

Cybersecurity

Windows 7 Personal File Encryption



Windows 7 Personal File Encryption Lab

- Materials needed
 - Windows 7 Virtual Machine (Either Enterprise or Ultimate edition)
- Software Tool used
 - EFS
 - TrueCrypt



Objectives Covered

- Security+ Objectives (SY0-601)
 - Objective 2.1 – Explain the importance of security concepts in an enterprise environment
 - Data protection
 - Encryption



What is encryption?

- Encryption is taking normal, plaintext, and applying some sort of mathematical algorithm on it to make it look random. This random looking string is known as ciphertext.
- Simple examples of encryption include a Caesar Cipher (shifting each letter a set amount in the alphabet), old newspaper Cryptoquips, and even the Enigma which the Germans used in WWII.
- The purpose is to protect data so even if someone gains access to the data, they won't be able to understand it.



Windows 7 Personal File Encryption Lab

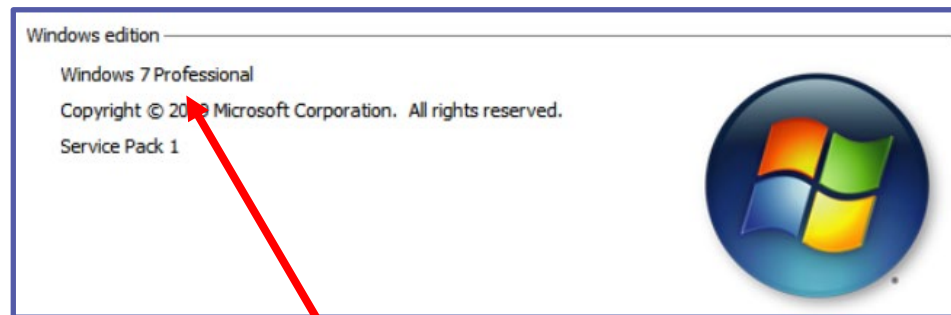
1. Setup VM environment and Verify Version
2. Create a File
3. Encrypt the File and Folder with EFS
4. Verify the Folder is Encrypted
5. Decrypt the Folder
6. Download and Install TrueCrypt
7. Create, Encrypt, and Mount a Container
8. Add a File in the Container
9. Mount on a Different Drive and Verify Contents



Setup Environments

- Log into your range
- Open the Windows 7 Environment
 - You should be on your Windows 7 Desktop
- Click the Start button, right-click "Computer", then click "Properties"

As long as your edition is NOT Home, this lab will work.

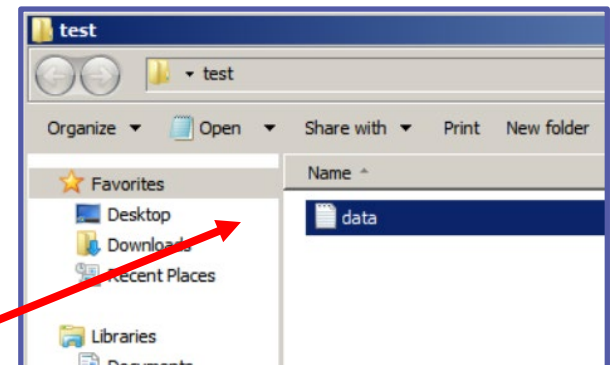


**Verify that this is not the
"Windows 7 Home Edition"**



Create a Folder and File

- On the desktop, right-click, select New, then select Folder
- Name the folder, "test"
- Open the test folder, right-click, select New, then select Text Document
- Name the text document, "data"

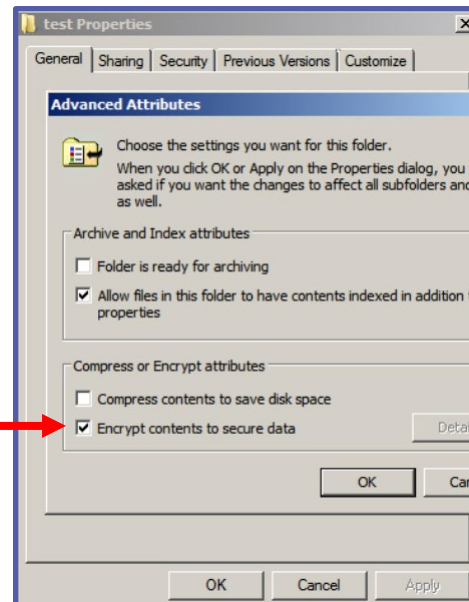


You should have a data text file inside of the test folder



Encrypt the File and Folder with EFS

- Back on the Desktop, right-click the test folder and click "Properties"
- Click "Advanced"
- Select the box for "Encrypt contents to secure data"
- Click "OK" (thrice)



