Introduction to BitLocker FVE

(Understanding the Steps Required to enable BitLocker)

Exploration of Windows 7
Advanced Forensic Topics – Day 3
What is BitLocker?

BitLocker Drive Encryption is a full disk encryption feature included with Microsoft's Windows Vista Ultimate, Windows Vista Enterprise, Windows Server 2008, Windows 7 Ultimate, and Windows 7 Enterprise operating systems designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm with a 128 bit key, combined with a diffuser for additional disk encryption specific security not provided by AES.
Why Bitlocker Exists

“Some of the largest and medium-sized U.S. airports report close to 637,000 laptops lost each year, according to the Ponemon Institute survey released Monday”
– PC World June 2008

“More than 100 USB memory sticks, some containing secret information, have been lost or stolen from the Ministry of Defense since 2004, it has emerged.”
– BBC News July 2008
BitLocker Requirements

- Windows 7 Enterprise or Ultimate
- TPM Chip version 1.2 or later (and/or) a BIOS capable of reading USB devices pre-boot
BitLocker Requirements

• BitLocker Installation
  – Operating System Installation
  – OPTIONAL: If not using TPM, edit Group Policy to allow USB key storage
  – Enabling of BitLocker and Volume Encryption
Enabling OS BitLocker via USB Key
Enabling BitLocker - OS
Enabling BitLocker - OS

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives 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?

BitLocker Drive Encryption - Hard Disk Drives

C: Off

Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

LOCKER (D:) Off

Turn On BitLocker
Enabling BitLocker - OS

Starting BitLocker

Please wait while BitLocker initializes the drive.

A compatible Trusted Platform Module (TPM) Security Device must be present on this computer, but a TPM was not found. Please contact your system administrator to enable BitLocker.

What are BitLocker's system requirements?
Enabling BitLocker - OS

Execute: gpedit.msc

Navigate: Computer Configuration\Administrative Templates\Windows Components
Enabling BitLocker – OS

![Image of the BitLocker configuration settings](image)

- **Options:**
  - Allow BitLocker without a compatible TPM

**Help:**

This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.

- **Note:** Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.

If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode a USB drive is required for start-up and the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable you will need to use one of the BitLocker recovery options to access the drive.

On a computer with a compatible TPM, four types of authentication methods can be used at startup to provide added protection for encrypted data. When the computer starts, it can use only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the
Enabling BitLocker - OS

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives 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?

BitLocker Drive Encryption - Hard Disk Drives

<table>
<thead>
<tr>
<th>Drive</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:</td>
<td>Off</td>
</tr>
</tbody>
</table>

BitLocker Drive Encryption - BitLocker To Go

<table>
<thead>
<tr>
<th>Drive</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCKER (D:)</td>
<td>Off</td>
</tr>
</tbody>
</table>

See also
- TPM Administration
- Disk Management
- Read our privacy statement online
Enabling BitLocker - OS

Checking your computer's configuration

BitLocker is verifying that your computer meets its system requirements. This might take a few minutes.

What are BitLocker's system requirements?
Enabling BitLocker - OS

Set BitLocker startup preferences

This computer does not appear to have a TPM. To use BitLocker Drive Encryption, a startup key on a USB flash drive will be required every time you start the computer.

- Use BitLocker without additional keys
- Require a PIN at every startup

Require a Startup key at every startup

Some settings are managed by your system administrator.

What is a BitLocker Drive Encryption startup key or PIN?
Enabling BitLocker - OS
Enabling BitLocker - OS

BitLocker Drive Encryption Recovery Key

The recovery key is used to recover the data on a BitLocker protected drive. To verify that this is the correct recovery key compare the identification with what is presented on the recovery key.

Recovery key identification: 1D8B346E-B8C4-47
Full recovery key identification: 1D8B346E-B8C4-47A6CD-FAE077F69A46

BitLocker Recovery Key:
045133-611842-097515-070279-679723-407099-551298-014080
Enabling BitLocker - OS

Are you ready to encrypt this drive?

The selected drive is C:

You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.

Run BitLocker system check

The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer to test the system before encrypting.

Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.
Enabling BitLocker

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives 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?

BitLocker Drive Encryption - Hard Disk Drives

C: Encrypting
  Turn Off BitLocker
  Manage BitLocker

BitLocker Drive Encryption - BitLocker To Go

LOCKER (D:)
  Off
  Turn On BitLocker

Encryption in progress
Encryption of C: by BitLocker Drive Encryption has started. Click for more information.
Enabling BitLocker - OS

Control Panel Home

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives 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?

