CompTIA Security+® Lab Series

Lab 20: Cryptography

CompTIA Security+® Domain 6 - Cryptography

Objective 6.1: Summarize General Cryptography Concepts

Document Version: 2013-08-02

Organization: Moraine Valley Community College
Author: Jesse Varsalone

Copyright © Center for Systems Security and Information Assurance (CSSIA), National Information Security, Geospatial Technologies Consortium (NISGTC)

The original works of this document were funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) at Moraine Valley Community College (MVCC).

This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. The National Information Security, Geospatial Technologies Consortium (NISGTC) is authorized to create derivatives of identified elements modified from the original works. These elements are licensed under the Creative Commons Attributions 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by/3.0/ or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

The Network Development Group (NDG) is given a perpetual worldwide waiver to distribute per US Law this lab and future derivatives of these works.

Contents

Introduction

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746. This work has been adapted by The Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

This lab includes the following tasks:

1 – Encryption with the Encrypted File System
2 – Backing up Encrypted File System Keys
3 – Encrypted File System File Recovery

Objectives: Explain the security function and purpose of network devices and technologies

Companies need to protect their internal resources. This is often done by using encryption. Encryption is a way of scrambling data so it cannot be read by others.

EFS – The Encrypted File System is a feature that can be utilized on NTFS volumes on Microsoft Windows operating systems used to protect data from being accessed.

NTFS – New Technology File System, or NTFS. An NTFS Volume is required to use EFS.

Recovery Agent – A recovery agent can recover files that were encrypted using EFS

Pfx file – A Personal Information Exchange file. It can be exported in Windows.

net user – The command allows you to view, create, and delete users in Windows.

Pod Topology

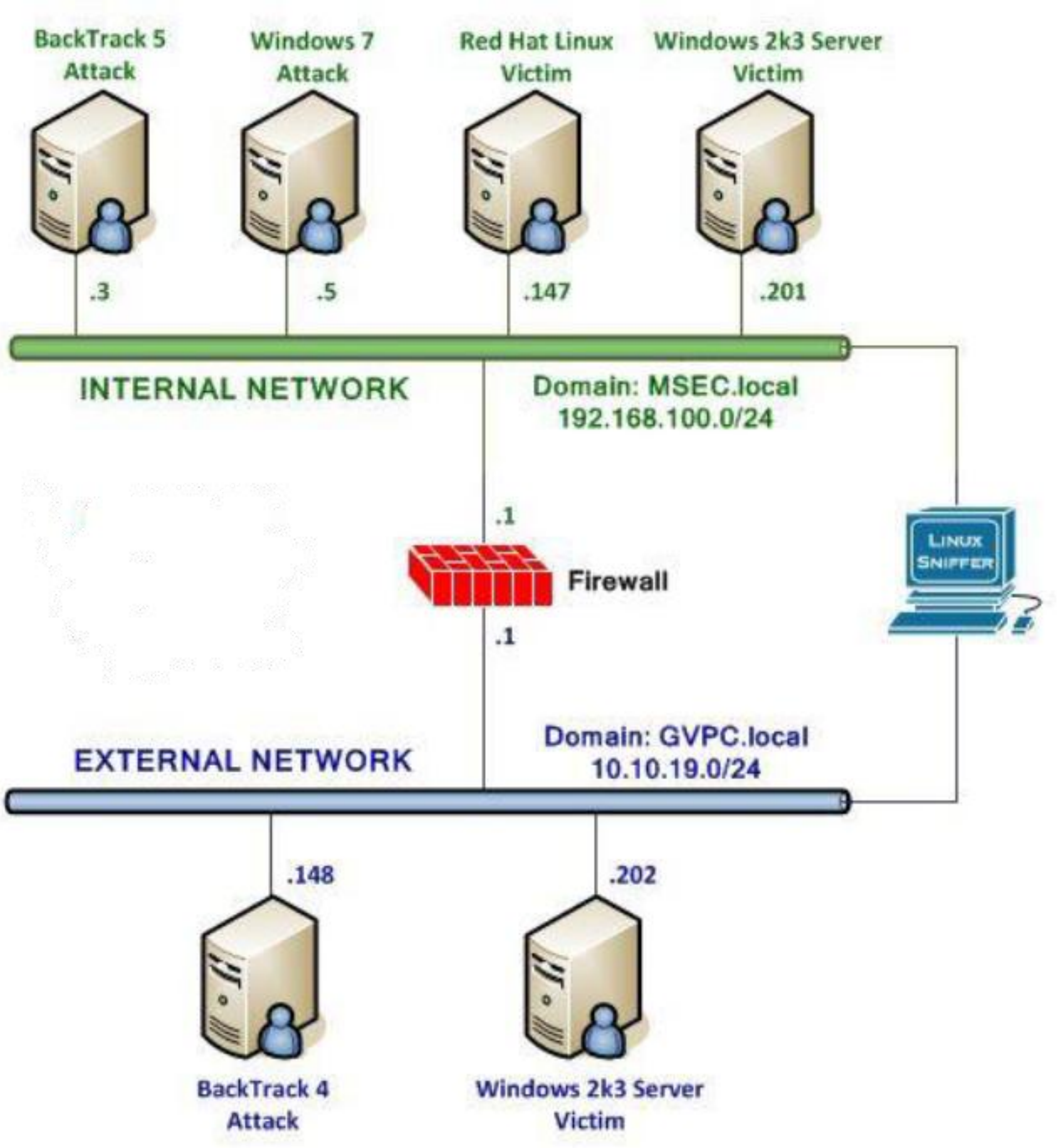


Figure 1: Topology

Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

Windows 7 Internal Attack Login:

1. Click on the Windows 7 Internal Attack icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

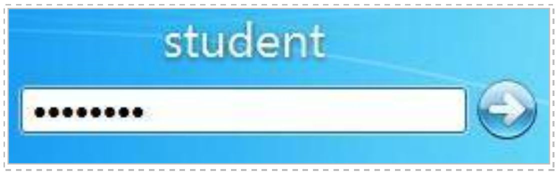


Figure 2: Windows 7 login

1 Encryption with the Encrypted File System

The encrypted file system allows a Microsoft Windows operating system user to protect their data so it cannot be read by anyone else using the system. EFS has been available since Windows 2000 and is only supported on New Technology File System (NTFS) drives. The user who encrypts the file does not need to provide a password to access it.

1.1 Using EFS

1. On the **Windows 7 Internal Attack Machine**, open a command prompt by clicking on the shortcut on the desktop.

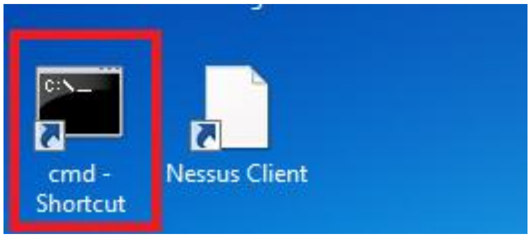
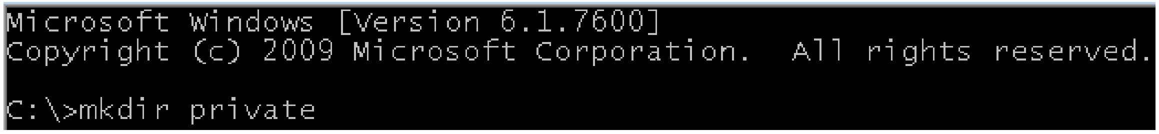


Figure 3: Opening the Command Prompt

2. Type the following command to make a directory called private on the root of C:
   C:\mkdir private

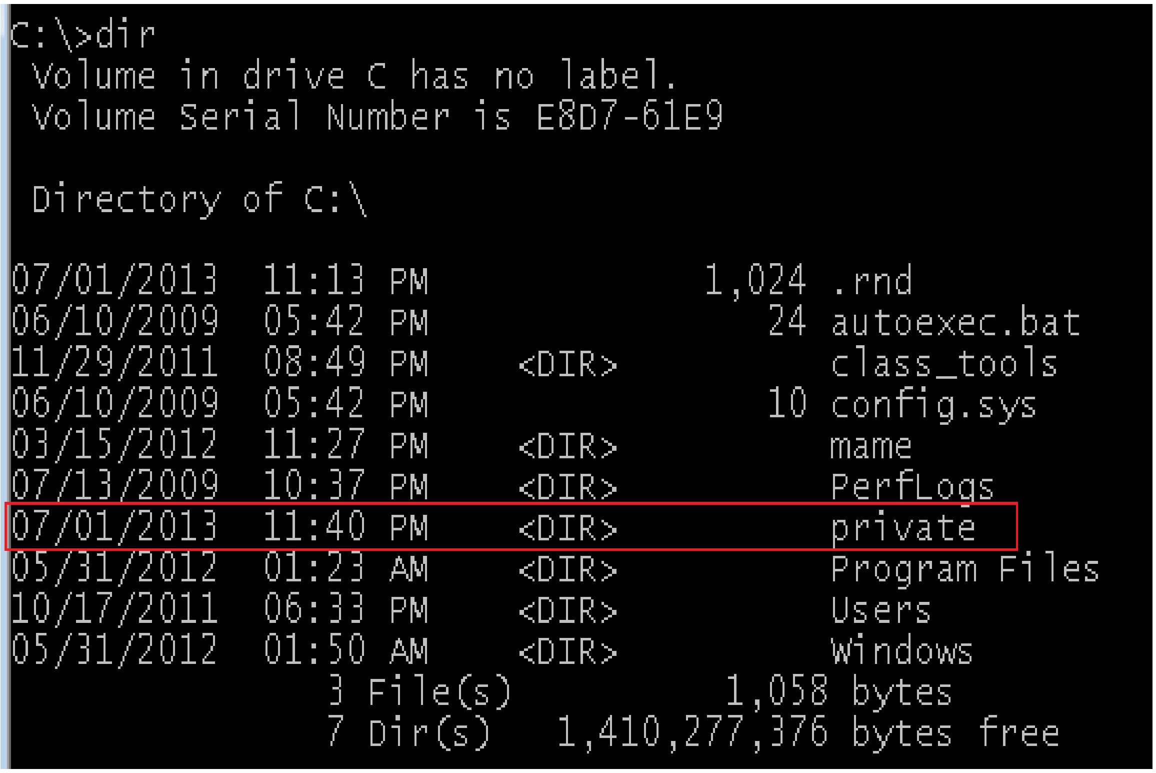


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>mkdir private
```

Figure 4: Making a Directory

3. Type the following command to list all files and folder on the root of C:
   C:\dir



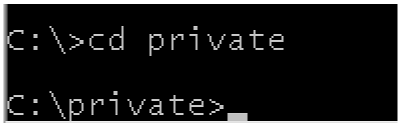
```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E8D7-61E9

 Directory of C:\

07/01/2013  11:13 PM             1,024 .rnd
06/10/2009  05:42 PM                24 autoexec.bat
11/29/2011  08:49 PM    <DIR>          class_tools
06/10/2009  05:42 PM                10 config.sys
03/15/2012  11:27 PM    <DIR>          mame
07/13/2009  10:37 PM    <DIR>          PerfLogs
07/01/2013  11:40 PM    <DIR>          private
05/31/2012  01:23 AM    <DIR>          Program Files
10/17/2011  06:33 PM    <DIR>          Users
05/31/2012  01:50 AM    <DIR>          Windows
               3 File(s)          1,058 bytes
               7 Dir(s)   1,410,277,376 bytes free
```

Figure 5: IP address of External BackTrack

4. Type the following command to enter the private directory on the root of C:
   C:\cd private

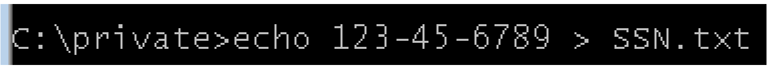


```
C:\>cd private

C:\private>_
```

Figure 6: Entering the Directory

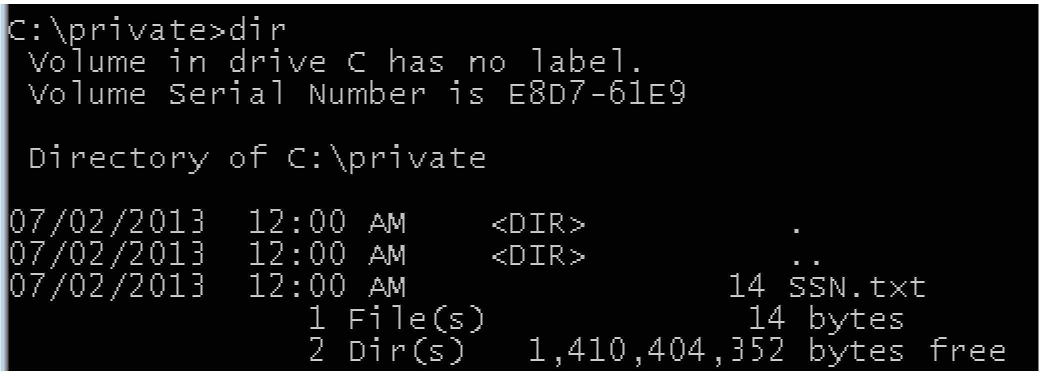
5. Create a file called SSN.txt that says 123-45-6789 by typing the following:
   C:\private>**echo 123-45-6789 > SSN.txt**



```
C:\private>echo 123-45-6789 > SSN.txt
```

Figure 7: Creating SSN.txt

6. Type the following to view the files and folders in the private directory:
   C:\>**dir**



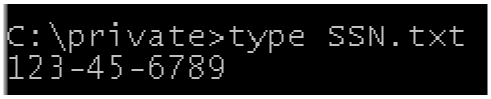
```
C:\private>dir
 Volume in drive C has no label.
 Volume Serial Number is E8D7-61E9

 Directory of C:\private

07/02/2013  12:00 AM    <DIR>          .
07/02/2013  12:00 AM    <DIR>          ..
07/02/2013  12:00 AM                14 SSN.txt
               1 File(s)             14 bytes
               2 Dir(s)   1,410,404,352 bytes free
```

Figure 8: Directory Listing

7. Type the following command to view the contents of the SSN.txt file:
   C:\ **type SSN.txt**



```
C:\private>type SSN.txt
123-45-6789
```

Figure 9: Viewing the Contents of the file

8. Type the following command to leave the command line environment:
   C:\exit

