Domain 04 Demo 09

Using Rohos Disk Encryption

Objective: To demonstrate the process of using Rohos Disk Encryption to create and manage encrypted virtual drives, ensuring the protection of sensitive data stored on local systems and portable devices

Tools required: Windows Server 2022 and Rohos Disk Encryption Software

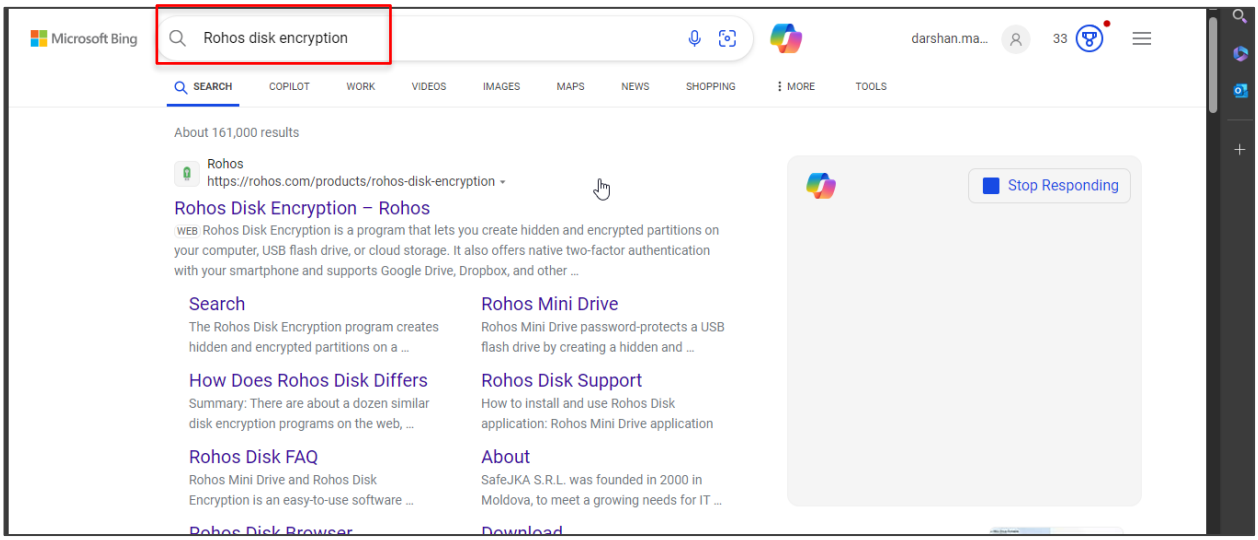
Prerequisites: None

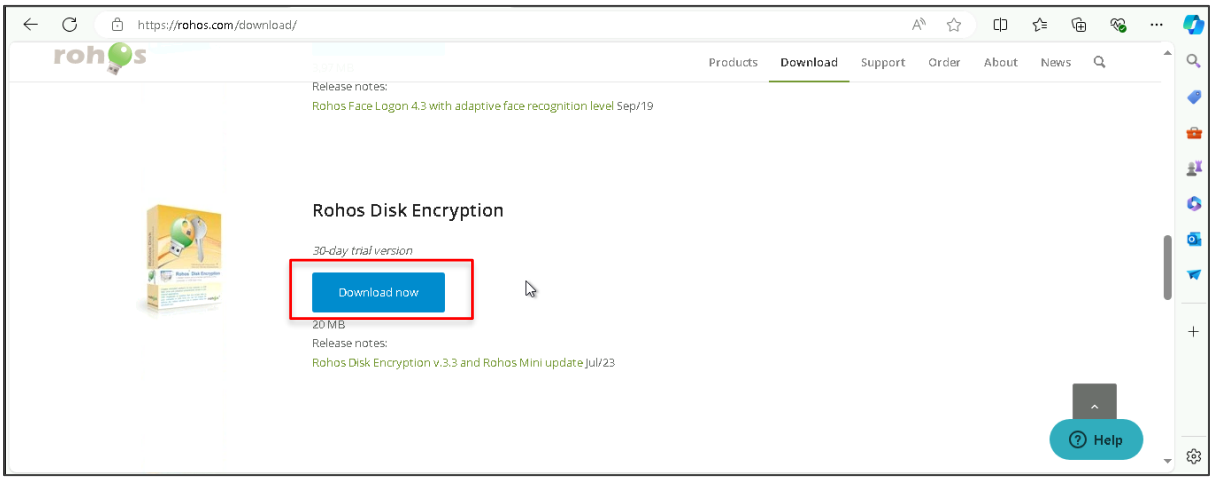
Steps to be followed:

