



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

The screenshot shows the Windows Control Panel interface for BitLocker Drive Encryption. At the top, the title bar reads "All Control Panel Items > BitLocker Drive Encryption". The main content area has a heading "Help protect your files and folders by encrypting your drives" followed by a description: "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." Below this is a link "What should I know about BitLocker Drive Encryption before I turn it on?".

The first section is titled "BitLocker Drive Encryption - Hard Disk Drives". It lists a drive "C:" with the status "Off" and a "Turn On BitLocker" button, which is circled in red.

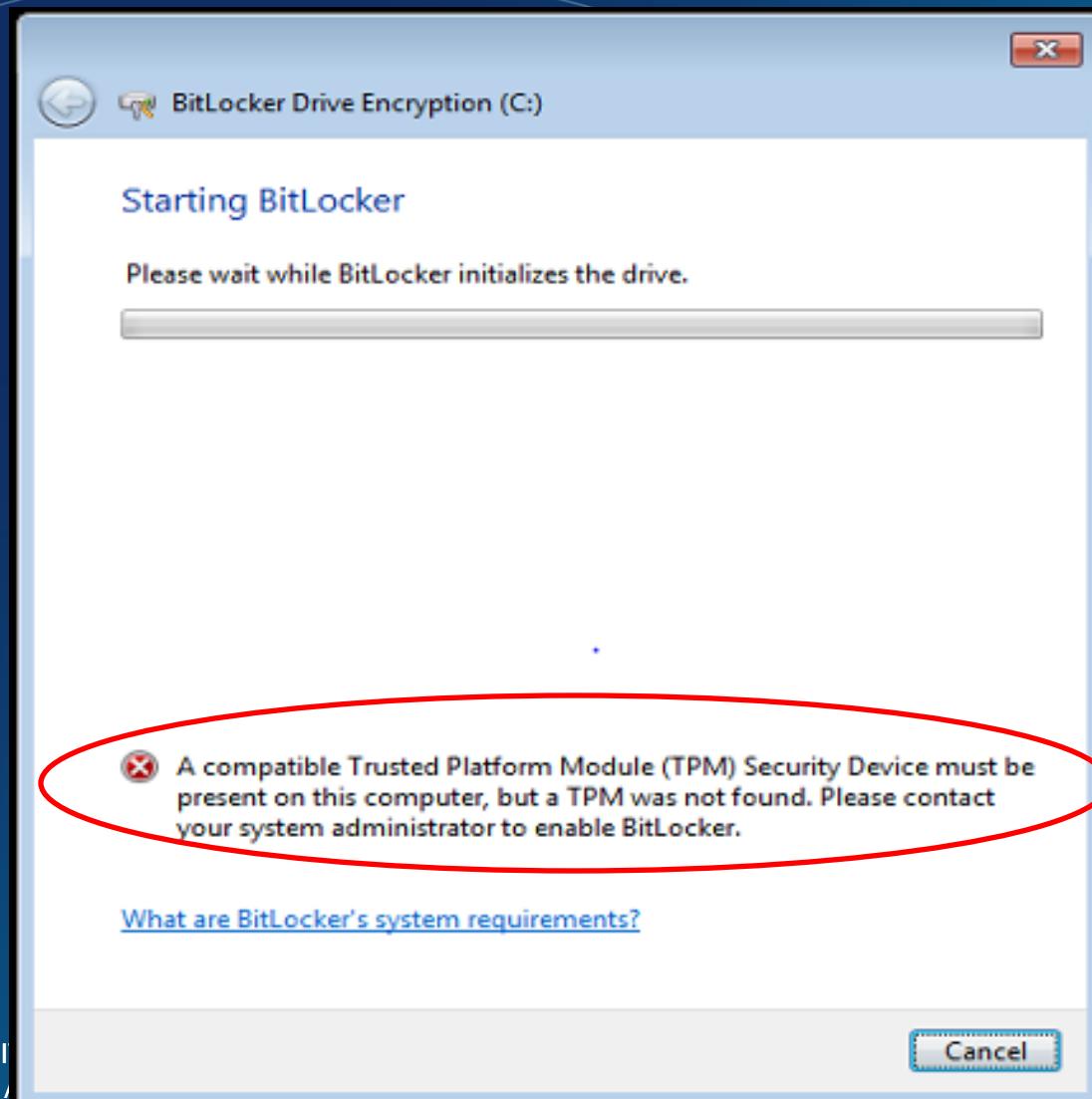
The second section is titled "BitLocker Drive Encryption - BitLocker To Go". It lists a drive "LOCKER (D:)" with the status "Off" and a "Turn On BitLocker" button.