Select the "Encrypt contents to secure data" option

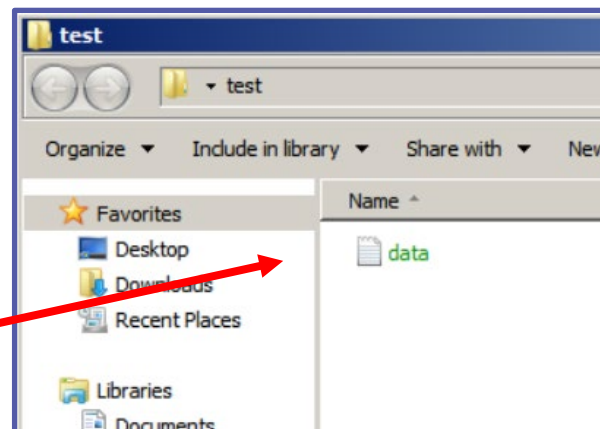


Verify the Folder is Encrypted

Because this folder and file were encrypted on your computer, it may be hard to know if it is actually encrypted. If you were to send a copy of this folder (say through email), the recipient would not be able to access it.

You know the contents are encrypted because the text for data is green

If you try to create a new file, it will also be green, meaning the contents are automatically encrypted within the test folder.



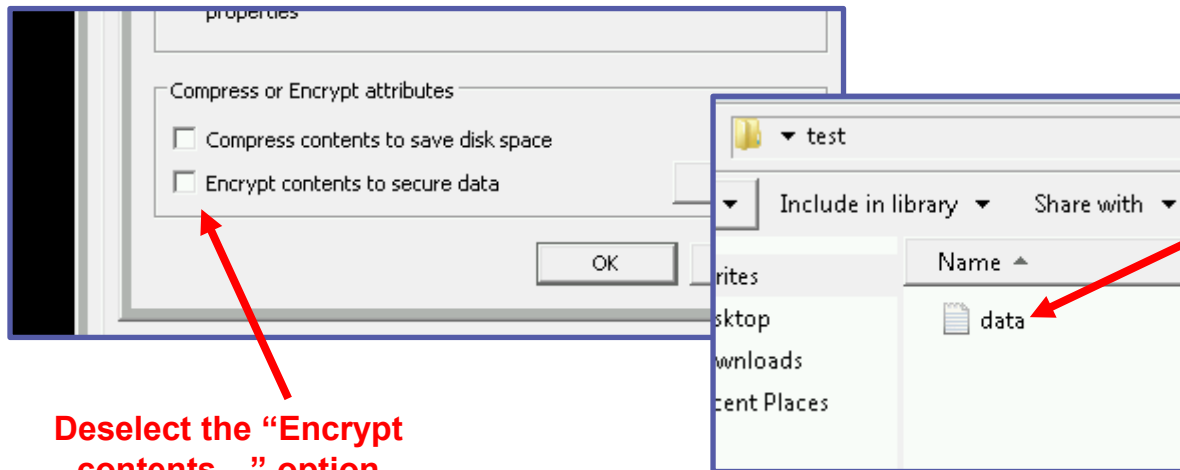
Verify the file is green, meaning that it is encrypted



Decrypt the Folder

- Back on the Desktop, right-click the test folder and click "Properties"
- Click "Advanced"
- Un-select the box for "Encrypt contents to secure data"
- Click "OK" (thrice)

The data file will no longer be green and any new files within the test folder will not be encrypted. This could only be encrypted on the same computer because the EFS key used to encrypt was stored locally.



Deselect the "Encrypt contents..." option

Verify the file is no longer green, thus no longer encrypted



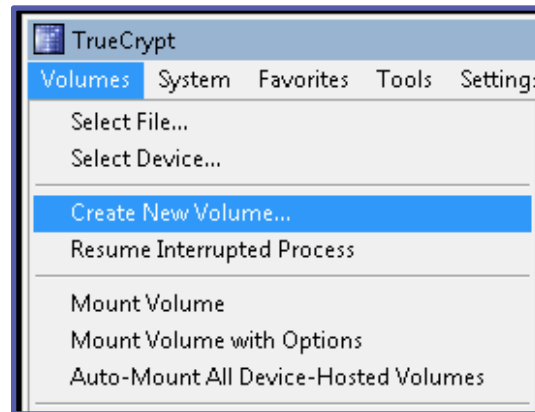
What is TrueCrypt?

TrueCrypt is a discontinued (because of security flaws) source-available freeware utility used for on-the-fly encryption. For this lab, we will use it to create and encrypt a container. In the real-world, this software (and others like it) can be used to encrypt the whole drive. Unfortunately, cyber ranges limit boot privileges so we will not be able to encrypt the whole drive in this lab.

