Cybersecurity 701

Windows 7 Personal File Encryption Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Windows 7 Personal File Encryption Materials

- Materials needed
  - Windows 7 Virtual Machine

- Software Tools used
  - Microsoft Windows Encrypting File System (EFS)
  - TrueCrypt

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 1.4 – Explain the importance of using appropriate cryptographic solutions
    - Encryption
      - Level
        - File

What is encryption?

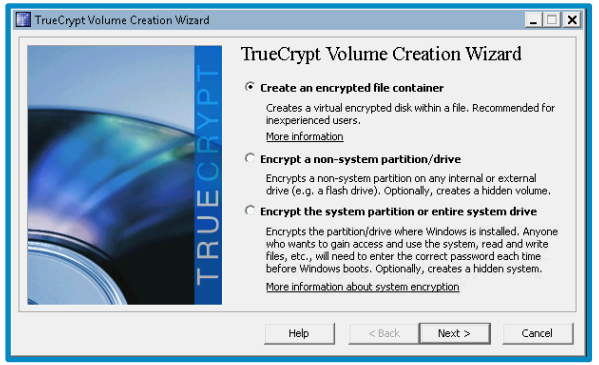
- Encryption is taking normal plaintext and applying some sort of mathematical algorithm to it to make it look random. This random-looking string is known as ciphertext.
- Simple examples of encryption include a Caesar Cipher (shifting each letter a set amount in the alphabet), old newspaper Cryptoquips,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

What are EFS and TrueCrypt

- For this lab we will use 2 encryption utilities:
  - Encrypting File System (EFS)
    - Microsoft's built-in encryption method for drives formatted with New Technology File System (NTFS)
    - Windows automatically creates and stores the certificate associated with the current user that acts as the key for encrypting/decrypting files and folders with EFS
    - Typically used to protect only some of the files and folders on a drive
    - Still in-use today
  - TrueCrypt
    - A source-available freeware utility for providing flexible encryption options
    - Supports 3 different ciphers and can run on many different operating systems
    - Can be used to encrypt an entire drive
    - Was discontinued in 2014 due to security flaws

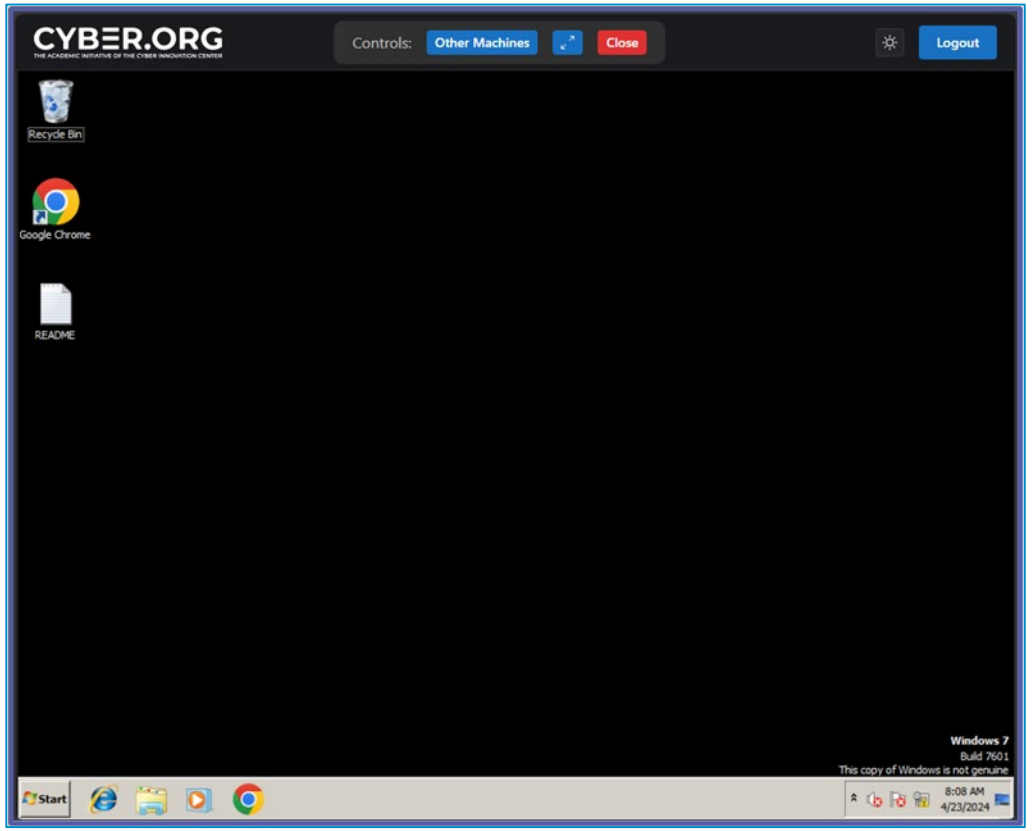
Windows 7 Personal File Encryption Lab Overview