1. Install Rohos disk encryption software
2. Utilize Rohos disk encryption software

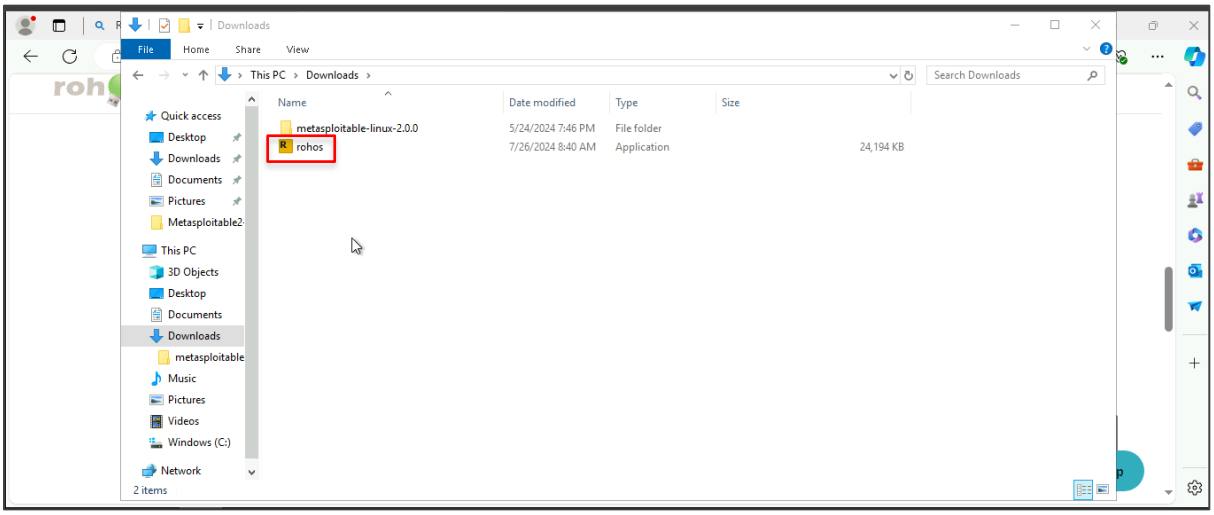
Step 1: Install Rohos disk encryption software

1.1 Open a web browser, search for **Rohos disk encryption**, and download the software from the official website

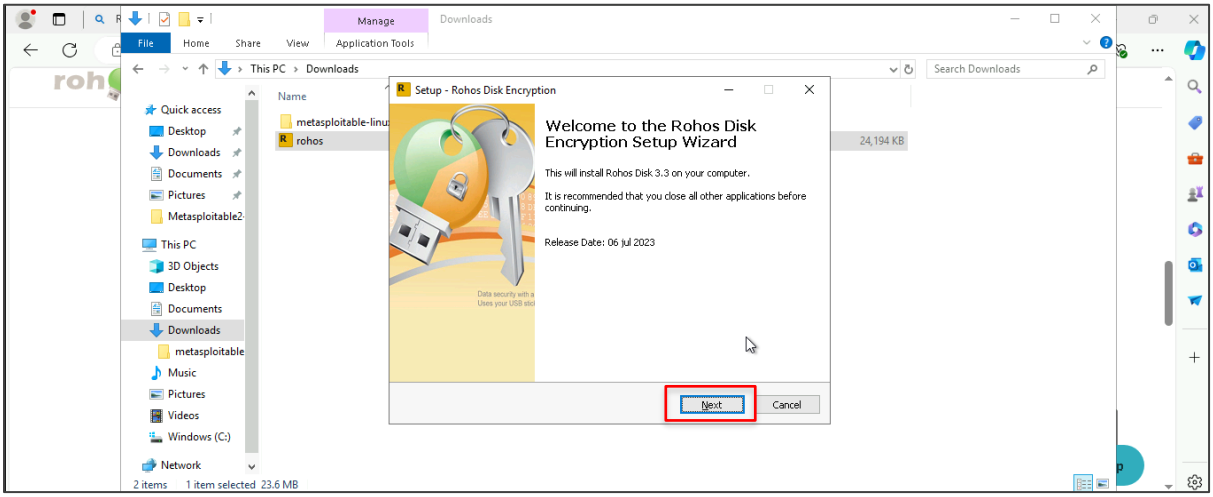




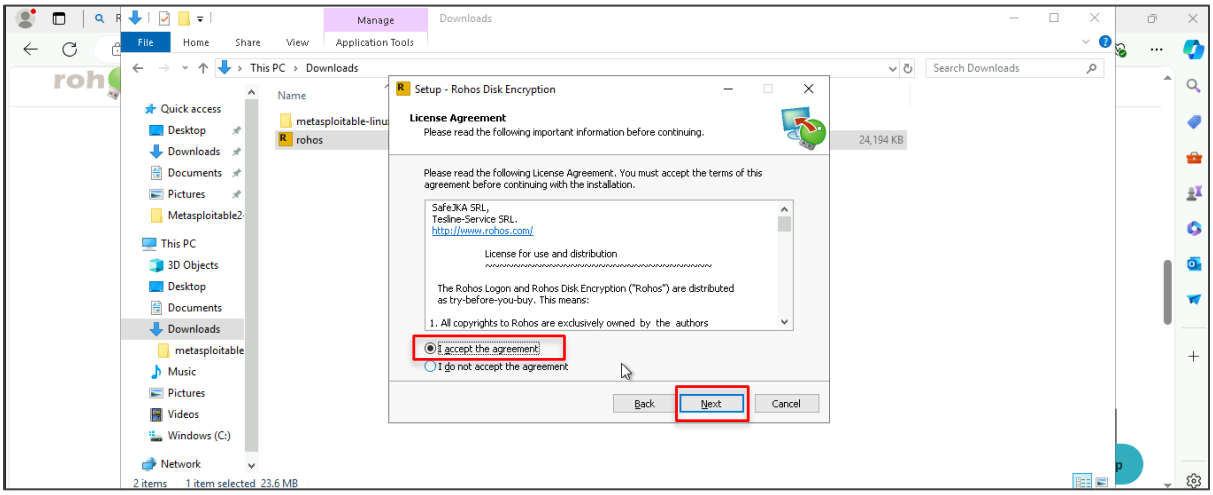
1.2 Once downloaded, double-click the installer file in the **Downloads** folder to start the installation process