BitLocker Drive Encryption - Hard Disk Drives

C:
Off

Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

USB THUMB (E:)

On

Turn Off BitLocker
Manage BitLocker

SD CARD (F:)
Off

Turn On BitLocker
Questions?
Enabling BitLocker “To Go”
Enabling BitLocker of USB Stick
Enabling BitLocker of USB Stick

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives 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?

BitLocker Drive Encryption - Hard Disk Drives

C:  
Off  

Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

USB THUMB (E:)
Off

Turn On Bit Locker

SD CARD (F:)
Off

Turn On Bit Locker
Enabling BitLocker of USB Stick

Starting BitLocker

Please wait while BitLocker initializes the drive.

⚠️ Do not remove your drive during BitLocker setup.

What are BitLocker’s system requirements?
Enabling BitLocker of USB Stick

Choose how you want to unlock this drive

- Use a password to unlock the drive
  Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.
  Type your password: 
  Retype your password:

- Use my smart card to unlock the drive
  You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?
Enabling BitLocker of USB Stick

Choose how you want to unlock this drive

- Use a password to unlock the drive
  - Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.
  - Type your password: ............................
  - Retype your password: ..........................

- Use my smart card to unlock the drive
  - You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.

How do I use these options?
Enabling BitLocker of USB Stick

BitLocker Drive Encryption Recovery Key

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

To verify that this is the correct recovery key compare the identification with what is presented on the recovery key.

Recovery key identification: 3C8062B5-D6A2-4F
Full recovery key identification: 3C8062B5-D6A2-4FDC-8E0D-0CF123CDCE88

BitLocker Recovery Key:
134882-198088-642180-567545-557920-569041-128777-202840
Enabling BitLocker of USB Stick
Unlocking your BitLocker enabled USB

- Insert USB device into PC and type your password when prompted

NOTE: The device can be unlocked on any Bitlocker To Go capable PC if you know the password
Unlocking your BitLocker enabled USB

- Insert USB device into PC and type your password when prompted

NOTE: The device can be unlocked on any BitLocker To Go capable PC if you know the password
USB is now encrypted… Now what!?

- If the encrypted USB is formatted with FAT then it can be used on down level Operating Systems
  - Win XP
  - Windows Vista

- How is this possible? These Operating Systems did not have Bitlocker to go functionality.
USB is now encrypted... Now what!?!
USB is now encrypted… Now what!?

- Previous versions of Windows can use BitLocker To Go with the help of the included BitLockerToGo.exe included on the encrypted drive.
- This app provides the user interface to unlock the encrypted drive. It allows only the ability to read and copy data from the drive. If you need full featured BitLocker, you must use it with a Win7 machine.
Enabling BitLocker with a Thumb drive as a startup key

Exercise
Enabling BitLocker Encryption of a Thumb drive

Exercise
BitLocker Technical Details

Exploration of Windows 7
Advanced Forensic Topics – Day 3
What is BitLocker

• Review: BitLocker is a mechanism by which entire volumes of data can be secured in Windows 7:
  – Enterprise
  – Ultimate

• Why is this important?
  – This mechanism helps to protect systems from offline attacks.
  – Tell me again, how do we examine a suspect machine?
How is BitLocker Implemented

TPM Only
“What it is.”
Protects against: SW-only attacks
Vulnerable to: HW attacks (including potentially “easy” HW attacks)

Dongle Only
“What you have.”
Protects against: All HW attacks
Vulnerable to: Losing dongle Pre-OS attacks

TPM + PIN
“What you know.”
Protects against: Many HW attacks
Vulnerable to: TPM breaking attacks

TPM + Dongle
“Two what I have’s.”
Protects against: Many HW attacks
Vulnerable to: HW attacks