At the bottom left, there is a "See also" section with links to "TPM Administration" and "Disk Management".

At the very bottom left, the text "LAW ENFOR" and "©2007 Micros" is visible.

ces

Enabling BitLocker - OS



Enabling BitLocker - OS

Execute: gpedit.msc

Navigate: Computer Configuration\Administrative Templates\Windows Components

The screenshot shows the Local Group Policy Editor window. The left navigation pane displays a tree structure of policy settings under 'Computer Configuration' and 'Administrative Templates'. A red circle highlights the 'BitLocker Drive Encryption' node under 'Windows Components'. The main pane shows the 'Operating System Drives' settings. A second red circle highlights the 'Require additional authentication at startup' setting in the list of policies.

Local Group Policy Editor

File Action View Help

System

Windows Components

ActiveX Installer Service

Application Compatibility

AutoPlay Policies

Backup

Biometrics

BitLocker Drive Encryption

- Fixed Data Drives
- Operating System Drives
- Removable Data Drives

Credential User Interface

Desktop Gadgets

Desktop Window Manager

Digital Locker

Event Forwarding

Event Log Service

Event Viewer

Game Explorer

HomeGroup

Internet Explorer

Internet Information Services

Location and Sensors

NetMeeting

Operating System Drives

Require additional authentication at startup

[Edit policy setting](#)

Requirements: Windows 7 family

Description:

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 Extended / Standard

Setting	State
Require additional authentication at startup	Not configured
Require additional authentication at startup (Windows Serve...	Not configured
Allow enhanced PINs for startup	Not configured
Configure minimum PIN length for startup	Not configured
Choose how BitLocker-protected operating system drives ca...	Not configured
Configure TPM platform validation profile	Not configured

6 setting(s)

Enabling BitLocker – OS

Require additional authentication at startup

Require additional authentication at startup

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: Windows 7 family

Options:

Allow BitLocker without a compatible TPM
(requires a startup key on a USB flash drive)

Settings for computers with a TPM:

Configure TPM startup: Allow TPM

Configure TPM startup PIN: Allow startup PIN with TPM

Configure TPM startup key: Allow startup key with TPM

Configure TPM startup key and PIN:
Allow startup key and PIN with 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

OK Cancel Apply

Enabling BitLocker - OS

The screenshot shows the Windows Control Panel interface for BitLocker Drive Encryption. At the top, the title bar reads "All Control Panel Items > BitLocker Drive Encryption". The main content area has a heading "Help protect your files and folders by encrypting your drives" followed by a description: "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." Below this is a link "What should I know about BitLocker Drive Encryption before I turn it on?".

The first section is titled "BitLocker Drive Encryption - Hard Disk Drives". It lists a drive "C:" with the status "Off" and a "Turn On BitLocker" button, which is circled in red.

