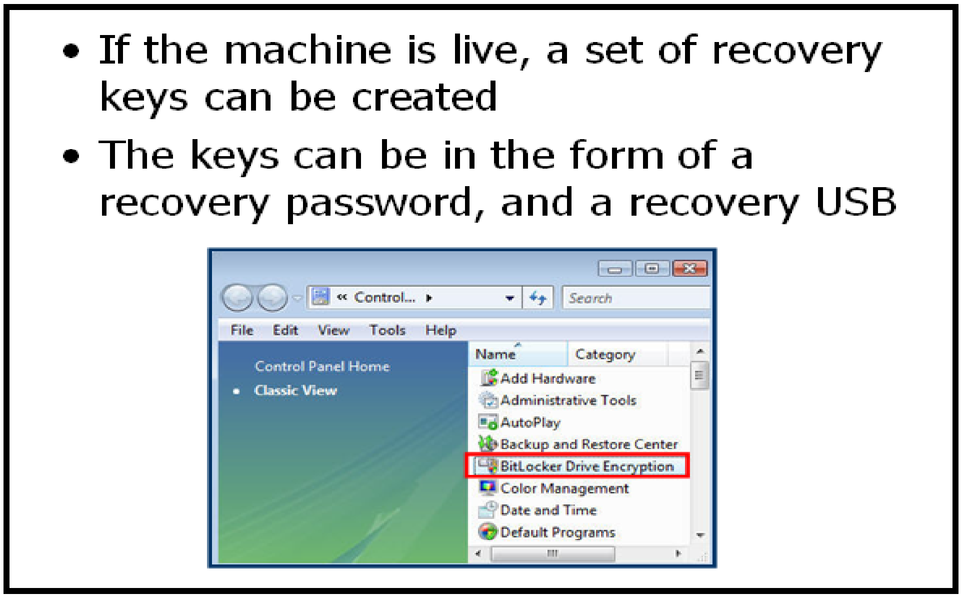
Windows Vista BitLocker

Creating a Recovery Key

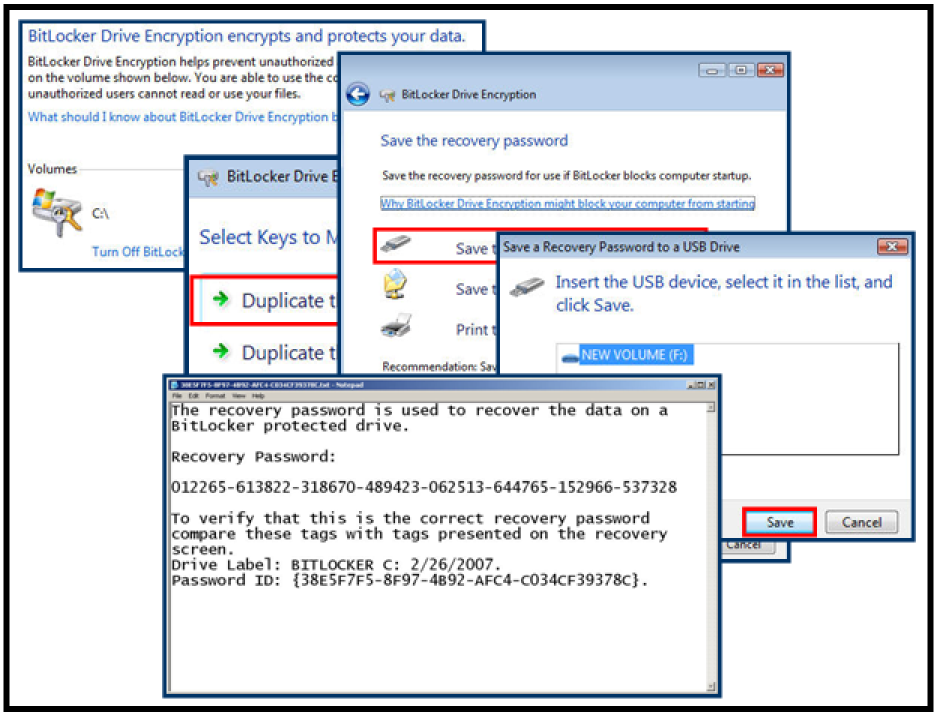


- If the machine is live, a set of recovery keys can be created
- The keys can be in the form of a recovery password, and a recovery USB

There are several methods available to generate a recovery key if the system is live when seized. While intrusive, it is not as intrusive as a live image and it still provides access to the data after it is downed. Recovery keys can be generated using the BitLocker utilities from the Control Panel.