1. Set up the Windows 7 VM environment
2. Create a Folder and a File
3. Encrypt the File and Folder with EFS
4. Verify the Folder is Encrypted
5. Decrypt the Folder
6. Open the TrueCrypt freeware application
7. Create, Encrypt, and Mount a Volume using TrueCrypt
8. Add a File to the Volume
9. Mount on a Different Drive and Verify Contents



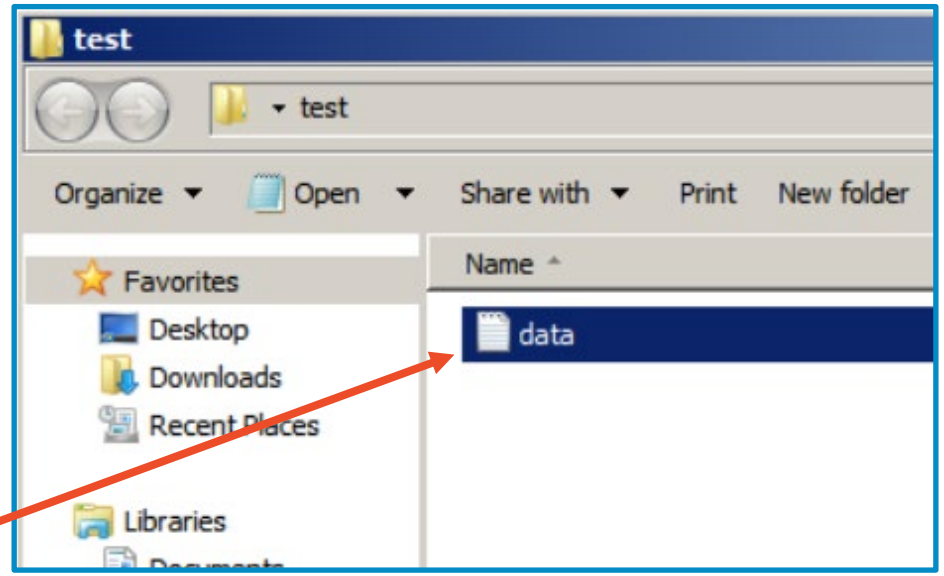
Set up Environment

- Log into the CYBER.ORG range
- Open the Windows 7 Environment



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"

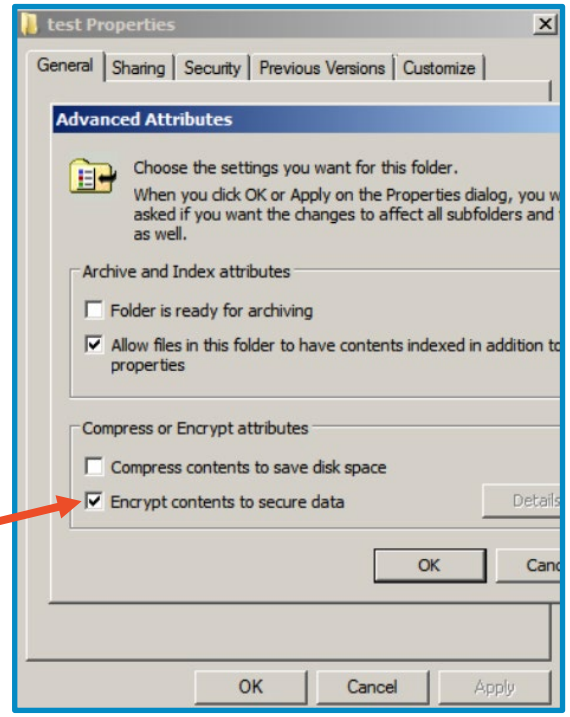


You should have a data text file inside of the test folder

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)