Ease of Use
Security
# BitLocker in Windows Vista

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Unlock Methods</th>
<th>Recovery Methods</th>
<th>Management</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System Drives</td>
<td>TPM</td>
<td>Recovery password</td>
<td>Group policy controlled options presented to users</td>
<td>Use of the BitLocker Drive Preparation Tool to create a system partition where boot files are located.</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN</td>
<td>Recovery Key</td>
<td></td>
<td>System partition size: 1.5GB</td>
</tr>
<tr>
<td></td>
<td>TPM+Start up key</td>
<td>Active Directory backup of recovery password</td>
<td></td>
<td>System partition assigned a drive letter</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN+Startup Key*</td>
<td>Startup key</td>
<td></td>
<td>NTFS file system.</td>
</tr>
<tr>
<td></td>
<td>Startup key</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Data Drives*</td>
<td>Automatic unlocking</td>
<td>Same as OS drive</td>
<td>No policies</td>
<td>Operating System drive must be encrypted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NTFS file system.</td>
</tr>
</tbody>
</table>

*Introduced in Windows Vista SP1
## BitLocker in Windows 7

### Operating system drive overview

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Unlock Methods</th>
<th>Recovery Methods</th>
<th>Management</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System Drives</strong></td>
<td>TPM</td>
<td>Recovery password</td>
<td>Robust and consistent Group Policy enforcement</td>
<td>Drive preparation fully integrated in BitLocker setup.</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN</td>
<td>Recovery Key</td>
<td>Minimum Pin Length</td>
<td>System partition size: 200MB without WinRE</td>
</tr>
<tr>
<td></td>
<td>TPM+Startup key</td>
<td>Active Directory backup of recovery password</td>
<td></td>
<td>400MB with WinRE</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN+Startup Key</td>
<td>Data Recovery Agent</td>
<td></td>
<td>System partition letterless</td>
</tr>
<tr>
<td></td>
<td>Startup key</td>
<td></td>
<td></td>
<td>NTFS file system.</td>
</tr>
</tbody>
</table>

- **Data Recovery Agent**
- **System partition letterless**

- **NTFS file system.**
BitLocker in Windows 7
Setup improvements

• Windows 7 is BitLocker ready
  – A separate system partition is now standard
  – System partition is now letter-less and hidden
  – BitLocker Drive Preparation Tool now integrated into the BitLocker setup experience

• Improved setup experience
  – Improved BitLocker setup wizard
  – Windows RE will be moved if installed on O/S partition
BitLocker in Windows 7
Specifications for split-loader configuration

<table>
<thead>
<tr>
<th>Windows RE</th>
<th>System Partition</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>250 MB</td>
<td>200 MB</td>
<td>Remaining Disk</td>
</tr>
<tr>
<td>NTFS</td>
<td>NTFS</td>
<td>NTFS</td>
</tr>
</tbody>
</table>

Note: An additional 50MB is required on the recovery partition for volume snapshots during Complete PC backups.
# Windows 7 BitLocker To Go

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Unlock Methods</th>
<th>Recovery Methods</th>
<th>Management</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable data drives</td>
<td>Passphrase</td>
<td>Recovery password</td>
<td>Robust and consistent group policy controls</td>
<td>File systems:</td>
</tr>
<tr>
<td>e.g.: USB flash drives</td>
<td>Smart card</td>
<td>Recovery Key</td>
<td>Ability to mandate encryption prior to granting write access</td>
<td>NTFS, FAT, FAT32, ExFAT</td>
</tr>
<tr>
<td>External Hard Drives</td>
<td>Automatic Unlocking</td>
<td>Active Directory backup of recovery password</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Recovery Agent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- File systems: NTFS, FAT, FAT32, ExFAT
Windows 7 BitLocker To Go
New unlock methods

• Roaming using a Passphrase
  – No specific hardware requirement
  – Easily roam inside and outside domains/organizations
  – Complexity and length requirements managed by Group Policy
Windows 7 BitLocker To Go
New unlock methods

• Roaming using Smart Cards
  – Leverages existing PKI infrastructure
  – Requires specific hardware
  – Can roam to any computer running Windows 7 or Server 2008 R2
  – Uses much stronger keys than passphrase Roaming using a Passphrase
Windows 7 BitLocker To Go
New recovery mechanism

• Data Recovery Agents (DRA)
  – Certificate-based key protector
    > A certificate containing a public key is distributed through Group Policy and is applied to any drive that mounts
    > The corresponding private key is held by a DRA in corpsec
  – Allows IT department to have a way to unlock all protected drives in an enterprise
  – Leverage existing PKI infrastructure
  – Saves space in AD – same Key Protector on all drives
  – Also applies to O/S and fixed drives
Windows 7 BitLocker To Go

