

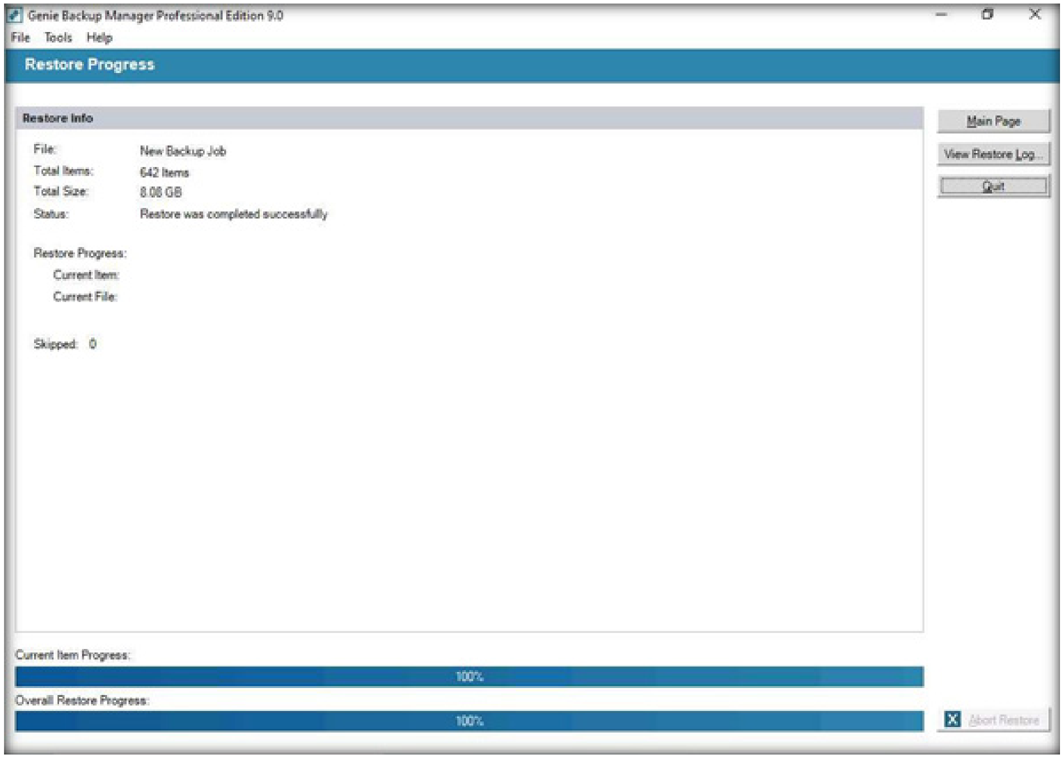
Restore files: Original location

Alternate location: C:\Users\Admin\Documents\My Restore

24. Restore Confirmation pop-up appears, click Restore Now.

25. After the restoration process completes, click Quit button from the right-pane.

EXERCISE 4: PERFORM DATA BACKUP USING GENIE BACKUP MANAGER



File: New Backup Job
Total Items: 642 Items
Total Size: 8.08 GB
Status: Restore was completed successfully

Restore Progress:
Current Item:
Current File:

Skipped: 0

Current Item Progress: 100%
Overall Restore Progress: 100%

26. In Quit GBM window, click Quit button.

27. Here, we have restored the backup file at the original location (Z:), however you can restore it at the location of your choice.

28. This concludes the demonstration showing how to perform data backups using Genie Backup Manager Pro tool.

29. Close all open windows.

EXERCISE 5: **FILE RECOVERY USING EASEUS DATA RECOVERY WIZARD**

EaseUS Data Recovery Wizard is a recovery software for Windows that supports files, partitions, and the complete recovery of data.

LAB SCENARIO

A security professional should know how to recover deleted files and partitions, which have been deleted accidentally by users or due to a natural disaster. They can use recovery techniques or proprietary applications to obtain critical information.

OBJECTIVE

The objective of this lab is to demonstrate how to use EaseUS Data Recovery Wizard, by intentionally deleting a few files and, subsequently, recovering them.

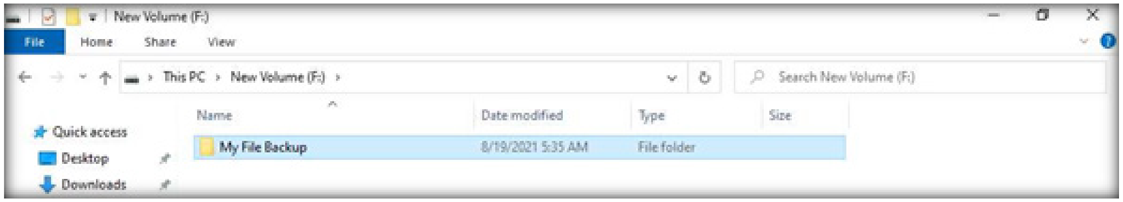
OVERVIEW OF RECOVERING DELETED FILES AND PARTITIONS

EaseUS Data Recovery Wizard solves all data loss problems; it recovers files emptied from the Recycle Bin or data loss due to a software crash, hard drive formatting or damage, virus attack, lost partition, and other unknown reasons in Windows. It recovers data from formatted partitions with the original file names and storage paths.

EXERCISE 5: FILE RECOVERY USING EASEUS DATA RECOVERY WIZARD

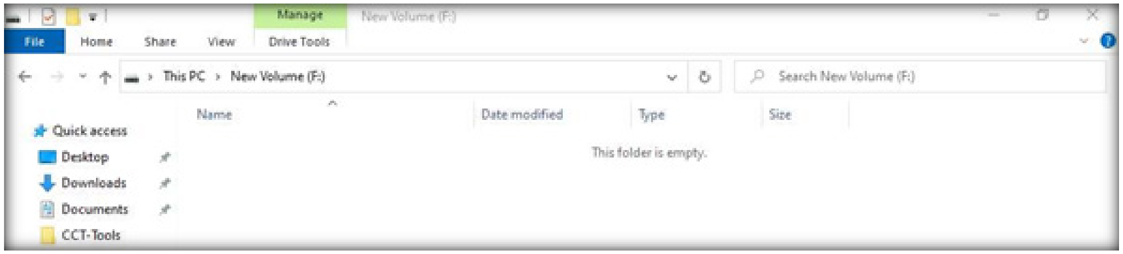
Note: Ensure that Admin Machine-1 and PfSense Firewall virtual machines are running.

1. In the Admin Machine-1 virtual machine, before running the tool, check for any available file (In this exercise, F:\My File Backup is used) to delete.
Note: If files or folders do not exist, create folders and documents under F:\ drive.



Name	Date modified	Type	Size
My File Backup	8/19/2021 5:35 AM	File folder	

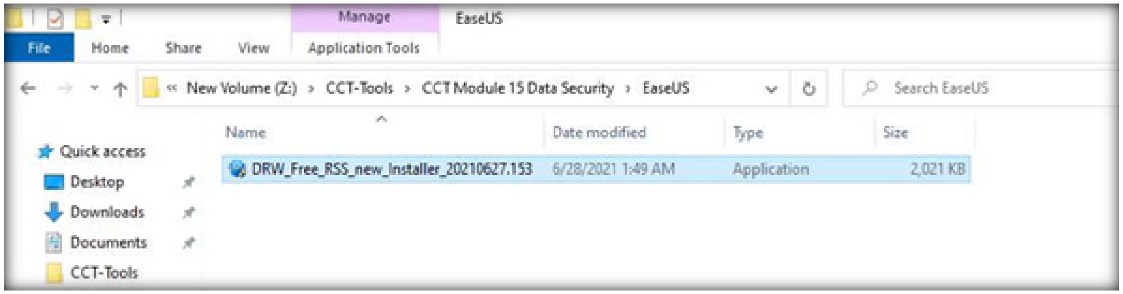
2. Delete the My File Backup folder. Here, we have performed an accidental deletion.



This folder is empty.

EXERCISE 5: FILE RECOVERY USING EASEUS DATA RECOVERY WIZARD

3. Navigate to Z:\CCT-Tools\CCT Module 15 Data Security\EaseUS. Double-click DRW_Free_RSS_new_Installer_20210627.153.exe.

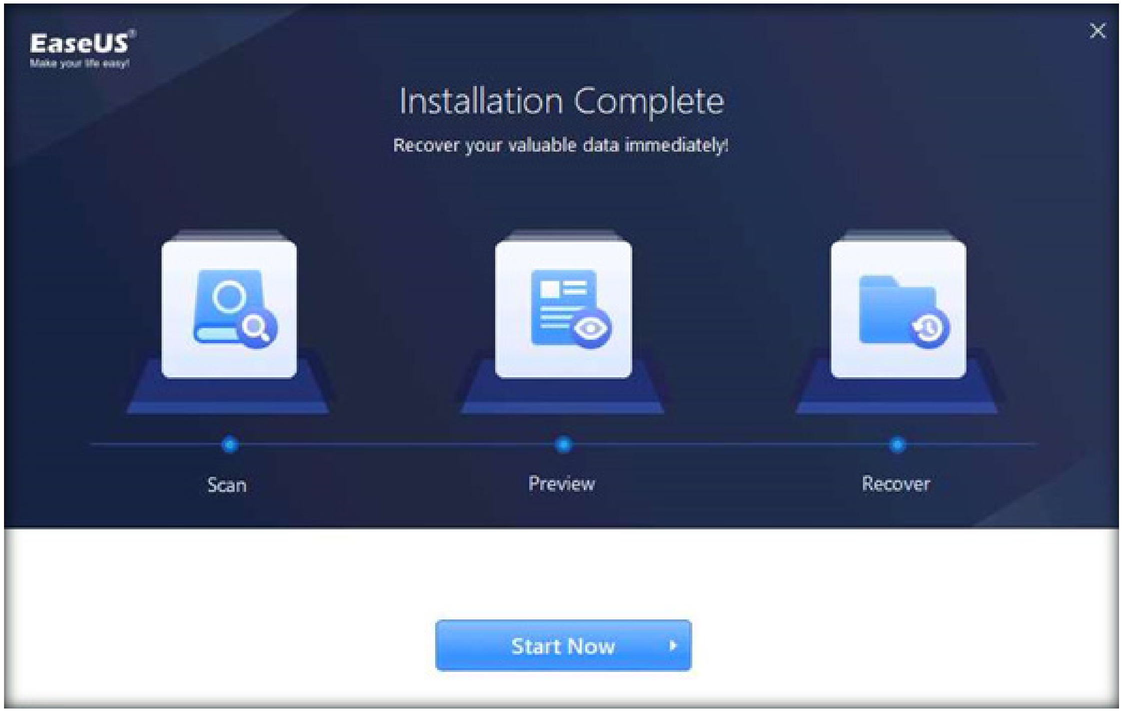


Name	Date modified	Type	Size
DRW_Free_RSS_new_Installer_20210627.153	6/28/2021 1:49 AM	Application	2,021 KB

4. The User Account Control pop-up appears. Click Yes.

5. The EaseUS Data Recovery Wizard Installer opens. Click Install Now.

6. Once the installation is complete Installation Complete wizard appears, click on Start Now.


EaseUS Make your life easy!

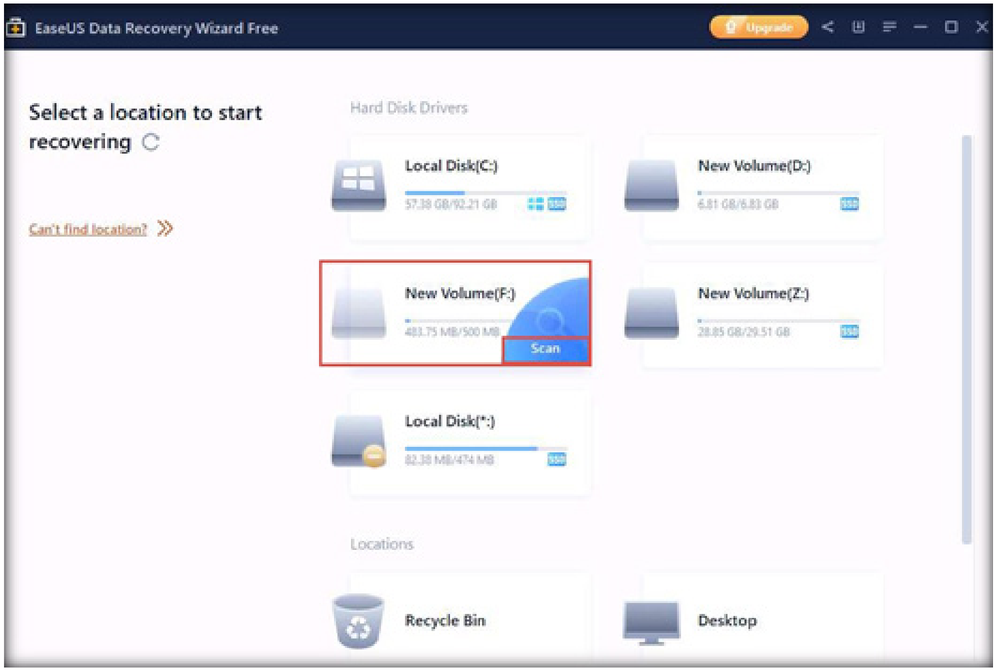
Installation Complete

Recover your valuable data immediately!