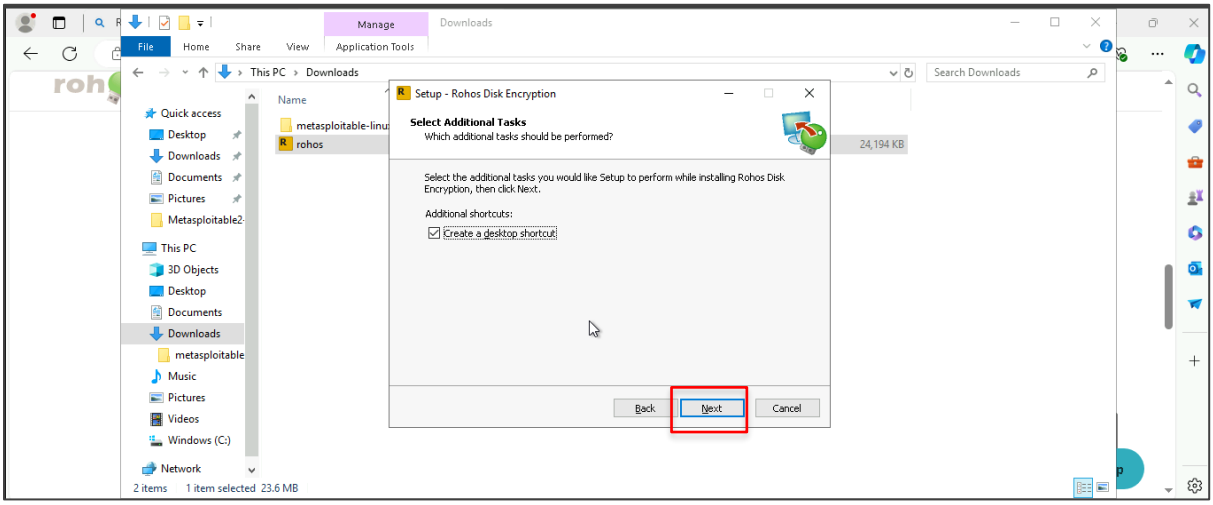
1.3 On the welcome screen of the setup wizard, click **Next** to continue



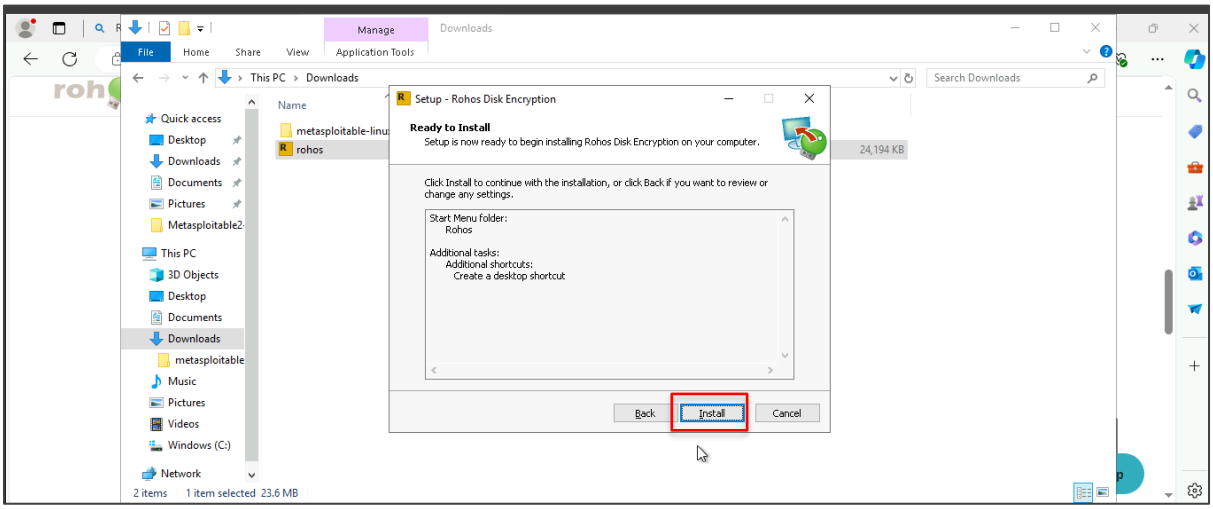
1.4 Read the license agreement, select the I **accept the agreement** option, and click **Next**