Managing BitLocker

- BitLocker from Windows Explorer
- Right click drives in Windows Explorer to:
  - Turn on BitLocker
  - Unlock a drive
  - Manage BitLocker
Windows 7 BitLocker To Go
Managing BitLocker removable drives

• Data Drives
  – Add, remove, or change their passphrase
  – Add or remove a smart card
  – Add or remove automatic unlocking
  – Duplicate their recovery key/password
Windows 7 BitLocker To Go - Enterprise

Mandating BitLocker on removable drives

• Requiring BitLocker for removable data drives
  – When this policy is enforced, all removable drives will require BitLocker protection in order to have write access
  – As soon as a drive is plugged into a machine, a dialog is displayed to the user to either enable BitLocker on the device or only have read-only access
Windows 7 BitLocker To Go

Mandating BitLocker on removable drives

- The user gets full RW access only after encryption is completed
- Users can alternatively enable BitLocker at a later time
Disk Layout and Key Storage

Operating system volume contains:
- encrypted OS
- encrypted page file
- encrypted temp files
- encrypted data
- encrypted hibernation file

Where’s the encryption key?
- SRK (Storage Root Key) contained in TPM
- SRK encrypts the VMK (Volume Master Key).
- VMK encrypts FVEK (Full Volume Encryption Key) – used for the actual data encryption.
- FVEK and VMK are stored encrypted on the Operating System Volume.

System volume contains:
- MBR
- Boot Manager
- Boot Utilities
BitLocker Explained

BitLocker can be implemented in a number of ways and can be thought of as a 2 phase approach to securing a machine

- Phase 1: Pre-OS Validation
- Phase 2: Full Volume Encryption

Note: Both phases may not be implemented depending on hardware and software versions
Drive Encryption Specifics

• Some of the tenants of BitLocker
  – Once enabled the data on the drive is always encrypted unless the volume is decrypted
  – FVEVOL.SYS sits underneath the file system driver and performs all encryption / decryption
  – The drive is encrypted a sector at a time and supports sector sized from 512 – 8192 bytes
Drive Encryption Specifics

Once enabled the data on the drive is always encrypted unless the volume is decrypted

• The initial process of enabling BitLocker takes a while as all of the data on the disk is encrypted.

• There are 2 options once a drive is encrypted:
  – Disabled: Volume is still encrypted but the VMK is stored in the clear (used for updates)
  – Decrypt: Decrypting the drive completely
Drive Encryption Specifics

FVEVOL.SYS sits underneath the file system driver and performs all encryption / decryption

- Once booted, Vista (and the user) sees no difference in experience
- The encryption / decryption happens at a lower level
Drive Encryption Specifics

*The drive is encrypted a sector at a time and supports sector sized from 512 – 8192 bytes*

- It would be impractical to encrypt the entire drive as one blob not to mention unmanageable given the number of reads and writes
- BitLocker encrypts the drive a sector at a time so that only the sectors that are being read or written have to be manipulated.
BitLocker Forensic View (Details and Artifacts in BitLocker Data)

Exploration of Windows Vista
Advanced Forensic Topics – Day 3
Examination of Physical Image

• Despite the fact that BitLocker implements full volume encryption, there are a number of locations that contain clear text data

• The BIOS Parameter Block (BPB) is the first 54 bytes in the first sector of a volume and has volume “signature” data
### Examination of Physical Image

<table>
<thead>
<tr>
<th>Offset (h)</th>
<th>Offset (d)</th>
<th>Size</th>
<th>Field</th>
<th>Required Value for BitLocker</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x003</td>
<td>3</td>
<td>8</td>
<td>Signature</td>
<td>‘-’, ’F’, ’V’, ’E’, ’-’, ’F’, ’S’, ’-’</td>
</tr>
<tr>
<td>0x00B</td>
<td>11</td>
<td>2</td>
<td>BytesPerSector</td>
<td></td>
</tr>
<tr>
<td>0x00D</td>
<td>13</td>
<td>1</td>
<td>SectorsPerCluster</td>
<td>One of 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40 or 0x80</td>
</tr>
<tr>
<td>0x00E</td>
<td>14</td>
<td>2</td>
<td>ReservedClusters</td>
<td>0x0000</td>
</tr>
<tr>
<td>0x010</td>
<td>16</td>
<td>1</td>
<td>FatCount</td>
<td>0x00</td>
</tr>
<tr>
<td>0x011</td>
<td>17</td>
<td>2</td>
<td>RootEntries</td>
<td>0x0000</td>
</tr>
<tr>
<td>0x013</td>
<td>19</td>
<td>2</td>
<td>Sectors</td>
<td>0x0000</td>
</tr>
<tr>
<td>0x016</td>
<td>22</td>
<td>2</td>
<td>SectorsPerFat</td>
<td>0x0000</td>
</tr>
<tr>
<td>0x020</td>
<td>32</td>
<td>4</td>
<td>LargeSectors</td>
<td>0x0000000000</td>
</tr>
<tr>
<td>0x038</td>
<td>56</td>
<td>8</td>
<td>MetadataLcn</td>
<td></td>
</tr>
</tbody>
</table>
Examination of Physical Image