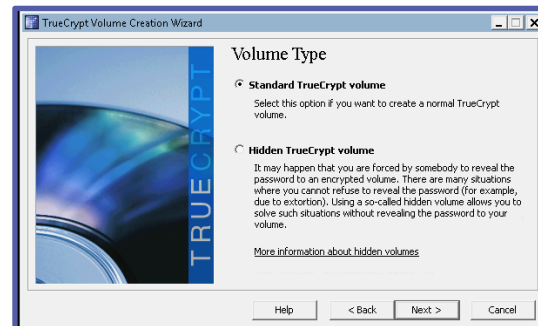
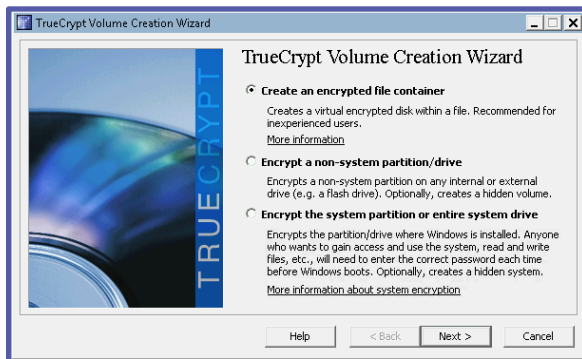


Create, Encrypt, and Mount a Container

- Click the Start button, then open TrueCrypt
- Click "Volumes" then click "Create New Volume..."



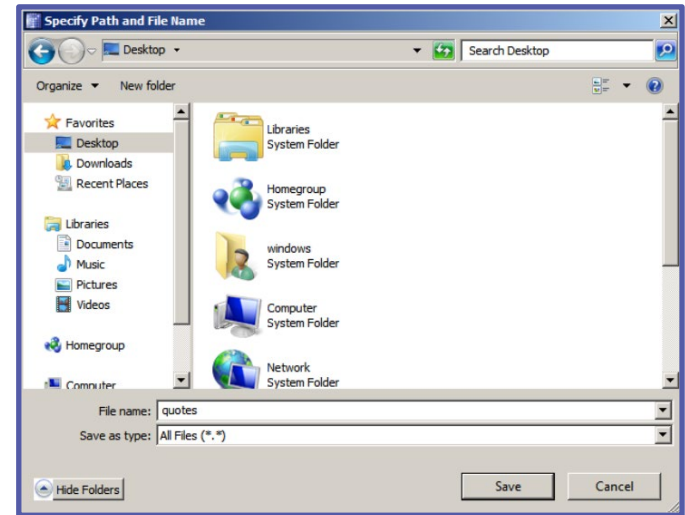
- Click "Next" (twice)



Create, Encrypt, and Mount a Container

- Click "Select File..."
- Click "Desktop"
- Name the container "quotes"
- Click "Save" then "Next"
- Click "Next"

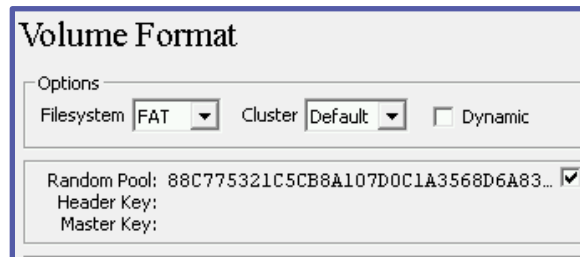
The default encryption settings are fine for the purposes of this lab.



Create, Encrypt, and Mount a Container

- Enter 80 (MB) for the container size and click "Next"
- You'll be asked to create a password, enter whatever you'd like but you need to remember it, we chose "password". Click "Next"

Notice the "Random Pool" is constantly changing, this is generating randomness so each user would have a unique encryption even if the contents are identical



Volume Format

Options

Filesystem Cluster Dynamic

Random Pool: 88C775321C5CB8A107D0C1A3568D6A83...