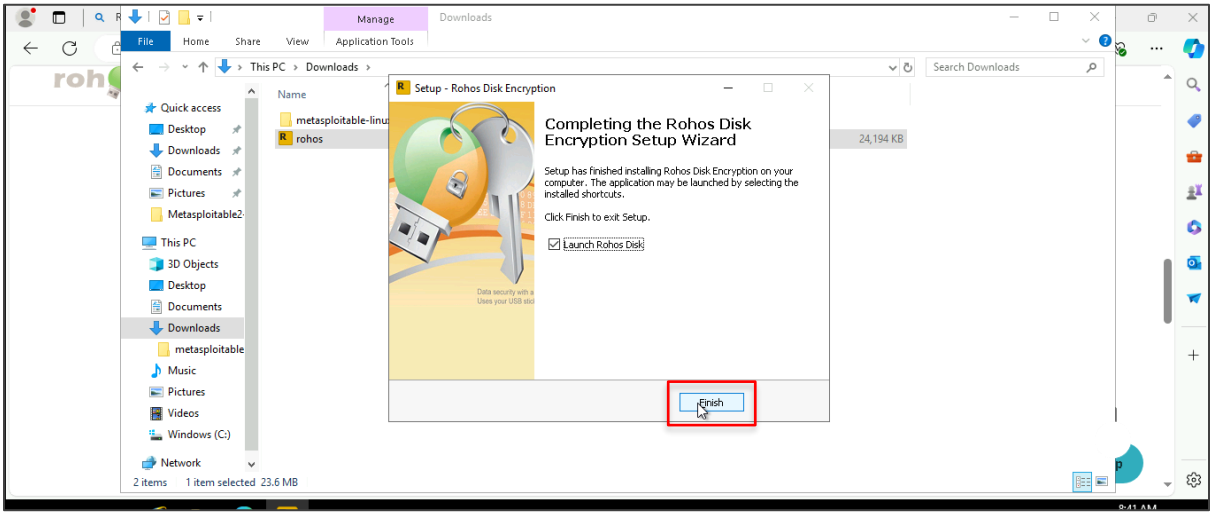
1.5 Choose whether to create a desktop icon and click **Next**



1.6 Review your settings and click **Install** to begin the installation



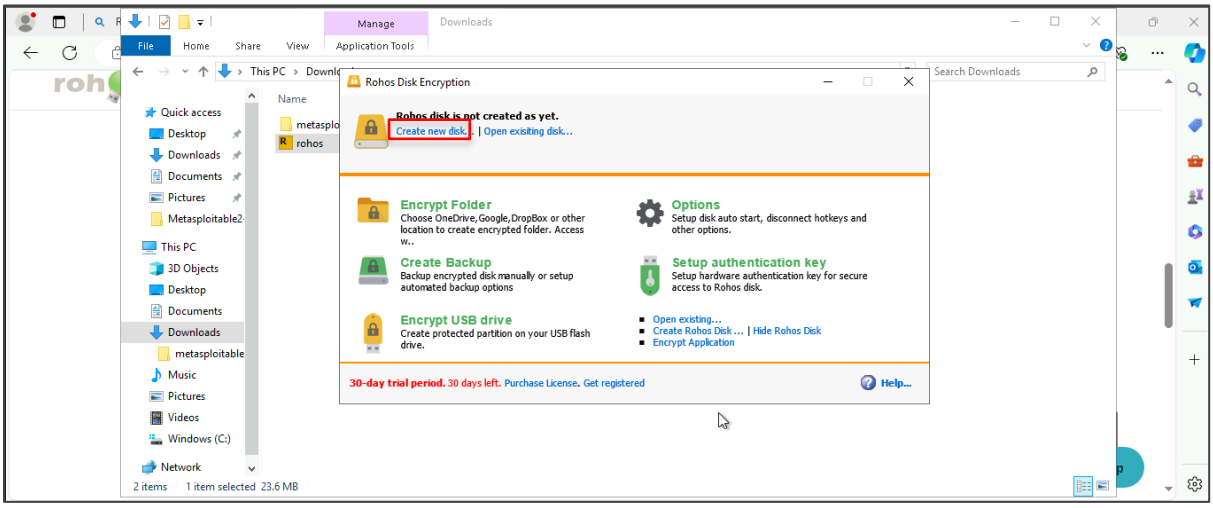
1.7 Once the installation is complete, click **Finish** to exit the setup wizard



