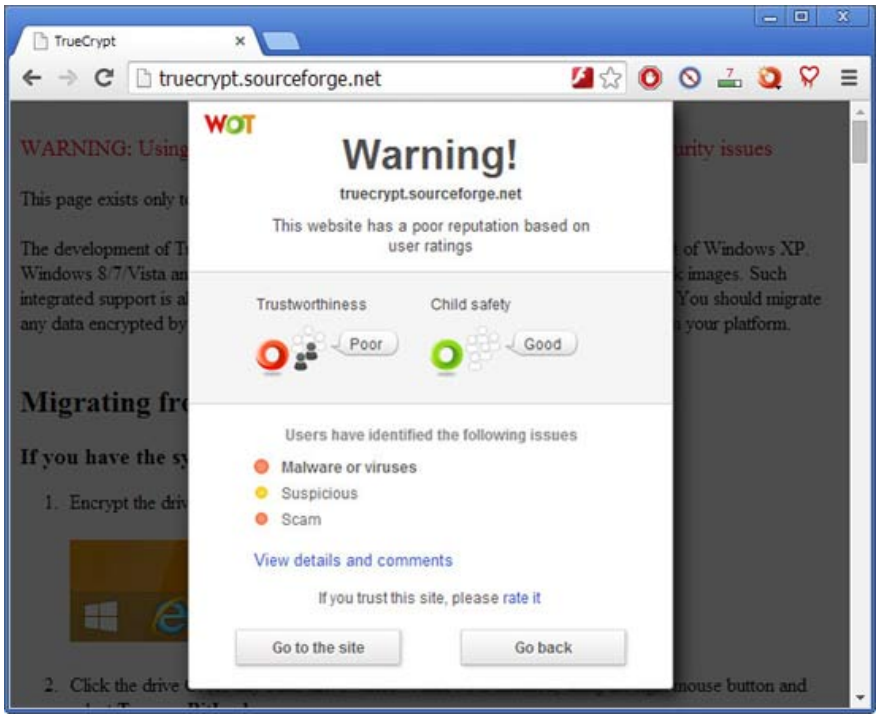
TrueCrypt encourages users to take other key measures

Unfortunately for fans of popular encryption software, TrueCrypt on the program's official website has a red text warning that TrueCrypt is no longer safe to continue using. The text is highlighted in red immediately after opening the Sourceforge homepage of TrueCrypt, explaining that due to unresolved security errors.

Unfortunately for fans of popular encryption software, TrueCrypt on the program's official website has a red text warning that TrueCrypt is no longer safe to continue using.

The text is highlighted in red when opening the **Sourceforge** homepage of TrueCrypt, explaining that due to unresolved security errors, **TrueCrypt is** no longer a secure encryption software - " ***WARNING: Using TrueCrypt is not secure as it may contain unfixed security issuee*** ".



Even if you access the TrueCrypt homepage on Google Chrome using the WOT plugin, the above warning will appear

Just below this text, the application developer further informed that the home page exists for the sole purpose of helping users transmit TrueCrypt-encoded data to another solution, such as feces. encrypted region or virtual

disk image. At the same time, the site claims that TrueCrypt stopped growing in May 2014 after Microsoft officially stopped supporting Windows XP.

This statement of TrueCrypt surprised many people.

After more than a decade of development, this free open source encryption tool has been used by many people to protect sensitive files or even encrypt the entire computer partition.

Even in 2013, when allegations were made that the NSA could decrypt a lot of encrypted information on the Internet, TrueCrypt supporters donated a large sum of money to prove that the software was extremely safe. all. The results of phase 1 of the audit show that there is no evidence of data leakage from TrueCrypt. This may indicate the user's preference for this encryption tool.

Despite being loved and widely used, but after the statement of TrueCrypt, we encourage users to switch to a new protection measure.

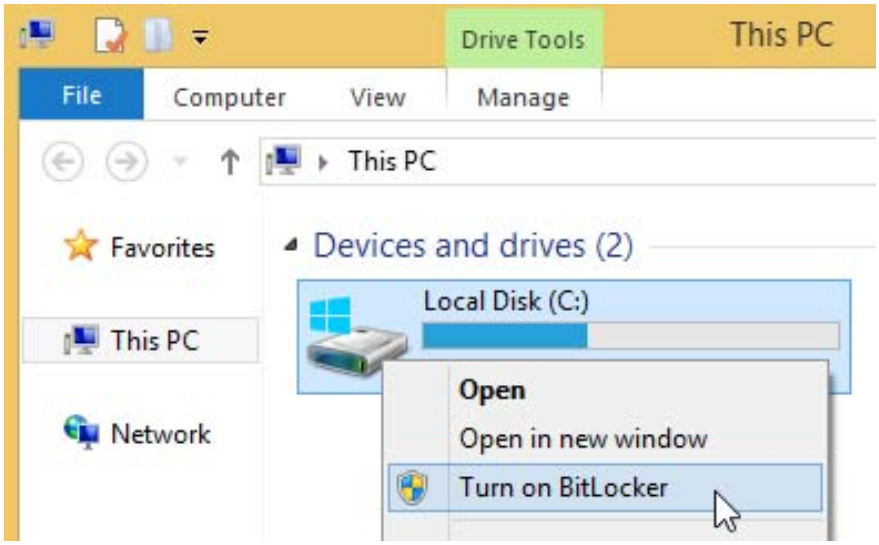
Specifically, on the TrueCrypt home page, in addition to information about the level of TrueCrypt security, the developer also gives instructions to **transfer encrypted data from TrueCrypt to another Microsoft protection solution, BitLocker** .