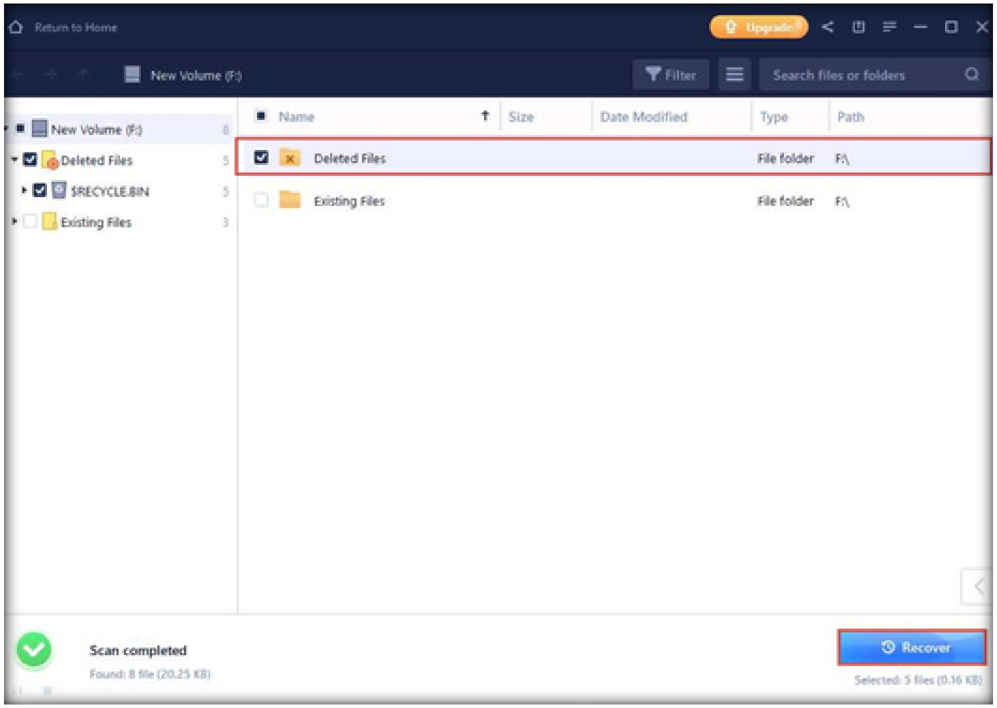
7. This action will open a browser. Close the opened browser.

8. The EaseUS Data Recovery Wizard Free window opens.
Note: If a EaseUS Data Recovery Wizard pop-up appears at the lower-right corner, close it.

9. Under Select a location to start recovering, select the partition from which you have to recover the files (F: drive). Click Scan.



10. Select the Deleted Files and click Recover.



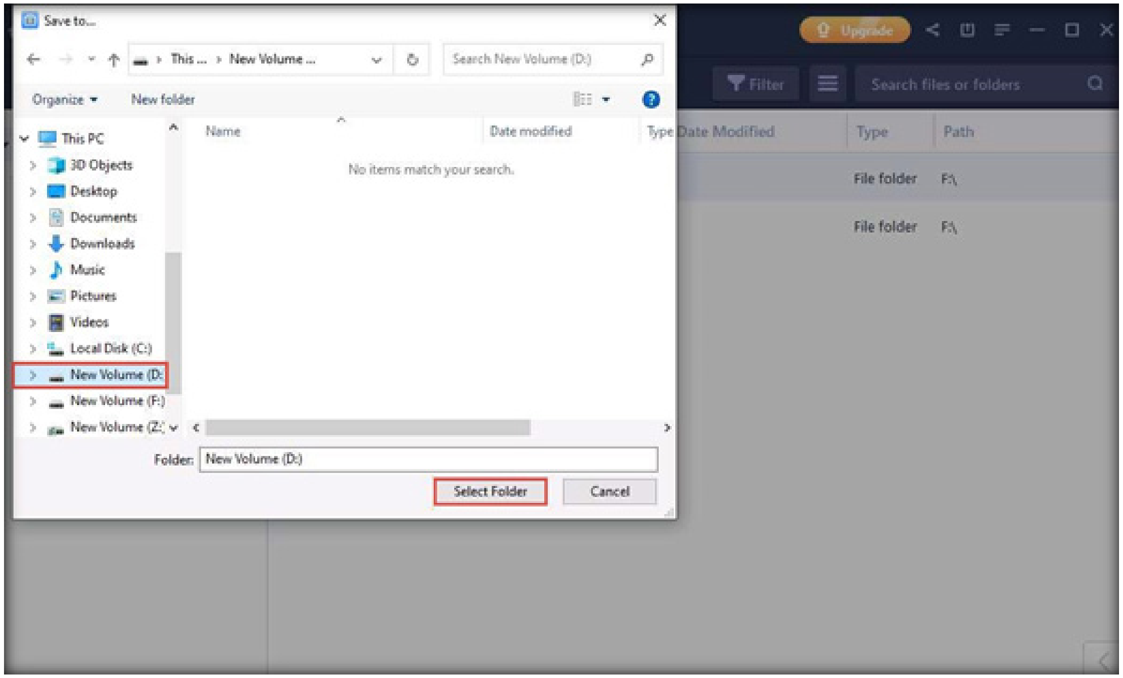
■	Name	Size	Date Modified	Type	Path
☑	Deleted Files			File folder	F:\
□	Existing Files			File folder	F:\

Scan completed

Found: 8 file (20.25 KB)

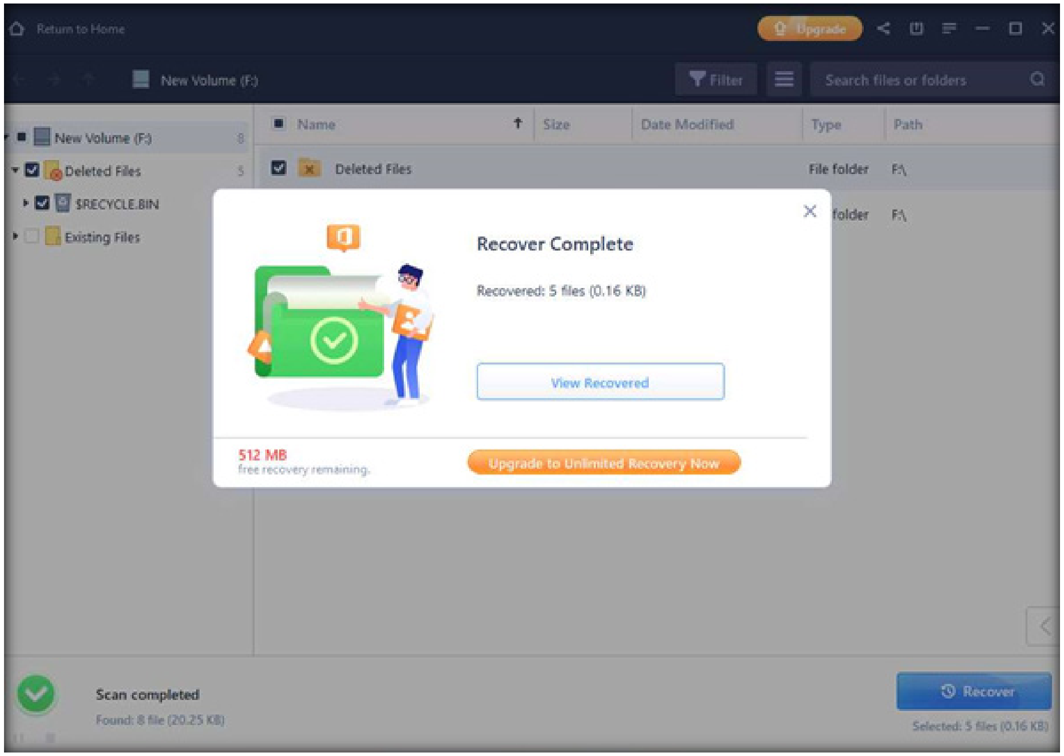
Selected: 5 files (0.16 KB)

11. Select a location to save the recovered files. Click Select Folder.



EXERCISE 5:
FILE RECOVERY
USING EASEUS
DATA RECOVERY
WIZARD

12. The files are saved. A recovery report will be displayed on the screen. You will be automatically redirected to the Recovery Data folder.



Name	Size	Date Modified	Type	Path
☑ Deleted Files			File folder	F:\
			folder	F:\

Recover Complete

Recovered: 5 files (0.16 KB)

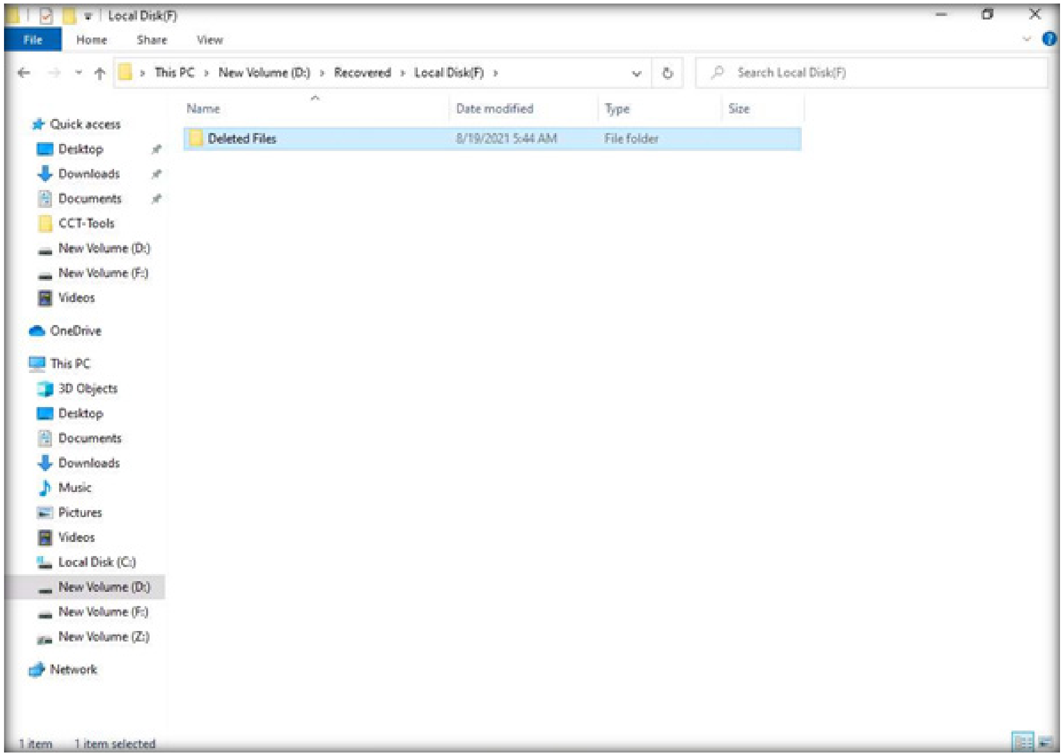
512 MB
free recovery remaining.

Scan completed
Found: 8 file (20.25 KB)

Selected: 5 files (0.16 KB)

EXERCISE 5:
FILE RECOVERY
USING EASEUS
DATA RECOVERY
WIZARD

13. Navigate to the location in which you have saved the recovered files. (This location usually appears automatically along with the new technology file system (NTFS) folder after the recovery).



Name	Date modified	Type	Size
Deleted Files	8/19/2021 5:44 AM	File folder	

14. This concludes the demonstration showing how to recovery file using EaseUS Data Recovery Wizard.

15. Close all open windows.

16. Turn off the Admin Machine-1 virtual machine.

EXERCISE 6: **BACK UP AND RESTORE DATA IN WINDOWS**

Data backup is the process of copying or storing important data.

LAB SCENARIO

A security professional should know how to recover deleted files and folders, which have been deleted accidentally by users or due to a natural disaster. They can use recovery techniques or proprietary applications to obtain sensitive and confidential information.

OBJECTIVE

The objective of this lab is to demonstrate how to backup crucial data on a Windows Server machine and using remote servers to store backup data which helps the organization in restoring the data in case of hard drive failure on the main server.

OVERVIEW OF BACK UP AND RESTORATION

For any organization it is important to perform data back up and in any circumstances if the data is lost then they must have the required procedure to restore it from the archives. Sometimes, the information is not useful at the moment, and need to be archived. The archived data can be later used for regulatory reasons. The archival policies minimize the amount of data the information systems can manage and allows secure retention. The data can be restored from archives when it is required.