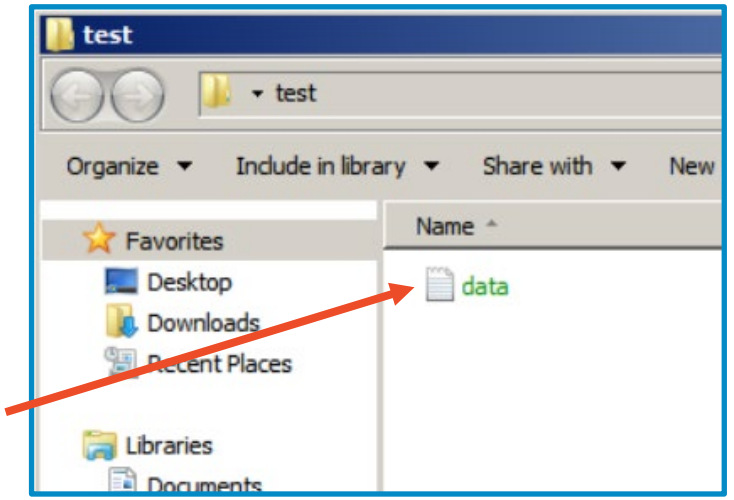
Select the "Encrypt contents to secure data" option



Verify the Folder is Encrypted

- Because this folder and file were encrypted by the operating system, it may be hard to know if it is actually encrypted
- You can know the contents are encrypted because the filename is now shown in green letters
- If you try to create a new file in an encrypted folder, it will also be green, meaning the contents are automatically encrypted

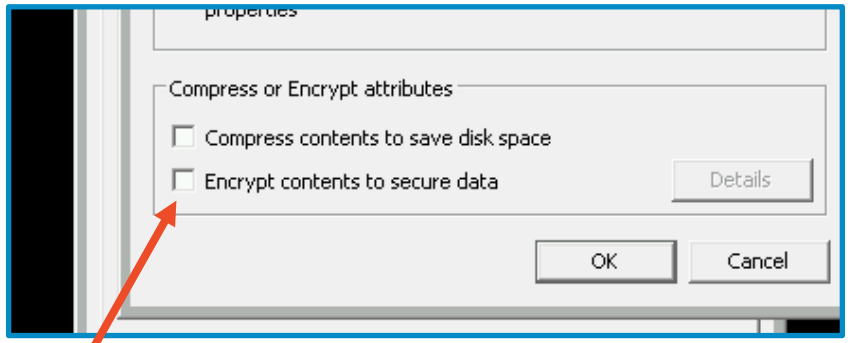
Verify the filename is green, meaning that it is encrypted



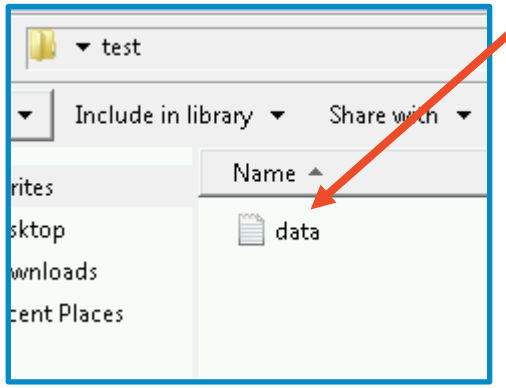
Decrypt the Folder

- 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 filename is no longer green, thus no longer encypted

What does EFS do to the data?

- Encrypting File System (EFS) is part of the New Technology File System (NTFS) included with Microsoft Windows
- Windows automatically creates a certificate associated with the user and uses it as a key to encrypt and decrypt the file/folder
- Unauthorized users cannot open, rename, move, or copy files and folders encrypted with EFS
- EFS is integrated into every version of Windows and using it is the same across all versions

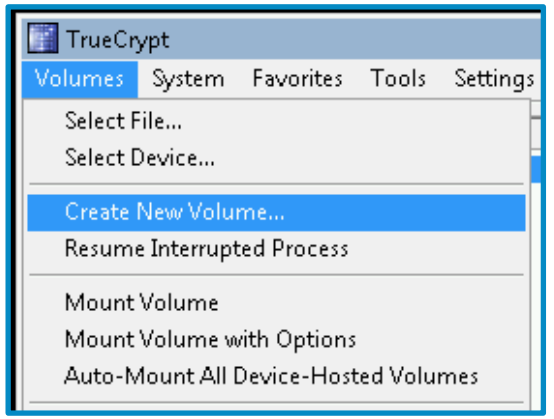
What is TrueCrypt?