You can follow the following instructions to transfer data:

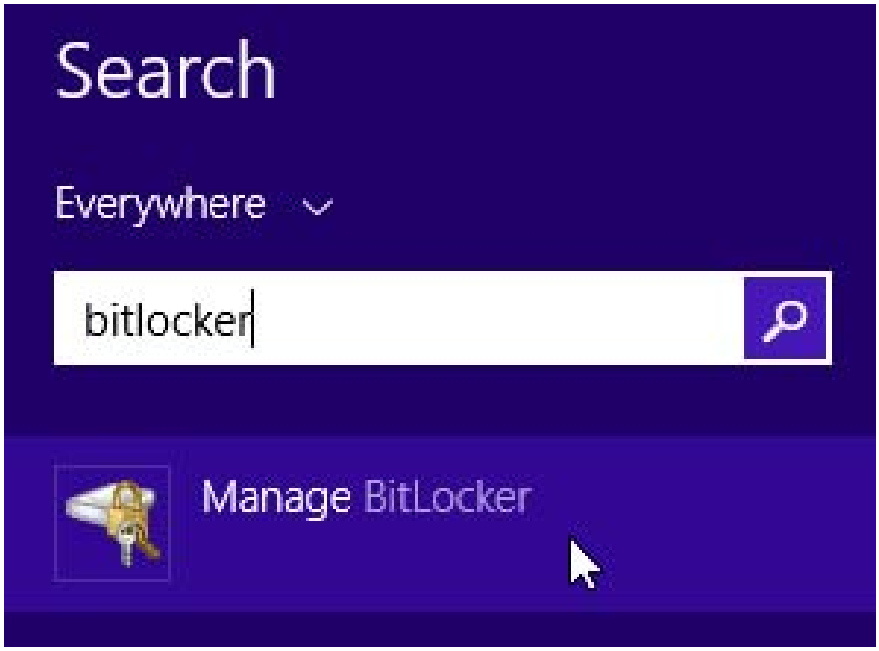
If the user is already using TrueCrypt to encrypt the system partition on the machine, the following instructions can be followed:

Step 1 : Open **Windows Explorer** window.

Step 2: Right-click on drive C (*or another drive where you installed Windows*) and select **Turn on BitLocker** . You have successfully transferred that encryption information to the protection of **BitLocker** .



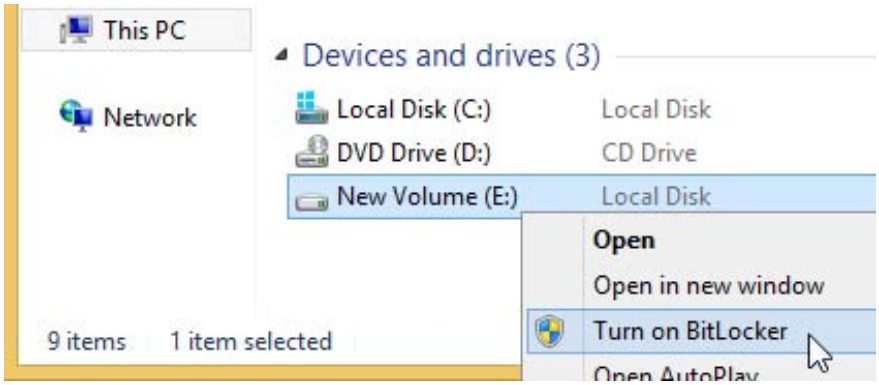
Another way to open **BitLocker** is to search for this keyword in the **Start** menu.



Step 3 : Finally, decrypt the computer hard drive with **TrueCrypt** : access the **System** menu and use the option **Permanently Decrypt System Drive.**

On the other hand, if there is no hard drive encrypted with TrueCrypt on the user's computer, you can follow the instructions below :

Step 1 : If the user has a hard drive that is large enough to store all of the encrypted data that you want to transfer to **BitLocker** , you can directly encrypt the drive in BitLocker. You can do this very easily: right-click the drive and select **Turn on BitLocker** . You need to have administrative rights to use this option.



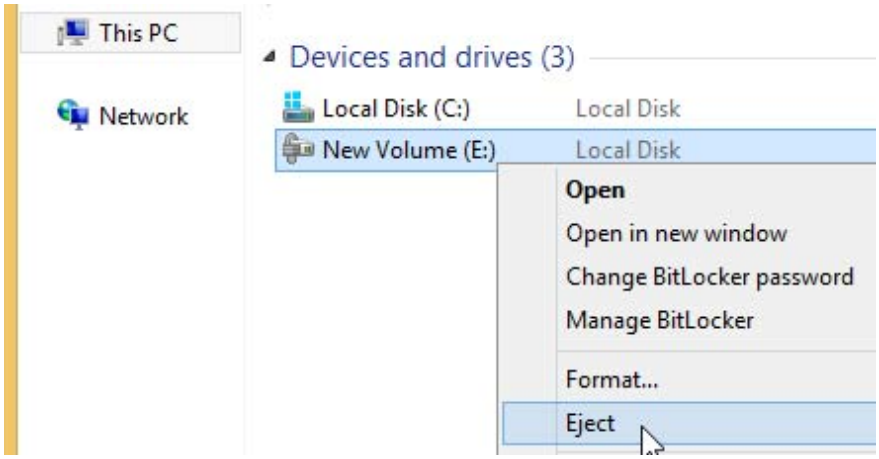
Step 2 : Copy all data from the hard drive encrypted by TrueCrypt to the hard drive encrypted by BitLocker.