```
C:\private>exit
```

Figure 10: Exiting the Command Line

9. Click on the **Start** Button and select **Computer** from the start menu.

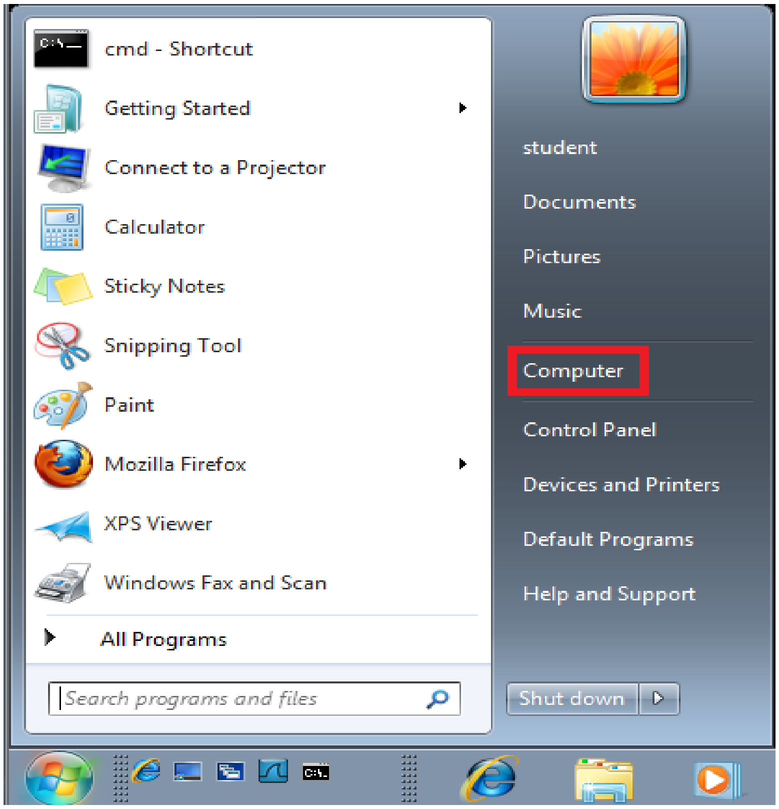


Figure 11: Start Menu

10. Under Hard Disk Drives (1), double-click on **Local Disk (C:).**

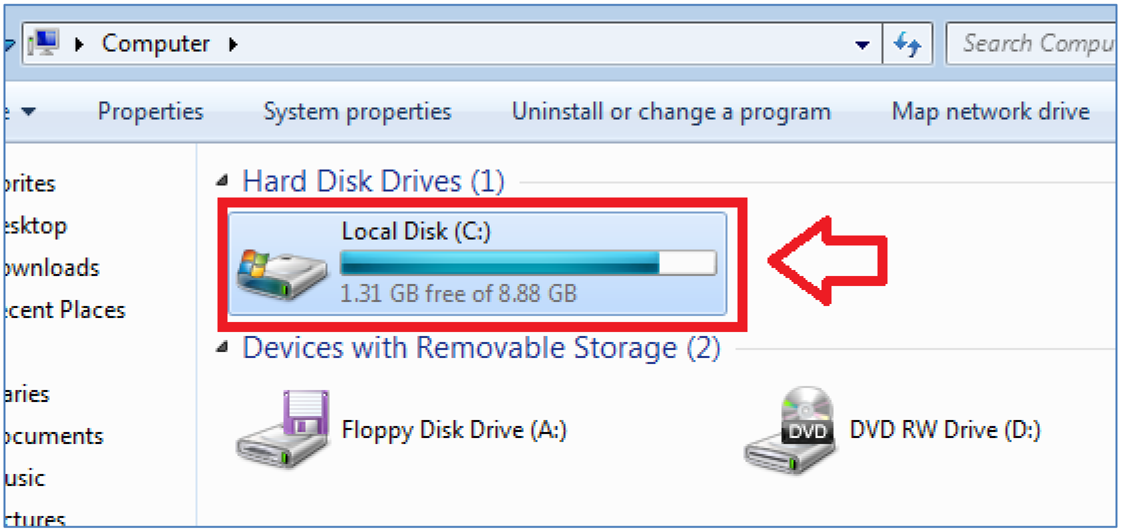
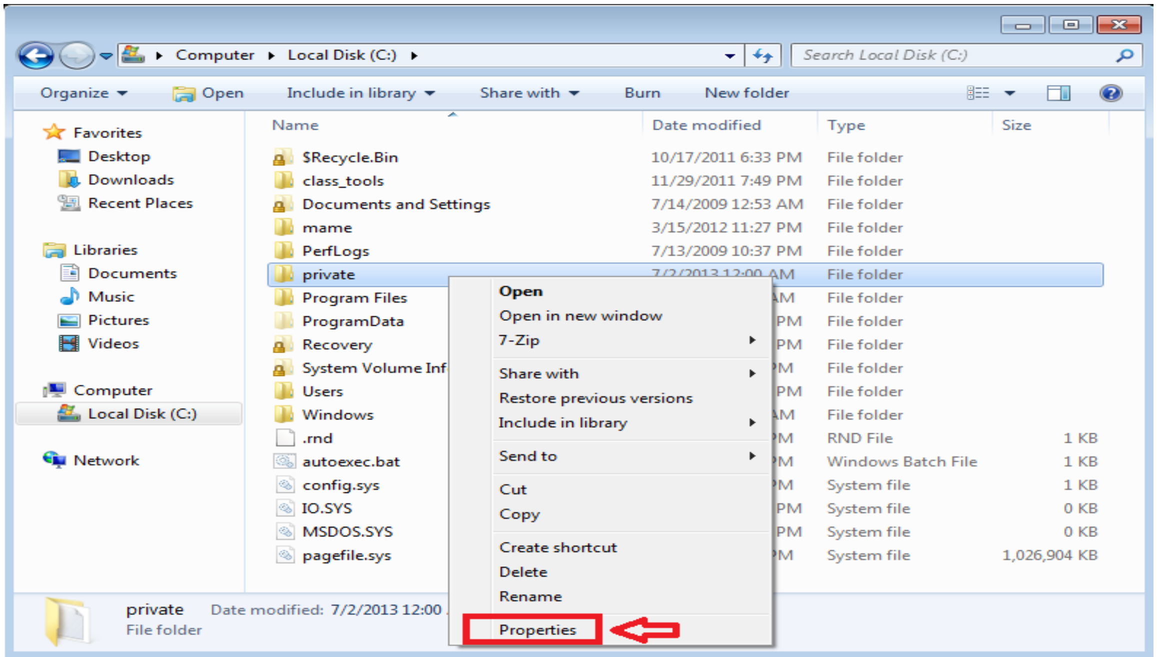


Figure 12: The C: Drive

Copyright © 2013 CSSIA, NISGTC

11. Right-click on the **Private** Folder in the list and select **Properties**.

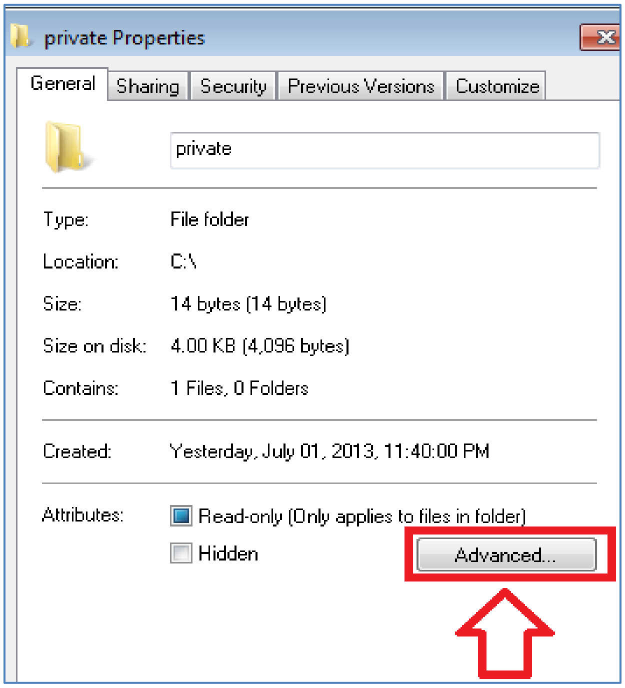


Name	Date modified	Type	Size
$Recycle.Bin	10/17/2011 6:33 PM	File folder	
class_tools	11/29/2011 7:49 PM	File folder	
Documents and Settings	7/14/2009 12:53 AM	File folder	
mame	3/15/2012 11:27 PM	File folder	
PerfLogs	7/13/2009 10:37 PM	File folder	
private	7/2/2013 12:00 AM	File folder	
Program Files	AM	File folder	
ProgramData	PM	File folder	
Recovery	PM	File folder	
System Volume Inf	M	File folder	
Users	PM	File folder	
Windows	AM	File folder	
.rnd	M	RND File	1 KB
autoexec.bat	M	Windows Batch File	1 KB
config.sys	M	System file	1 KB
IO.SYS	PM	System file	0 KB
MSDOS.SYS	PM	System file	0 KB
pagefile.sys	M	System file	1,026,904 KB

private Date modified: 7/2/2013 12:00
File folder

Figure 12: Properties of the Folder

12. On the **General** tab, click the **Advanced** button.



private

Type: File folder

Location: C:\

Size: 14 bytes (14 bytes)

Size on disk: 4.00 KB (4,096 bytes)

Contains: 1 Files, 0 Folders

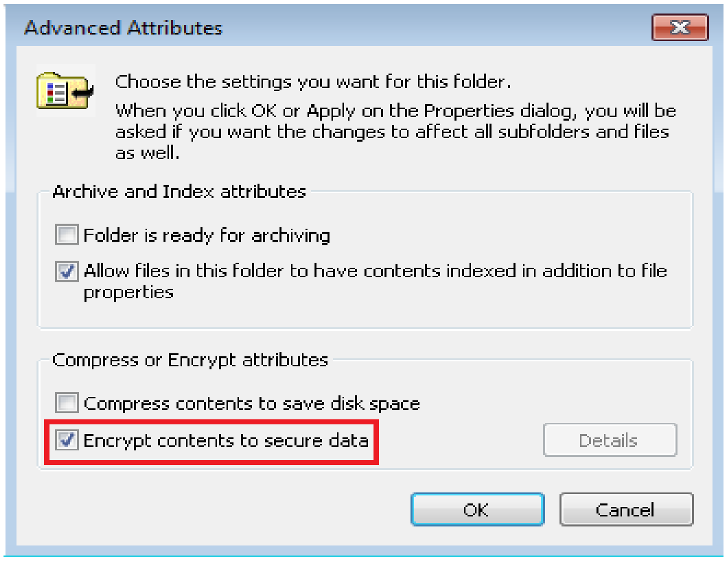
Created: Yesterday, July 01, 2013, 11:40:00 PM

Attributes: ■ Read-only (Only applies to files in folder)
□ Hidden

Figure 13: Advanced Tab

Copyright © 2013 CSSIA, NISGTC

13. Check the box that states **Encrypt contents to secure data**. Click **OK**.



Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☐ Folder is ready for archiving

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

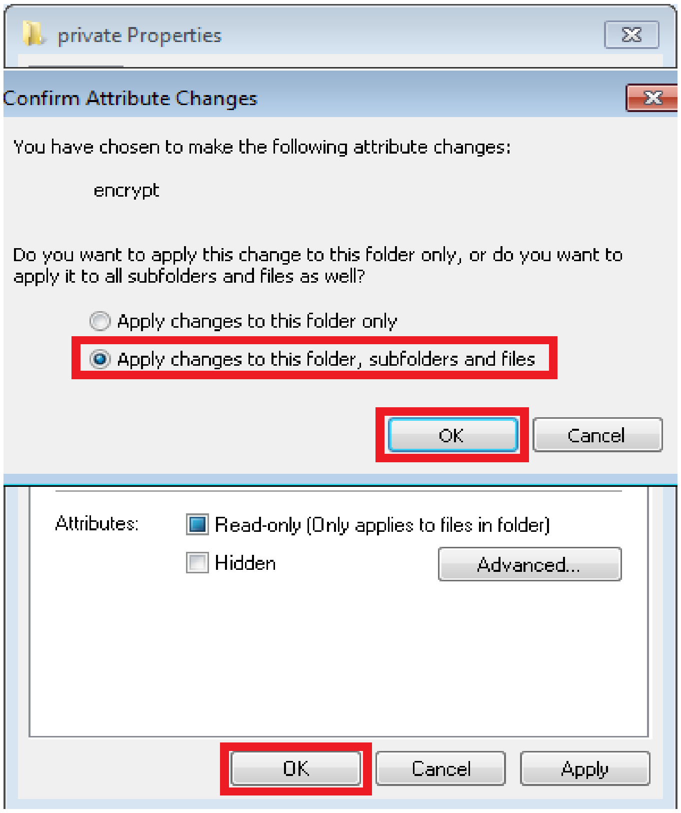
Compress or Encrypt attributes

☐ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 14: Encrypt Contents

14. Click **OK.** Select **Apply changes to this folder, subfolder and files**. Click **OK**.



private Properties

Confirm Attribute Changes

You have chosen to make the following attribute changes:

encrypt

Do you want to apply this change to this folder only, or do you want to apply it to all subfolders and files as well?

○ Apply changes to this folder only

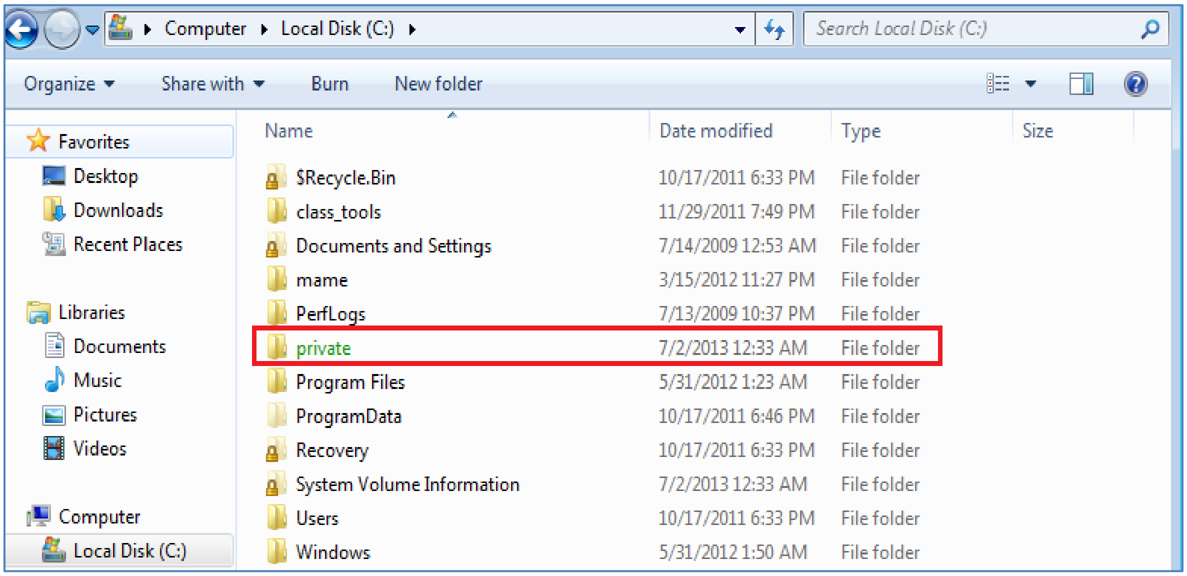
● Apply changes to this folder, subfolders and files

Attributes: ■ Read-only (Only applies to files in folder)

☐ Hidden

Figure 15: Applying Changes to the Folder

15. View the **private** folder on the C: Drive; the color of the file changed to green.



Name	Date modified	Type	Size
$Recycle.Bin	10/17/2011 6:33 PM	File folder	
class_tools	11/29/2011 7:49 PM	File folder	
Documents and Settings	7/14/2009 12:53 AM	File folder	
mame	3/15/2012 11:27 PM	File folder	
PerfLogs	7/13/2009 10:37 PM	File folder	
private	7/2/2013 12:33 AM	File folder	
Program Files	5/31/2012 1:23 AM	File folder	
ProgramData	10/17/2011 6:46 PM	File folder	
Recovery	10/17/2011 6:33 PM	File folder	
System Volume Information	7/2/2013 12:33 AM	File folder	
Users	10/17/2011 6:33 PM	File folder	
Windows	5/31/2012 1:50 AM	File folder	

Figure 17: Encrypted Folder

16. Open a command prompt by clicking on the shortcut on the desktop.

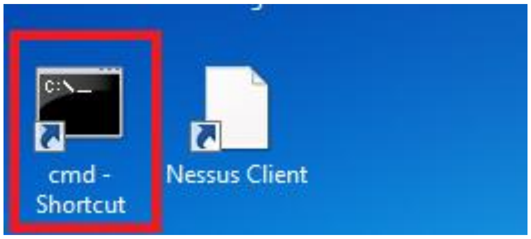
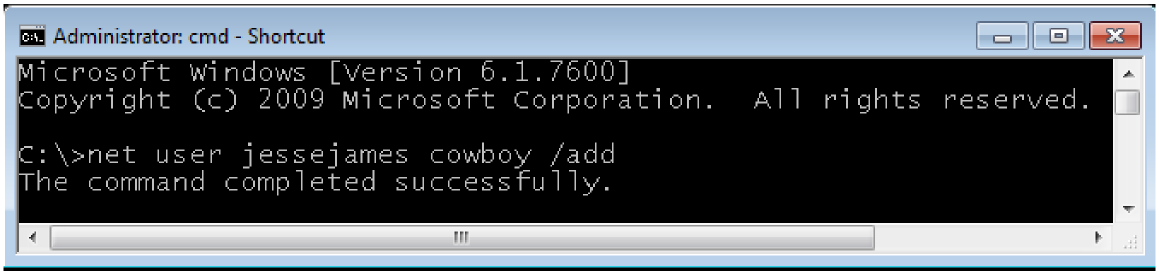


Figure 18: Opening the Command Prompt

17. Create a user on the Windows 7 system by typing the following command:
C:\>**net user jessejames cowboy /add**

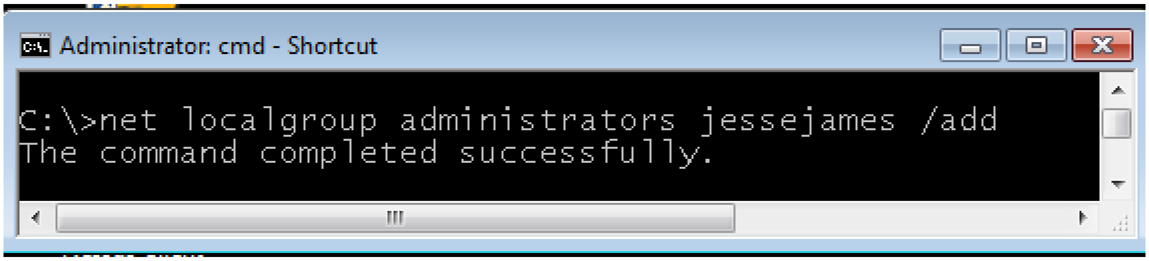