To generate a set of recovery keys while the system is live:

1. Open the Control Panel and click **Classic View** in the upper left of the panel.
2. Double-click the **BitLocker Drive Encryption** icon.
3. The BitLocker utility locates the BitLocker encrypted drives.
4. Click **Manage BitLocker Keys** at the bottom of the screen.


BitLocker Drive Encryption encrypts and protects your data.
What should I know about BitLocker Drive Encryption b
Volumes
C:\
Turn Off BitLock
BitLocker Drive E
Select Keys to M
Duplicate t
Duplicate t
BitLocker Drive Encryption
Save the recovery password
Why BitLocker Drive Encryption might block your computer from starting
Save t
Save t
Print t
Recommendation: Sa
Save a Recovery Password to a USB Drive
NEW VOLUME (F:)
Save
Cancel
Cancel

BitLocker Drive Encryption helps prevent unauthorized
on the volume shown below. You are able to use the c
unauthorized users cannot read or use your files.

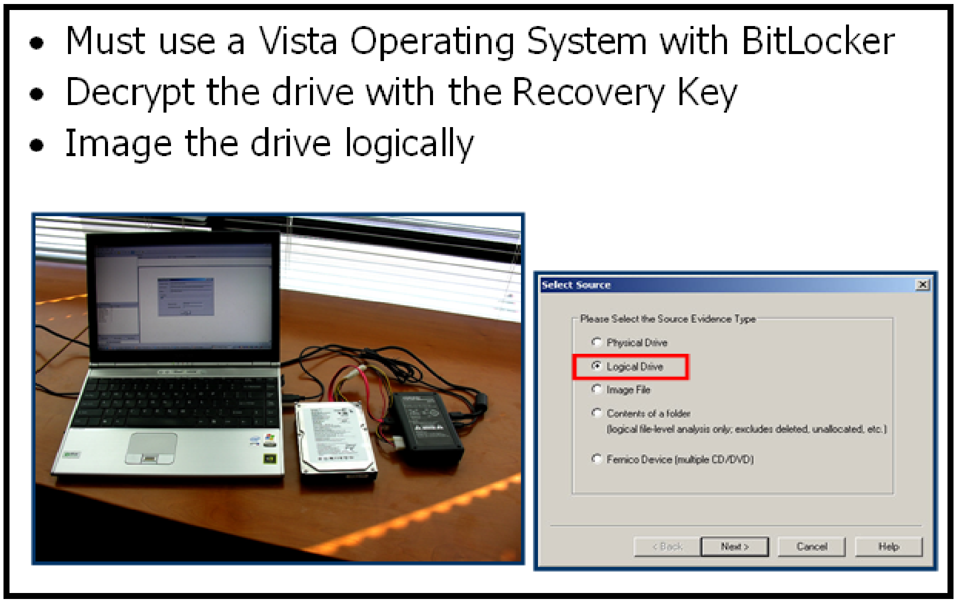
Save the recovery password for use if BitLocker blocks computer startup.

Insert the USB device, select it in the list, and click Save.

```
The recovery password is used to recover the data on a
BitLocker protected drive.

Recovery Password:

012265-613822-318670-489423-062513-644765-152966-537328

To verify that this is the correct recovery password
compare these tags with tags presented on the recovery
screen.
Drive Label: BITLOCKER C: 2/26/2007.
Password ID: {38E5F7F5-8F97-4B92-AFC4-C034CF39378C}.
```

5. Vista asks if you want to duplicate the recovery password and the startup key.
6. Select **Duplicate the Recovery Password**.
7. The utility gives the option of saving the password to a USB device or folder, or to print the password. When saving to a USB device, Vista displays all local removable devices currently attached to the system.
8. Select the method you want and it copies the .txt file identified by a GUID to the device.