In case the user does not have an empty hard drive on the user's computer, just **decrypt the encrypted TrueCrypt drive** . To do this, select the hard drive in the **TrueCrypt** window, open the **Volumes** menu and select **Permanently Decrypt** .

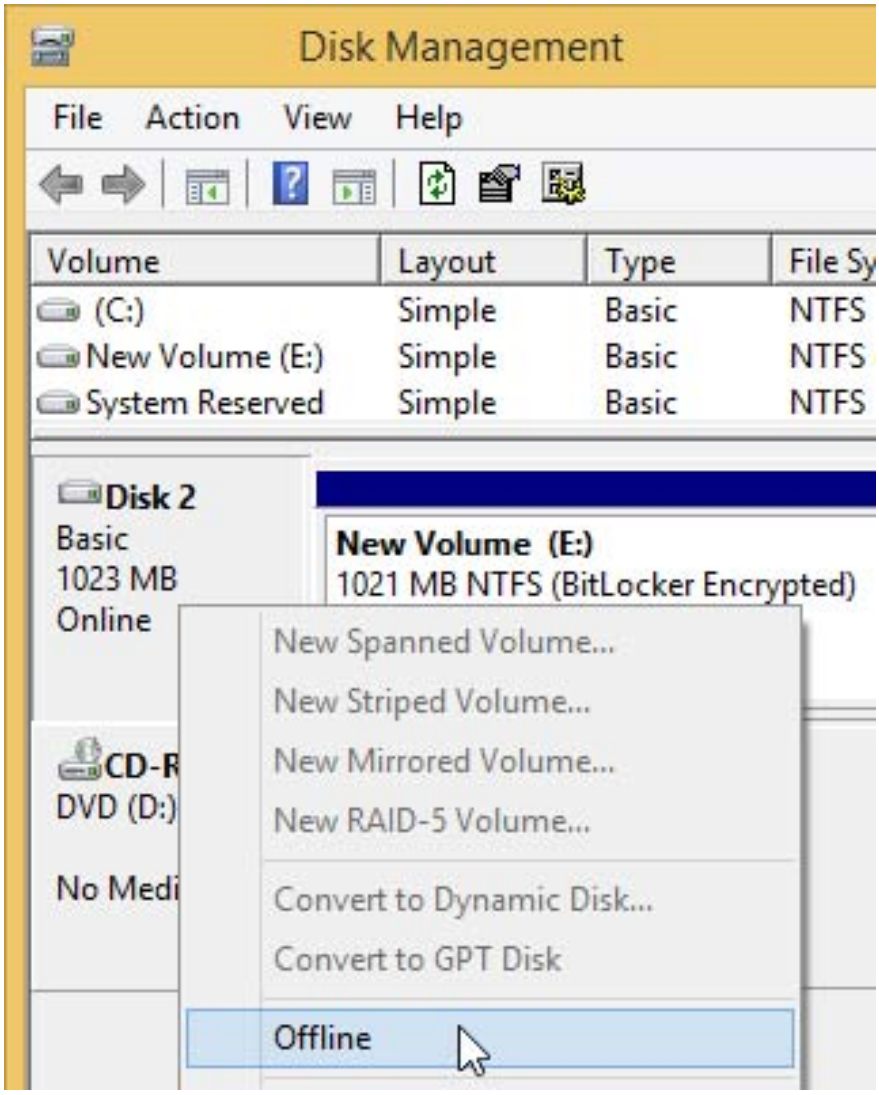
Next, users only need to re-encrypt the drive with **BitLocker** .

To install a drive encrypted by **BitLocker** , users only need to open the partition in **Windows Explorer** .

To uninstall a removable drive encrypted by **BitLocker** , right-click on the drive or click the **Safely Remove** icon on the toolbar and select **Eject** .