```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>net user jessejames cowboy /add
The command completed successfully.
```

Figure 16: Creating a User

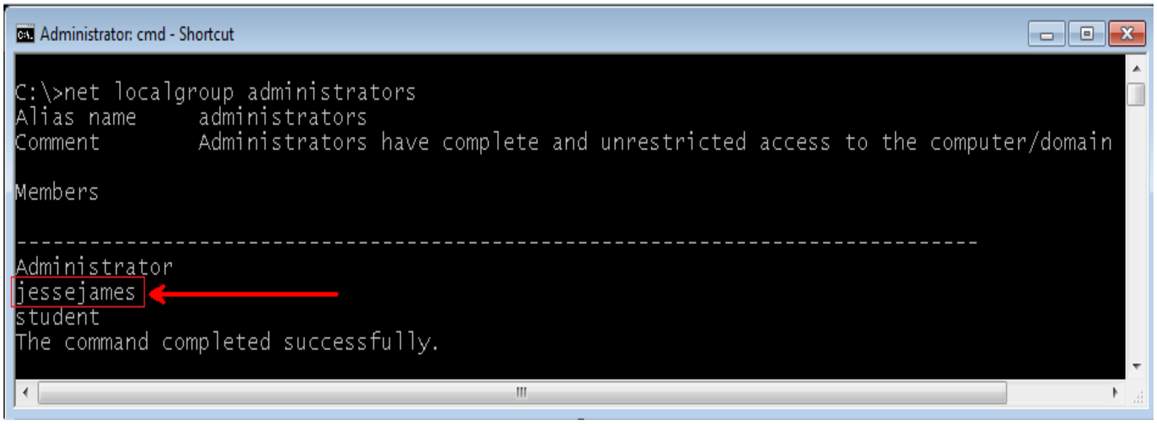
18. Type the following command to add the user to the local administrators group:
    C:\>**net localgroup administrators jessejames /add**



```
C:\>net localgroup administrators jessejames /add
The command completed successfully.
```

Figure 20: Adding the User to Administrators

19. Verify that the user has been added to the administrators group by typing:
    C:\>**net localgroup administrators**