Imaging a BitLocker Encrypted Drive



- Must use a Vista Operating System with BitLocker
- Decrypt the drive with the Recovery Key
- Image the drive logically

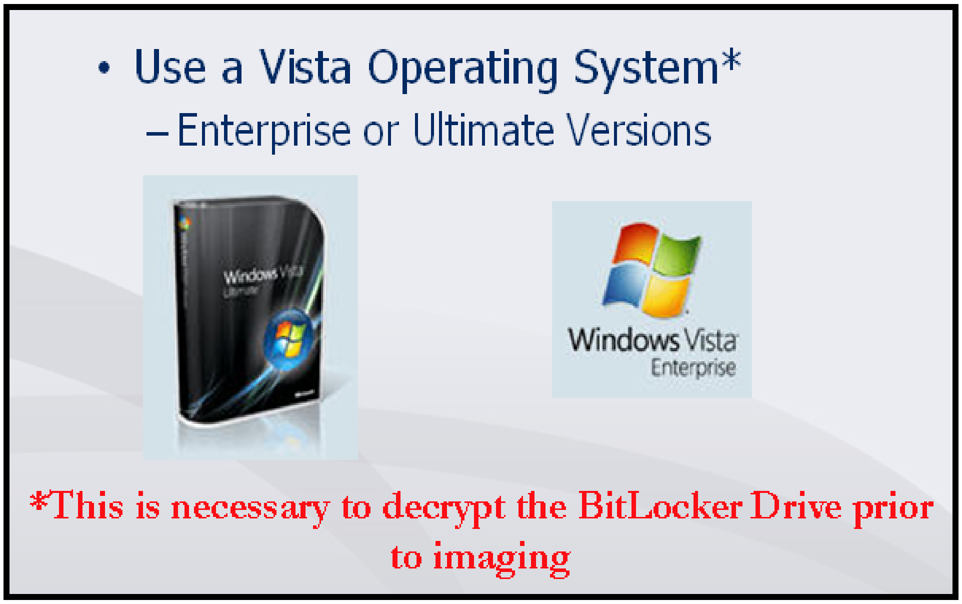
Select Source

Please Select the Source Evidence Type

○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Fernico Device (multiple CD/DVD)

To image a BitLocker encrypted drive:

1. Boot an investigative computer that has a version of Vista that supports BitLocker.



- Use a Vista Operating System*
  - Enterprise or Ultimate Versions

*This is necessary to decrypt the BitLocker Drive prior to imaging

Windows Vista
Ultimate
Windows Vista
Enterprise

2. The encrypted drive is unlocked using the investigative BitLocker utility by applying the recovery key. The drive must then be imaged logically.

3. Connect the source drive to the investigative computer.

Remove suspect drive and mount it as a foreign volume with a write protect device

4. Use a write-block device to protect the source drive and boot the Vista system.

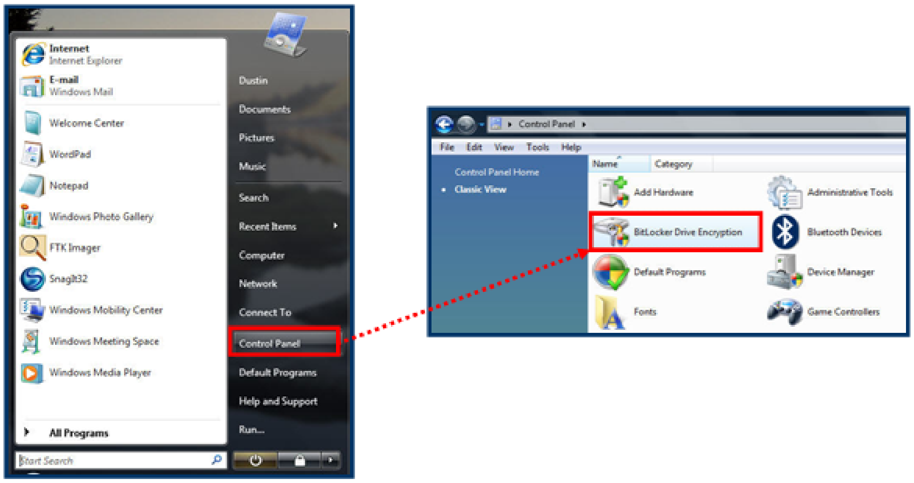
5. Vista is used to mount the drive as a foreign drive if it has been removed from the suspect's computer.