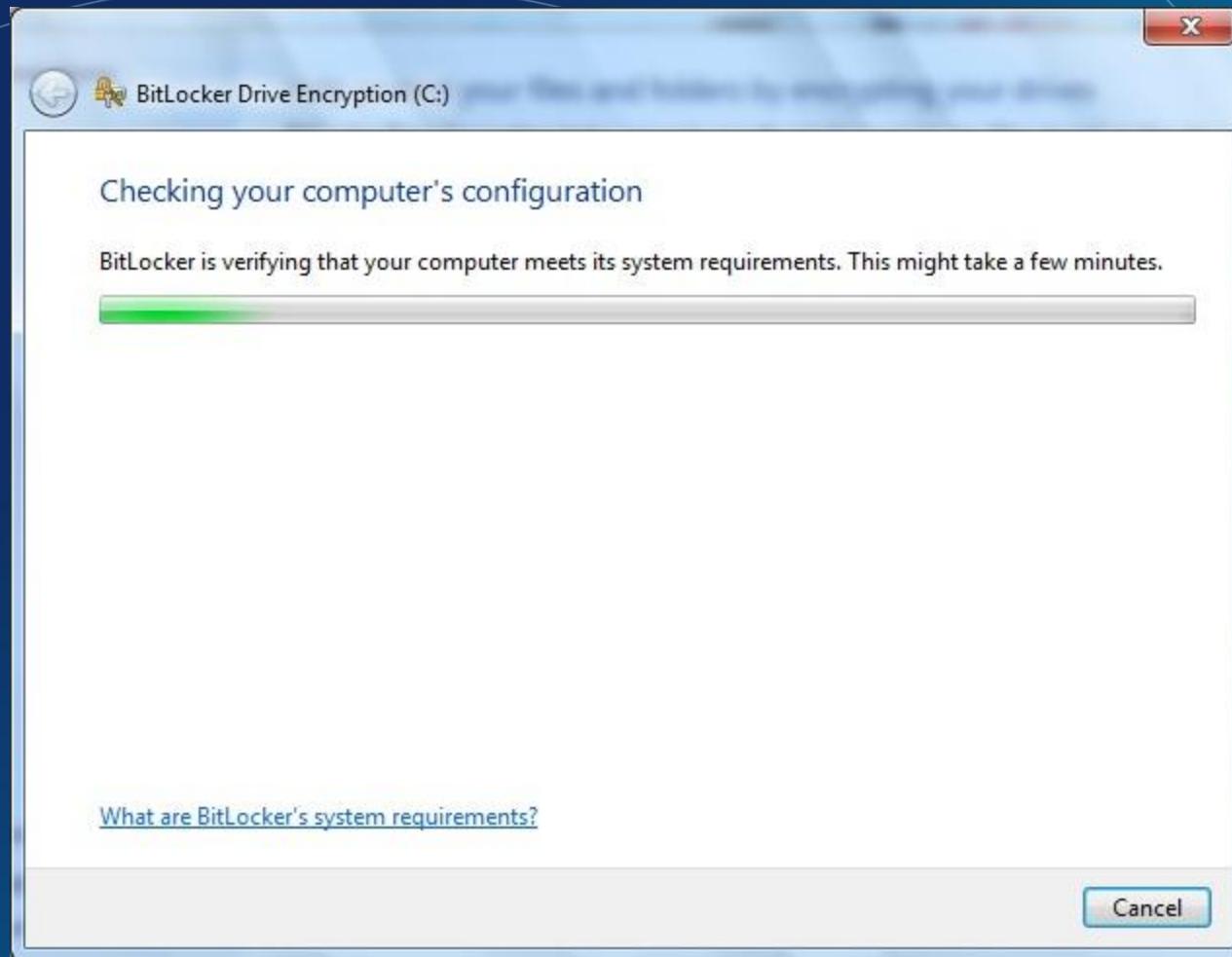
The second section is titled "BitLocker Drive Encryption - BitLocker To Go". It lists a drive "LOCKER (D:)" with the status "Off" and a "Turn On BitLocker" button.

At the bottom left, there is a "See also" section with links to "TPM Administration" and "Disk Management".