```
C:\>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
jessejames
student
The command completed successfully.
```

Figure 21: Viewing the administrators group

20. Click on the **Start** Button, click to the right of shutdown, and select **Log off.**

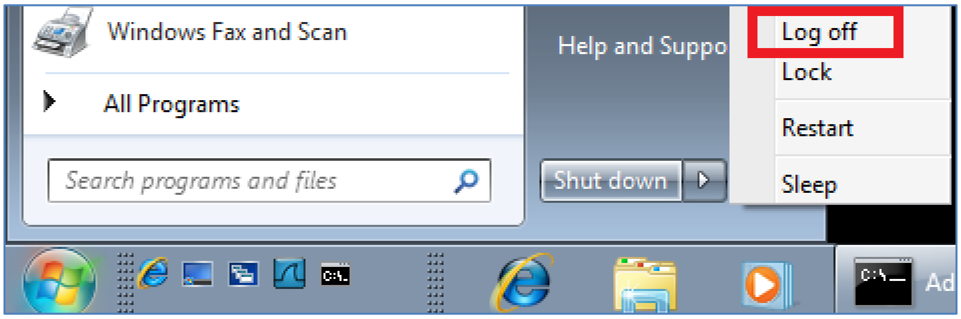


Figure 22: Log Off

21. Click on the icon with the name **jessejames** at the Welcome page.

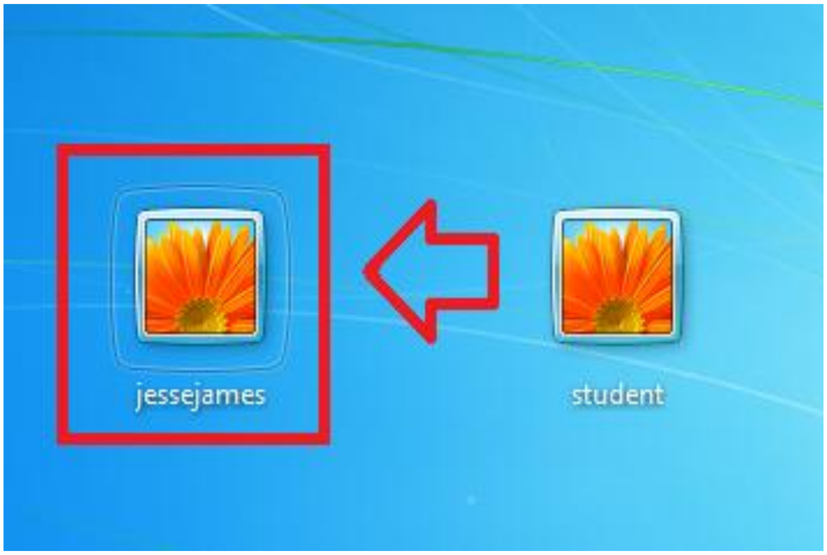


Figure 17: Selecting the User

22. Type **cowboy** for the password for the **jessejames** account.

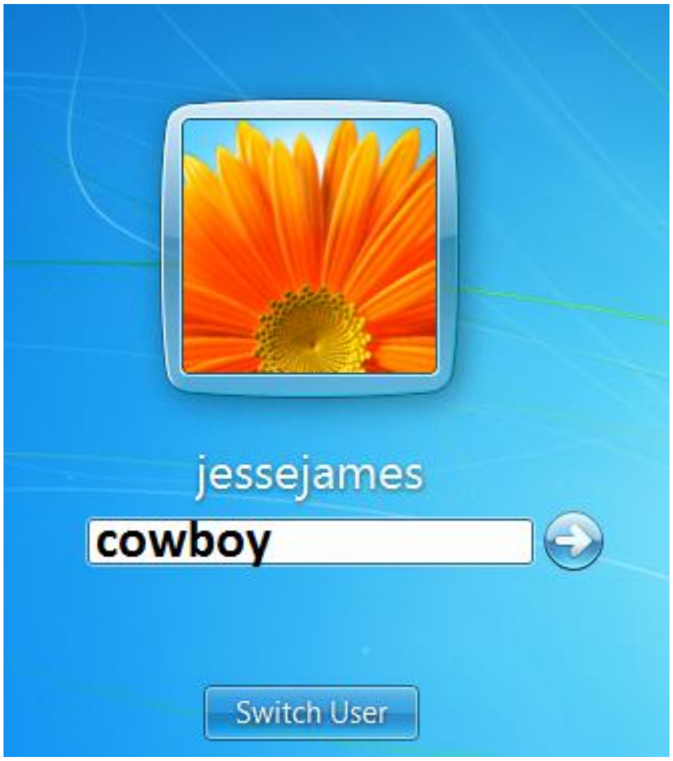


Figure 18: Typing the Password

23. Click on the **Start** Button and select **Computer** from the start menu.

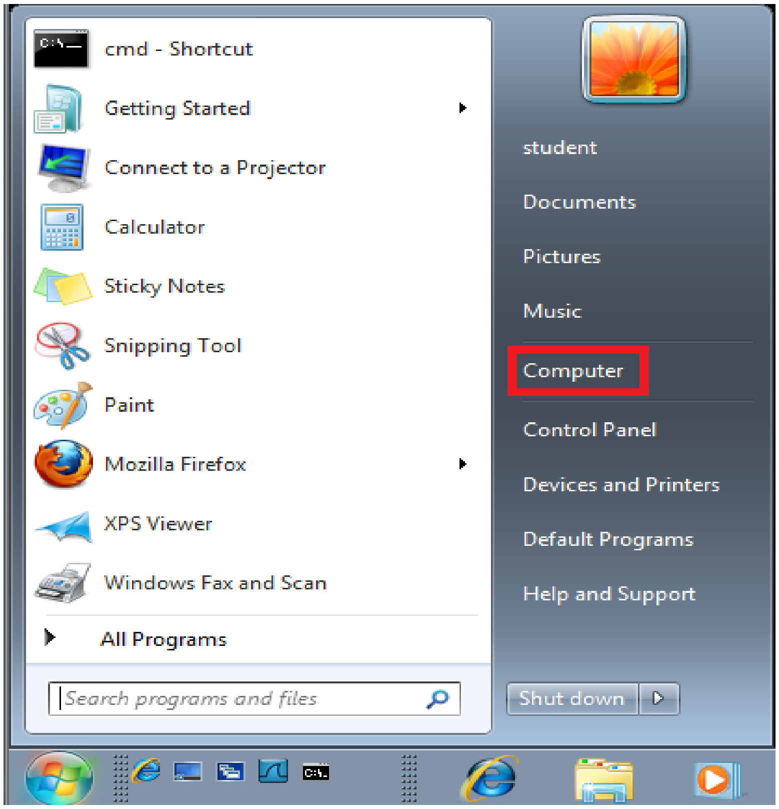


Figure 19: Start Menu

24. Under **Hard Disk Drives (1),** double-click on **Local Disk (C:).**

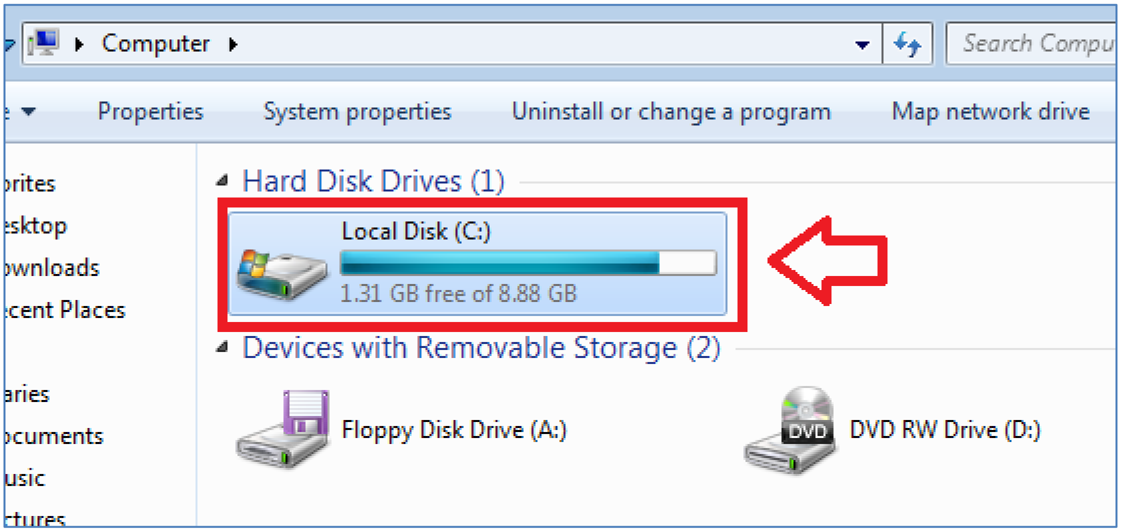
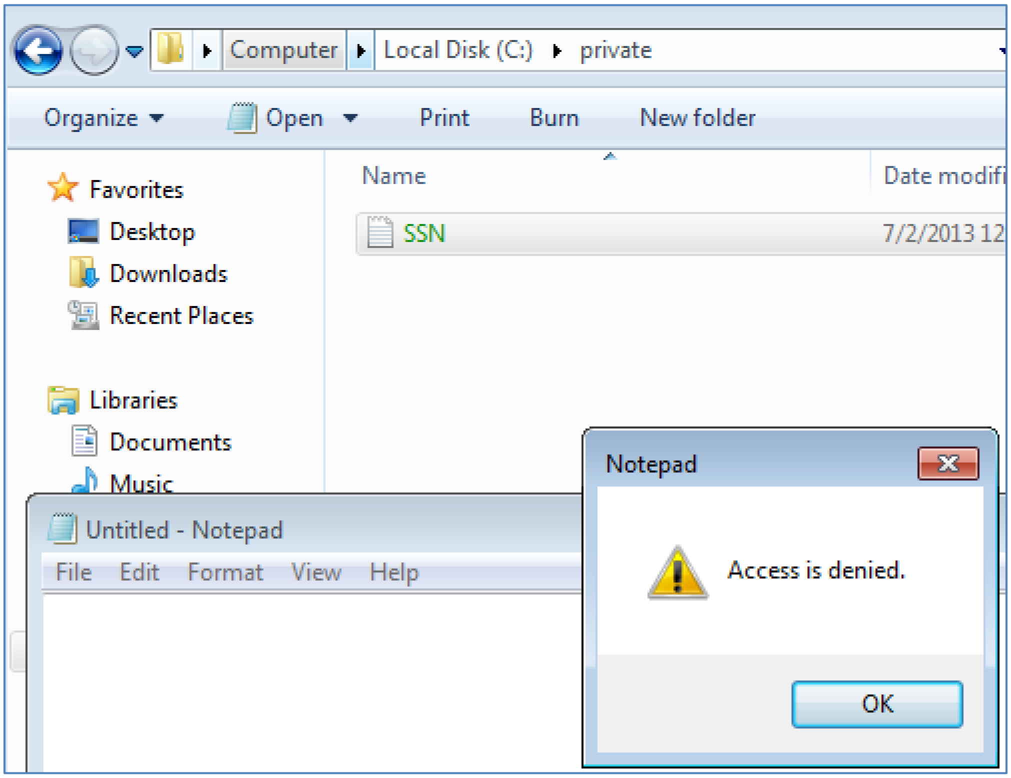


Figure 26: The C: Drive

25. Double-click on the **Private** Folder. Try to open **SSN.txt**. Access is denied.



Access is denied.

Figure 20: Access is Denied

1.2 Conclusion

The Encrypted File System, or EFS, is a way for a user to protect personal data on a machine that may be shared by several users. In order to use EFS, the Windows operating system must have a New Technology File System (NTFS) partition.

1.3 Discussion Questions

1. What File System is required in order to use EFS?
2. What command allows you to add a user from the command line?
3. What command can be utilized to create a file from the command line?
4. What command allows you to create a directory from the command line?

2 Backing up Encrypted File System Keys

A user can select or create keys, back up their EFS key, update their key, or configure the use of a smart card. A smart card is a physical device that the user would need to carry with them in order to authenticate. The use of smart cards is common within organizations where security is paramount, such as the United States Department of Defense.

2.1 Backing up the EFS Key

1. Click on the **Start** Button, click to the right of shutdown, and select **Log off.**

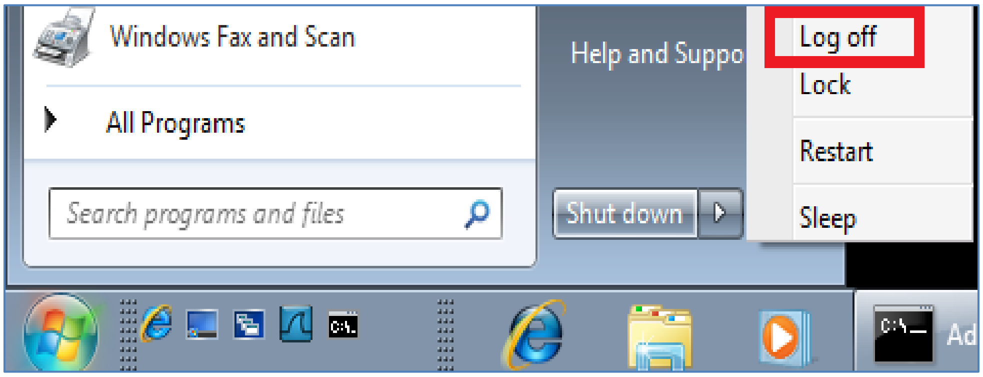


Figure 21: Log Off

2. Click on the icon with the name **student** at the Welcome page.

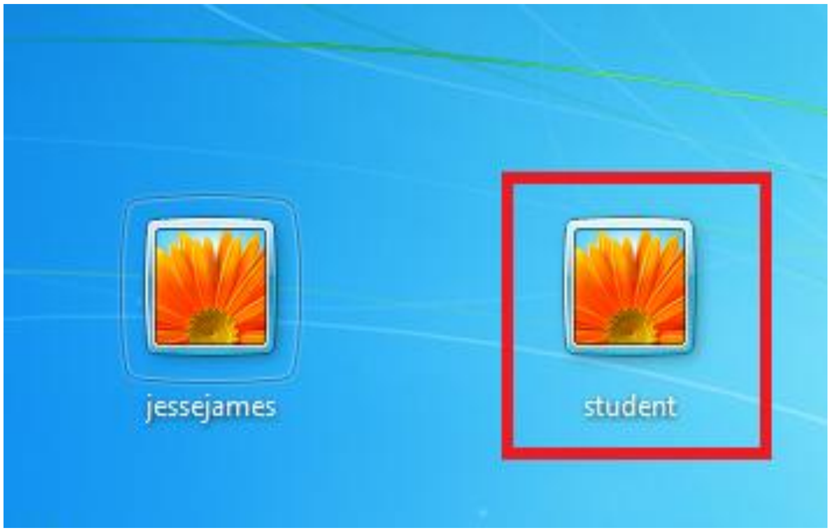


Figure 22: Log on as Student

3. Log on to Windows 7 Internal Attack Machine as **student** with the password of **password**.

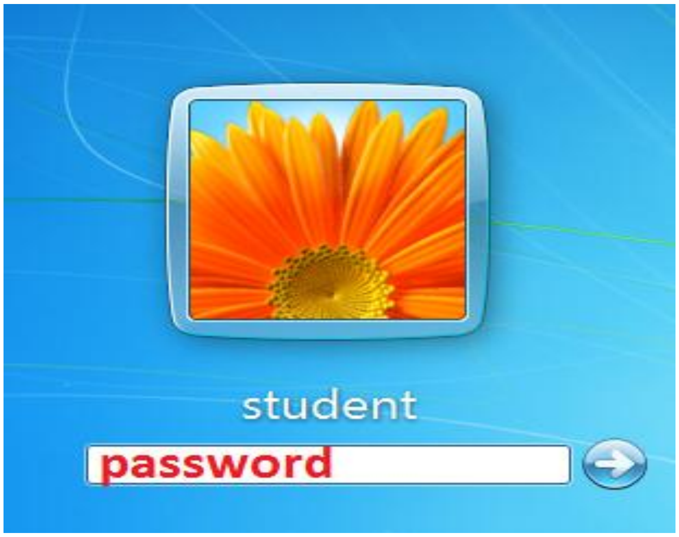


Figure 23: Logging on to the Windows 7 Machine

4. Click on the **Start** button and select **Computer** from the start menu.

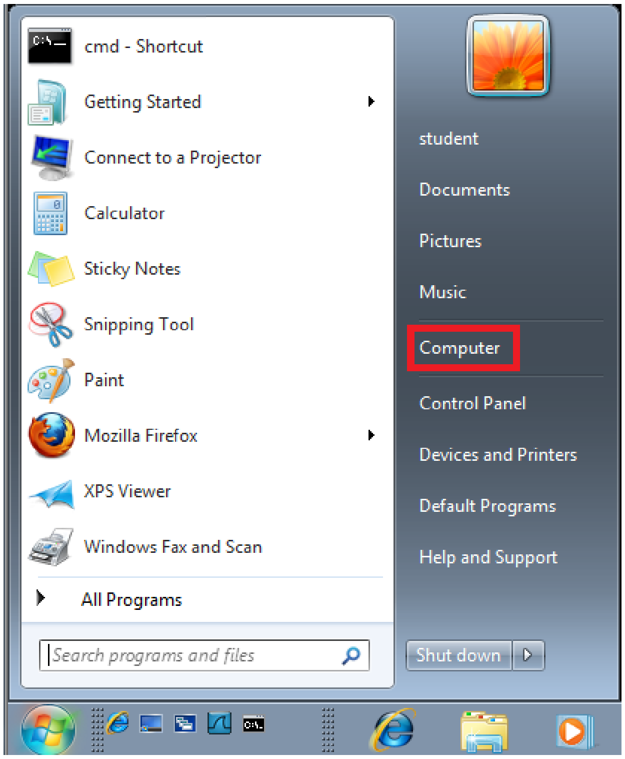


Figure 24: Start Menu

5. Under **Hard Disk Drives (1**), double-click on **Local Disk (C:).**

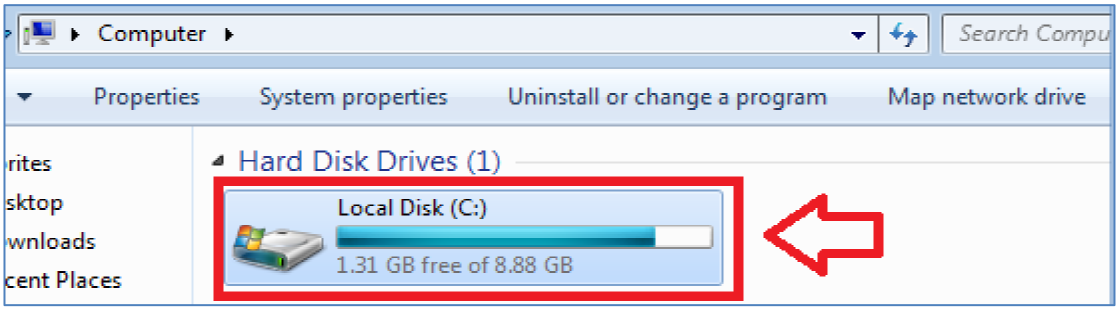


Figure 25: The C: Drive

6. Double-click on the **private** folder located on the root of the C: Drive.

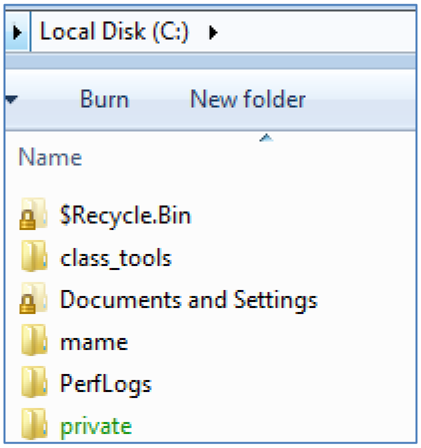
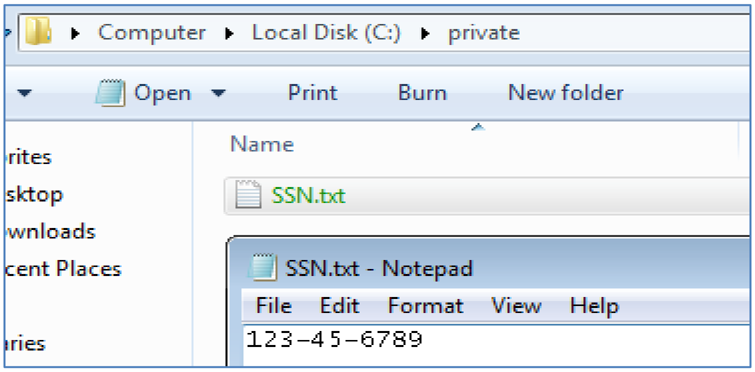


Figure 26: The Private Folder

7. Verify that student can still access the **SSN.txt**