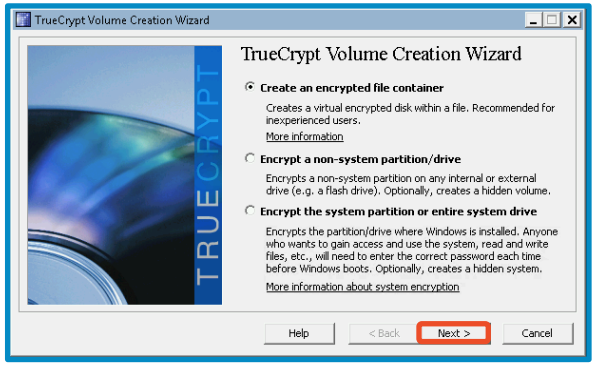
TrueCrypt is a source-available freeware utility used for encryption of files, partitions, volumes, and drives. It was discontinued in 2014 due to security vulnerabilities. TrueCrypt is pre-installed on the Windows 7 image in the cyber range.

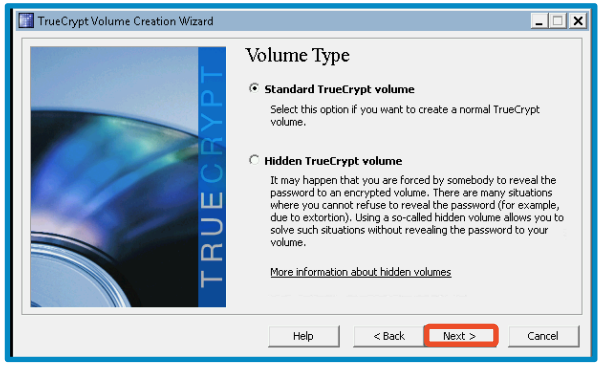
For this lab, we will use TrueCrypt to create and encrypt a volume. In the real-world, this software (and others like it) can be used to encrypt entire drives. Due to the limitations of our cyber range, we will not be able to encrypt the entire drive in this lab.

Create a Volume

- Click the Start button, then open TrueCrypt
- Select "Create New Volume..." from the "Volumes" menu
- You can read the other options, but we will "Create an encrypted file container"
- Click "Next"
- Click "Next" again to create a Standard TrueCrypt volume

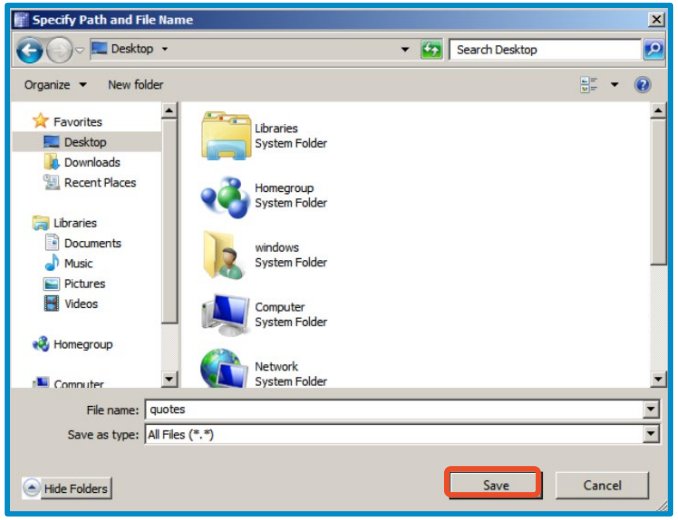






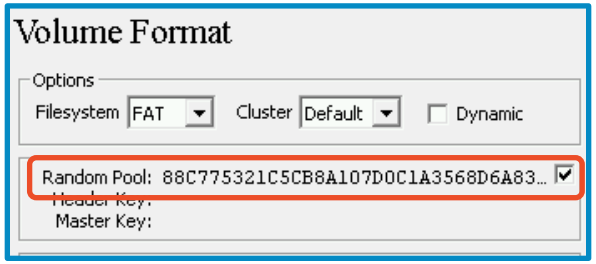
Choose Encryption Options

- Click "Select File..."
- Click "Desktop"
- Name the container "quotes"
- Click "Save" then "Next" to accept the Volume Location (Desktop)
- Click "Next" to accept the default Encryption and Hash Algorithms