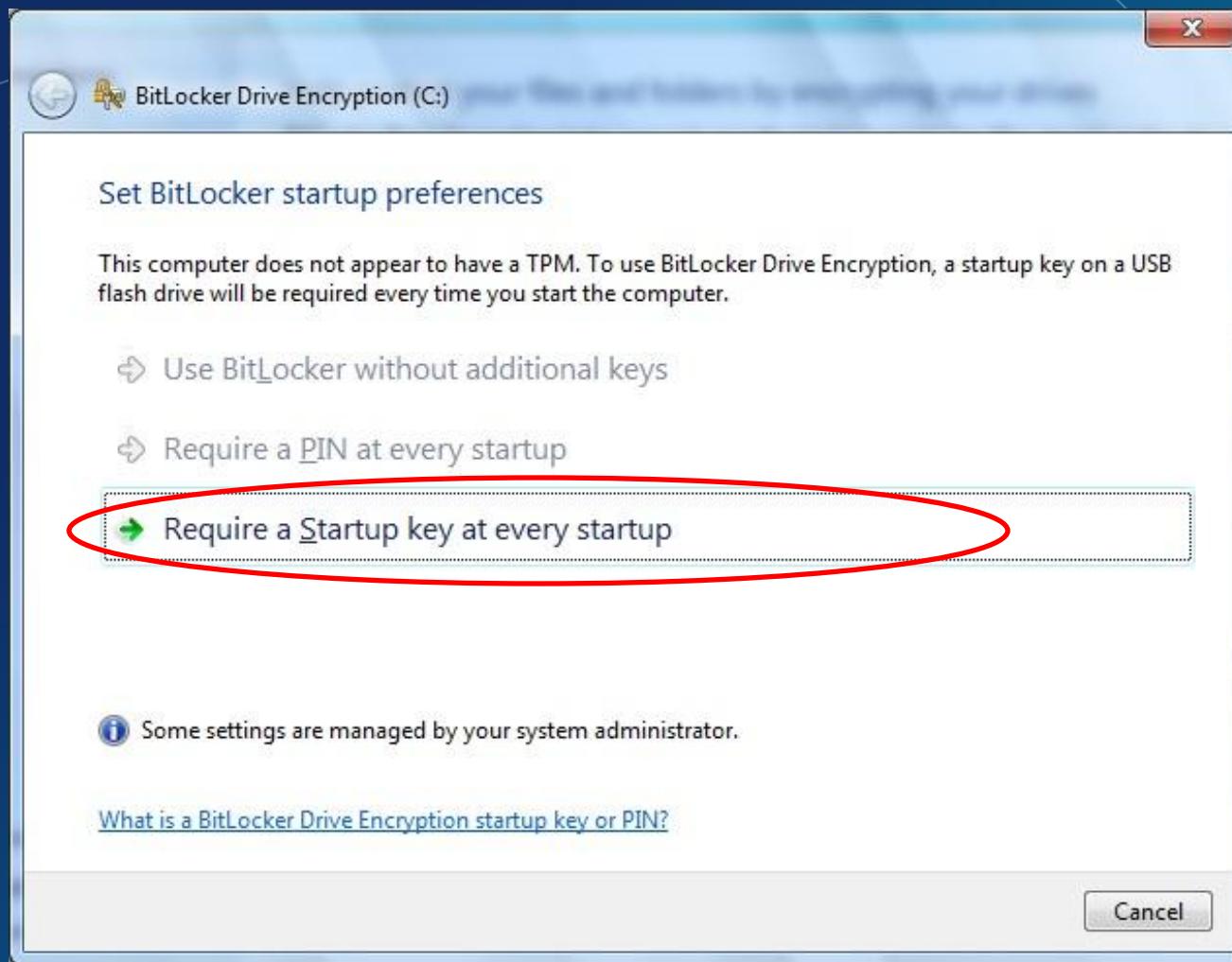
At the very bottom left, the text "LAW ENFOR" and "©2007 Micros" is visible.