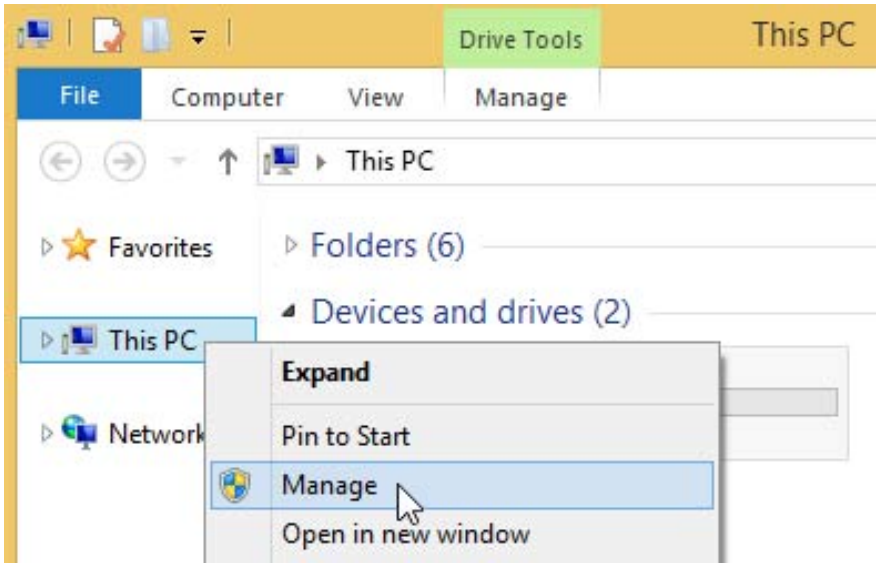
To uninstall a fixed drive protected by **BitLocker** , you can use the **Offline** option in the right-click menu of the drive in the **Disk Management** window **.**



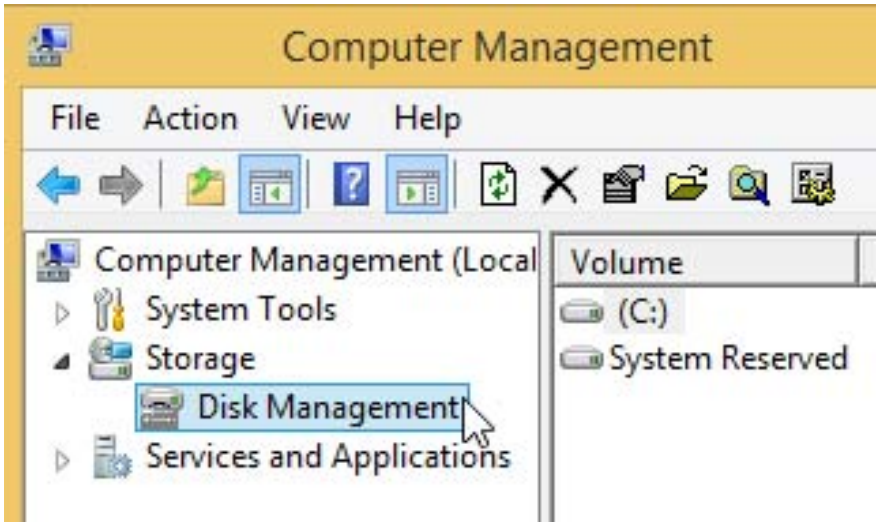
To reinstall the disk, use the **Online** option.

If the user has a folder containing files protected by TrueCrypt, follow the instructions below:

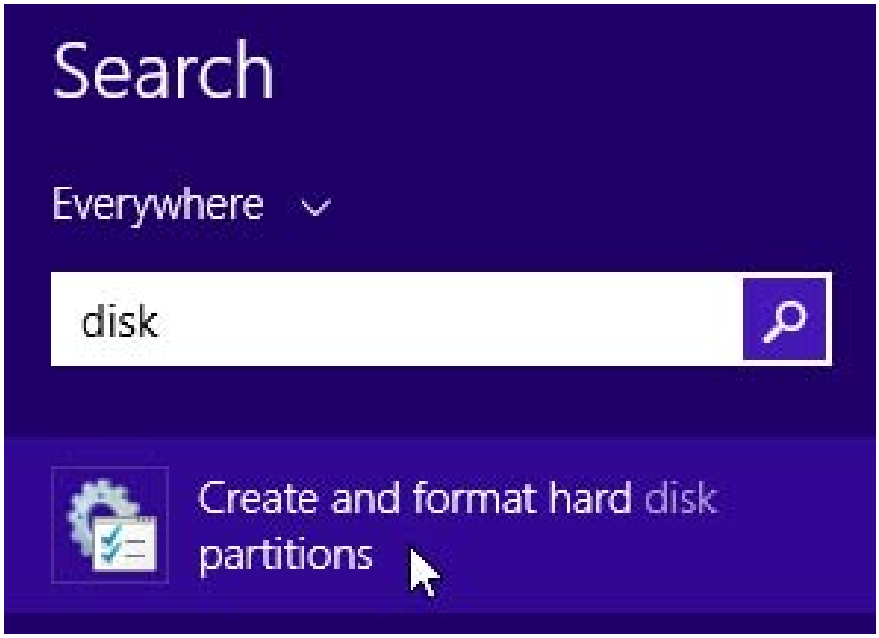
Step 1: Open the **Computer Management** window by right-clicking on the **Computer** or **PC** icon and selecting **Manage** .