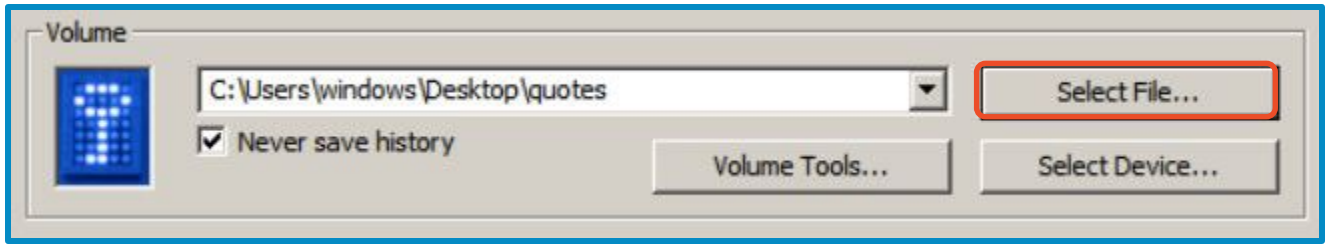
Set Volume Size and Password

- Enter 80 (MB) for the container size and click "Next"
- You can create an up-to 64-character password; for this lab, use "password" (a very bad password), but take a minute to internalize the (very good) password advice given in the window
- Click "Next" and click "Yes" to ignore the bad password warning
- Notice the "Random Pool" is constantly changing, this is generating randomness so a new volume would have a unique ciphertext even if the contents are identical



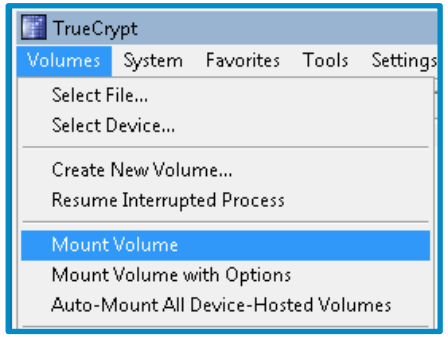
Format the Volume

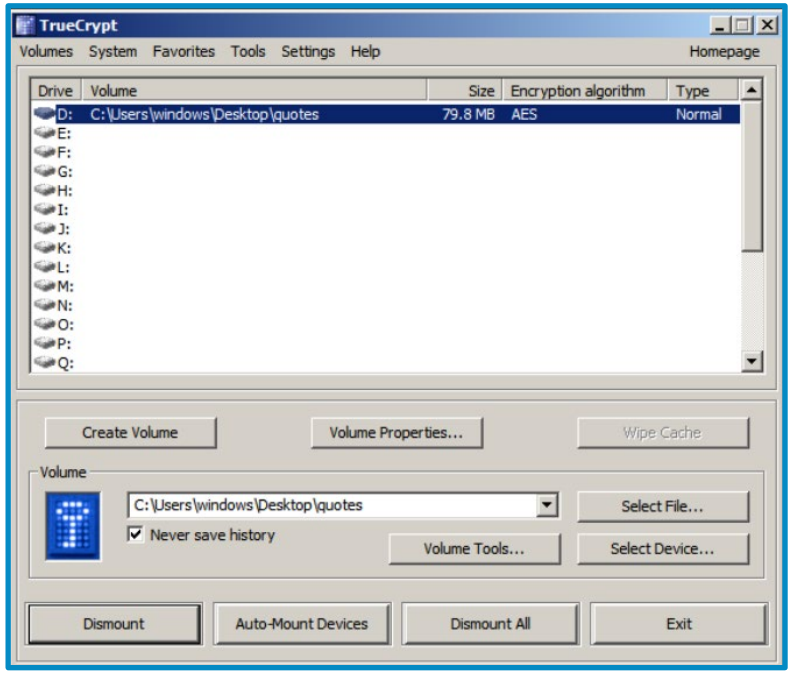
- Click "Format", "OK", then "Exit"
- A container, with a paper icon titled "quotes" should appear on the Desktop. If you attempt to open it, regardless of the software options listed, e.g. Internet Explorer, Windows Media Center, etc., nothing will "work"
- Back within the TrueCrypt GUI, click "Select File" then chose the "quotes" container (saved to the Desktop)



Mount the Volume

- Select the "D:" drive
- Select "Mount Volume" from the "Volumes" menu
- Input the password you created ("password")
- Click "OK"
- You have now mounted the volume you created as an 80MB drive labeled "D:"