Header Key:

Master Key:

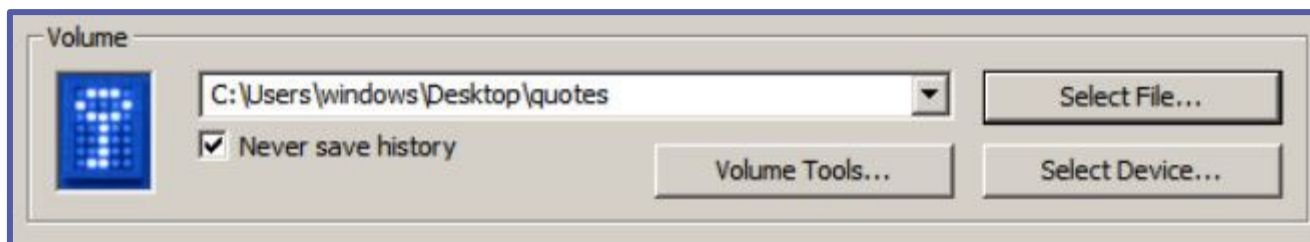


Create, Encrypt, and Mount a Container

- Click "Format", "OK", then "Exit"

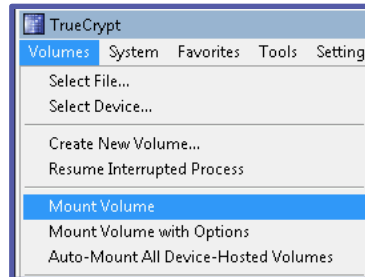
A container, with a paper icon titled "quotes" should appear on the Desktop. If you attempt to open it, regardless of the software options listed, e.g. Internet Explorer, Windows Media Center, etc., nothing will "work"

- Back within the TrueCrypt GUI, click "Select File" then chose the "quotes" container

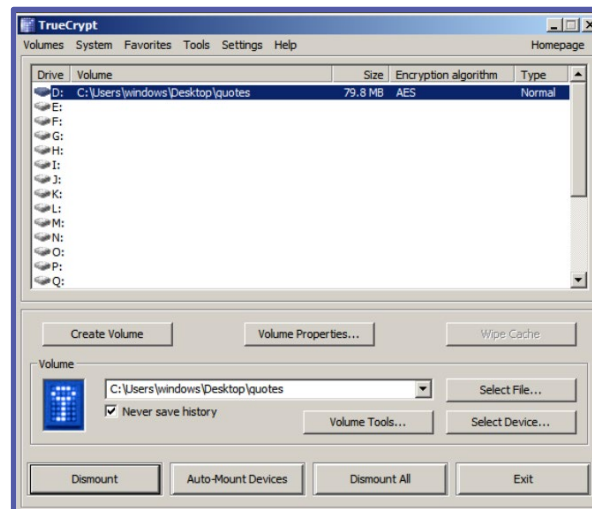


Create, Encrypt, and Mount a Container

- Click "Volumes" then "Mount Volume"



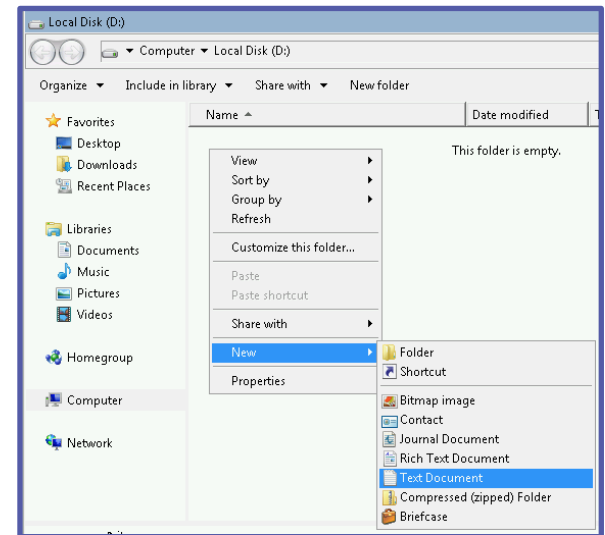
- With the "D:" drive selected, click "Mount" on the bottom. You will be prompted for the password you created.



Add a File in the Container

- Now we can utilize the container. Double click
D: C:\Users\windows\Desktop\quotes
(Yours may look slightly different depending on the username)
- Within the GUI that popped up, right-click, scroll to "New", then select "Text Document"
- Name the file "FavoriteQuotes"

This can only be accessed with the TrueCrypt software. Because of the encryption, you couldn't access it otherwise.



Add a File in the Container

- Double-click the "FavoriteQuotes" file and insert your favorite quotes
 - For example: "Wikipedia is the best thing ever. Anyone in the world can write anything they want about any subject so you know you are getting the best possible information -Michael Scott"
- Save your edit and close the text document.

Again, this information is only accessible via the TrueCrypt software, in part with the unique encryption key generated by the software.



Mount on a Different Drive and Verify Contents

- Back in the TrueCrypt GUI, with the "D:" drive selected, click "Dismount" on the bottom. Notice the container is gone and currently inaccessible.
- Choose a different drive, we chose "E:", click "Mount" and enter your password.
- Double-click the newly mounted container and verify the FavoriteQuotes file with your favorite quote