EXERCISE 6: BACK UP AND RESTORE DATA IN WINDOWS

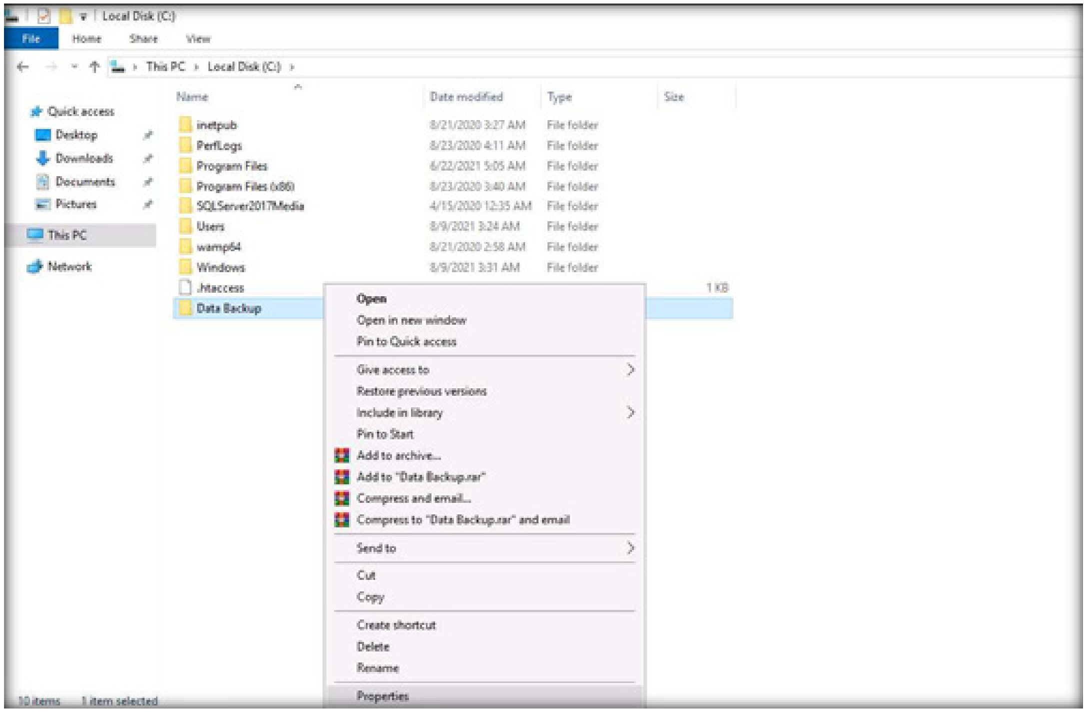
Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on AD Domain Controller and Web Server virtual machines.

2. Switch to AD Domain Controller and log in with the credentials CCT\Administrator and admin@123.
Note: The network screen appears, click Yes.

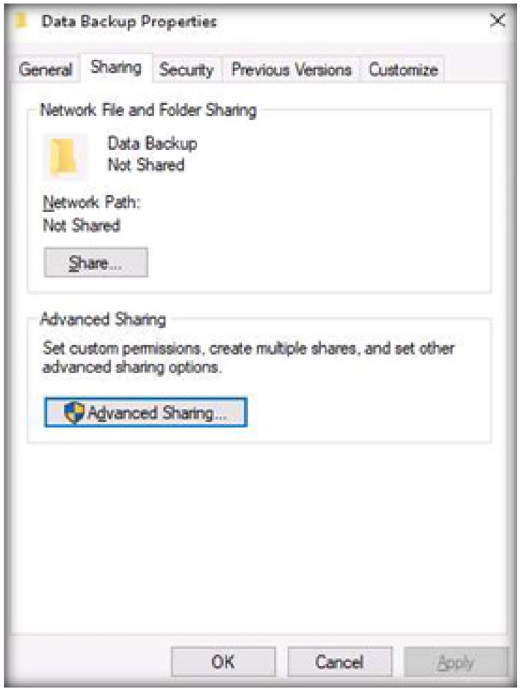
3. Open File Explorer and navigate to C: drive. Create a new folder and name it as Data Backup.

4. Now, we will share this folder (Data Backup). To do so, right-click the folder, select Properties.

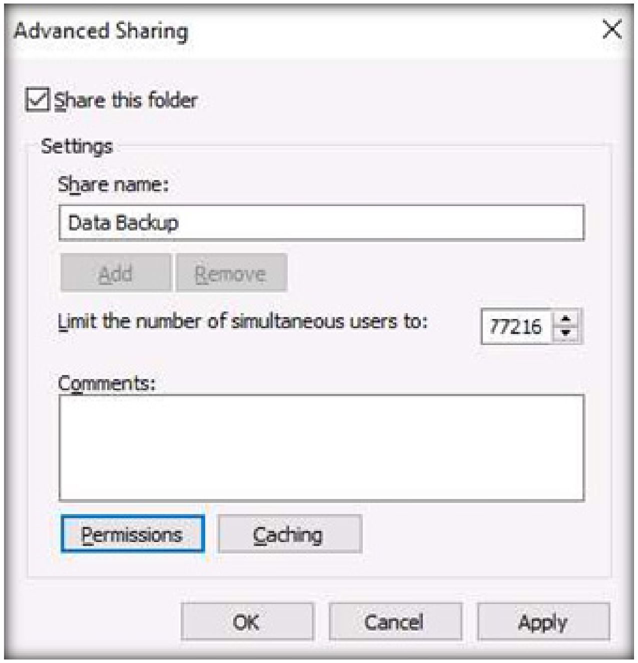


Name	Date modified	Type	Size
inetpub	8/21/2020 3:27 AM	File folder	
PerfLogs	8/23/2020 4:11 AM	File folder	
Program Files	6/22/2021 5:05 AM	File folder	
Program Files (x86)	8/23/2020 3:40 AM	File folder	
SQLServer2017Media	4/15/2020 12:35 AM	File folder	
Users	8/9/2021 3:24 AM	File folder	
wamp64	8/21/2020 2:58 AM	File folder	
Windows	8/9/2021 3:31 AM	File folder	
.htaccess			1 KB
Data Backup			

5. Data Backup Properties window appears, navigate to the Sharing tab, and select Advanced Sharing.



6. Check Share this Folder checkbox and click Permissions.



Advanced Sharing

☑ Share this folder

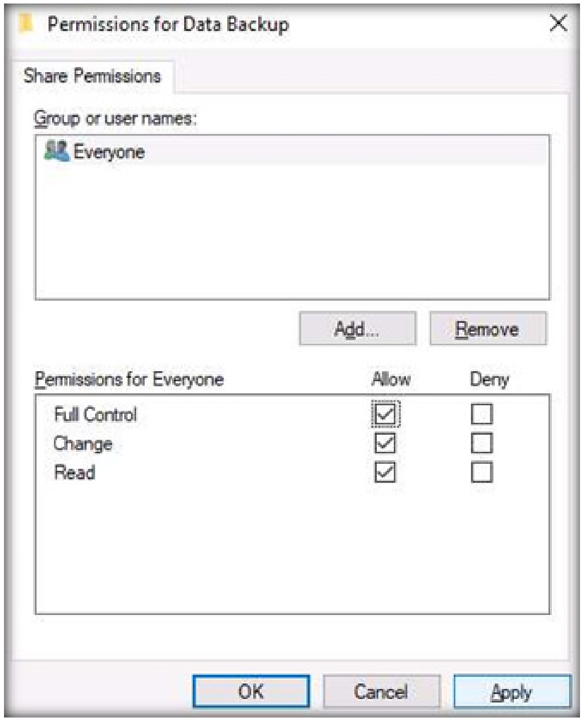
Settings

Share name: Data Backup

Limit the number of simultaneous users to: 77216

Comments:

7. In Permissions for Data Backup window, check Full Control checkbox to give full control to Everyone. Click Apply and OK.



Permissions for Data Backup

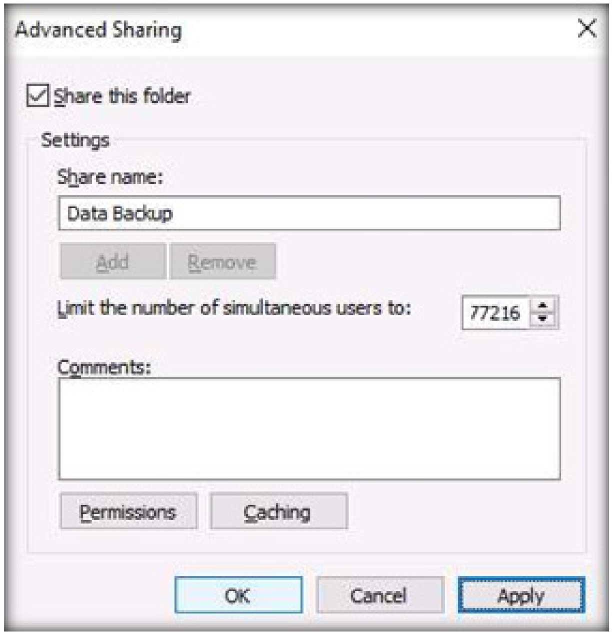
Share Permissions

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

8. In Advanced Sharing window, click Apply and OK.



☑ Share this folder

Settings

Share name: Data Backup

Limit the number of simultaneous users to: 77216

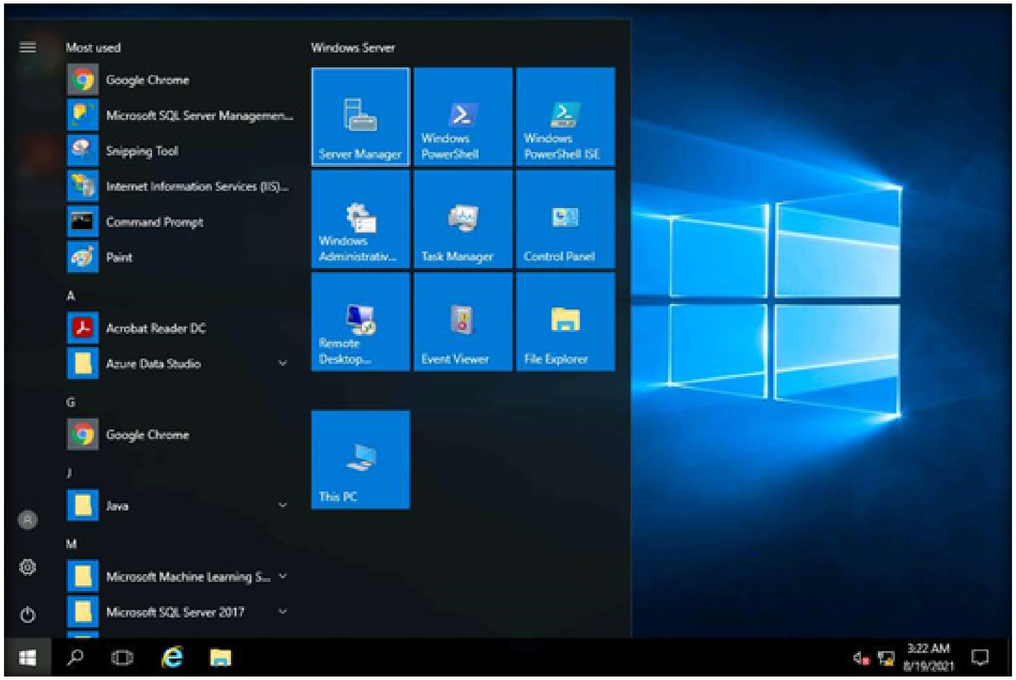
Comments:

9. Close the Data Backup Properties window.

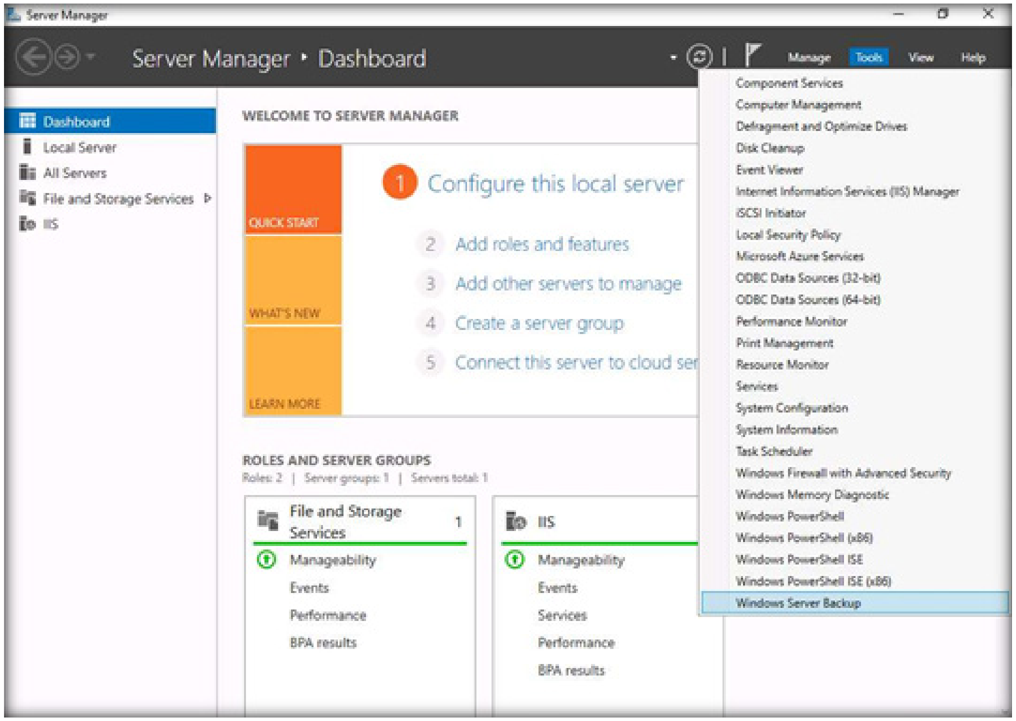
10. Switch to the Web Server virtual machine.