6. Start the BitLocker Drive Encryption Utility.

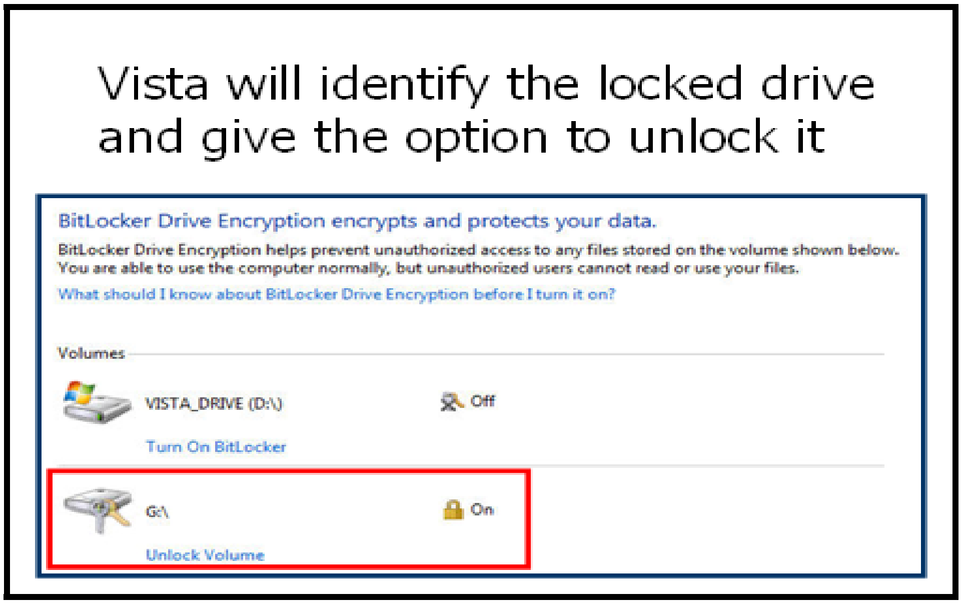
7. Open the Control Panel.

8. Double-click BitLocker Drive Encryption.

Launch BitLocker from the Control Panel



9. Vista identifies the volumes that have BitLocker encryption by displaying a golden lock icon.



Vista will identify the locked drive and give the option to unlock it

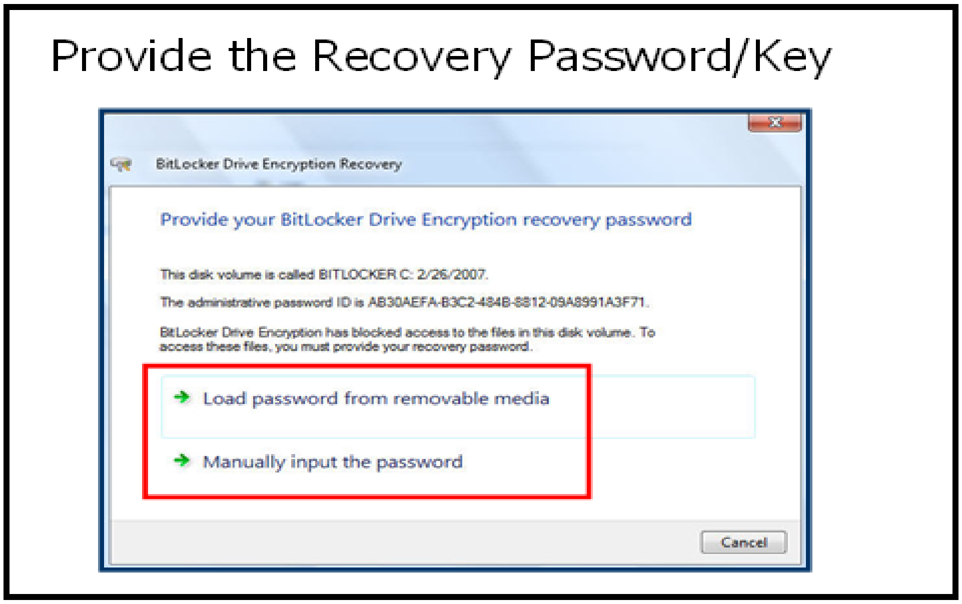
BitLocker Drive Encryption encrypts and protects your data.

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the volume shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

What should I know about BitLocker Drive Encryption before I turn it on?

10. For those volumes, BitLocker also has an Unlock Volume link to decrypt the data.

11. Once the partition is selected, click Load password from removable media or manually input the password (the 48-character recovery password).



Provide the Recovery Password/Key

BitLocker Drive Encryption Recovery

Provide your BitLocker Drive Encryption recovery password

This disk volume is called BITLOCKER C: 2/26/2007.

The administrative password ID is AB30AEFA-B3C2-484B-8812-09A8991A3F71.