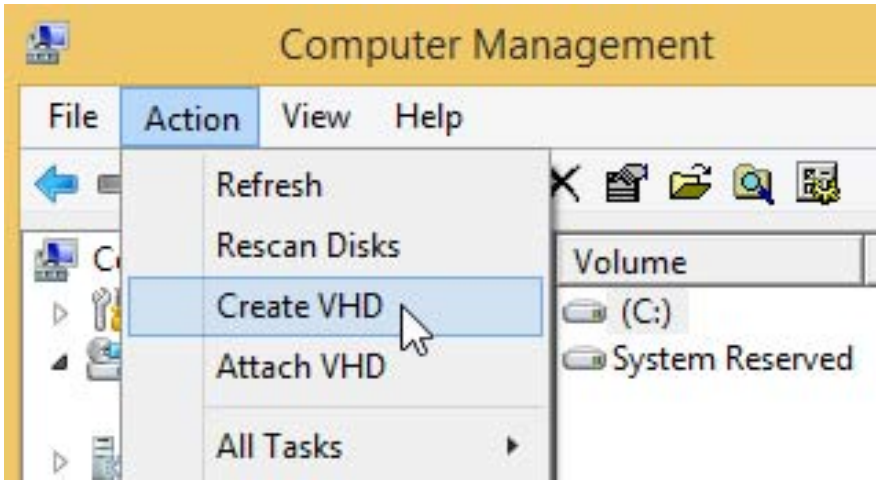
Step 2 : Select the **Disk Management** icon.



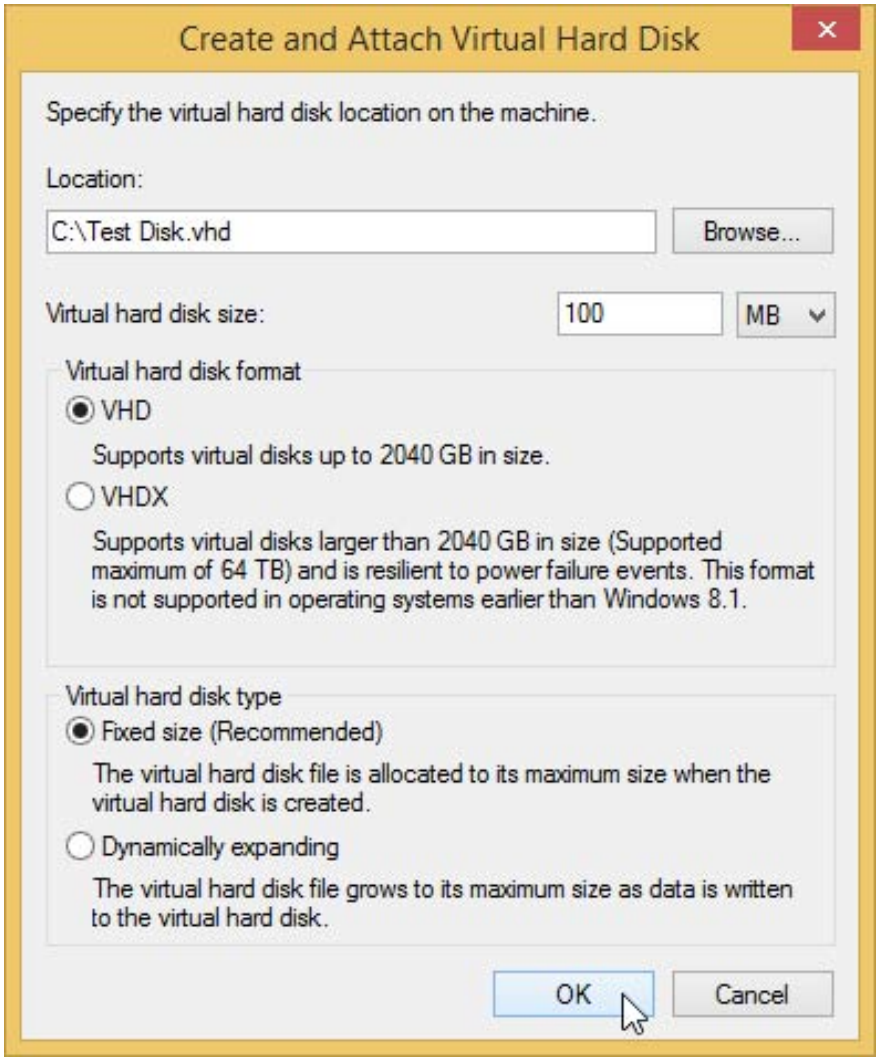
Another way is to search in *Search Charm* with the keyword " **disk** ".