11. Log in with the credentials Administrator and admin@123.
Note: The network screen appears, click Yes.

12. Click Start icon on the Desktop and click Server Manager.

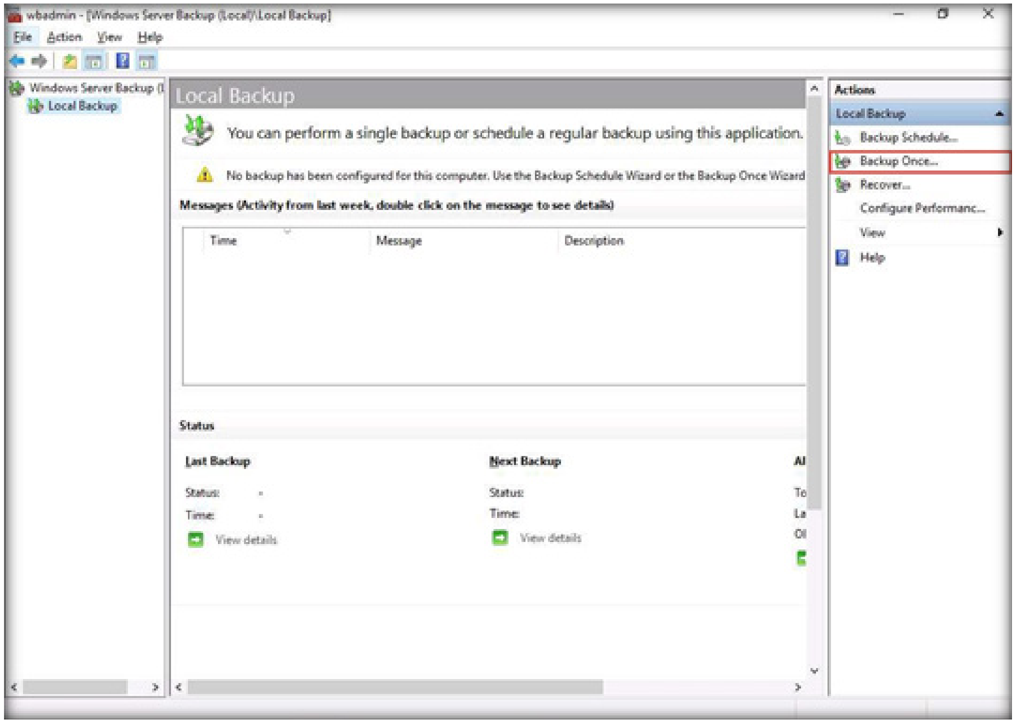


13. In the Server Manager window, click Tools and select Windows Server Backup.



14. A wbadmin window appears, click Local Backup node from the left-pane.

15. In the right-pane under Actions section, click Backup Once... option.



wbadmin - [Windows Server Backup (Local)\Local Backup]

Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description

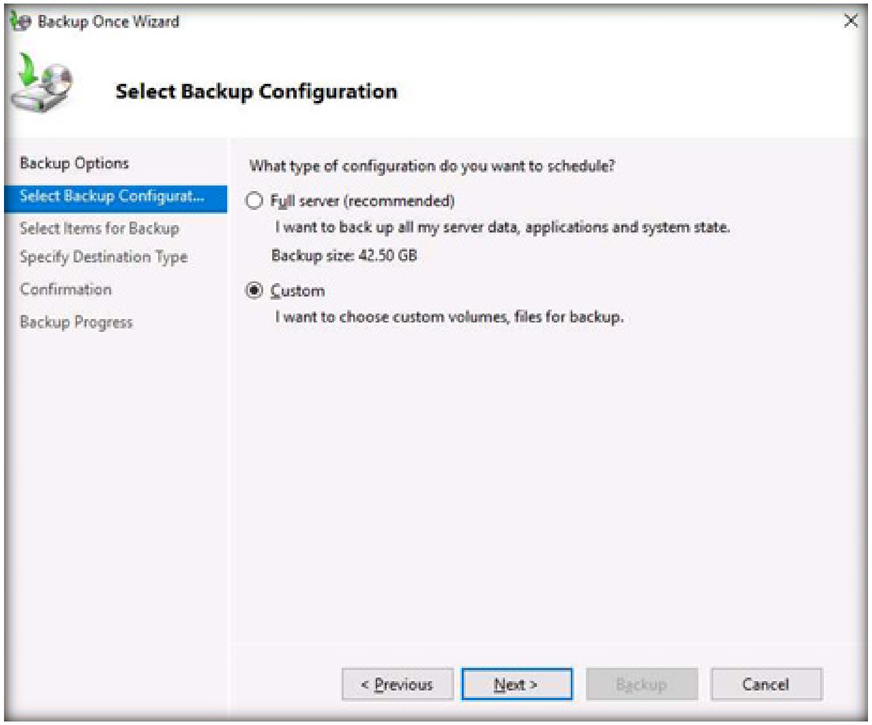
Status

Last Backup
Status: -
Time: -
View details

Next Backup
Status:
Time:
View details

16. Backup Once Wizard window appears, click Next.

17. In Select Backup Configuration wizard, select Custom radio-button and click Next.



Backup Once Wizard

Select Backup Configuration

What type of configuration do you want to schedule?

○ Full server (recommended)

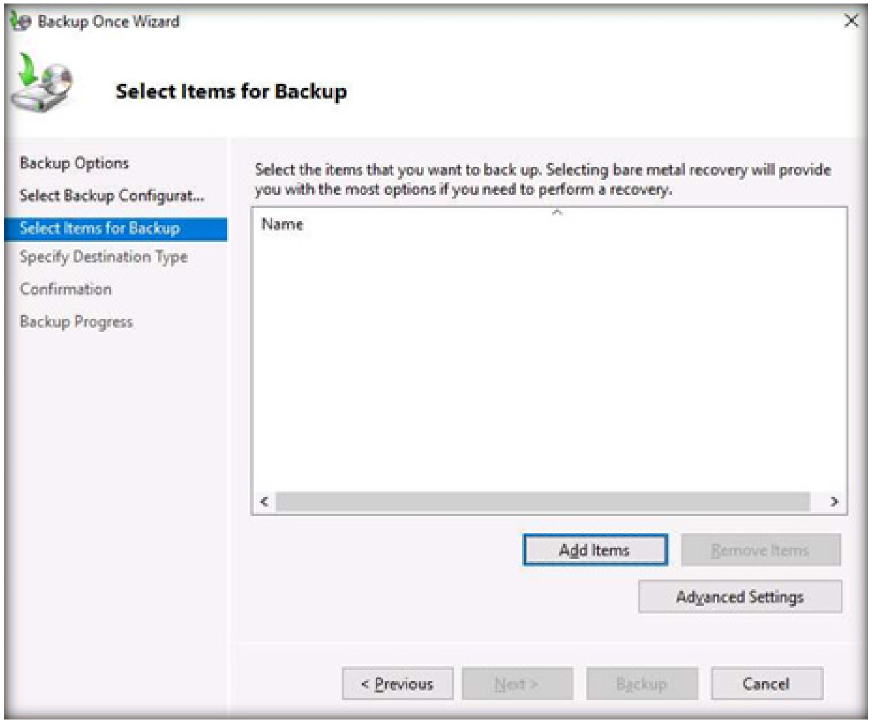
I want to back up all my server data, applications and system state.

Backup size: 42.50 GB

● Custom

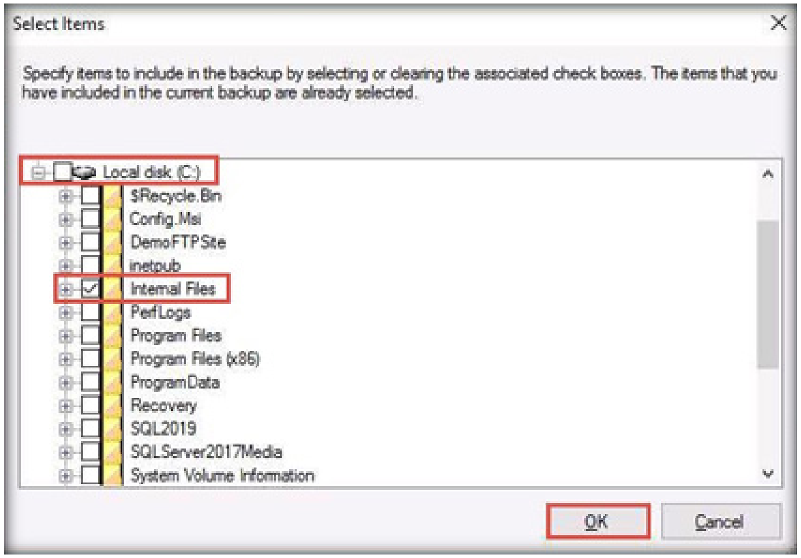
I want to choose custom volumes, files for backup.

18. In Select Items for Backup wizard, click Add Items button.



Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.

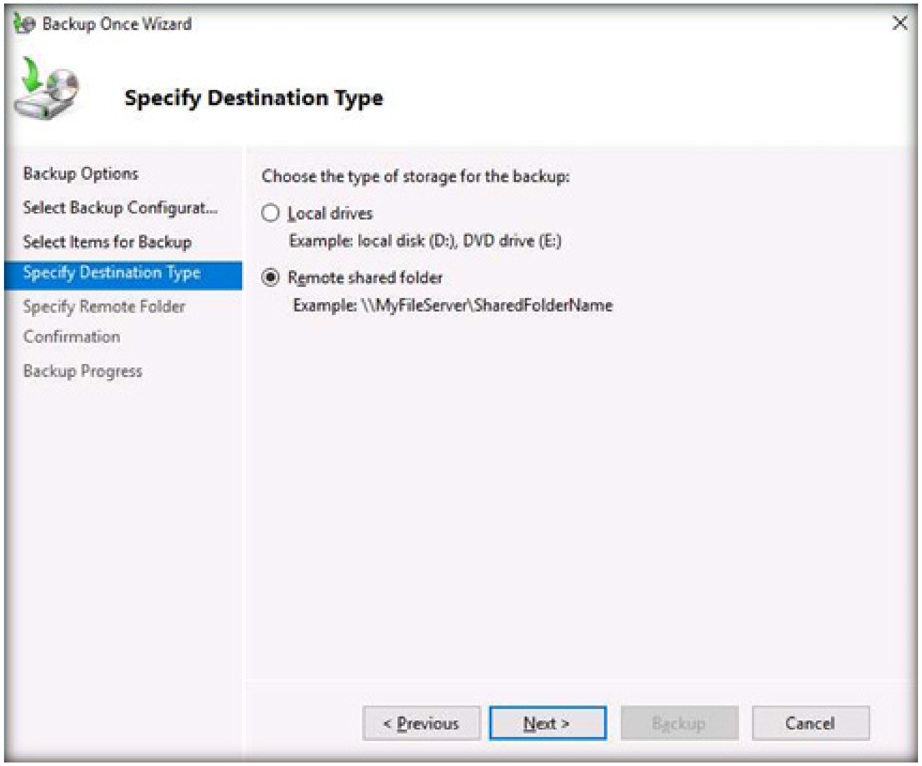
19. Select Items window appears, expand Local Disk (C:) and select Internal Files folder to back up the entire folder. Click OK.



Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

20. You can observe that the selected folder (Internal Files) appears in the selected items field, click Next.

21. In Specify Destination Type wizard, select Remote shared folder radio-button and click Next.



Backup Once Wizard

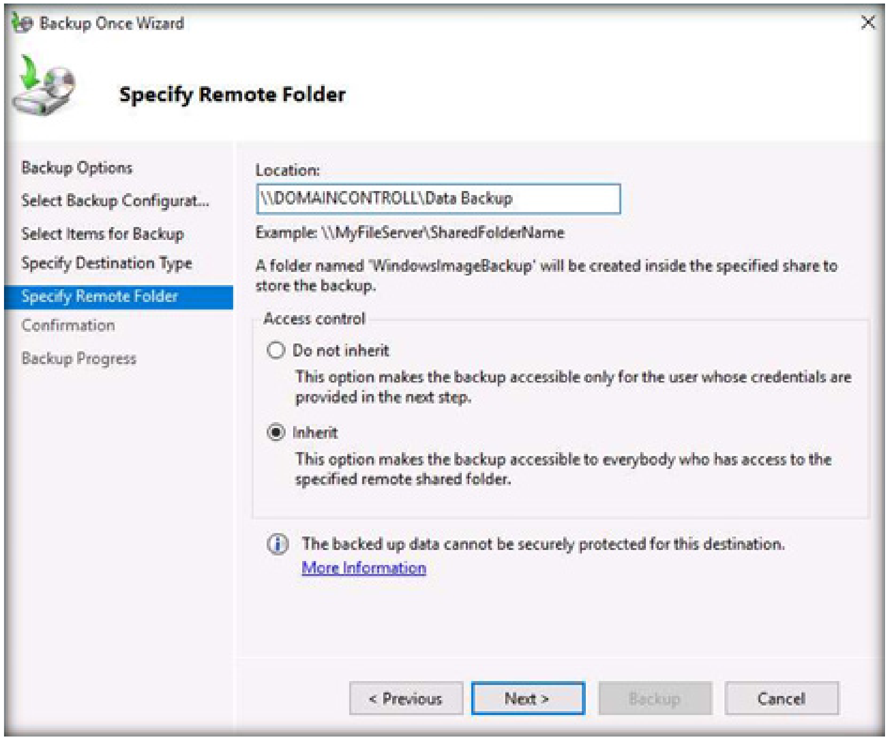
Specify Destination Type

Choose the type of storage for the backup:

○ Local drives
Example: local disk (D:), DVD drive (E:)

● Remote shared folder
Example: \\MyFileServer\SharedFolderName

22. Specify Remote Folder wizard appears, under Location field enter \\DOMAINCONTROLL\Data Backup and click Next.



Backup Once Wizard

Specify Remote Folder

Location: \\DOMAINCONTROLL\Data Backup

Example: \\MyFileServer\SharedFolderName

A folder named 'WindowsImageBackup' will be created inside the specified share to store the backup.

Access control

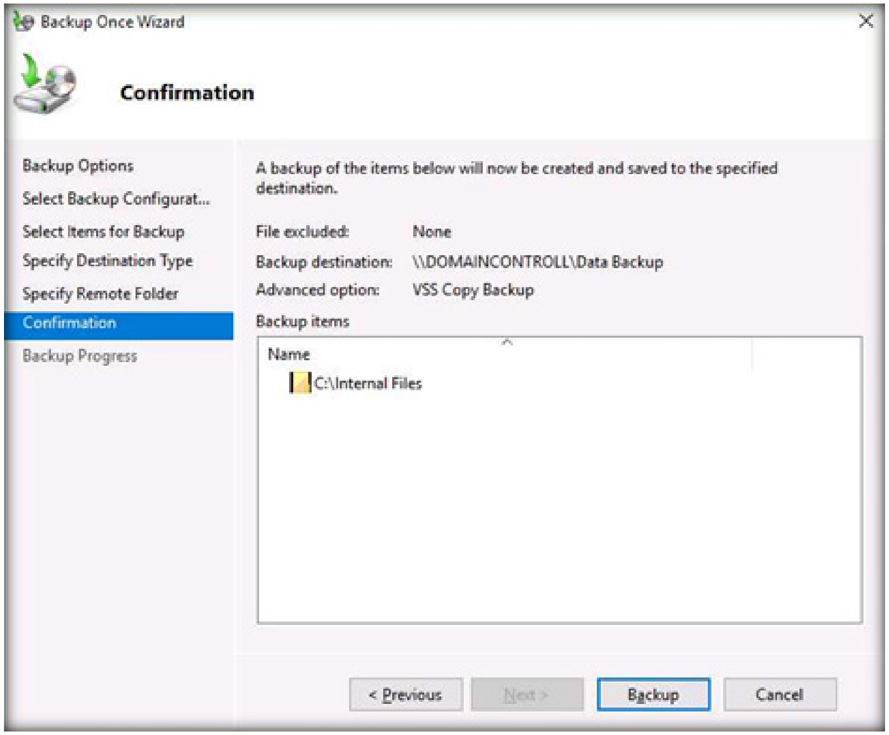
○ Do not inherit
This option makes the backup accessible only for the user whose credentials are provided in the next step.

● Inherit
This option makes the backup accessible to everybody who has access to the specified remote shared folder.

The backed up data cannot be securely protected for this destination.
More Information

EXERCISE 6: BACK UP AND RESTORE DATA IN WINDOWS

23. In the Confirmation wizard, click Backup.



Backup Once Wizard

Confirmation

A backup of the items below will now be created and saved to the specified destination.

File excluded: None

Backup destination: \\DOMAINCONTROLL\Data Backup

Advanced option: VSS Copy Backup

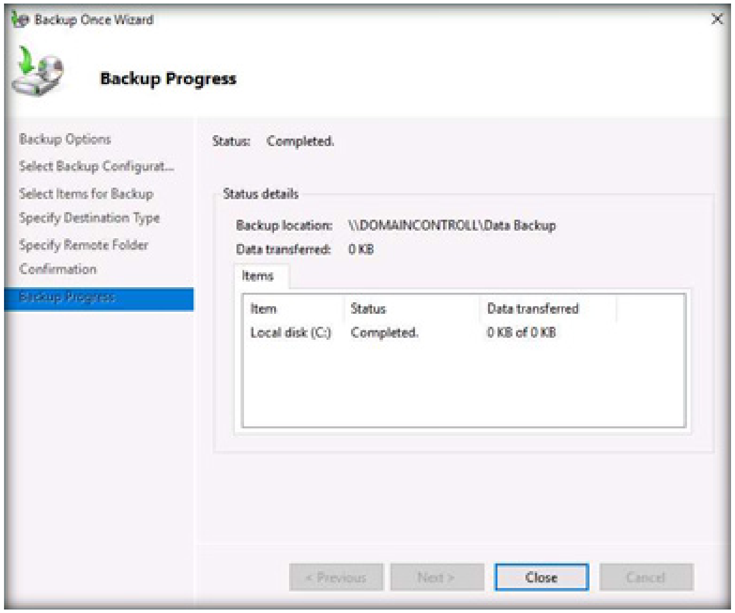
Backup items

Name

C:\Internal Files

24. The backup process initializes, and Backup Progress wizard appears.
Note: Wait for a while for the backup to complete.

25. After the completion of backup process, Status is displayed as Completed. Click Close.



Backup Progress

Status: Completed.

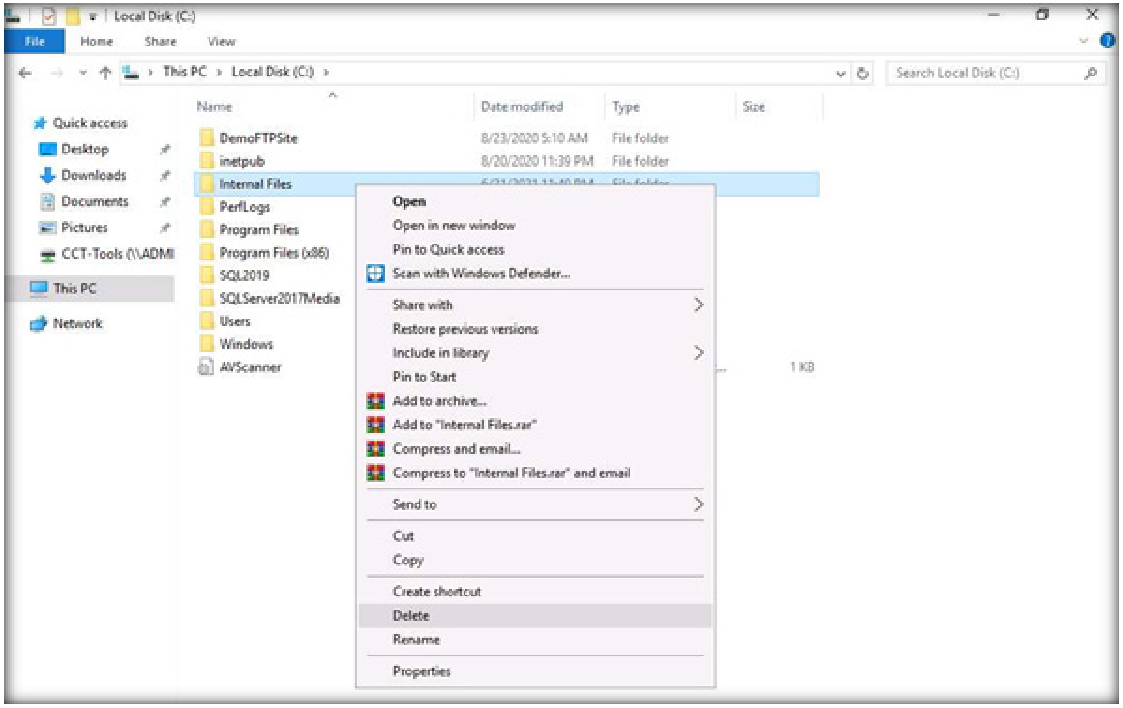
Status details

Backup location: \\DOMAINCONTROLL\Data Backup
Data transferred: 0 KB

Item	Status	Data transferred
Local disk (C:)	Completed.	0 KB of 0 KB

26. Leave wbadmin window running.

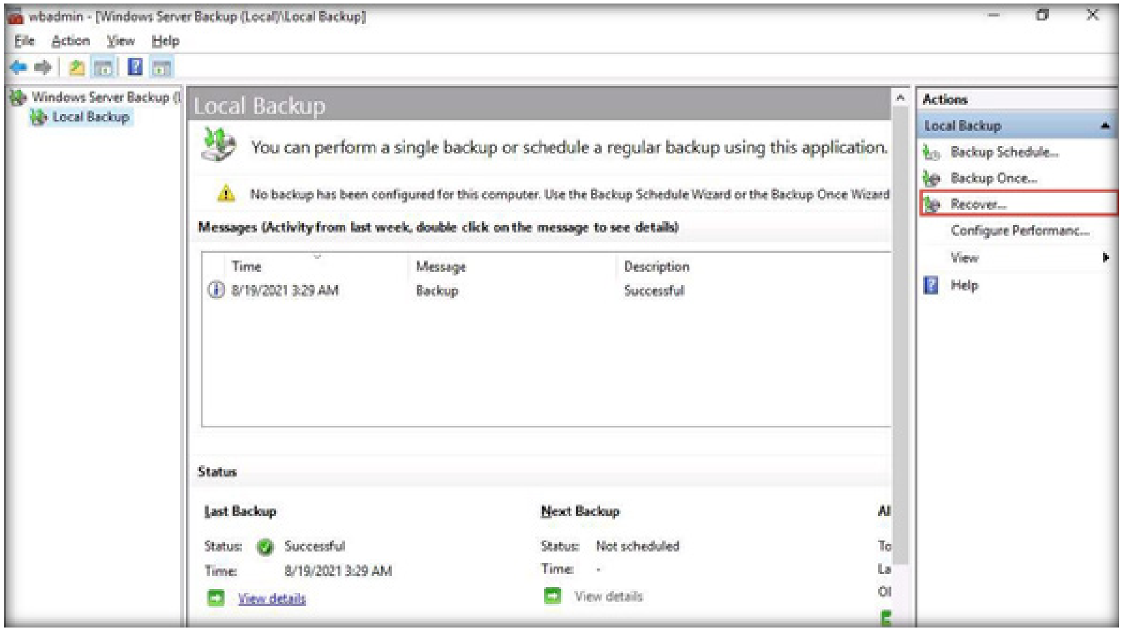
27. Navigate to C: drive and delete Internal Files folder in order to stimulate the loss of valuable data.