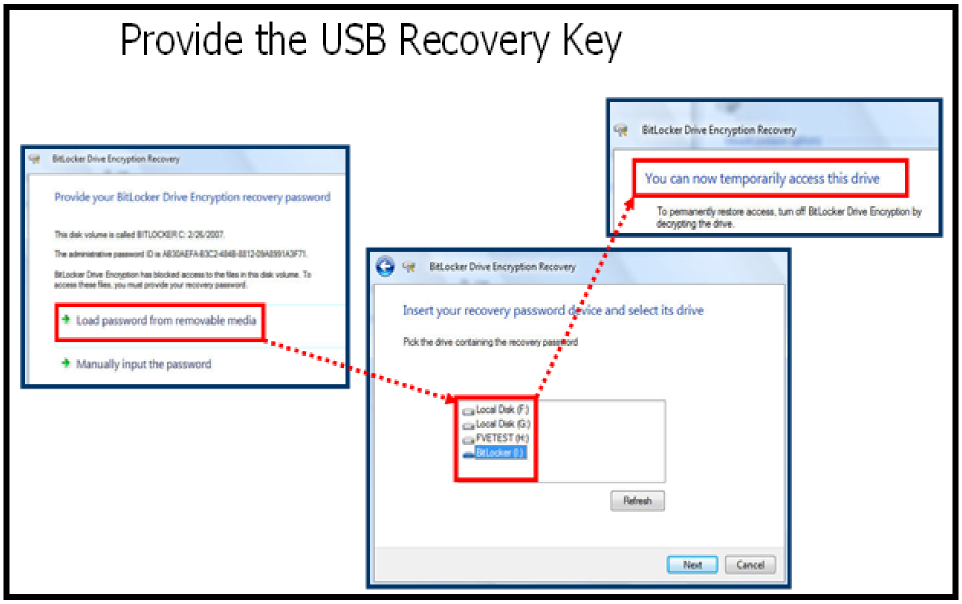
BitLocker Drive Encryption has blocked access to the files in this disk volume. To access these files, you must provide your recovery password.

Load password from removable media
Manually input the password
Cancel

12. If you choose to load the password from removable media, Vista displays only the available removable drives.

13. Provide the decryption credentials.

14. Select the drive that contains the USB Recovery Key.



Provide the USB Recovery Key

BitLocker Drive Encryption Recovery

Provide your BitLocker Drive Encryption recovery password

This disk volume is called BITLOCKER C: 2/26/2007.

The administrative password ID is AB30AEFA-B3C2-4848-8812-09A8991A3F71.

BitLocker Drive Encryption has blocked access to the files in this disk volume. To access these files, you must provide your recovery password.

BitLocker Drive Encryption Recovery

Insert your recovery password device and select its drive

Pick the drive containing the recovery password

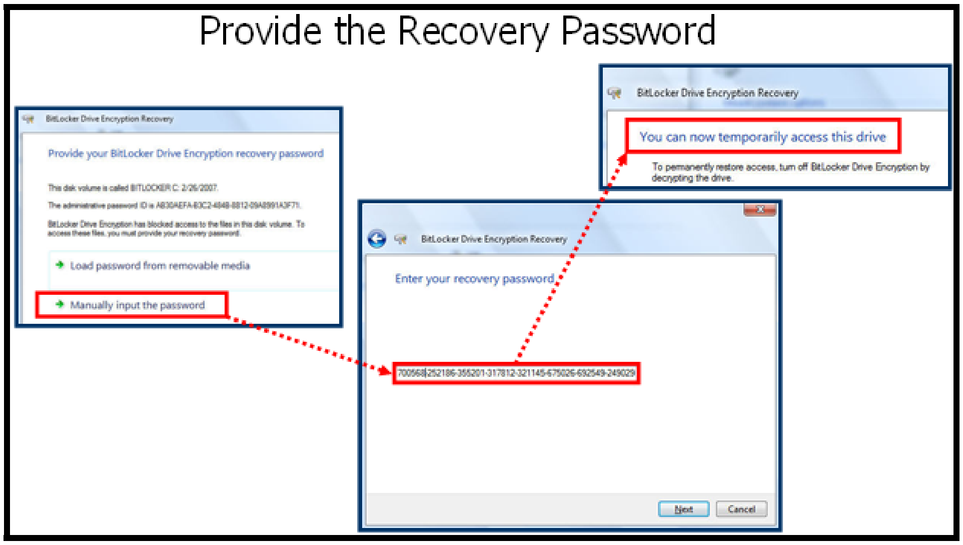
BitLocker Drive Encryption Recovery

You can now temporarily access this drive

To permanently restore access, turn off BitLocker Drive Encryption by decrypting the drive.