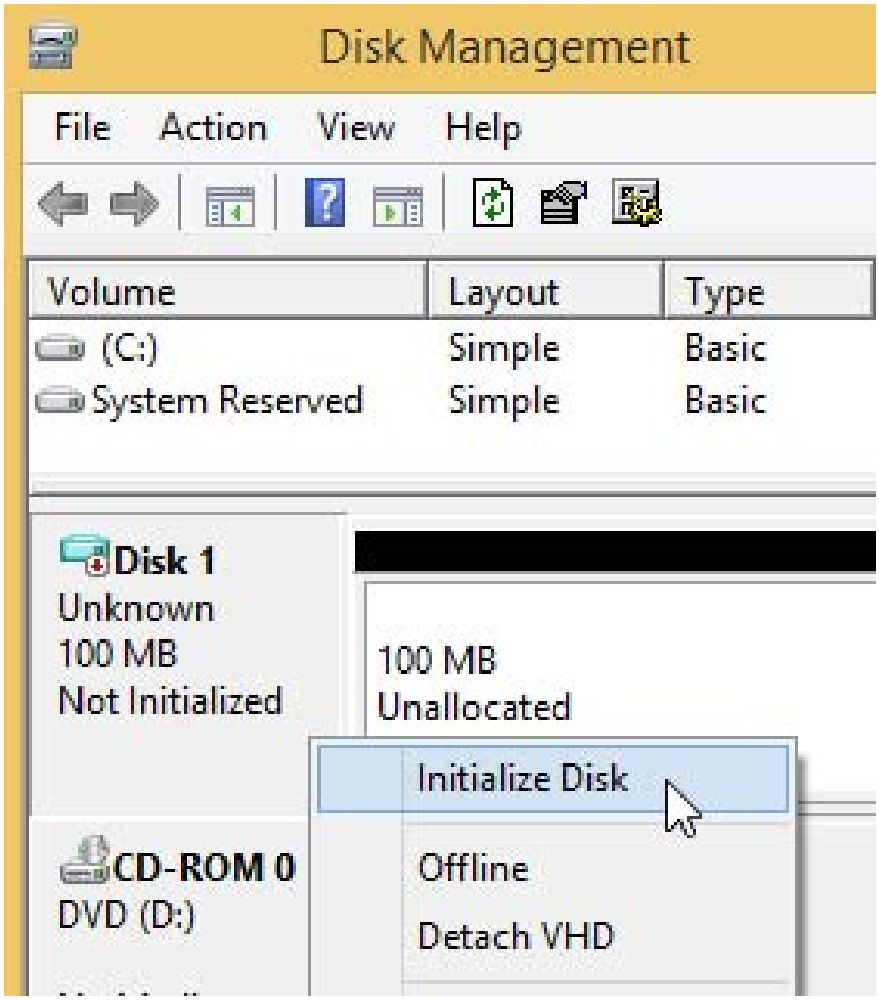
Step 3: Open the **Action** menu in the **Disk Management** window and select **Create VHD** to create a new virtual drive file.



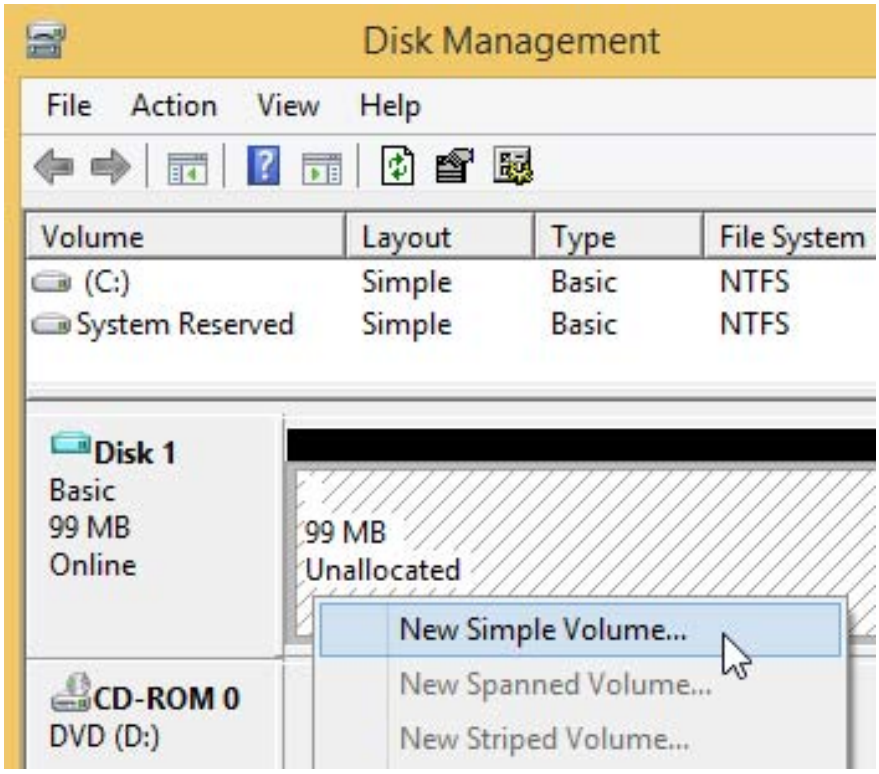
Step 4 : Create and attach a new virtual disk file.



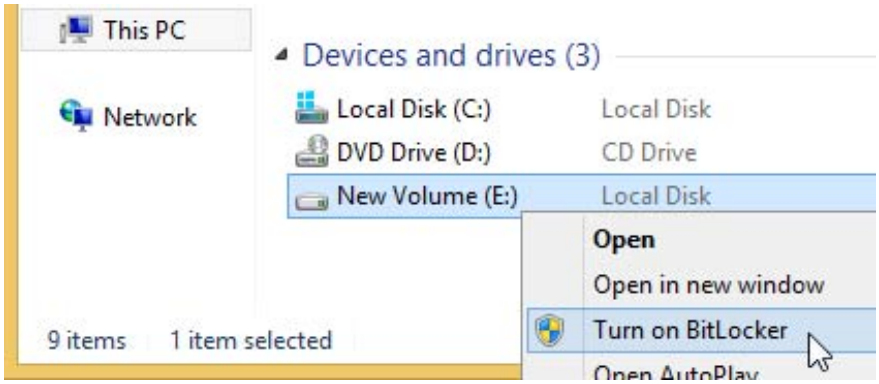
Step 5: Start the new virtual drive: **Right-click the new drive icon** and select **Initialize Disk** .