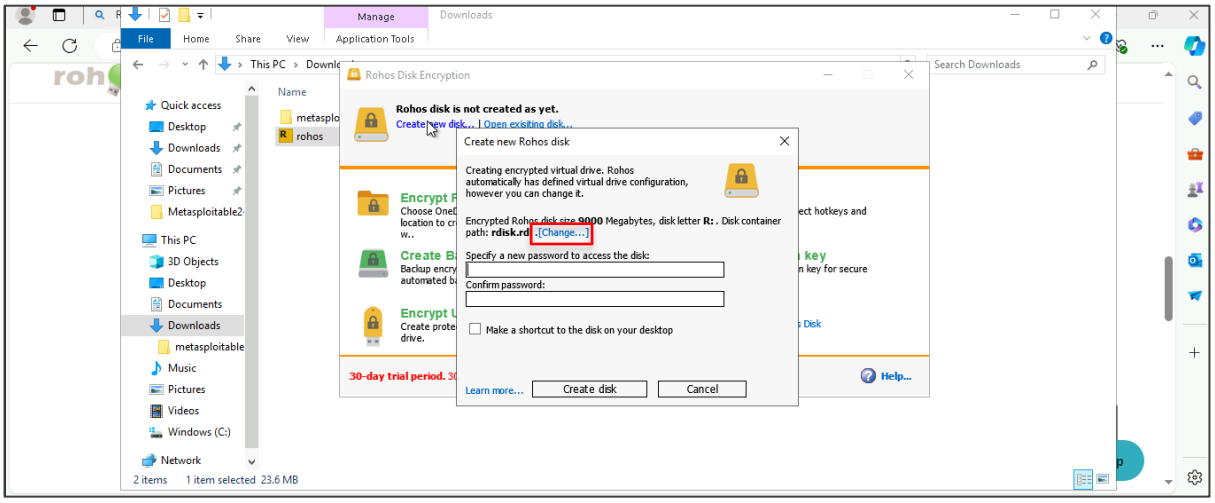
The Rohos Disk Encryption application will open automatically after installation.

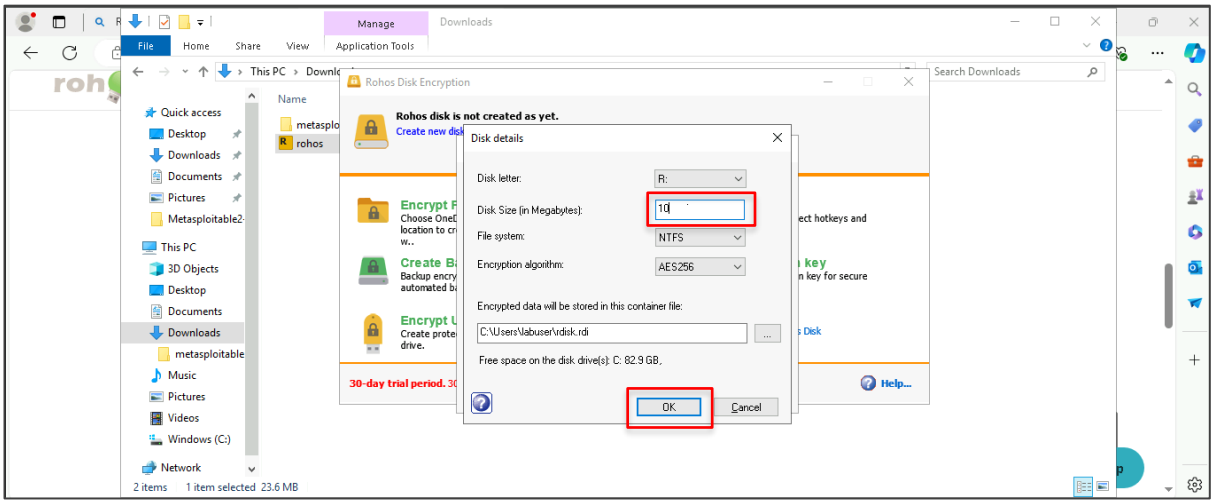
Step 2: Utilize Rohos disk encryption software

2.1 In the Rohos Disk Encryption interface, click **Create new disk**

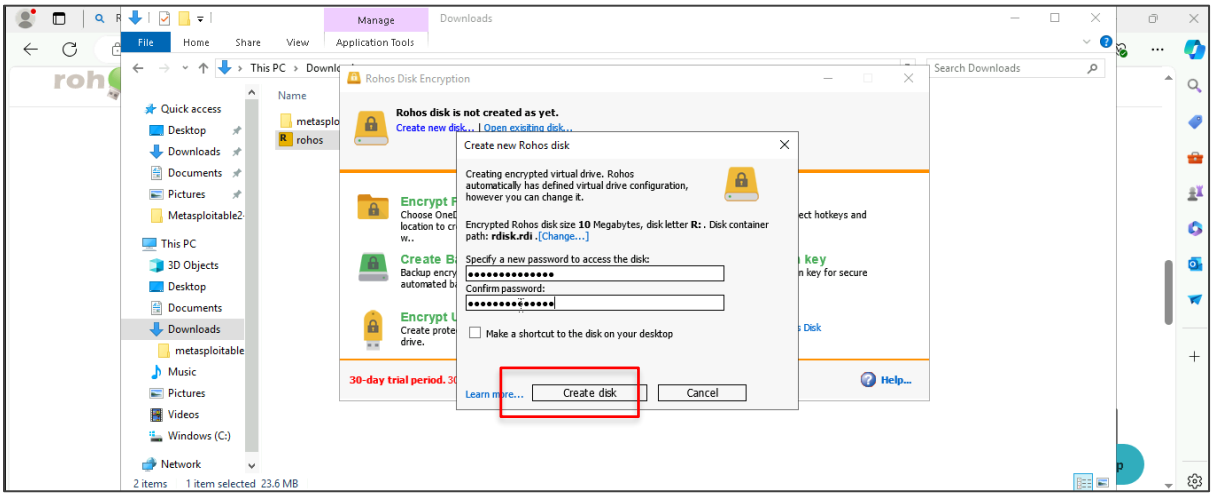


2.2 In the Create new Rohos disk window, click the **Change...** option, set the size of the encrypted disk to 10 MB, and click **OK**