Name	Date modified	Type	Size
DemoFTPSite	8/23/2020 5:10 AM	File folder	
inetpub	8/20/2020 11:39 PM	File folder	
Internal Files	6/21/2021 11:40 PM	File folder	
PerfLogs			
Program Files			
Program Files (x86)			
SQL2019			
SQLServer2017Media			
Users			
Windows			
AVScanner			1 KB

28. Now, we will restore the files that were deleted accidentally.

29. In the wbadmin window, click Recover... from the right-pane under Actions section.



Local Backup

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description
8/19/2021 3:29 AM	Backup	Successful

Status

Last Backup

Status: Successful

Time: 8/19/2021 3:29 AM

View details

Next Backup

Status: Not scheduled

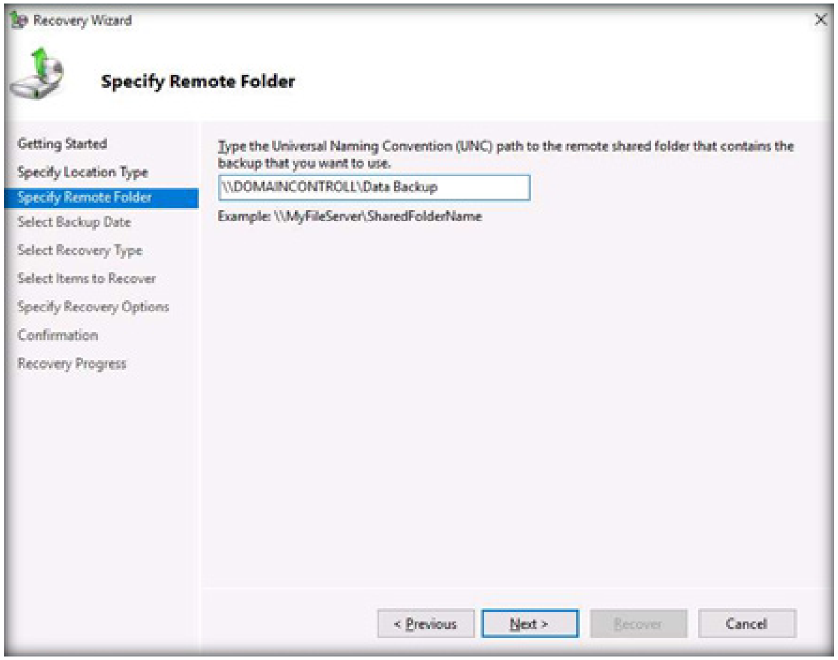
Time: -

View details

30. Getting Started wizard appears, select A backup stored on another location radio-button and click Next.

31. In Specify Location Type wizard, select Remote shared folder radio-button and click Next.

32. Specify Remote Folder wizard appears, enter \\DOMAINCONTROLL\Data Backup in the field and click Next.



Recovery Wizard

Specify Remote Folder

Type the Universal Naming Convention (UNC) path to the remote shared folder that contains the backup that you want to use.

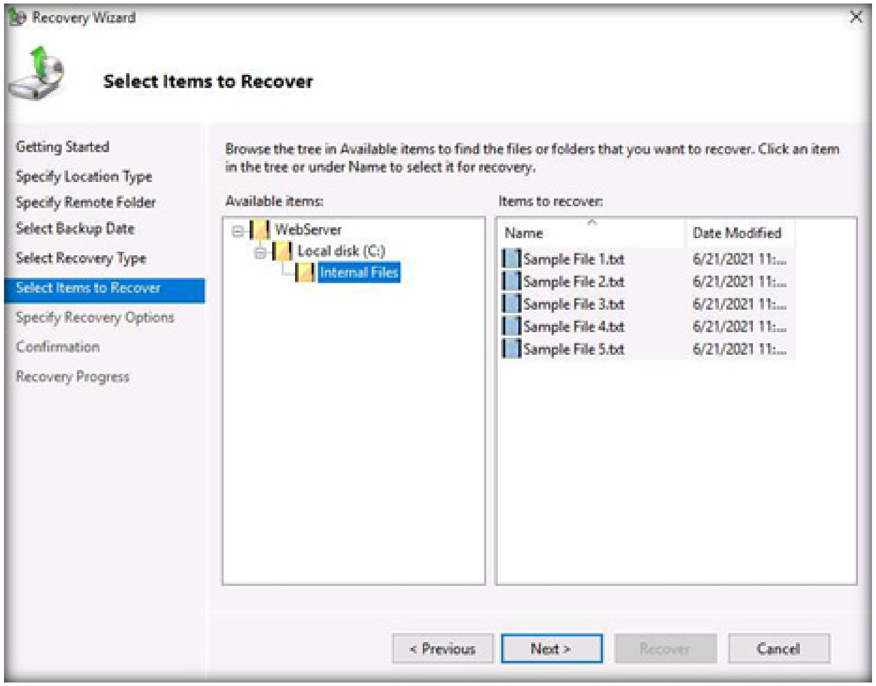
\\DOMAINCONTROLL\Data Backup

Example: \\MyFileServer\SharedFolderName

33. In Select Backup Date wizard, leave the settings as default and click Next.

34. In Select Recovery Type wizard, click Next.

35. In Select Items to Recover wizard, under Available items section, navigate to WebServer → Local Disk (C:) and select Internal Files folder. Click Next.



Select Items to Recover

Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.

Available items:

- WebServer
  - Local disk (C:)
    - Internal Files

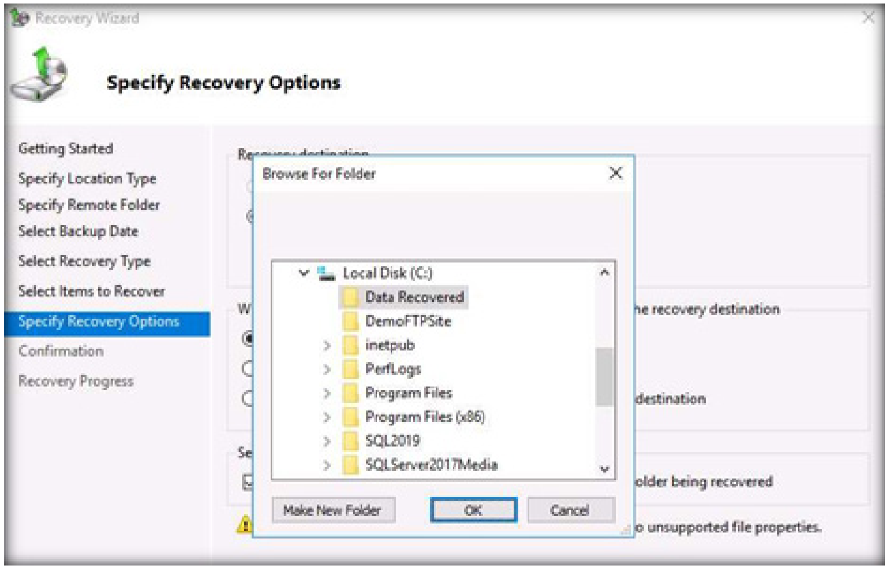
Items to recover:

Name	Date Modified
Sample File 1.txt	6/21/2021 11:...
Sample File 2.txt	6/21/2021 11:...
Sample File 3.txt	6/21/2021 11:...
Sample File 4.txt	6/21/2021 11:...
Sample File 5.txt	6/21/2021 11:...

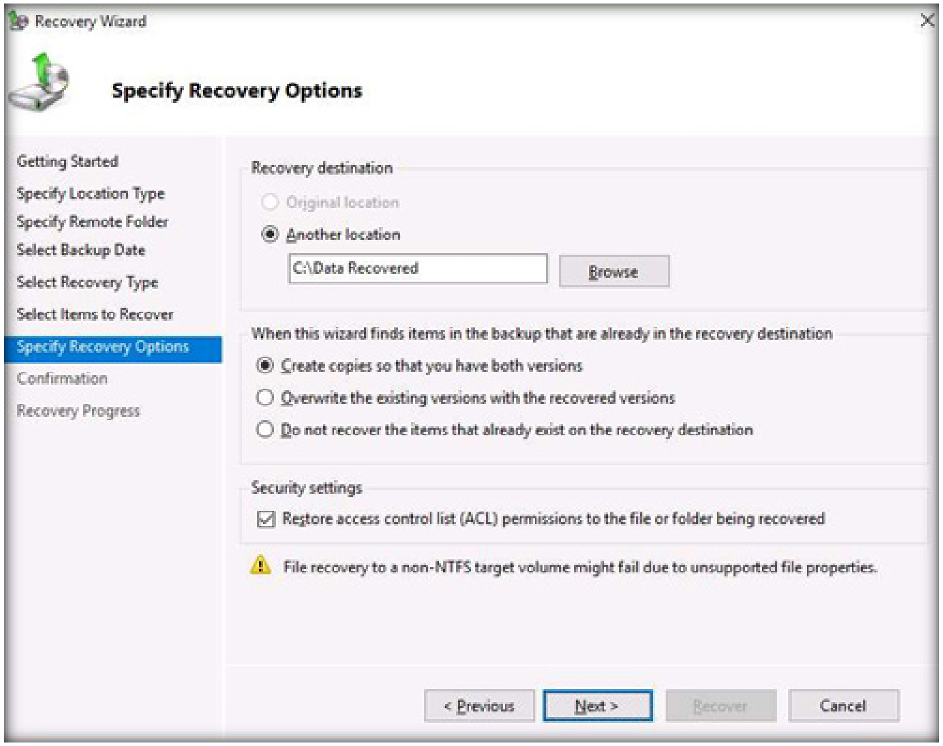
36. In Select Recovery Options wizard, under Another location, click Browse button.

37. Browse For Folder window appears, navigate to This PC → Local Disk (C:) and click Make New Folder.

38. Name the folder as Data Recovered and click OK.



39. You can observe that the selected location appears under Another location field, click Next.



Recovery Wizard

Specify Recovery Options

Recovery destination

○ Original location

● Another location

C:\Data Recovered

When this wizard finds items in the backup that are already in the recovery destination

● Create copies so that you have both versions

○ Overwrite the existing versions with the recovered versions

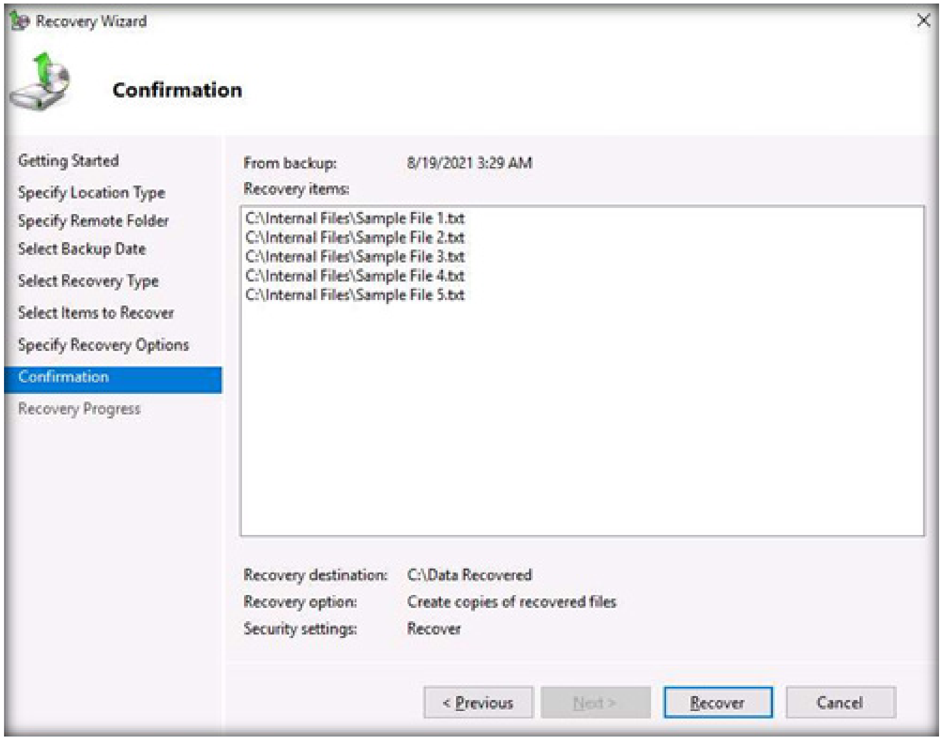
○ Do not recover the items that already exist on the recovery destination

Security settings

☑ Restore access control list (ACL) permissions to the file or folder being recovered

File recovery to a non-NTFS target volume might fail due to unsupported file properties.

40. In the Confirmation wizard, click Recover.



From backup: 8/19/2021 3:29 AM

Recovery items:

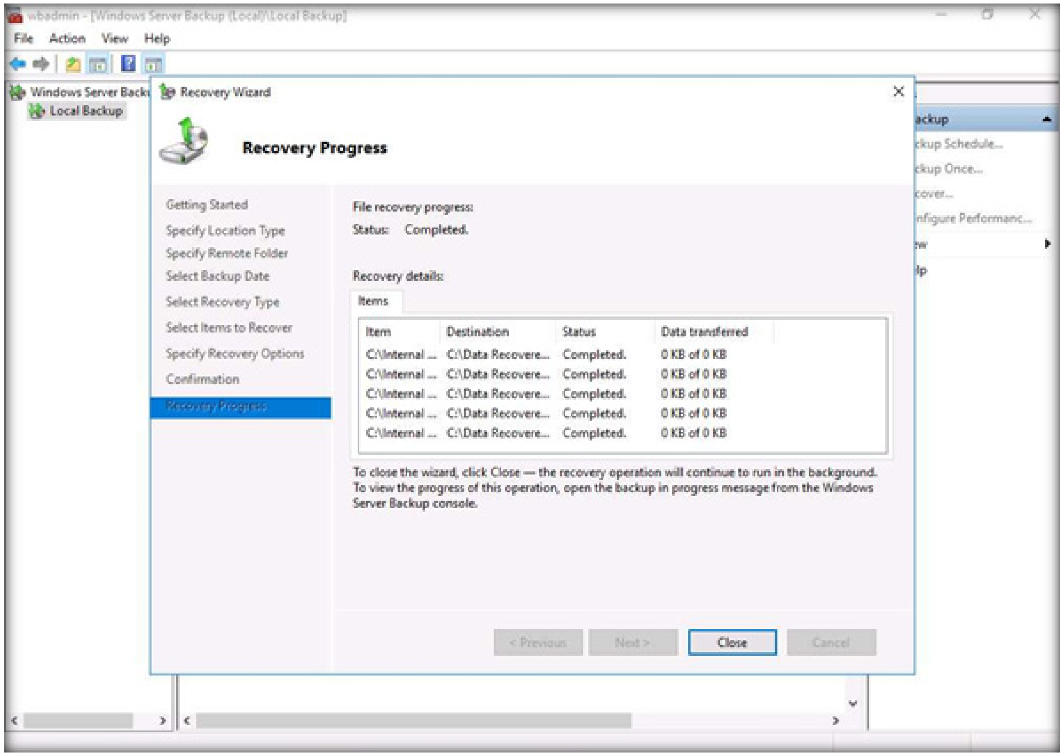
```
C:\Internal Files\Sample File 1.txt
C:\Internal Files\Sample File 2.txt
C:\Internal Files\Sample File 3.txt
C:\Internal Files\Sample File 4.txt
C:\Internal Files\Sample File 5.txt
```

Recovery destination: C:\Data Recovered

Recovery option: Create copies of recovered files

Security settings: Recover

41. Recovery Progress wizard appears and the recover process initializes. After the completion of recovery, Status as Completed is displayed. Click Close.