```
123-45-6789
```

Figure 27: Accessing the Encrypted File

8. Click on the **Start** button and select the **Control Panel**.

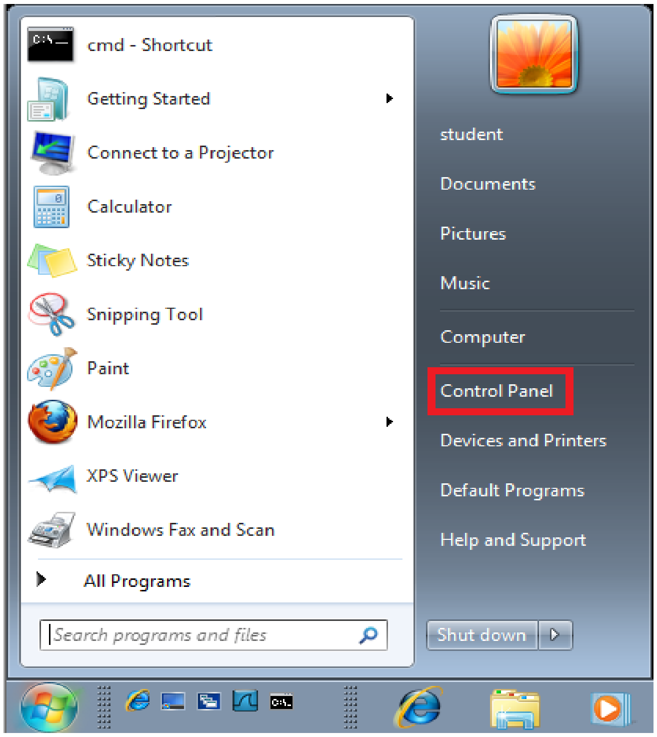


Figure 28: Control Panel

9. Within the Control Panel, click on **User Accounts and Family Safety**.

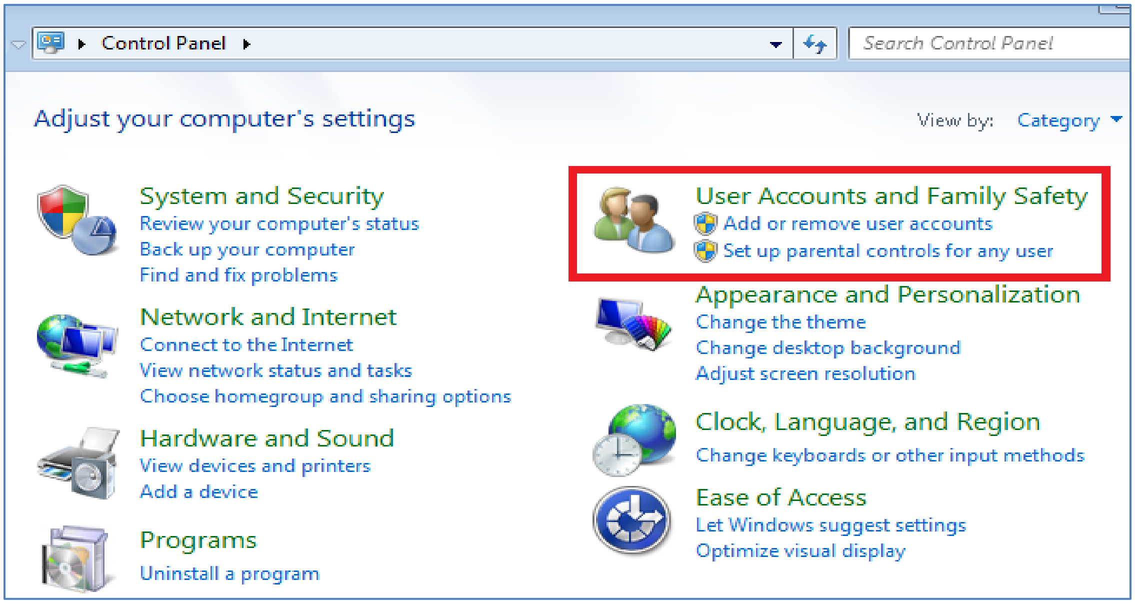

Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
Connect to the Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

Figure 29: User Accounts and Family Safety

10. Click the **User Accounts** link under the User Accounts and Family Saftey.

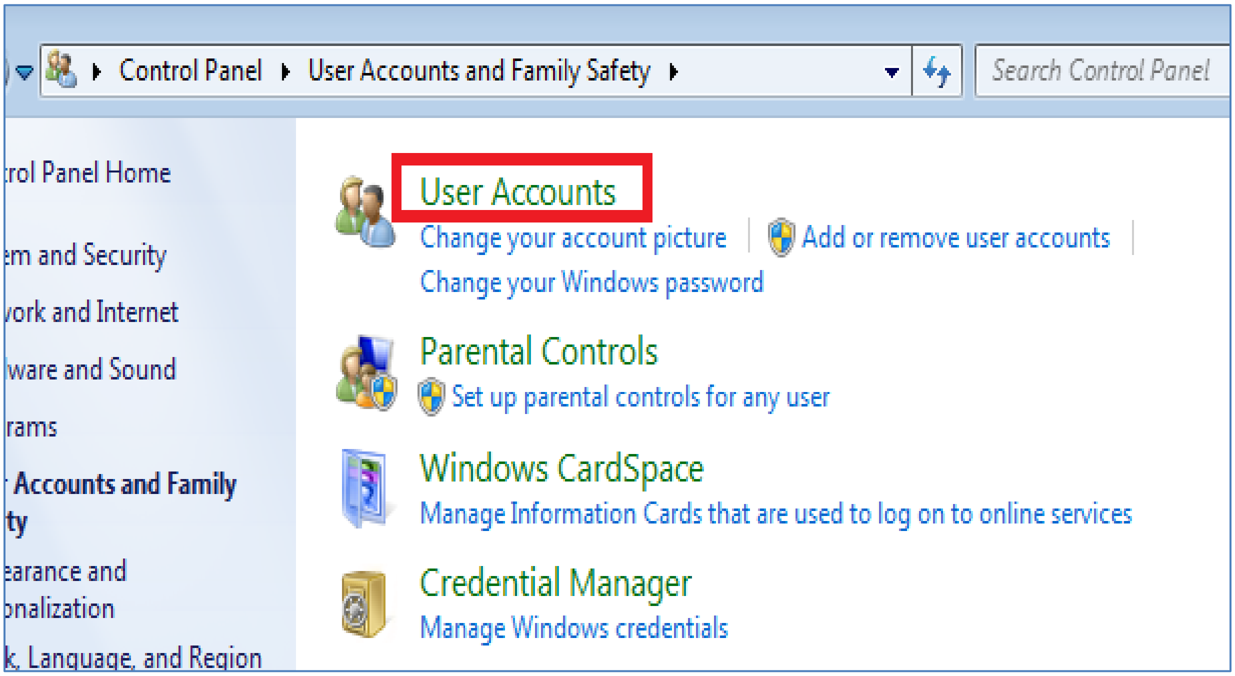

Control Panel ▸ User Accounts and Family Safety ▸
Search Control Panel
trol Panel Home
em and Security
work and Internet
ware and Sound
rams
Accounts and Family
ty
earance and
onalization
k, Language, and Region
User Accounts
Change your account picture
Add or remove user accounts
Change your Windows password
Parental Controls
Set up parental controls for any user
Windows CardSpace
Manage Information Cards that are used to log on to online services
Credential Manager
Manage Windows credentials

Figure 37: User Accounts Link

11. Click the **Manage your file encryption certificates** link on the left.

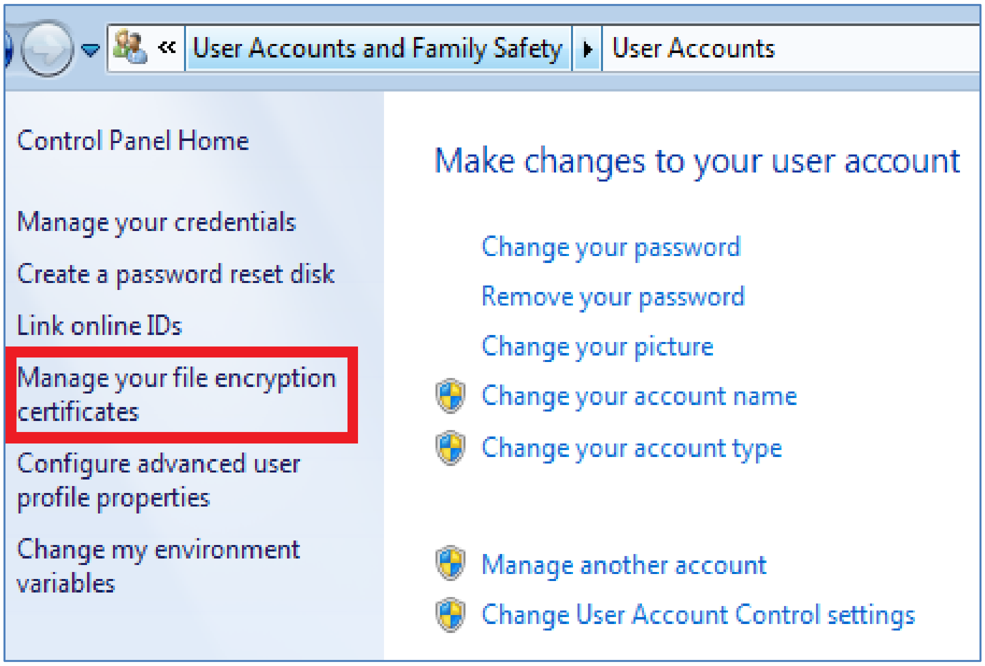
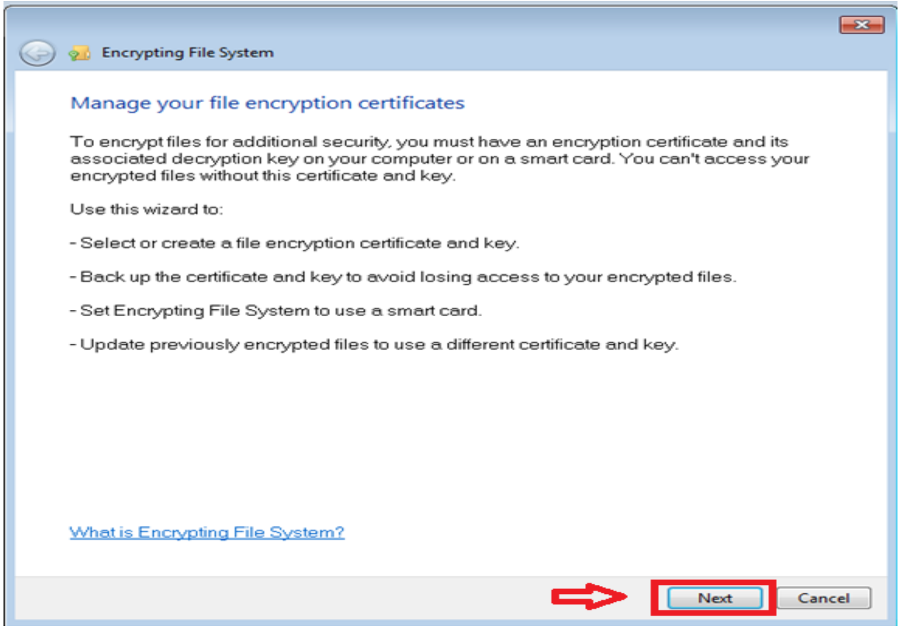

« User Accounts and Family Safety ▸ User Accounts
Control Panel Home
Manage your credentials
Create a password reset disk
Link online IDs
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Change your password
Remove your password
Change your picture
Change your account name
Change your account type
Manage another account
Change User Account Control settings

Figure 30: Manage Certificates

12. Click **Next** at the Manage you file encyrption certificates screen:



Encrypting File System

Manage your file encryption certificates

To encrypt files for additional security, you must have an encryption certificate and its associated decryption key on your computer or on a smart card. You can't access your encrypted files without this certificate and key.

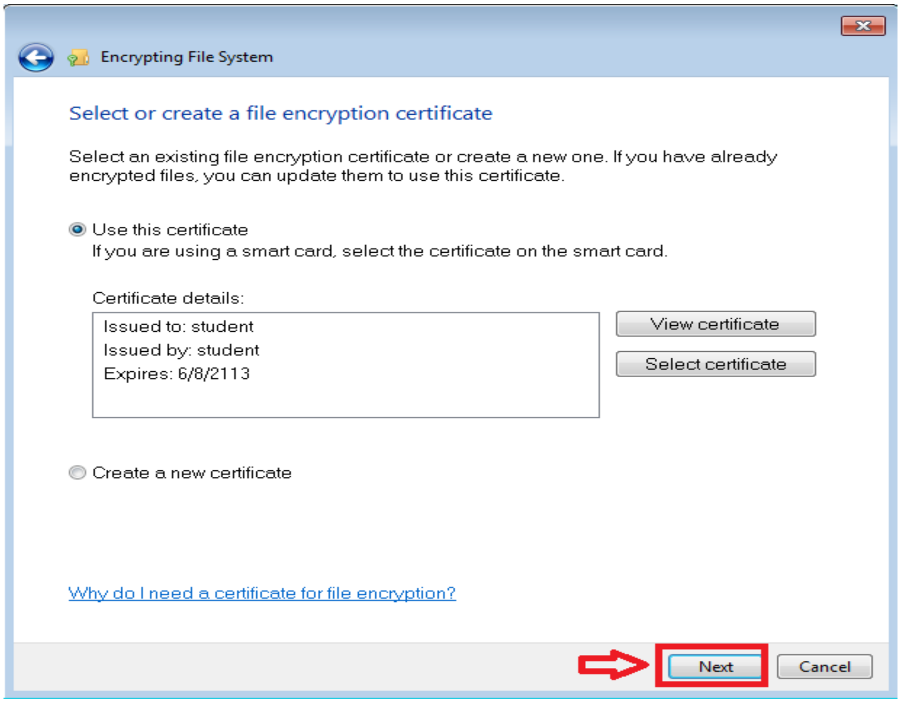
Use this wizard to:

- Select or create a file encryption certificate and key.
- Back up the certificate and key to avoid losing access to your encrypted files.
- Set Encrypting File System to use a smart card.
- Update previously encrypted files to use a different certificate and key.

What is Encrypting File System?

Figure 31: Managing File Certificates

13. Click **Use this certificate** and click **Next.**



Encrypting File System

Select or create a file encryption certificate

Select an existing file encryption certificate or create a new one. If you have already encrypted files, you can update them to use this certificate.

● Use this certificate
If you are using a smart card, select the certificate on the smart card.

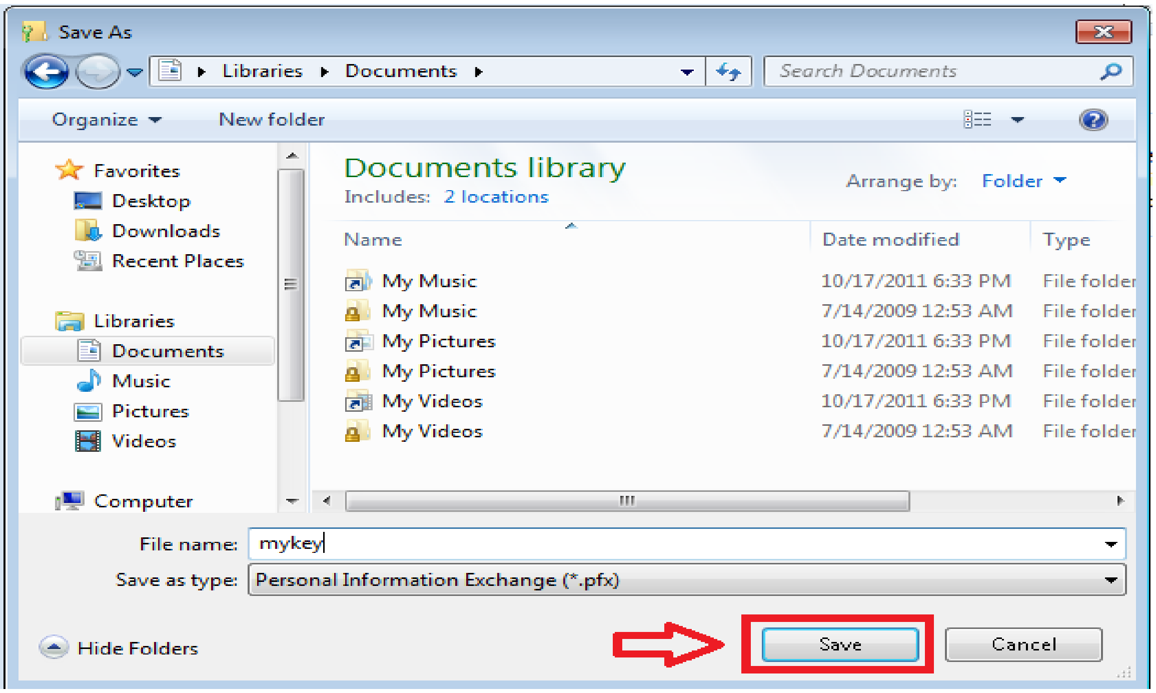
Certificate details:
Issued to: student
Issued by: student
Expires: 6/8/2113

○ Create a new certificate

Why do I need a certificate for file encryption?

Figure 32: Use this Certificate