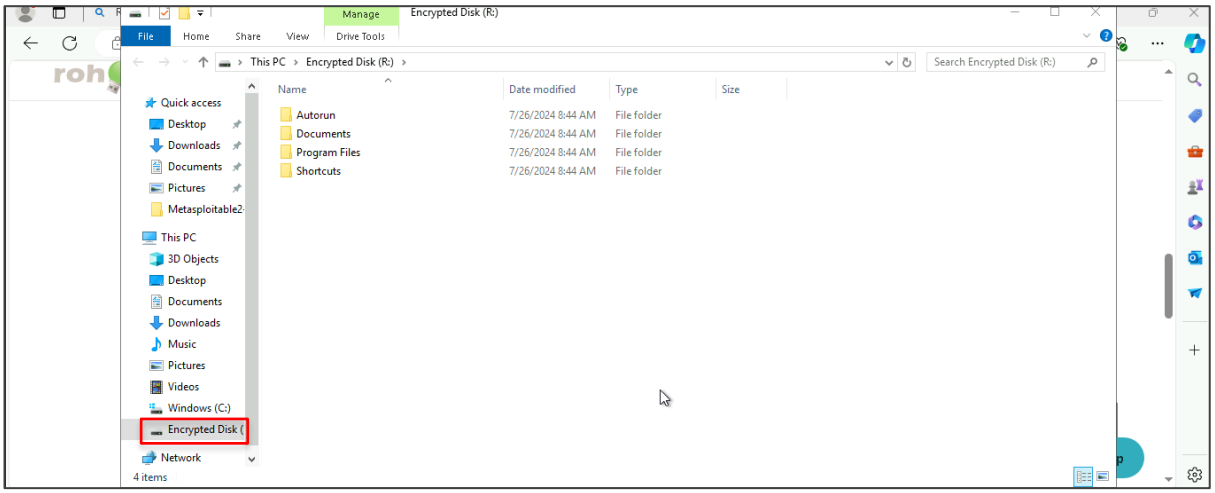


2.3 Provide a password for the new encrypted disk in the **Specify a new password to access the disk** field, confirm it in the **Confirm password** field, and click **Create disk**