15. Provide the Recovery Password.

16. If you choose to manually input the password, Vista displays an entry box for the key.



Provide the Recovery Password

BitLocker Drive Encryption Recovery

Provide your BitLocker Drive Encryption recovery password

This disk volume is called BITLOCKER C: 2/26/2007.

The administrative password ID is AB30AEFA-B3C2-4848-8812-09A8991A3F71.

BitLocker Drive Encryption has blocked access to the files in this disk volume. To access these files, you must provide your recovery password.

BitLocker Drive Encryption Recovery

Enter your recovery password

700568-252186-355201-317812-321145-675026-692549-249029

BitLocker Drive Encryption Recovery

You can now temporarily access this drive

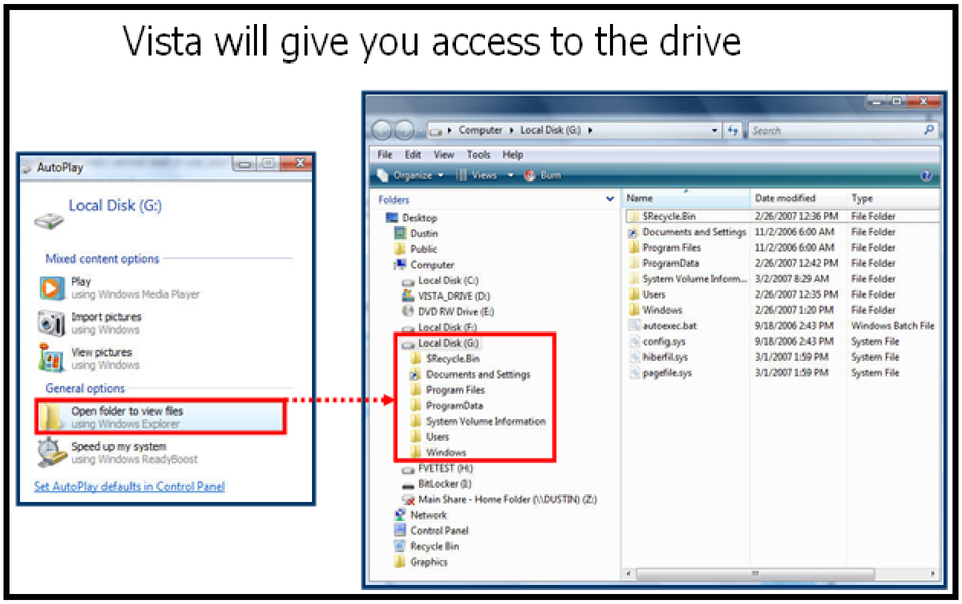
To permanently restore access, turn off BitLocker Drive Encryption by decrypting the drive.