- In addition to the data in the volume signature field, BitLocker stores copies of the metadata in other locations.

- First location is calculated with the following data from the signature field:

\[
\text{MetadataLCN} \times \text{SectorsPerCluster} \times \text{BytesPerSector}
\]
## Examination of Physical Image

<table>
<thead>
<tr>
<th>Offset (h)</th>
<th>Offset (d)</th>
<th>Size</th>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x000</td>
<td>0</td>
<td>8</td>
<td>Signature</td>
<td>&quot;-&quot; , 'F' , 'V' , 'E' , 'F' , 'S' , '-'</td>
</tr>
<tr>
<td>0x008</td>
<td>8</td>
<td>2</td>
<td>Size</td>
<td>Size of structure. Validation data follows this structure.</td>
</tr>
<tr>
<td>0x002</td>
<td>2</td>
<td>10</td>
<td>Version</td>
<td>0x0001 for current version.</td>
</tr>
<tr>
<td>0x004</td>
<td>4</td>
<td>12</td>
<td>Version specific content.</td>
<td></td>
</tr>
</tbody>
</table>

- Additionally a text string search for –FVE-FS- to find this location and verify the calculation
Examination of Physical Image - VISTA

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”
Examination of Physical Image – Win 7

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”
Examination of Physical Image – BL To Go DOS – IS THIS RIGHT?

• Viewing the volume signature in your favorite forensic tool makes the issue very clear

• Notice the signature “FVE!”
Examination of Physical Image – BL To Go NTFS

<table>
<thead>
<tr>
<th>00000000</th>
<th>eb 58 90 2d</th>
<th>46 56 45 2d-46 53</th>
<th>2d 00 02 08 00 00</th>
<th>eX-FVE-FS</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000010</td>
<td>00 00 00 00 f8 00 00-3f 00 ff 00 20 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000020</td>
<td>00 00 00 00 e0 1f 00 00-00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000030</td>
<td>01 00 06 00 00 00-00 00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000040</td>
<td>80 00 29 00 00 00 00 4e-4f 20 4e 41 4d 45 20 20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000050</td>
<td>20 20 46 41 54 33 32 20-20 20 33 c9 8e d1 bc f4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000060</td>
<td>7b 8e c1 8e d9 bd 00 7c-a0 fb 7d b4 7d 8b f0 ac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000070</td>
<td>98 40 74 0c 48 74 0e b4-0e bb 07 00 cd 10 eb ef</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000080</td>
<td>a0 fd 7d eb e6 cd 16 cd-19 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00000090</td>
<td>00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000000a0</td>
<td>3b d6 67 49 29 2e d8 4a-83 99 f6 a3 39 e3 d0 01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000000b0</td>
<td>00 00 10 02 00 00 00 00 00-00 e0 47 29 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Viewing the volume signature in your favorite forensic tool makes the issue very clear
- Notice the signature “-FVE-FS-”
Examination of the BEK File

• We can also see the Recovery Key ID number (i.e. the GUID like name of the BEK file)

Offset 56(d), Length 4 bytes (Reversed)
Offset 60(d), Length 2 bytes (Reversed)
Offset 62(d), Length 2 bytes (Reversed)
Offset 64(d), Length 2 bytes (Forward)
Offset 66(d), Length 6 bytes (Forward)
Examination of the BEK File

Recovery Key:
ID: {7C6CA4B3-F630-4BE2-A23E-5CF79BADA160}

External Key File Name:
7C6CA4B3-F630-4BE2-A23E-5CF79BADA160.BEK
Examination of the BEK File

• When implementing BitLocker with a Startup Key (USB drive or encrypting a data volume) we can get additional information from the file itself.
  – Date of key generation
  – Time of key generation