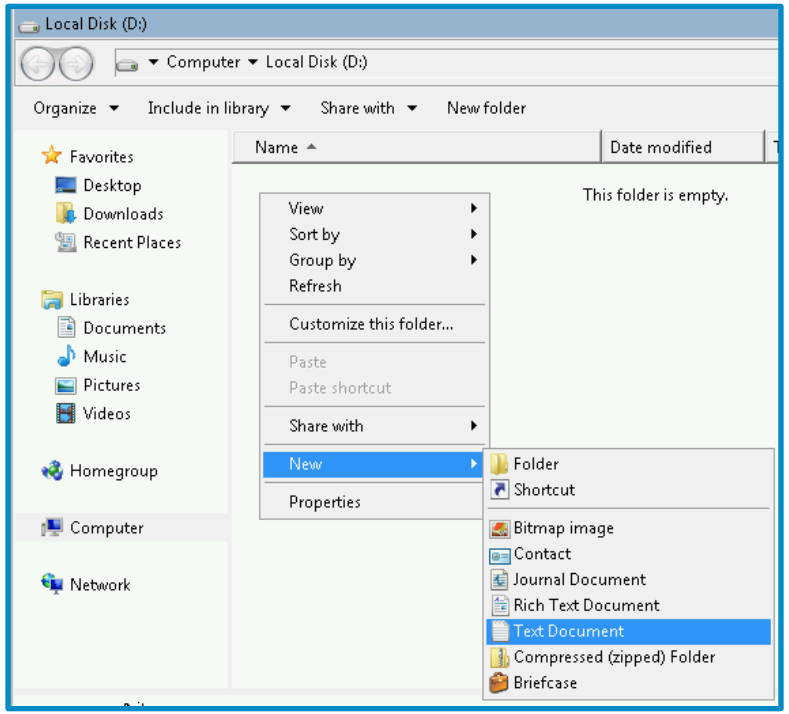




CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Save a File to Your New Encrypted Volume

- Now we can utilize the container like a drive
- In the TrueCrypt window, double click
  - D: C:\Users\windows\Desktop\quotes
- Within the blank area in the middle of the ‘Local Disk (D:)’ window, right-click, scroll to "New", then select "Text Document"
- Name the file "FavoriteQuotes"
- This .txt file is stored in the encrypted container you created; it can only be accessed using TrueCrypt and the password you chose

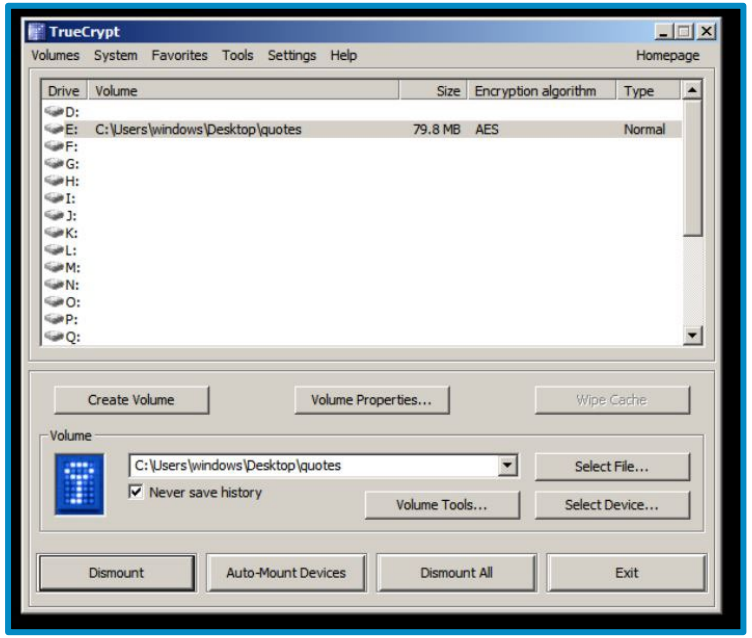


Add Some Data to Your File

- 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 combination with the correct password

Mount on a Different Drive Letter and Verify Contents

- Back in the TrueCrypt GUI, with the "D:" drive selected, click "Dismount" on the bottom
- Notice the container no longer appears in the Volume listing
- Choose a different drive letter, click "Mount" and enter your password
- Double-click the newly mounted volume and verify the FavoriteQuotes file with your favorite and now highly-protected quote



Thinking About Encryption

- Having used the built-in EFS and the installed TrueCrypt freeware application, what are some of the similarities and differences between the two?
  - Which one allows you to choose the encryption algorithm for your data?
  - Which one uses your user login to access the encryption key to decrypt your data?
- What are some situations in which you might choose one or the other?
- What are some organizations/applications that might need encryption to ensure confidentiality and integrity of their data?
- What kind of data warrants this level of protection? Why?