File recovery progress:

Status: Completed.

Recovery details:

Items

Item	Destination	Status	Data transferred
C:\Internal ...	C:\Data Recovere...	Completed.	0 KB of 0 KB
C:\Internal ...	C:\Data Recovere...	Completed.	0 KB of 0 KB
C:\Internal ...	C:\Data Recovere...	Completed.	0 KB of 0 KB
C:\Internal ...	C:\Data Recovere...	Completed.	0 KB of 0 KB
C:\Internal ...	C:\Data Recovere...	Completed.	0 KB of 0 KB

To close the wizard, click Close — the recovery operation will continue to run in the background. To view the progress of this operation, open the backup in progress message from the Windows Server Backup console.

42. Close wbadmin window.

43. Now, navigate to the C:\Data Recovered to view the restored files in order to confirm that the recovery process worked correctly.

44. This concludes the demonstration showing how to back up and restore data in Windows.

45. Close all open windows.

46. Turn off AD Domain Controller and Web Server virtual machines.

EXERCISE 7: PERFORM DATA DESTRUCTION USING WINDOWS DISKPART UTILITY

Data destruction is the process of destructing the stored data in electronic media such as hard drives, flash drives, tapes, etc.

LAB SCENARIO

Computers, smartphones, and other devices store a large amount of data, some of which may be sensitive and critical, such as emails, documents, personal photos, etc. Once not in use, the user deletes the data presuming that the information is deleted and cannot be recovered. If not deleted properly, the information still exists on the hard drive or memory chip, and anyone accessing such a system can recover these deleted files. The best way to permanently delete files or sensitive data is by implementing data destruction methods

A security professional must have a required knowledge to destroy data permanently so that it cannot be retrieved or recovered.

OBJECTIVE

This lab will demonstrate how to perform data destruction using Windows utility such as DiskPart.

OVERVIEW OF DATA DESTRUCTION

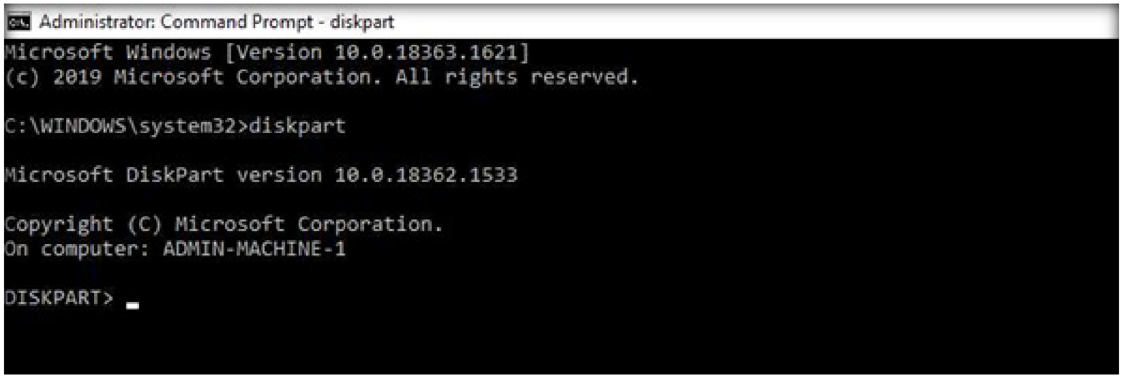
Data destruction converts the data into an unreadable form that cannot be accessed or exploited for unauthorized purposes. The main purpose of data destruction is to restrict the unauthorized disclosure of information through proper disposal and destruction of devices, equipment, computers, and media that store sensitive data.

DiskPart is a command utility to manage drives, partitions, and volumes. It can be used when other tools such as Disk Management and Format are unable to resolve the problem. It quickly removes data and partitions from a hard drive using the command prompt.

A security professional can use Windows DiskPart Utility as a proof of concept to perform data destruction of organization’s data.

Note: Ensure that the PfSense Firewall virtual machine is running.

1. Turn on the Admin Machine-1 virtual machine.
2. Log in with the credentials Admin and admin@123.
Note: If the network screen appears, click Yes.
3. Click the Type here to search field present at the bottom-left corner of Desktop and type cmd. Command Prompt appears in the search results, from the right-pane, select Run as administrator option.
4. User Account Control window appears, click Yes to proceed.
5. Switch to the Command Prompt window. In the Command Prompt window, type diskpart and press Enter to launch DiskPart.

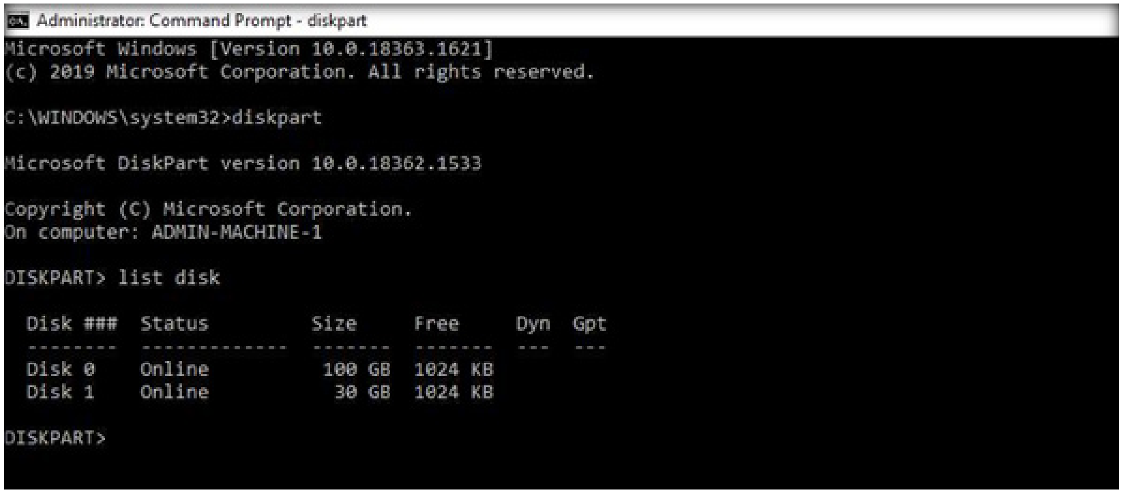


```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.18362.1533

Copyright (C) Microsoft Corporation.
On computer: ADMIN-MACHINE-1

DISKPART> _
```

EXERCISE 7: PERFORM DATA DESTRUCTION USING WINDOWS DISKPART UTILITY

6. Diskpart prompt appears, type list disk and press Enter to display all the disks on the system.

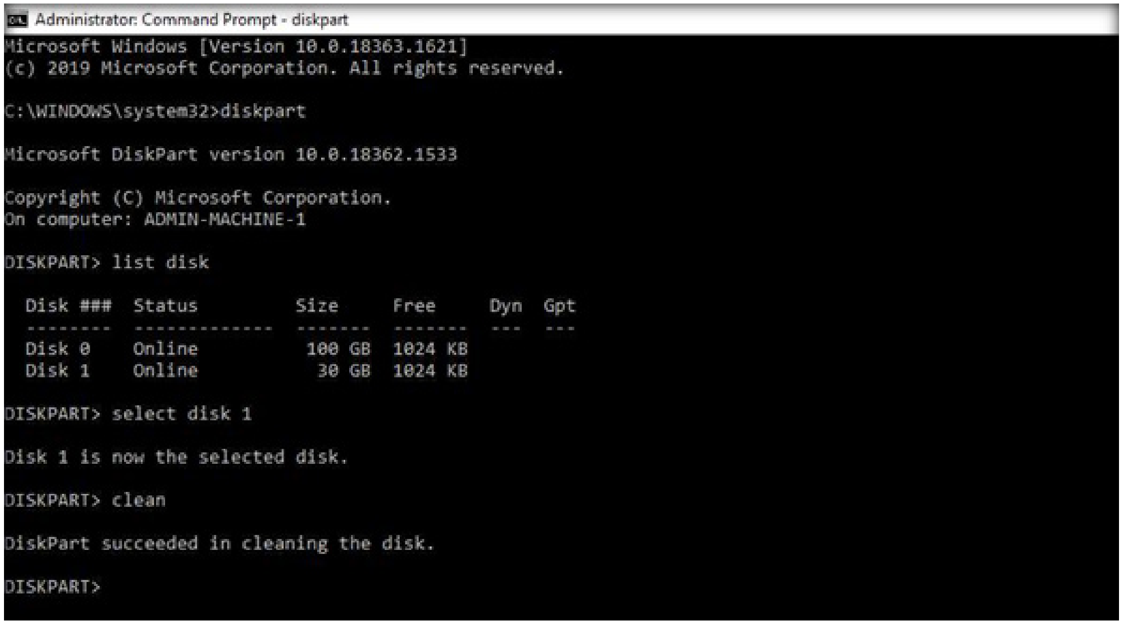
7. The result appears, displaying two disks: Disk 0 and Disk 1 with Status as Online along with the total Size and Free space, as shown in the screenshot below.



```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.18362.1533

Copyright (C) Microsoft Corporation.
On computer: ADMIN-MACHINE-1

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
  Disk 1    Online           30 GB  1024 KB

DISKPART>
```

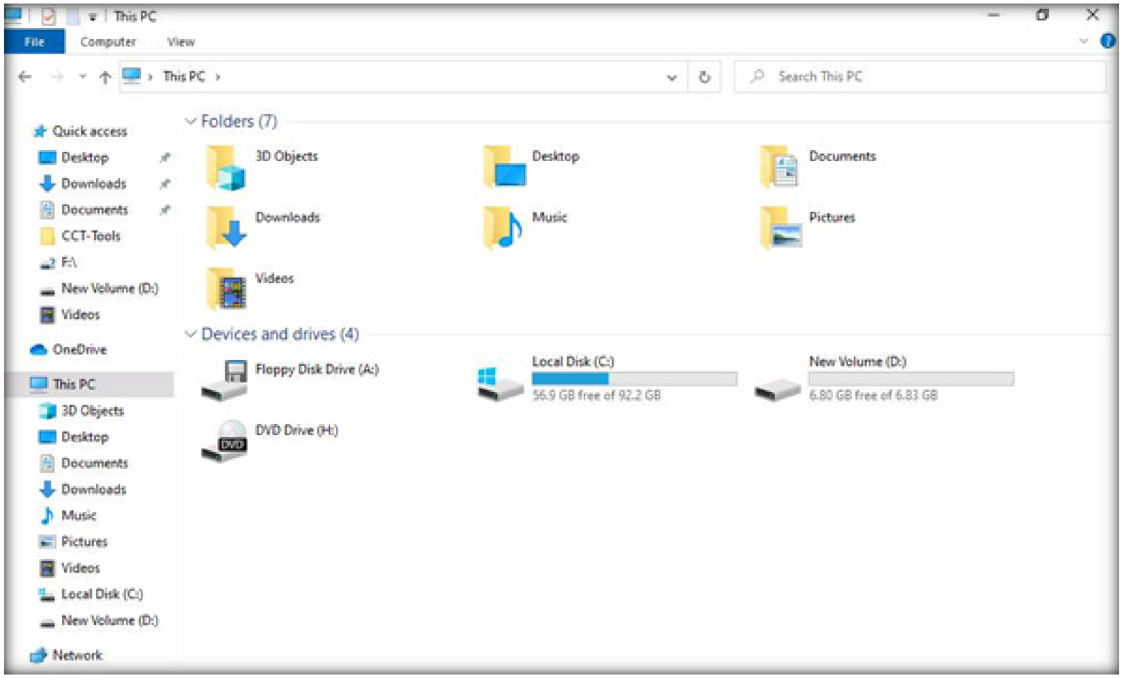
8. Type select disk 1 and press Enter to select the disk needs to be cleaned.