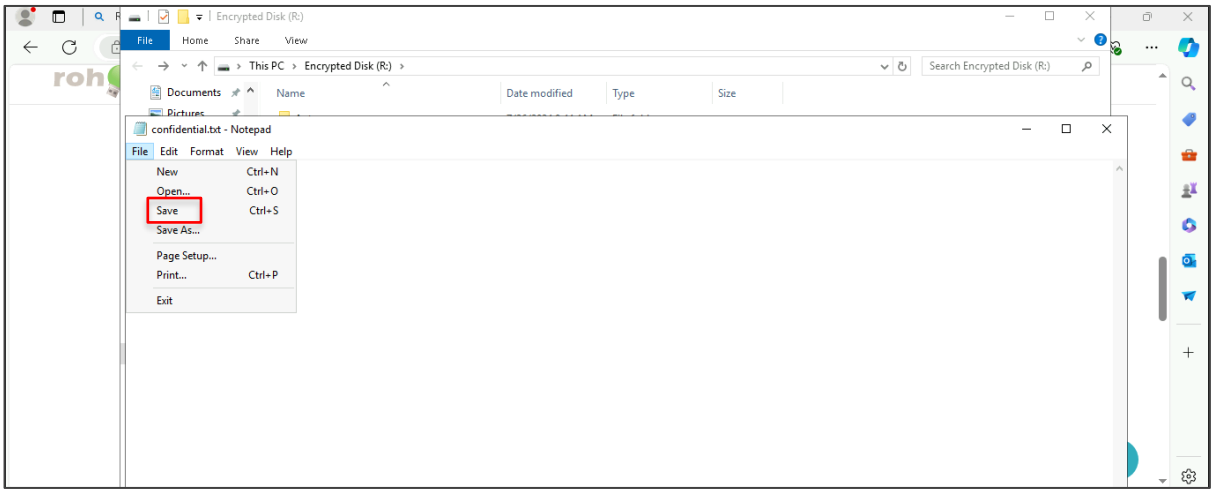


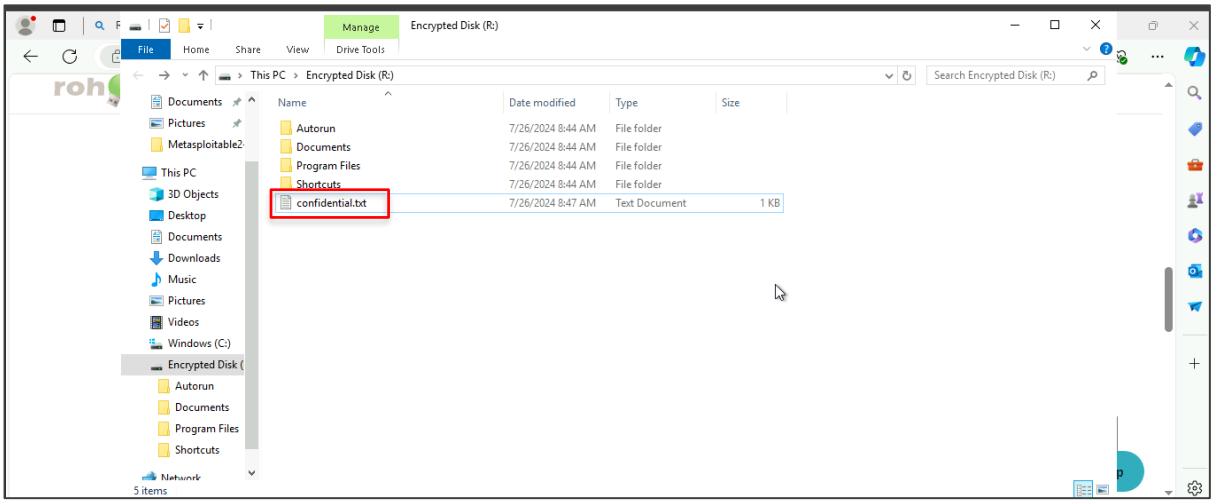
Wait for the encrypted volume to be created. The time taken will depend on the specified disk size.

Once created, the encrypted disk will appear as an **Encrypted Disk**; you can store sensitive files here.

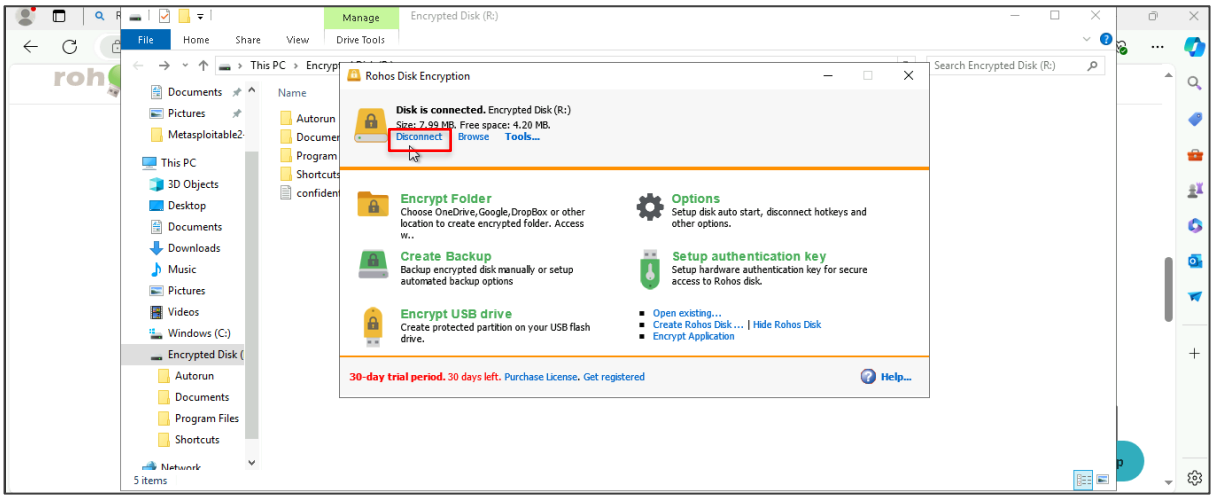


2.4 To store files securely, create a text file named **confidential.txt**, add content, save it, and copy it to the encrypted disk