14. Click **Browse** next to Backup location. For the filename, type **mykey**, and click **Save** to save to the default location of **Documents**.



Documents library

Includes: 2 locations

Arrange by: Folder ▾

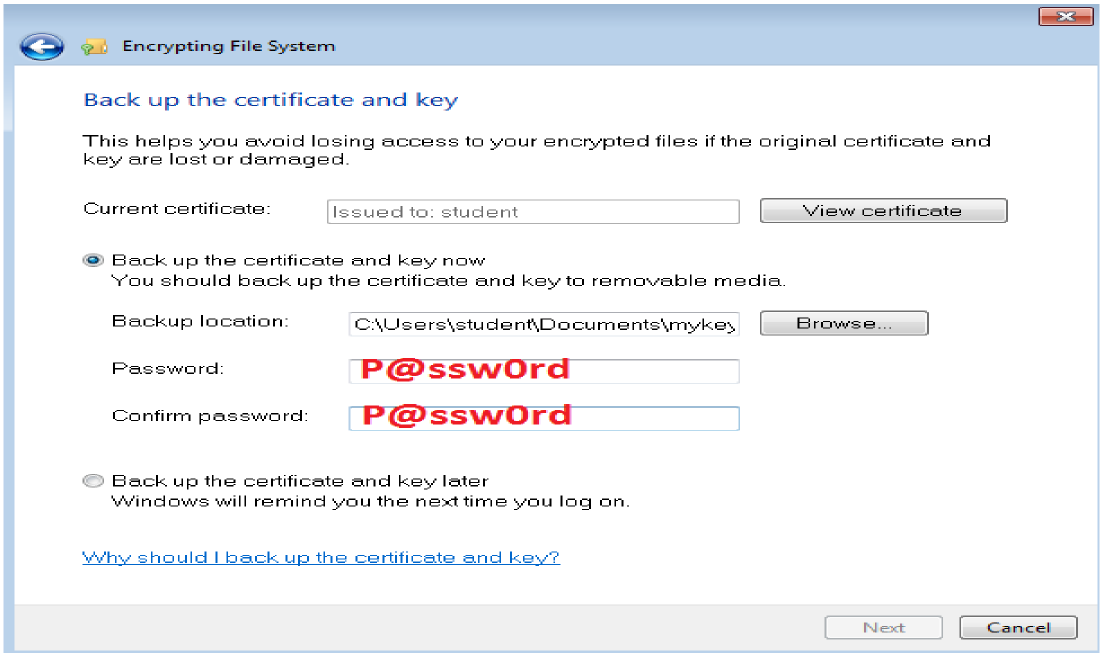
Name	Date modified	Type
My Music	10/17/2011 6:33 PM	File folder
My Music	7/14/2009 12:53 AM	File folder
My Pictures	10/17/2011 6:33 PM	File folder
My Pictures	7/14/2009 12:53 AM	File folder
My Videos	10/17/2011 6:33 PM	File folder
My Videos	7/14/2009 12:53 AM	File folder

File name: mykey

Save as type: Personal Information Exchange (*.pfx)

Figure 33: Save the file

15. For the password and confirm password, type **P@ssw0rd**. Click **Next**.



Back up the certificate and key

This helps you avoid losing access to your encrypted files if the original certificate and key are lost or damaged.

Current certificate: Issued to: student

● Back up the certificate and key now
You should back up the certificate and key to removable media.

Backup location: C:\Users\student\Documents\mykey

Password: P@ssw0rd

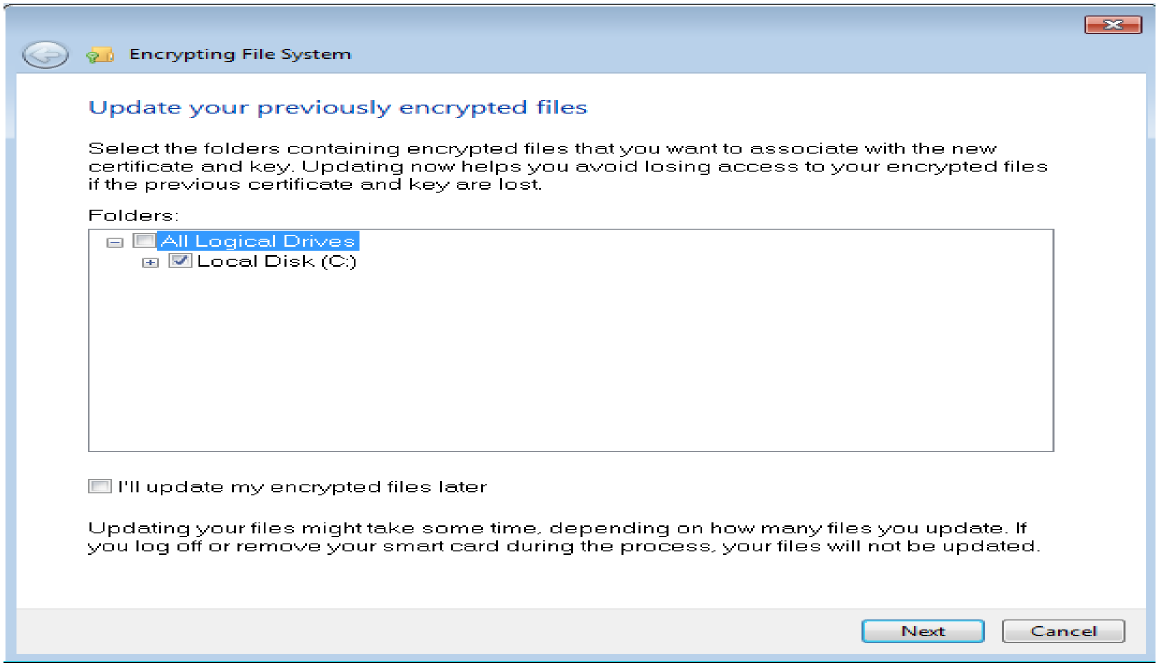
Confirm password: P@ssw0rd

○ Back up the certificate and key later
Windows will remind you the next time you log on.

Why should I back up the certificate and key?

Figure 34: Setting the password

16. Expand **All Logical Drives**, Select **Local Disk (C:)**, and click **Next.**



Encrypting File System

Update your previously encrypted files

Select the folders containing encrypted files that you want to associate with the new certificate and key. Updating now helps you avoid losing access to your encrypted files if the previous certificate and key are lost.

Folders:

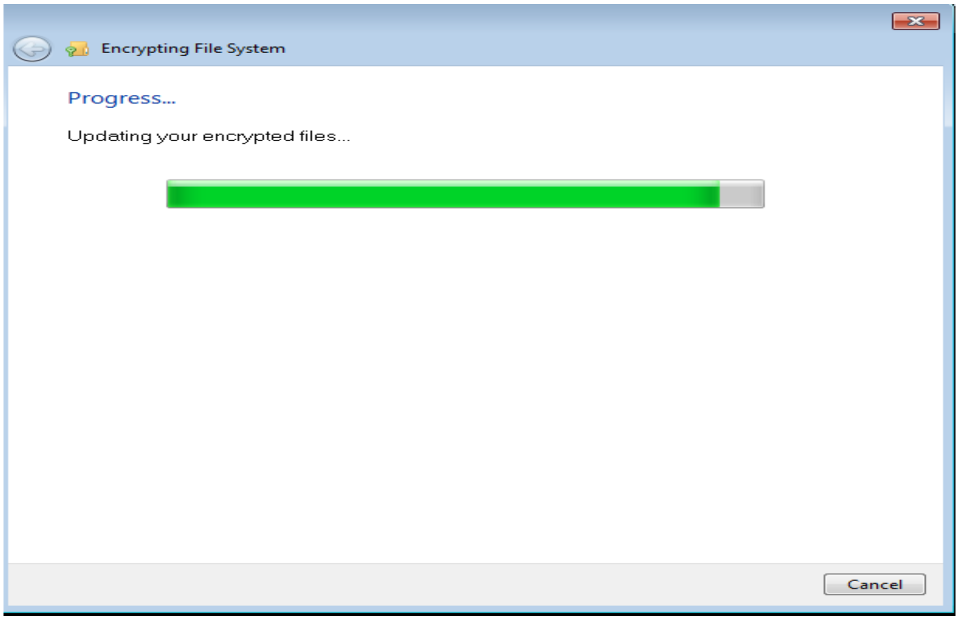
- ⊟ □ All Logical Drives
  - ⊞ ☑ Local Disk (C:)

□ I'll update my encrypted files later

Updating your files might take some time, depending on how many files you update. If you log off or remove your smart card during the process, your files will not be updated.

Figure 35: Setting the password

A Progress Screen will appear that indicates it is updating your encrypted files.



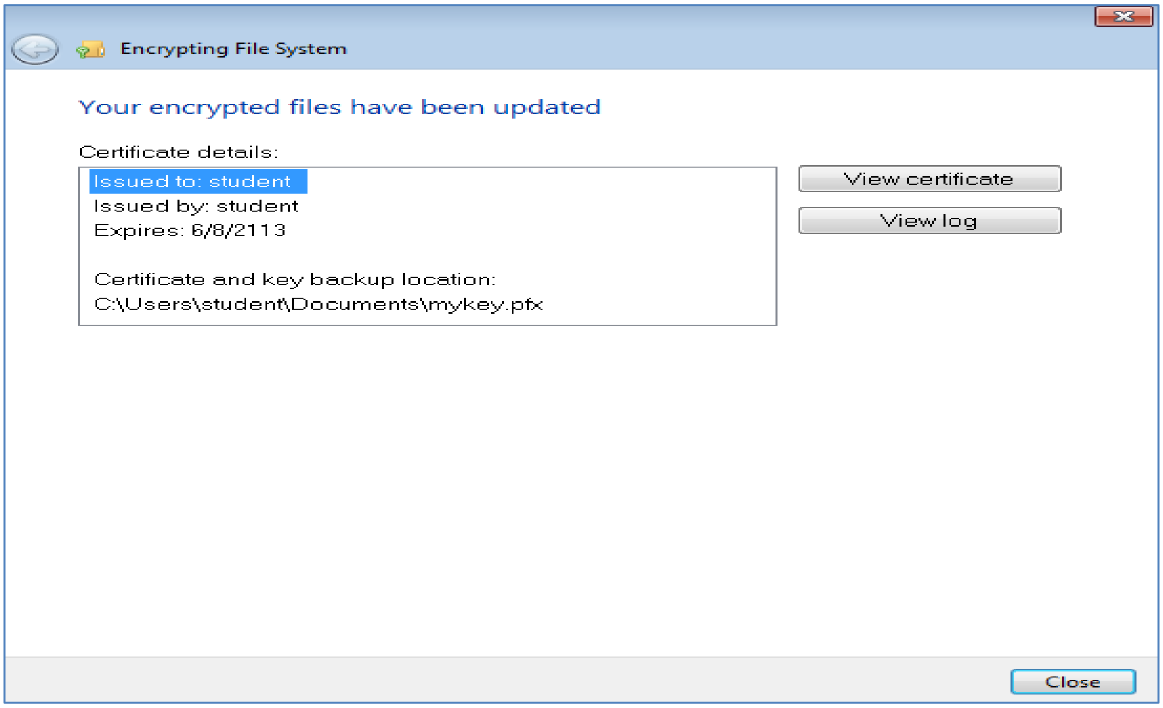
Encrypting File System

Progress...

Updating your encrypted files...

Figure 36: Progress Screen

17. Click **Close** at the screen that states, **Your Encrypted files have been updated.**



Your encrypted files have been updated

Certificate details:

Issued to: student
Issued by: student
Expires: 6/8/2113

Certificate and key backup location:
C:\Users\student\Documents\mykey.pfx

Figure 37: EFS has been updated

If the user's password is changed, they will no longer be able to access their EFS files.

18. Open a command prompt by clicking on the shortcut on the desktop.

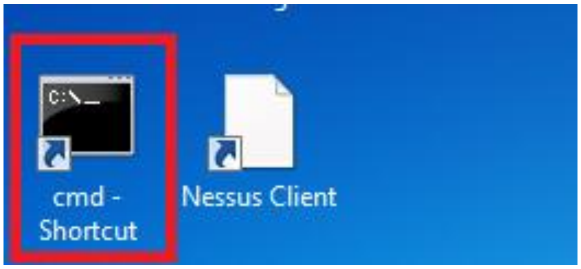
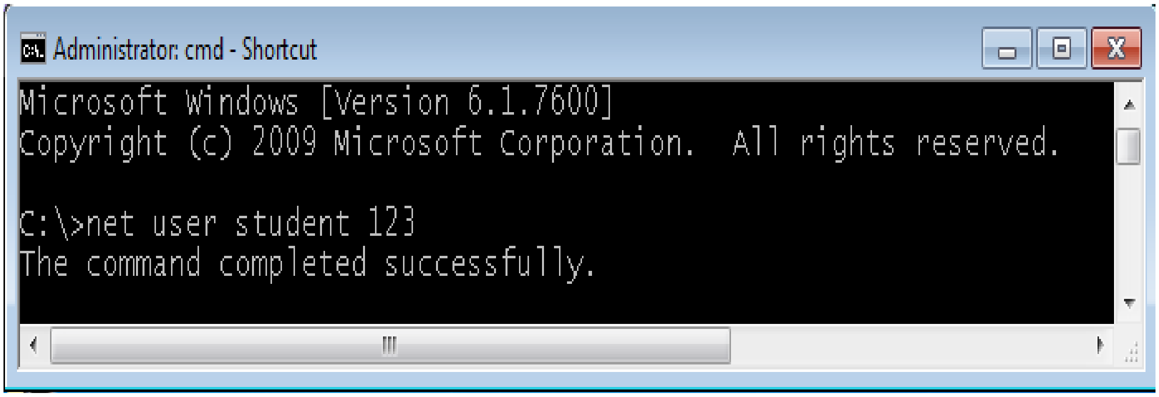


Figure 38: Opening the Command Prompt

19. Change the password for the **student** user to **123** by typing the following command:
    C:\>net user student 123



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>net user student 123
The command completed successfully.
```