Load password from removable media
Manually input the password
Next
Cancel

17. Enter only the numeric values (and not the hyphens).

18. After you enter the correct password, Vista displays the message, “You can now temporarily access this drive.”

19. You can now access the drive.



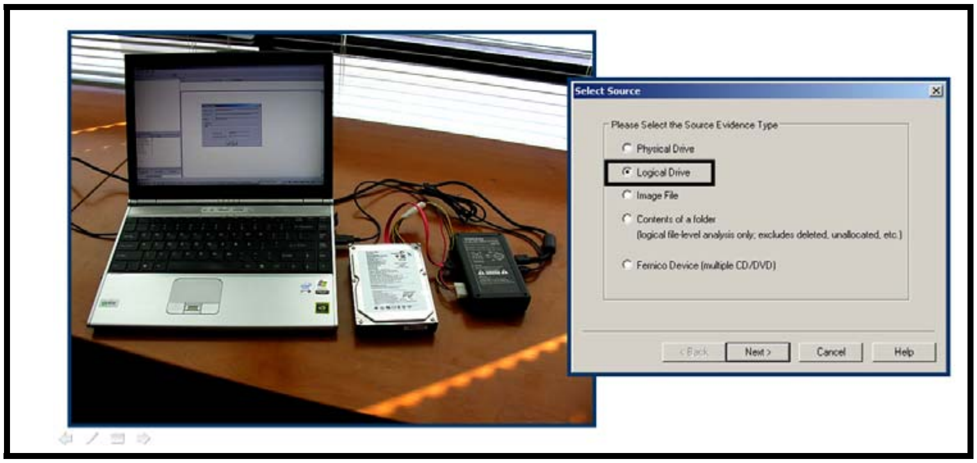
Vista will give you access to the drive

Name	Date modified	Type
$Recycle.Bin	2/26/2007 12:36 PM	File Folder
Documents and Settings	11/2/2006 6:00 AM	File Folder
Program Files	11/2/2006 6:00 AM	File Folder
ProgramData	2/26/2007 12:42 PM	File Folder
System Volume Inform...	3/2/2007 8:29 AM	File Folder
Users	2/26/2007 12:35 PM	File Folder
Windows	2/26/2007 1:20 PM	File Folder
autoexec.bat	9/18/2006 2:43 PM	Windows Batch File
config.sys	9/18/2006 2:43 PM	System File
hiberfil.sys	3/1/2007 1:59 PM	System File
pagefile.sys	3/1/2007 1:59 PM	System File

After the drive is unlocked, Vista displays the encrypted drive in a Windows Explorer view.

You can turn off BitLocker encryption. However, merely turning it off does not decrypt the drive. It unlocks the FVEK so that it is not encrypted during the boot process. The system boots normally and continues to decrypt the drive in memory. A full decryption must be completed to remove the BitLocker encryption from the drive.

At this point, the drive can be imaged as any other drive.



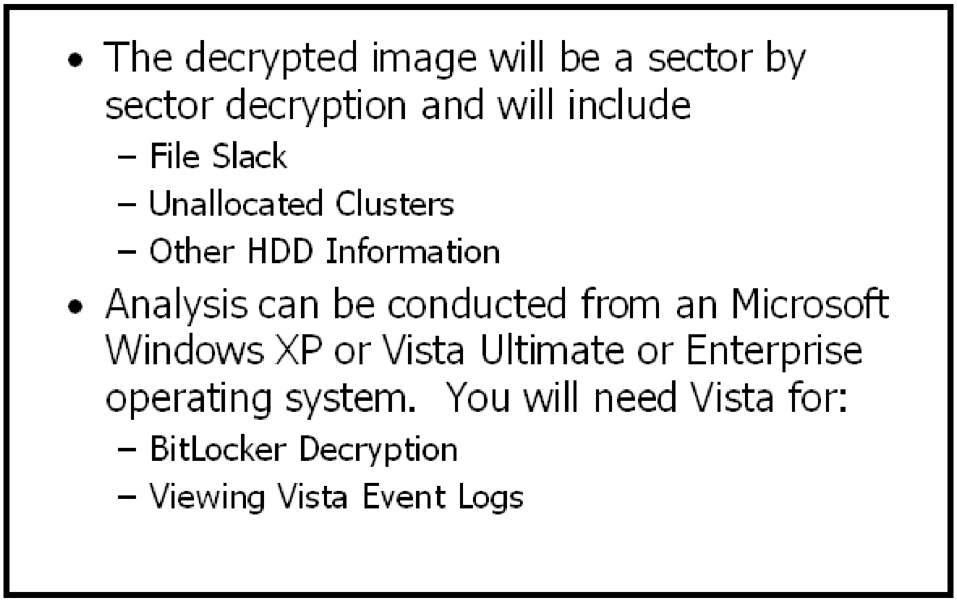
Select Source

Please Select the Source Evidence Type

○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Fernico Device (multiple CD/DVD)

The image must be a logical image. If you make a physical image of the drive, it is just encrypted data. By making a logical image, BitLocker decrypts the data in memory as it is streamed to the destination drive.

BitLocker Analysis



- The decrypted image will be a sector by sector decryption and will include
  - File Slack
  - Unallocated Clusters
  - Other HDD Information
- Analysis can be conducted from an Microsoft Windows XP or Vista Ultimate or Enterprise operating system. You will need Vista for:
  - BitLocker Decryption
  - Viewing Vista Event Logs

The decrypted data contains file slack—data in unallocated clusters and all other artifacts as in a normal logical image. Because the data is encrypted on a sector-by-sector basis, the operating system doesn’t distinguish between allocated and unallocated sectors/clusters and decrypts all logical sectors in that partition.

When conducting your analysis, you can use either Microsoft Windows XP or Vista Ultimate or Enterprise. You will need Vista if you need to decrypt BitLocker and view event logs.