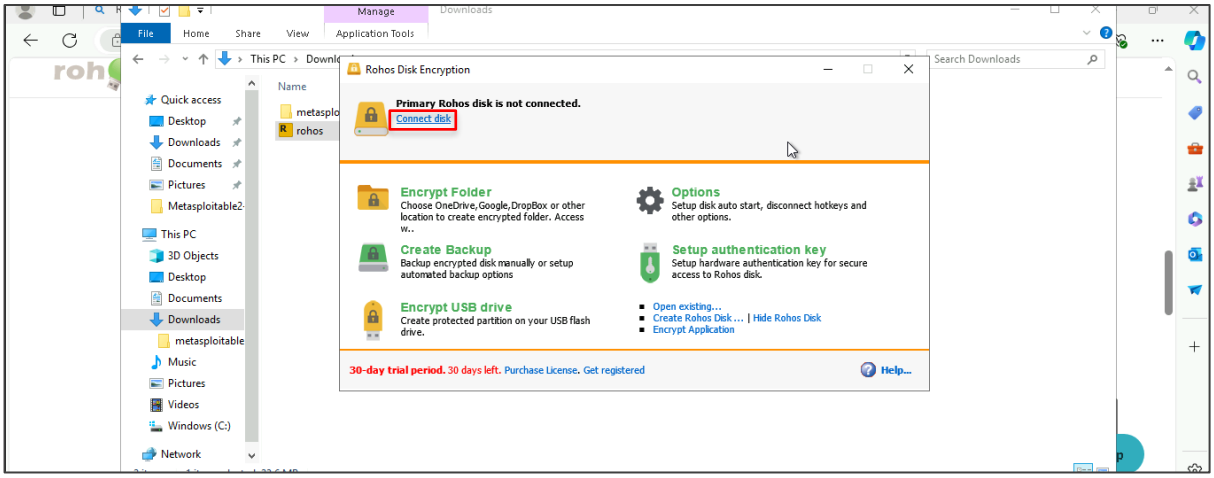


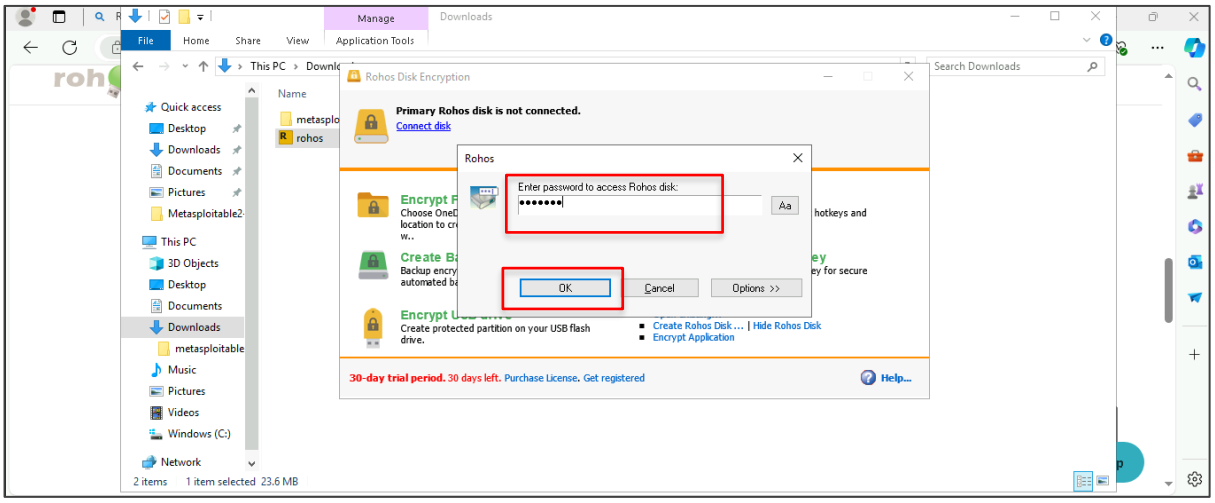


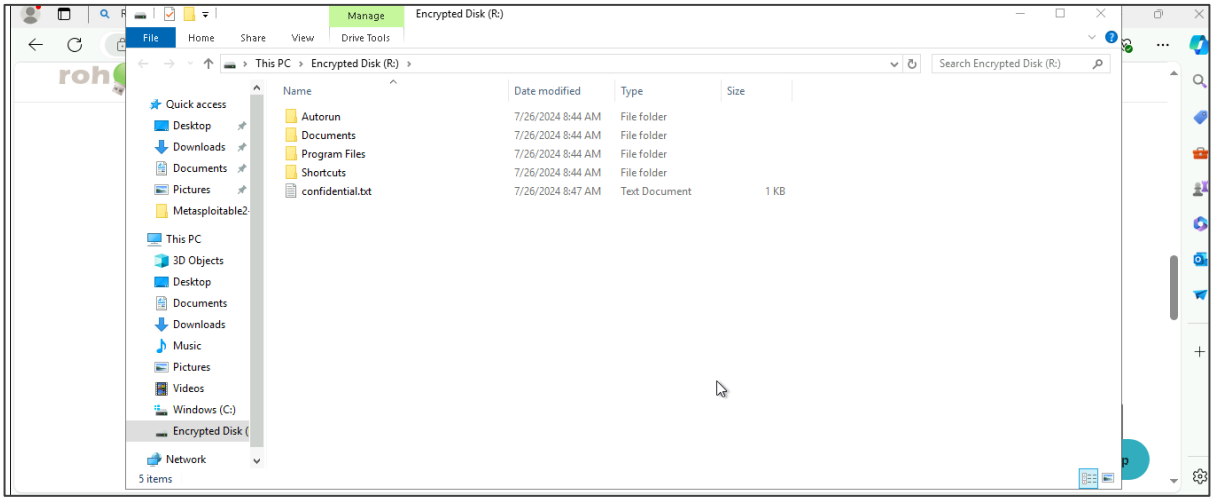
2.5 In the Rohos Disk Encryption window, click **Disconnect** to dismount the encrypted disk



2.6 To access the disk again, click **Connect disk**, enter the password, explore the contents as needed, and click on **OK**







By following these steps, you have successfully installed Rohos Disk Encryption, created an encrypted virtual drive, and secured your data. This process enhances data security by ensuring that sensitive information is accessible only with the appropriate password, thus protecting against unauthorized access.