Figure 39: Changing the password to 123

20. Click on the **Start** Button, click to the right of shutdown, and select **Log off**

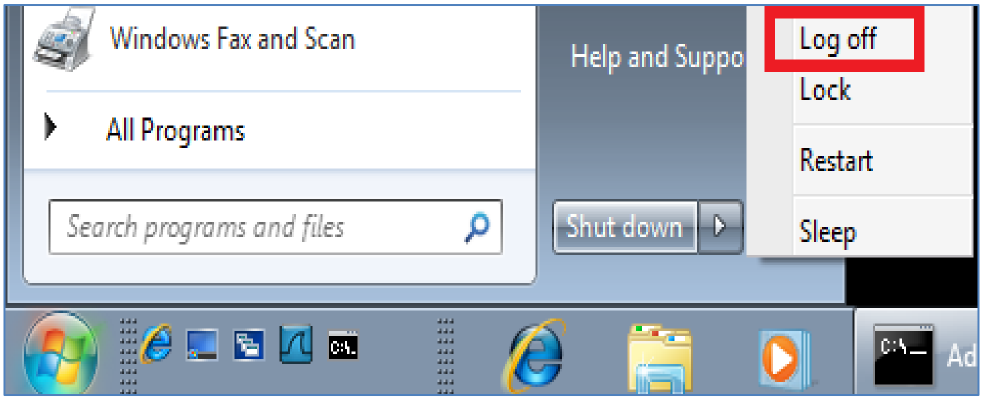


Figure 40: Log Off

21. Click on the icon with the name **student** at the Welcome Page

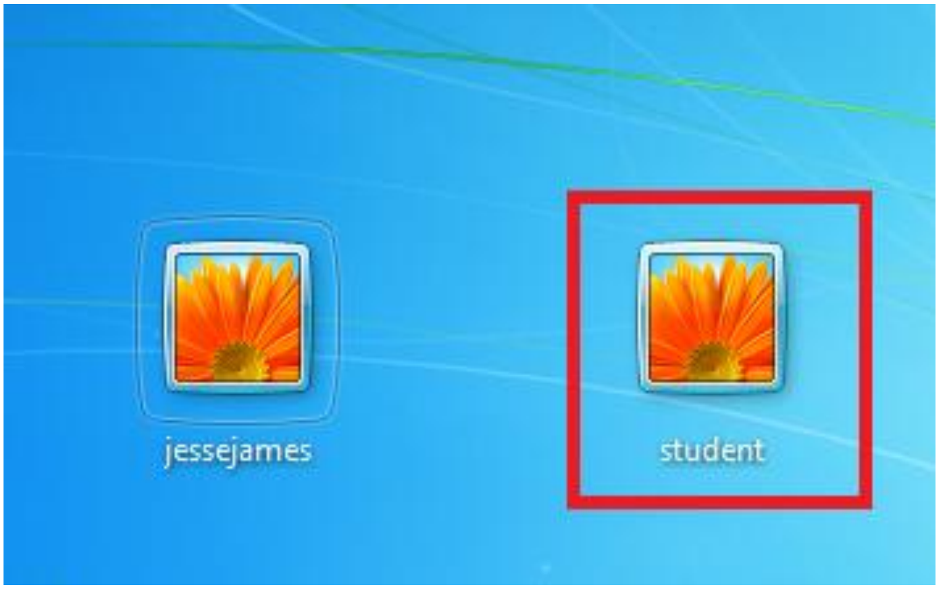


Figure 41: Log on as Student

22. Log on to the Windows 7 Internal Attack Machine, as **student** with the password of **123**.

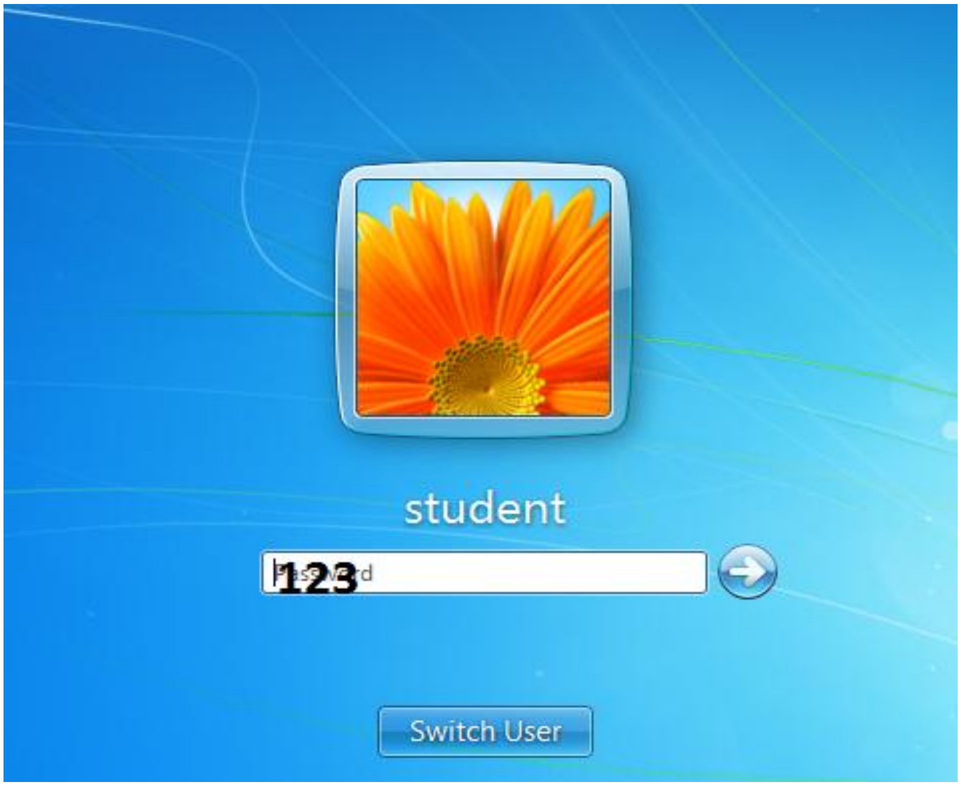


Figure 42: Logging on to the Windows 7 Machine

23. Click on the **Start** Button and select **Computer** from the Start Menu.

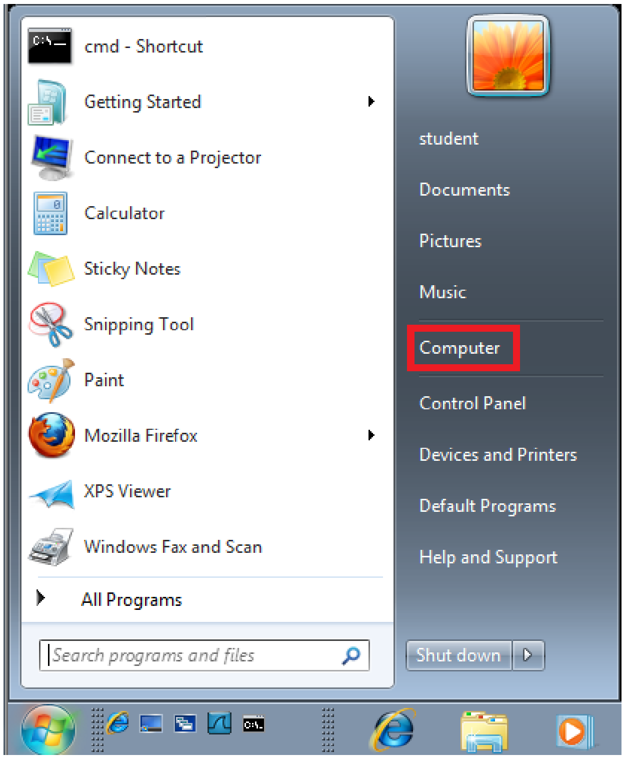


Figure 43: Start Menu

24. Under **Hard Disk Drives (1),** double-click on **Local Disk (C:).**

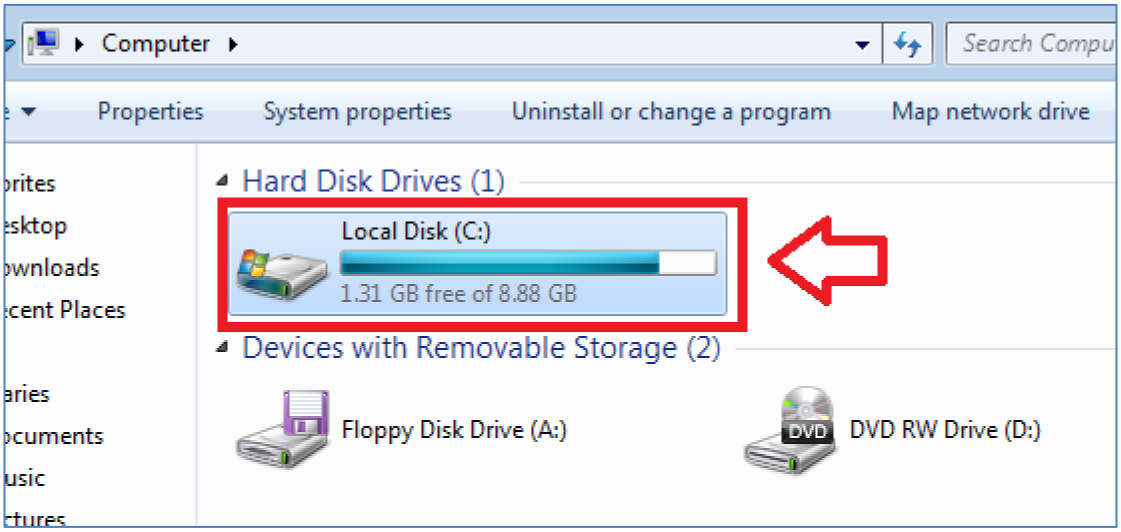


Figure 44: The C: Drive

25. Double-click on the **private** folder located on the root of the C: Drive.

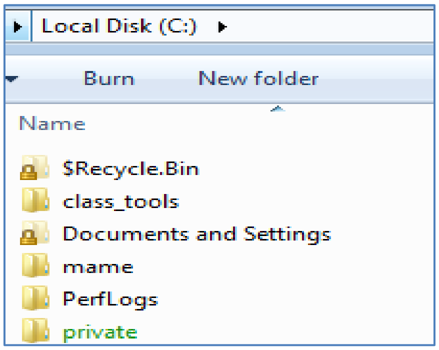
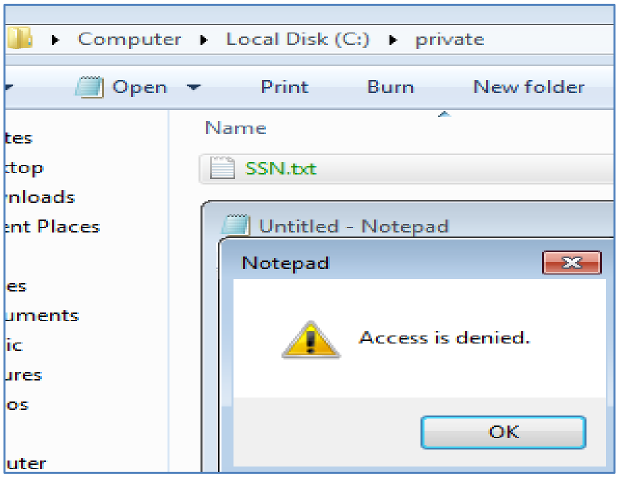


Figure 45: The Private Folder

26. Try to open **SSN.txt**. Access is denied.



Access is denied.

Figure 46: Access is Denied

2.2 Conclusion

EFS keys can be backed up. It is important to back up the EFS key because if the user's password is changed, they will no longer be able to access their EFS files. It is very important to set a very strong password when you are generating the recover key.

2.3 Discussion Questions

1. Where does a user go to back up their Encrypted File System keys?
2. Will a user be able to access their EFS files after they change their password?
3. What is the command to change the user student's password to 123?
4. Why is it important to set a strong password when generating a recover key?

3 Encrypted File System Key Recovery

If a user's password is changed, they cannot access their EFS files. However, if the certificate was backed up prior to changing the password, the file can be recovered. EFS files can be recovered by installing the Personal Information Exchange File (PFX) file.

3.1 File Recovery by Installing the PFX File

1. Click on the **Start** Button and select **Documents** from the start menu.

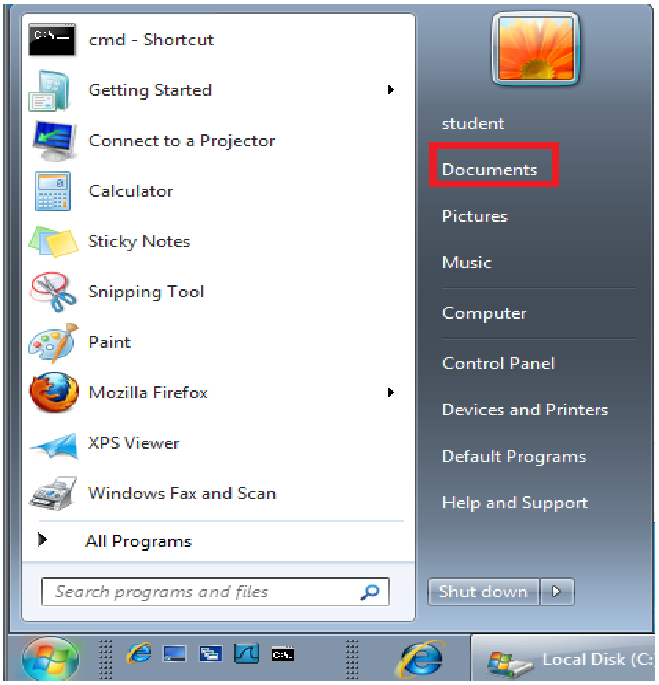


Figure 47: Documents Link

2. Right-click on the **mykey.pfx** file and select **Install PFX**.

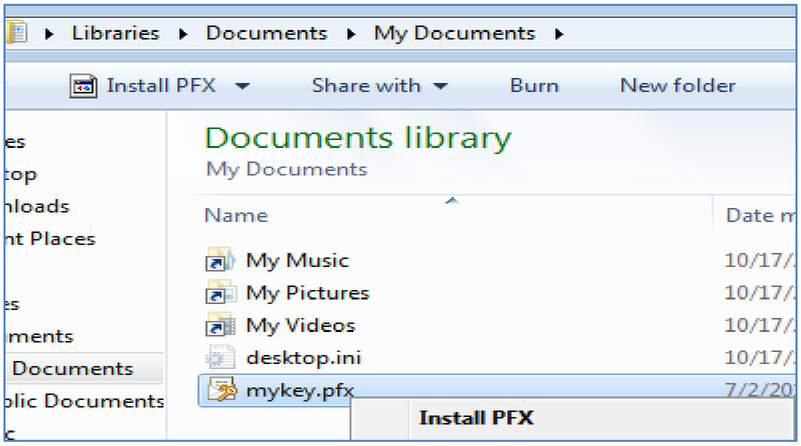
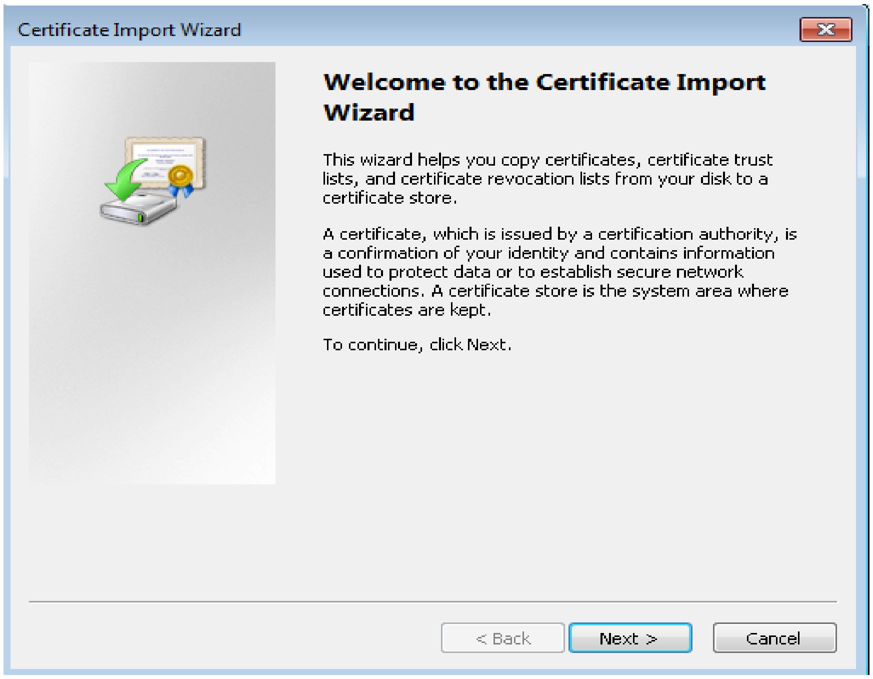


Figure 48: Install PFX

Copyright © 2013 CSSIA, NISGTC

3. Click **Next** at the Welcome to the Certificate Import Wizard Screen



Certificate Import Wizard

Welcome to the Certificate Import Wizard

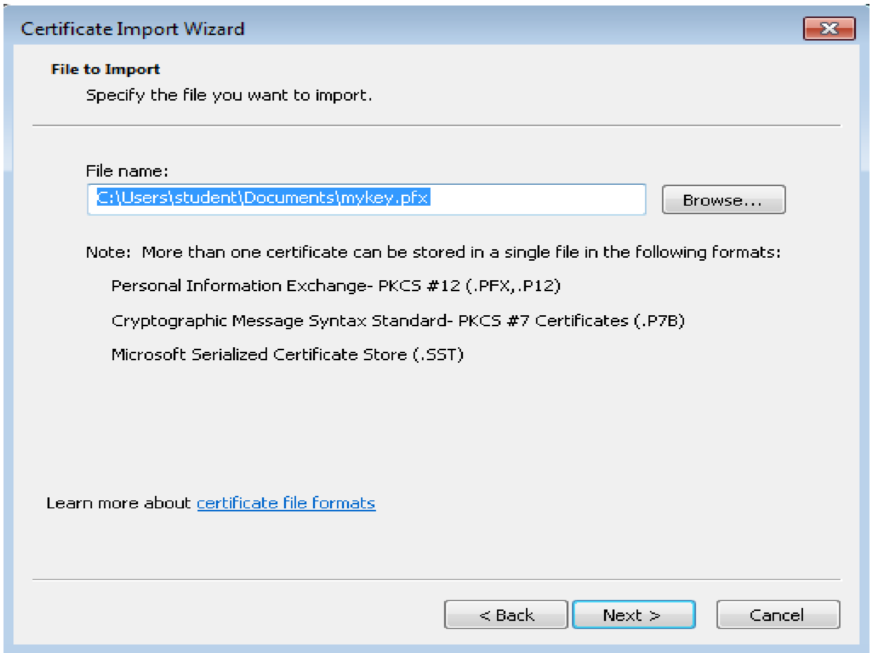
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 49: Certificate Import Wizard

4. Click **Next** at the **File to Import Screen**



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\student\Documents\mykey.pfx