Step 6 : Create a partition on the virtual drive: Right-click the unused volume on the virtual drive and select **New Simple Volume** .

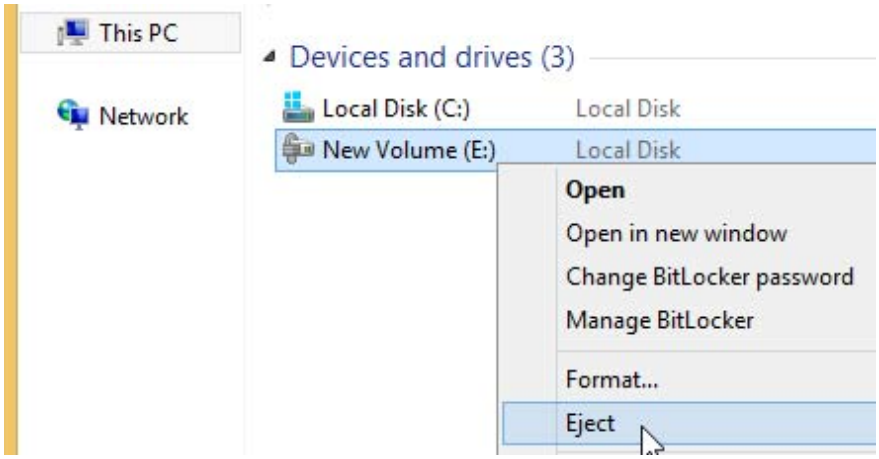


Step 7 : Encrypt the new virtual drive with **BitLocker** : **Right-click the virtual drive** in Windows Explorer and select **Turn on BitLocker** .

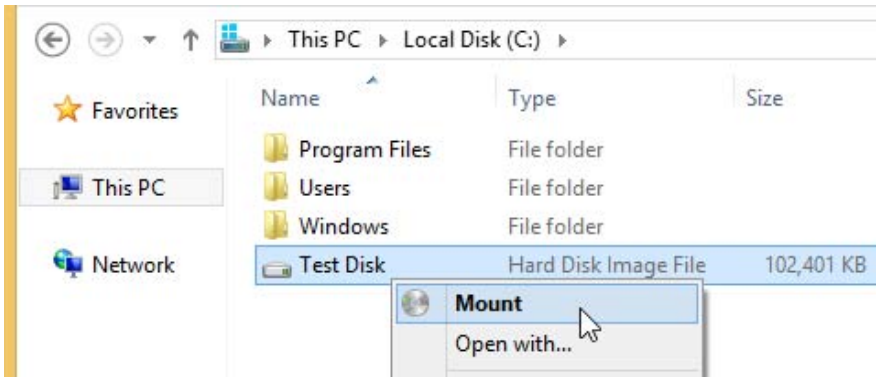


Step 8 : Copy all data folder containing **TrueCrypt** file that has been installed to the newly created virtual drive.

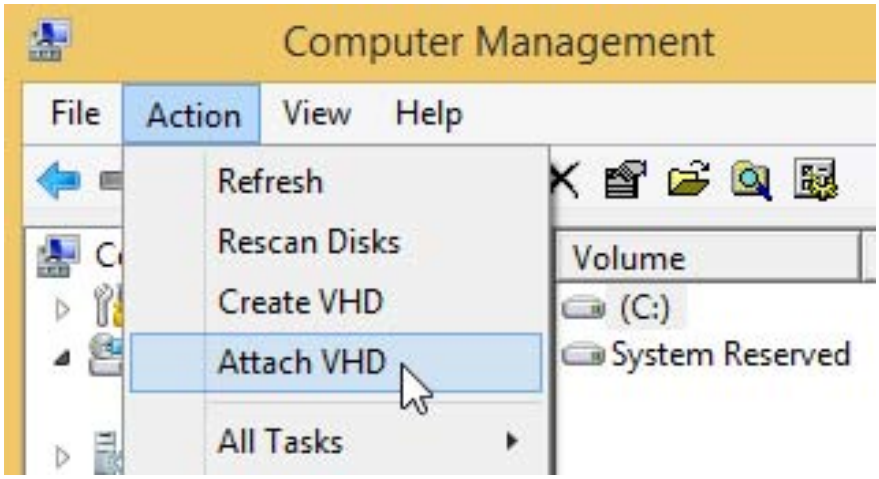
To uninstall the drive, right-click the drive and select **Eject** .



To reinstall the drive again, double click on the virtual drive file (*requires a Windows 8 or later computer*).