Offset 72(d), Length 8 bytes (Little endian)
BitLocker Investigative Impact

• What do investigators have on our side?
  – BitLocker is only available in Windows Enterprise and Ultimate SKUs
  – BitLocker has a number of “Recovery” scenarios that we can exploit
  – Encryption is “scary” to users (even criminals)
  – BitLocker, at its core, is a password technology, we simply have to get the password from our suspect or surroundings
BitLocker Investigative Impact

• What do investigators have on our side?
  – We are investigators, and should be aware if our suspect is using encryption technology prior to entry
  – BitLocker in the Enterprise should have a high likelihood of recovery information availability
  – BitLocker protected drives can be mounted and examined forensically if we can get in
  – We are the good guys!
BitLocker Investigative Impact

- What do investigators have working against us?
  - BitLocker has very low user interaction after the initial setup
  - BitLocker has <5% overhead on performance
  - If used in the TPM + PIN scenario, we need the user to provide the PIN or recovery info
  - If used in the TPM + USB scenario, we need the USB drive or user supplied recovery info
BitLocker Investigative Impact

• What do investigators have working against us?
  – BitLocker uses US Government grade encryption in 128 bit or 256 bit AES keying
  – BitLocker operates at a lower level of the OS so security technologies can be layered (EFS)
BitLocker Investigative Impact

• Introduction of this security technology in Windows Vista and Windows 7 does not amount to an overwhelming blow to the efforts of law enforcement

• As has been true throughout history the dumb criminals will be easy to catch and the smart ones harder…
Questions?
Enabling BitLocker on Data volumes

Exercise 6
Mounting BitLocker Protected Volumes

Exploration of Windows 7
Advanced Forensic Topics – Day 3
Requirements – NEED TO TEST Versions

• Examiner System must be running either Windows Win 7 Enterprise or Ultimate
• BitLocker does NOT have to be enabled on the Examiner system
• All obvious write protection mechanisms should be in place – Forensics 101
Mounting a BitLocker Drive

- Investigators can use the recovery mechanisms built into the BitLocker mechanism to access the protected drive
- Just like EFS

WE STILL NEED THE PASSWORD!!!
Mounting a BitLocker Drive

• Physical Mount
  – Install the “suspect” drive as a secondary drive through a write blocker
  – Boot to a BitLocker capable version of Win 7
  – Access the BitLocker MMC
  – You should see the “suspect” drive
  – Use the BitLocker recovery process to temporarily access the data
Mounting a BitLocker Drive

- The drive is recognized but it cannot be read.
- Details are unavailable.
Mounting a BitLocker Drive

The BitLocker MMC is "sees the drive as protected" - "Unlock"
Mounting a BitLocker Drive

Choose password format: "USB Key" or "Manually"
Mounting a BitLocker Drive

- We have the Recovery Key Password so we type it in.
Mounting a BitLocker Drive

- “You can now temporarily access this drive”
Mounting a BitLocker Drive

- Granted access to a BitLocker protected drive!
Mounting a BitLocker Drive

Drive details are now available and we can process the drive.
Bitlocker “Cold Boot” attack?

This policy setting controls computer restart performance at the risk of exposing BitLocker secrets. This policy setting is applied when you turn on BitLocker. BitLocker secrets include key material used to encrypt data. This policy setting applies only when BitLocker protection is enabled.

If you enable this policy setting, memory will not be overwritten when the computer restarts. Preventing memory overwrite may improve restart performance but will increase the risk of exposing BitLocker secrets.

If you disable or do not configure this policy setting, BitLocker secrets are removed from memory when the computer restarts.
Questions?
Tools for Dealing with BitLocker Evidence

Exploration of Windows 7
Advanced Forensic Topics – Day 3
BitLocker Aware Forensic Tools

- Some tools already handle disk images of encrypted drives provided the investigator has recovery or startup key material.
Alternatives

• If the tool used does not support BitLocker, an investigator should obtain 2 images of the suspect system
  – Physical – To allow for booting and testing
  – Logical – To allow for examination in the tool
Alternatives

• The increase in use of encryption and the number of most technically savvy criminal necessitates the move from traditional offline only forensic to a hybrid online / offline approach where two sets of data are collected and examined.
Dealing with BitLocker on a Live System