9. Now, type clean and press Enter to wipe out the select drive (here, Disk 1).



```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.18362.1533

Copyright (C) Microsoft Corporation.
On computer: ADMIN-MACHINE-1

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
  Disk 1    Online           30 GB  1024 KB

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART>
```

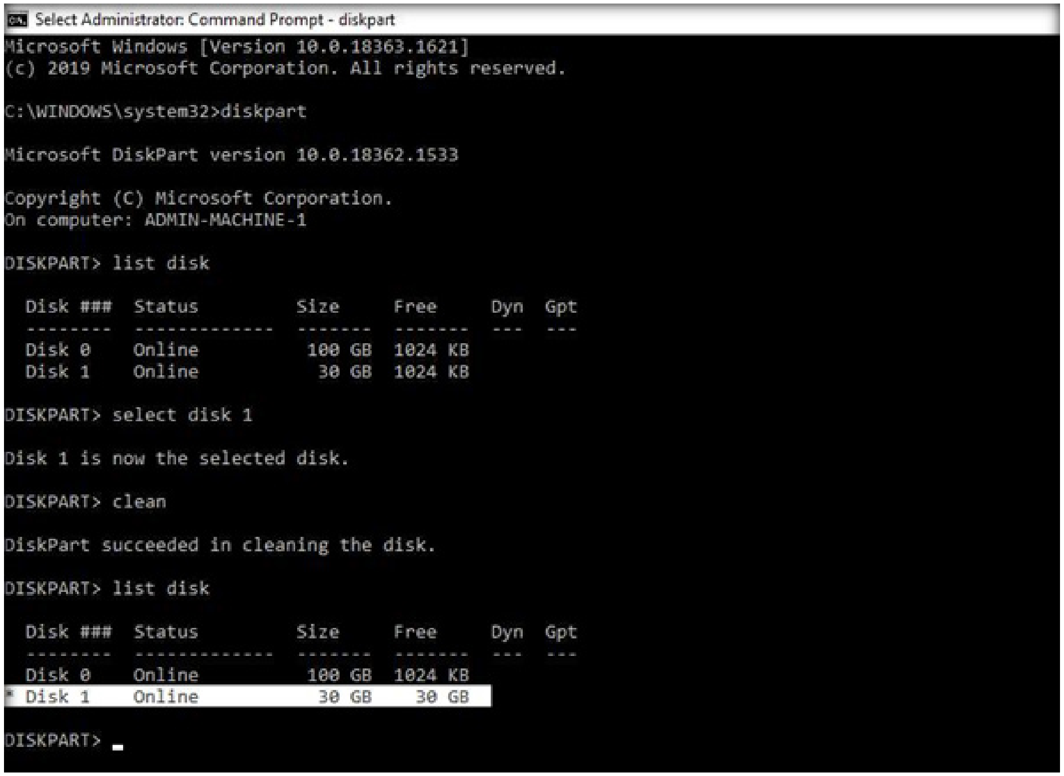
10. Open File Explorer window and navigate to This PC. You can observe that the New Volume (Z:) has been removed.



11. Switch back to the Command Prompt window.

12. In the Diskpart prompt, type list disk and press Enter to confirm that all the data in Disk 1 has been wiped out.

13. The result appears, observe that Disk 1 is now empty as the Size and Free space is same (i.e., 30 GB), as shown in the screenshot below.

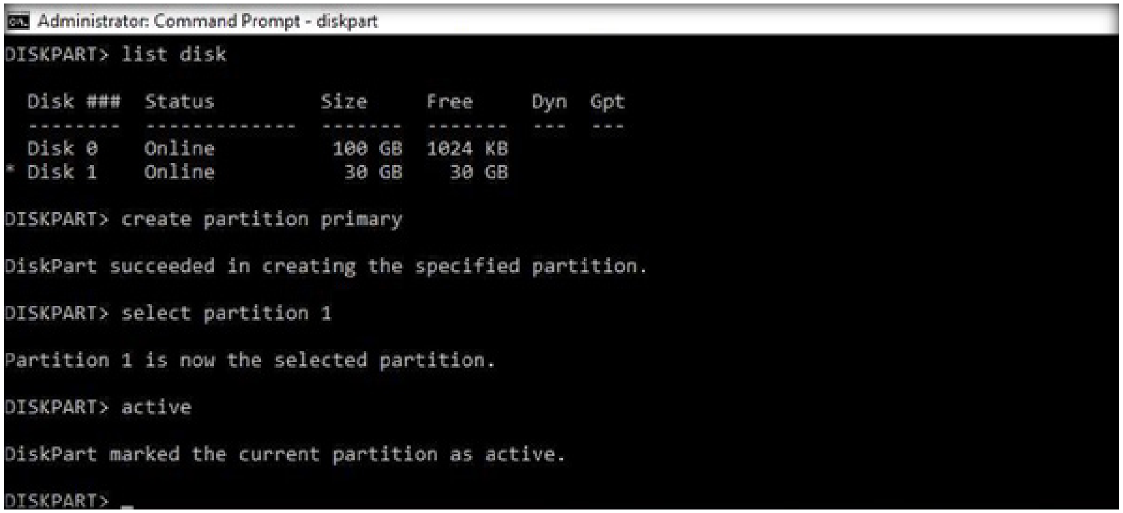


```
Microsoft Windows [Version 10.0.18363.1621]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>diskpart

Microsoft DiskPart version 10.0.18362.1533

Copyright (C) Microsoft Corporation.
On computer: ADMIN-MACHINE-1

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
  Disk 1    Online           30 GB  1024 KB

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> clean

DiskPart succeeded in cleaning the disk.

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
* Disk 1    Online           30 GB    30 GB

DISKPART> _
```

14. Now, type create partition primary and press Enter to create a new partition on the drive.

15. Type select partition 1 and press Enter to select the new primary partition.

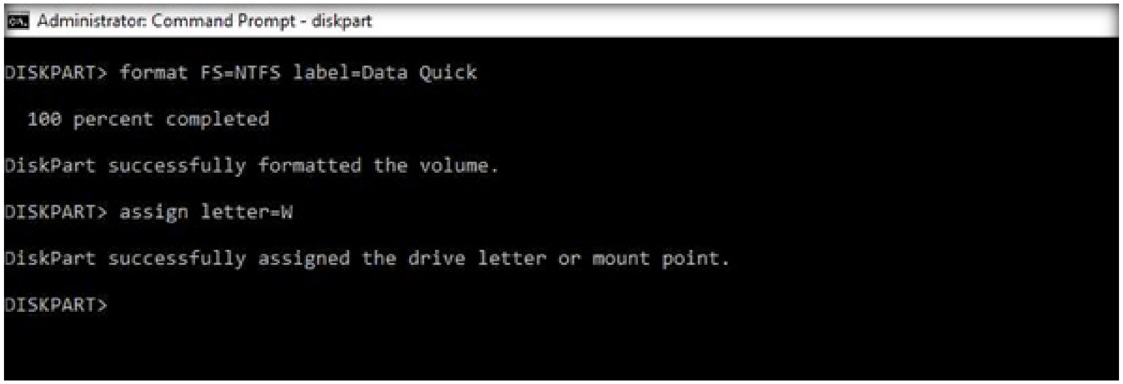
16. Type active and press Enter to activate the selected partition.



```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          100 GB  1024 KB
* Disk 1    Online           30 GB    30 GB

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.

DISKPART> select partition 1

Partition 1 is now the selected partition.

DISKPART> active

DiskPart marked the current partition as active.

DISKPART> _
```

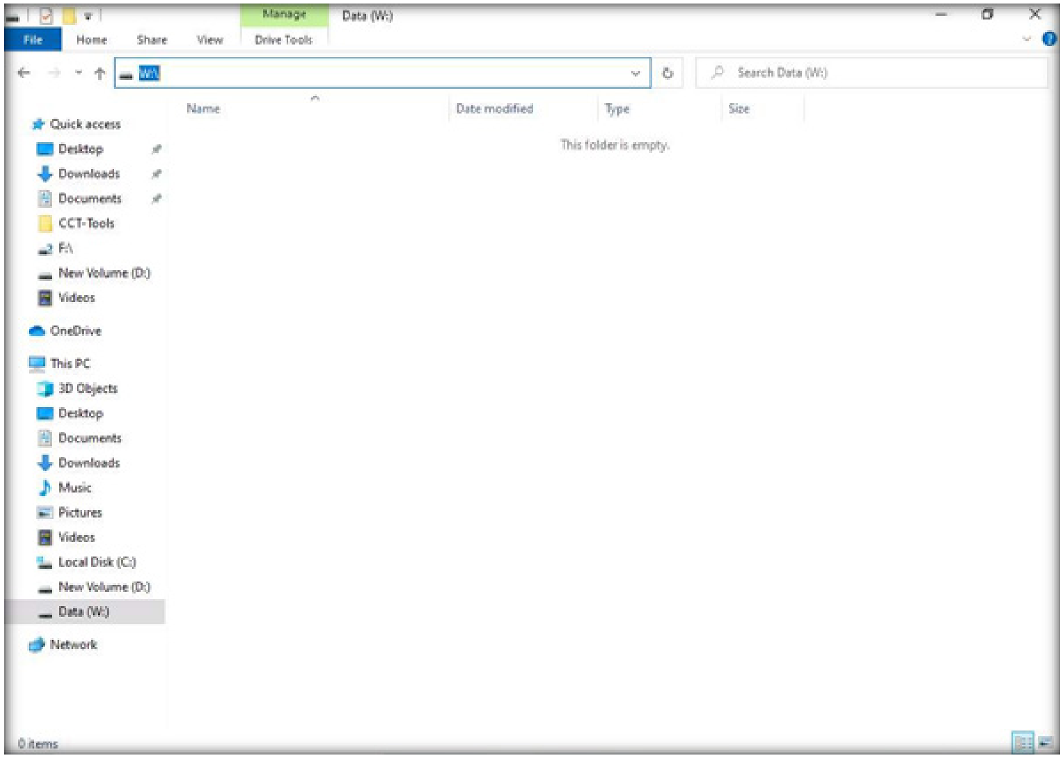
17. Now, type format FS=NTFS label=Data Quick and press Enter to format the partition and set a drive label.

18. Type assign letter=W and press Enter to assign a letter and make the drive available in File Explorer.



```
DISKPART> format FS=NTFS label=Data Quick

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> assign letter=W

DiskPart successfully assigned the drive letter or mount point.

DISKPART>
```

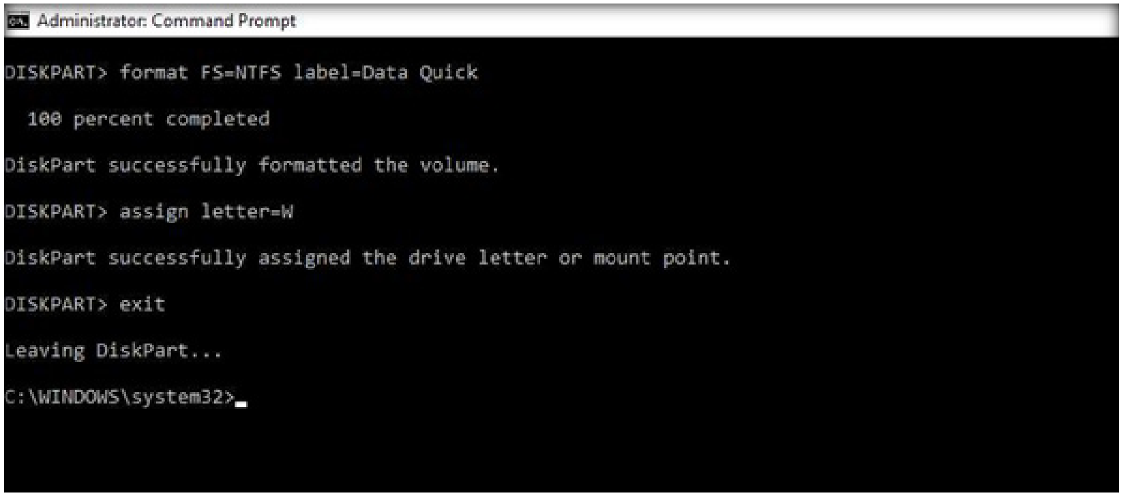
19. File Explorer window appears automatically, displaying newly created Data (W:) drive, as shown in the screenshot below.



This folder is empty.

20. Close File Explorer window and switch to the Command Prompt window.

21. In the Diskpart prompt, type exit and press Enter to terminal Diskpart.



```
DISKPART> format FS=NTFS label=Data Quick

  100 percent completed

DiskPart successfully formatted the volume.

DISKPART> assign letter=W

DiskPart successfully assigned the drive letter or mount point.

DISKPART> exit

Leaving DiskPart...

C:\WINDOWS\system32>_
```

22. This concludes the demonstration showing how to wipe out data in a drive and creating a new drive using DiskPart utility.

23. Close all open windows.

24. Turn off Admin Machine-1 and PfSense Firewall virtual machines.

EXERCISE 7: PERFORM DATA DESTRUCTION USING WINDOWS DISKPART UTILITY

EC-Council