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

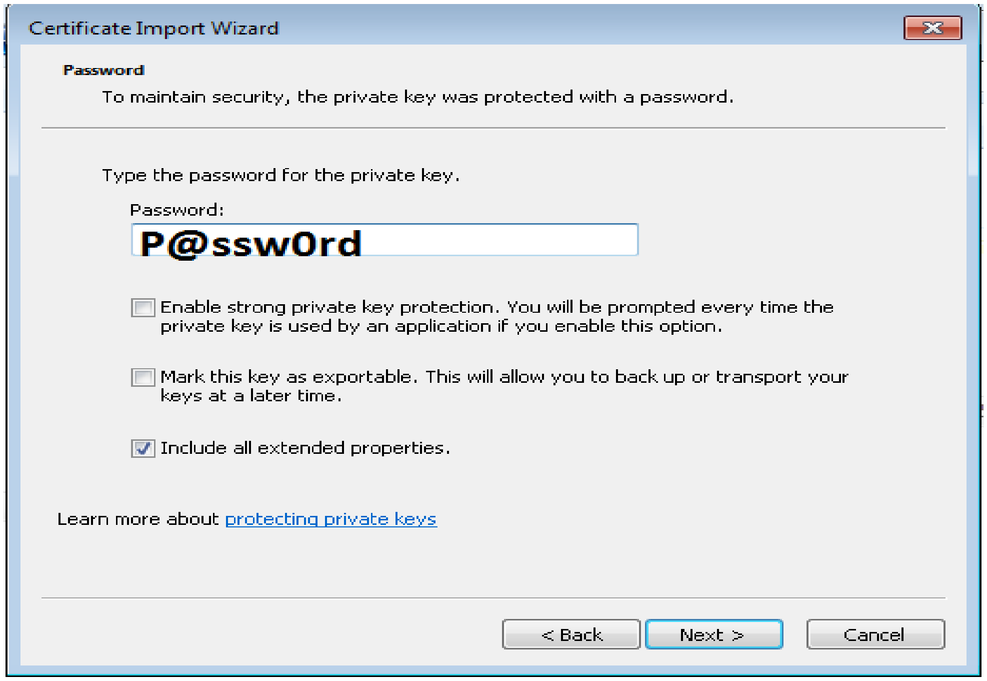
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 50: File to Import Screen

5. Type the password of **P@ssw0rd** for the Private key and click **Next.**



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: P@ssw0rd

□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

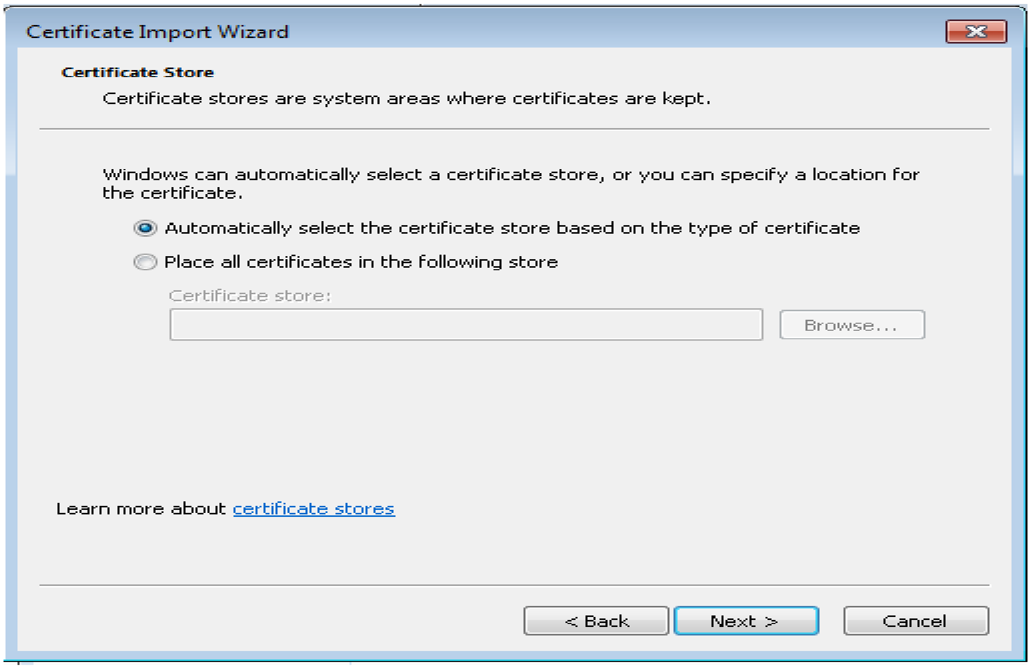
□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

Figure 51: Configuring the Firewall Rules

6. Click **Next** at the **Certificate Import Wizard**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

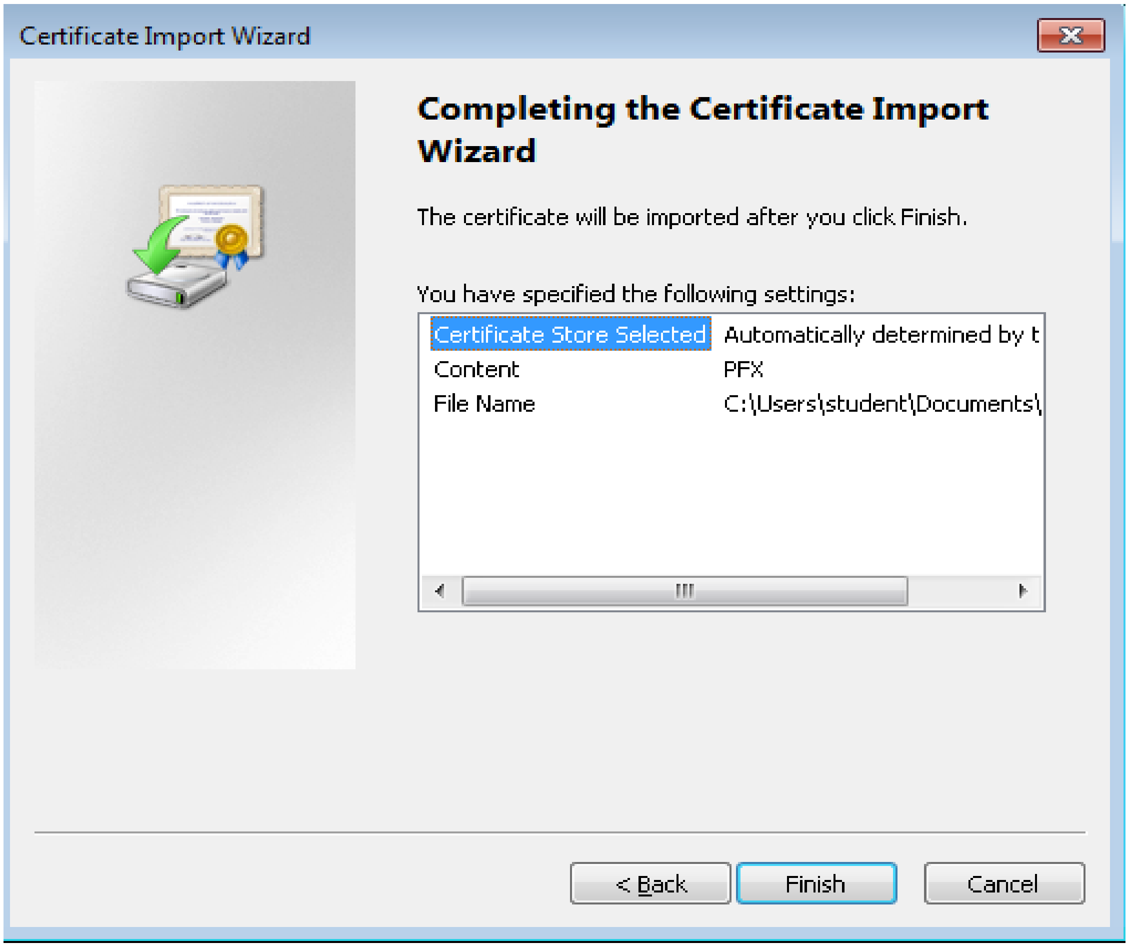
○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

Figure 52: Certificate Store

7. Click **Finish** the Completing the Certificate Import Wizard.



Completing the Certificate Import Wizard

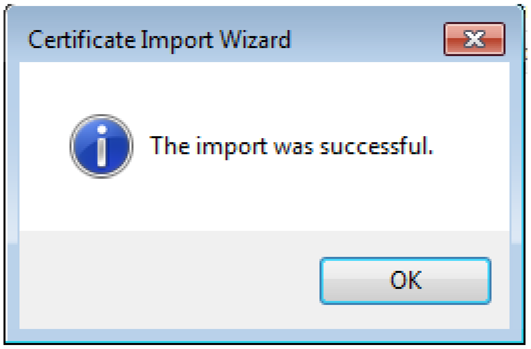
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\student\Documents\

Figure 53: Finishing the Import

8. Click **OK** to the message box that states, *the import was successful*.



The import was successful.

Figure 54: The Key was Imported

9. Click on the **Start** Button and select **Computer** from the start menu.

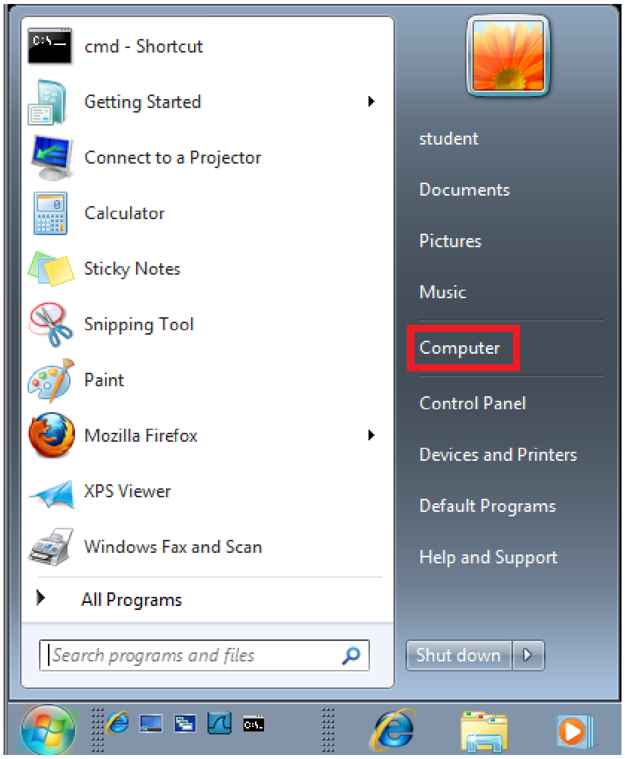


Figure 63: Start Menu

10. Under **Hard Disk Drives (1),** double-click on **Local Disk (C:).**

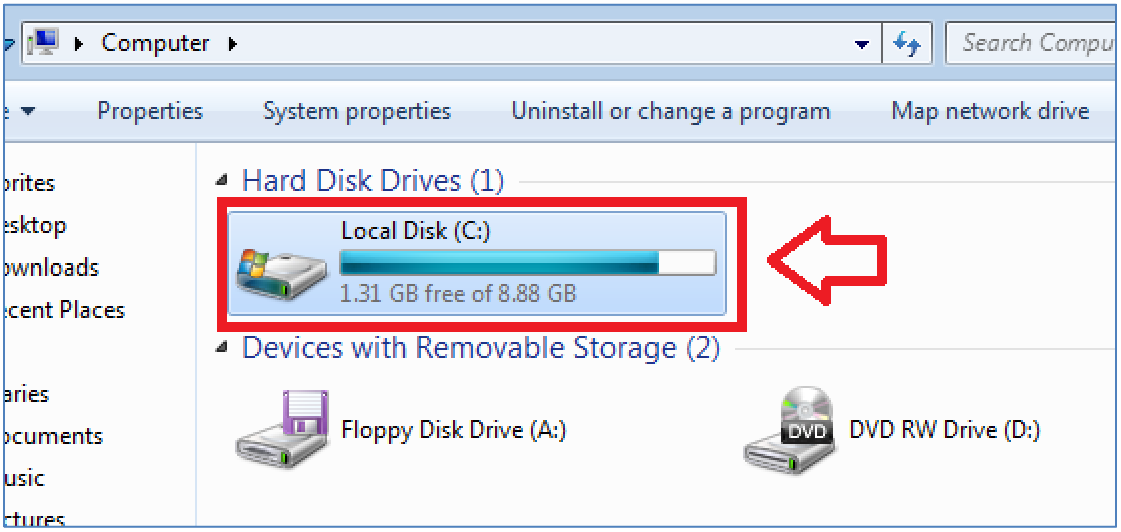


Figure 55: The C: Drive

11. Double-click on the **private** folder located on the root of the C: Drive.

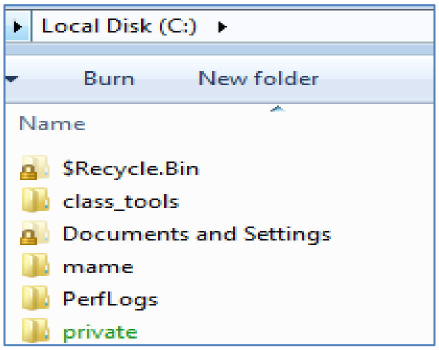
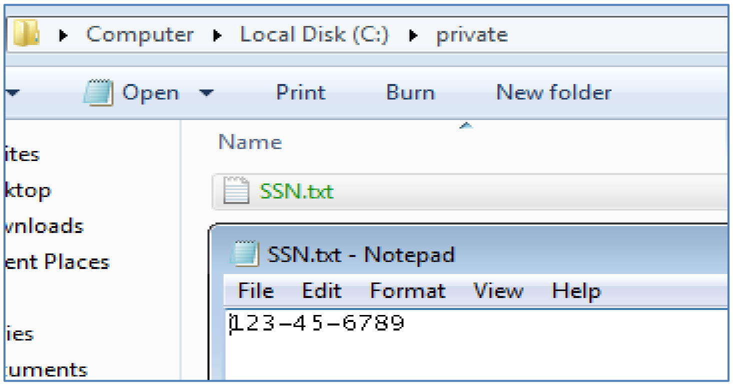


Figure 56: The Private Folder

12. Try to open **SSN.txt.** Access has been restored.



```
123-45-6789
```

Figure 57: The File Opens

3.2 Conclusion

When you change your password, you can no longer access your EFS files. However, if you back up the recovery key before the password is changed, EFS files can be recovered. In order to recover the EFS files, you must install the saved PFX file.

3.3 Discussion Questions

1. What needs to be provided when installing a PFX key?
2. What is the default color of EFS files and folders?
3. How can you determine if the certificate was imported successfully?
4. Install the PFX file to recover EFS files and folders. What does PFX stand for?

Copyright © 2013 CSSIA, NISGTC

References

1. Invalid Social Security Numbers:
   http://www.nesug.org/proceedings/nesug07/ap/ap19.pdf

2. Overview of EFS:
   http://technet.microsoft.com/en-us/library/cc700811.aspx

3. Net user command:
   http://ss64.com/nt/net_useradmin.html

4. Echo command:
   http://www.computerhope.com/echohlp.htm

5. PFX files:
   http://en.wikipedia.org/wiki/PKCS_%E2%99%AF12

Copyright © 2013 CSSIA, NISGTC