Exploration of Windows Vista
Advanced Forensic Topics – Day 3
Manage-BDE

- In Vista this tool was a script. Manage-BDE.WSF
- In Win7 it was converted to an EXE.
- C:\Windows\System32\Manage-BDE.exe
- Manage-BDE and Repair tool are now part of Windows PE, Windows RE and Windows 7
Manage-BDE

- This tool can manage every aspect of BitLocker on a system
  - Encrypt drives
  - Lock and Unlock drives
  - Decrypt drives
  - Manage BitLocker Keys
  - View Recovery Key information
Manage-BDE

• Viewing if BitLocker is enabled on any drive on a live system:

Note: You must run as Administrator

manage-bde -status
C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 6.1.7072
Copyright (C) Microsoft Corporation. All rights reserved.
Disk volumes that can be protected with BitLocker Drive Encryption:
Volume D: [ ]
[Data Volume]
Size: 1.89 GB
BitLocker Version: None
Conversion Status: Fully Decrypted
Percentage Encrypted: 0%
Encryption Method: None
Protection Status: Protection Off
Lock Status: Unlocked
Identification Field: None
Automatic Unlock: Disabled
Key Protectors: None Found
Volume C: [ ]
[OS Volume]
Size: 144.02 GB
BitLocker Version: Windows 7
Conversion Status: Fully Encrypted
Percentage Encrypted: 100%
Encryption Method: AES 128 with Diffuser
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: None
Key Protectors: External Key
Numerical Password
Manage-BDE

• What about recovery information?

`manage-bde –protectors –get c:`

Note: You will need to run this for all drives attached to the system. i.e.

`manage-bde –protectors –get d`

`manage-bde –protectors –get e:`
Manage-BD

C:\Windows\system32>manage-bde -protectors -get c:
BitLocker Drive Encryption: Configuration Tool version 6.1.7072
Copyright (C) Microsoft Corporation. All rights reserved.
Volume C: []
All Key Protectors
  External Key:
    ID: {B2EDF460-234E-40D4-8F2D-14DC4D29722C}
  External Key File Name:
    B2EDF460-234E-40D4-8F2D-14DC4D29722C.BEK
Numerical Password:
  ID: {738C71C6-8CEA-4273-81EC-8A2F23A7DF21}
  Password:
    290103-627220-601392-709918-475816-546480-189739-185042
Manage-BDE

• We can even unlock the drive with the manage-bde tool.

• Remember unlocking the drive leaves the data encrypted but simply stores the Volume Master Key (VMK) in the clear so the system can boot without a startup key.

manage-bde –unlock c:
manage-bde –autounlock –enable c:
Forensic First Responders

• Inclusion of this tool in any first responder toolkit is a must.

• A script can be leveraged to detect BitLocker on a live system and automatically obtain Recovery Key data and/or unlock the drive
Questions?
Mounting BitLocker Protected Volumes for Preview

Exercise

30 Minutes
Imaging Implications for BitLocker Protected Drives

Exercise
Examining File system Signatures of BitLocker Protected Volumes

Exercise
## BitLocker in Win7 at a Glance

<table>
<thead>
<tr>
<th>Drive Type</th>
<th>Unlock Methods</th>
<th>Recovery Methods</th>
<th>Management</th>
<th>Other requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System Drives</td>
<td>TPM</td>
<td>Recovery password</td>
<td>Robust and consistent Group Policy enforcement</td>
<td>Drive preparation fully integrated in BitLocker setup.</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN</td>
<td>Recovery Key</td>
<td>Minimum Pin Length</td>
<td>System partition size: 200MB without WinRE 400MB with WinRE</td>
</tr>
<tr>
<td></td>
<td>TPM+Startup key</td>
<td>Active Directory recovery password</td>
<td></td>
<td>System partition letterless</td>
</tr>
<tr>
<td></td>
<td>TPM+PIN+Startup Key</td>
<td>Domain Recovery Agent</td>
<td></td>
<td>NTFS file system.</td>
</tr>
<tr>
<td></td>
<td>Startup key</td>
<td></td>
<td></td>
<td>File systems: NTFS FAT FAT32 ExFAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Drives <em>Includes fixed and removable</em></td>
<td>Passphrase</td>
<td>Same as OS drives</td>
<td>Robust and consistent group policy controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart Card</td>
<td></td>
<td>Ability to mandate encryption prior to granting write access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic Unlocking</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>