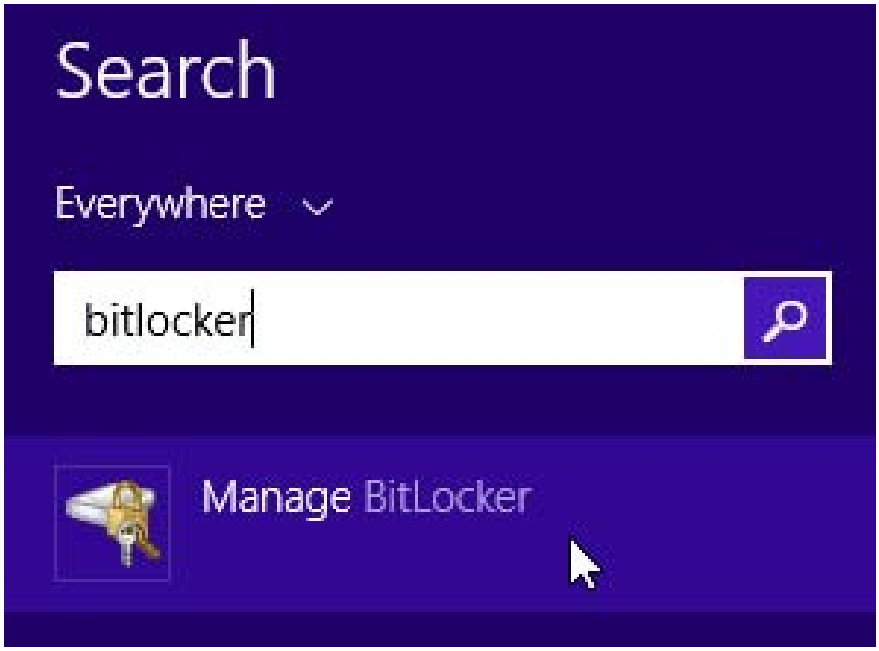


Alternatively, you can access **Disk Management** => **Action** => **Attach VHD** .

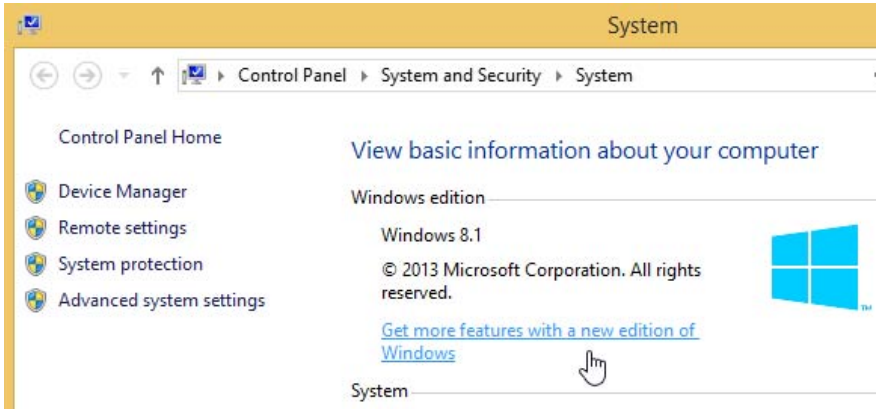


How to fix if you don't see the BitLocker icon in the right-click menu:

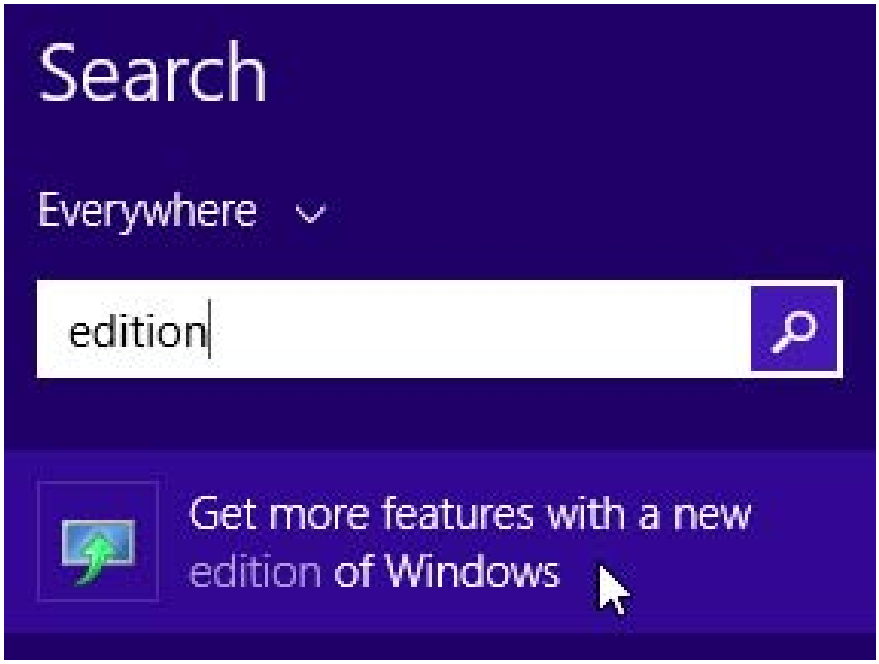
Method 1 : Search for **BitLocker** or **encryption** in the **Start** menu.



Method 2: Access **System Control Panel => Get more features with a new edition of Windows** . This operation will not require users to reinstall Windows.



Alternatively, you can search for this option using the keyword **Edition** .



Thuy Van

You finished reading the article "**TrueCrypt encourages users to take other key measures**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