ces

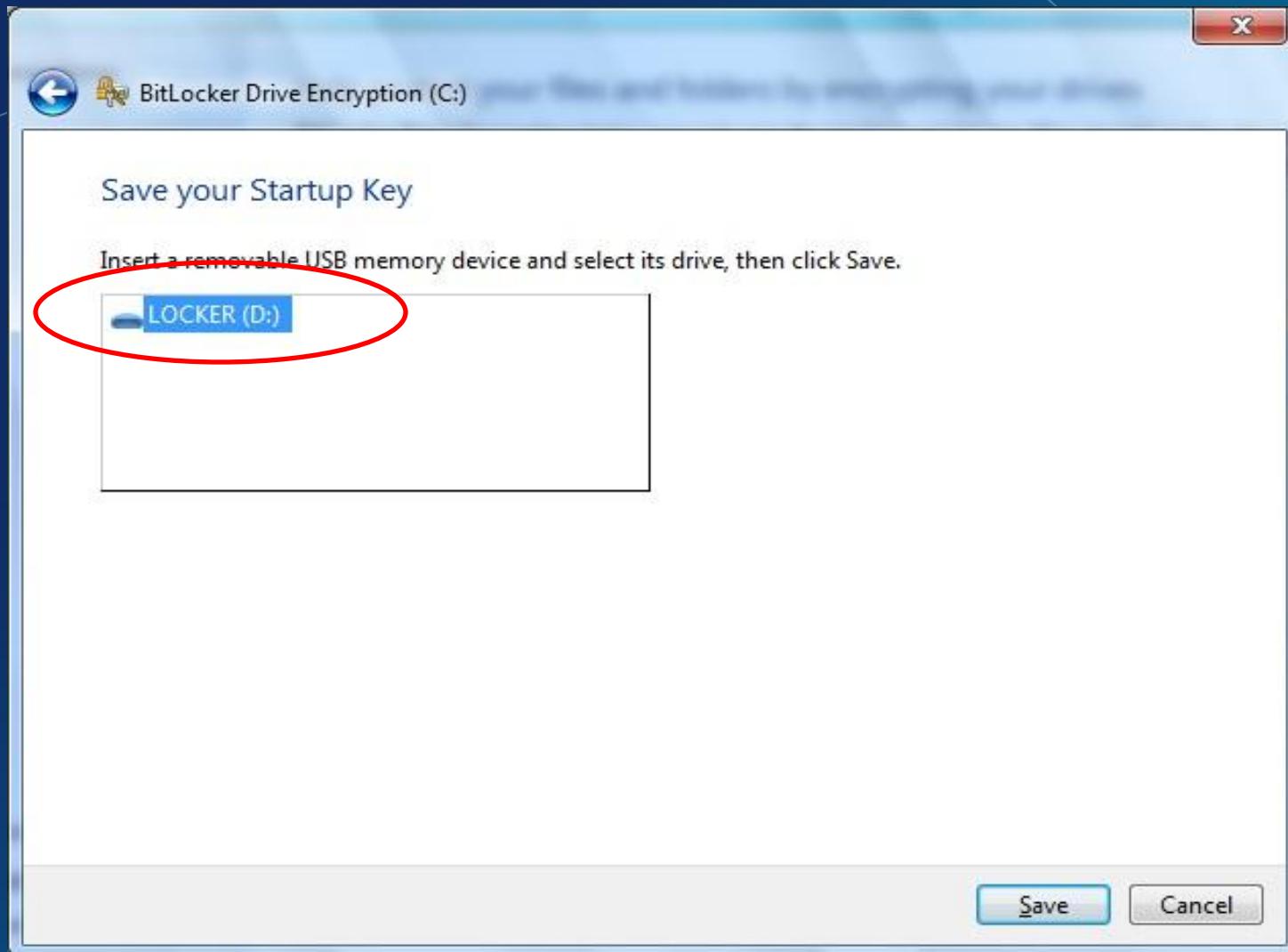
Enabling BitLocker - OS



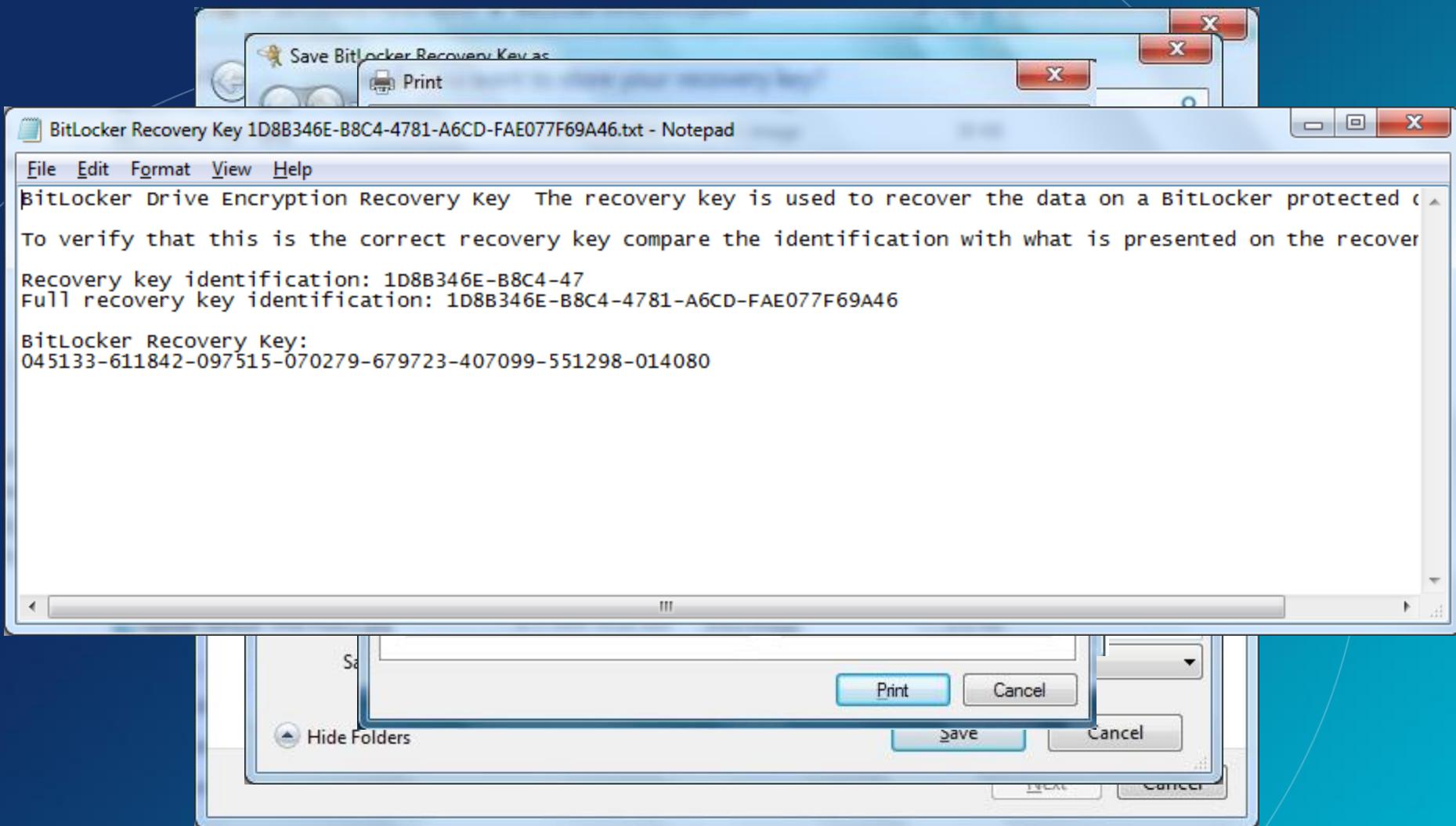
Enabling BitLocker - OS



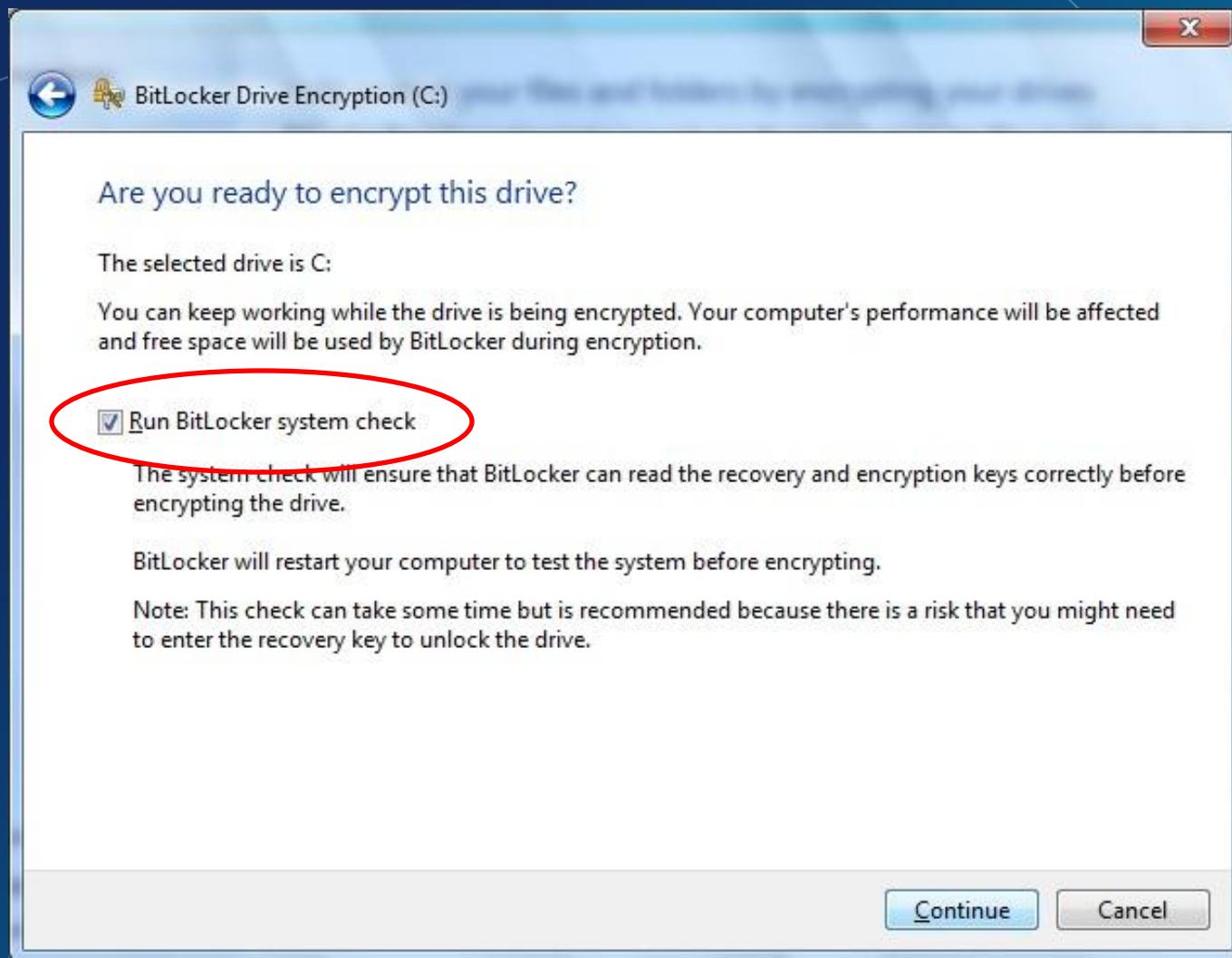
Enabling BitLocker - OS



Enabling BitLocker - OS



Enabling BitLocker - OS



Enabling BitLocker

The screenshot shows the Windows Control Panel interface. The title bar reads "All Control Panel Items > BitLocker Drive Encryption". The main content area displays information about BitLocker Drive Encryption, including a note to "Help protect your files and folders by encrypting your drives" and a warning that it prevents unauthorized access to files on the drives shown below. A link to "What should I know about BitLocker Drive Encryption before I turn it on?" is provided.

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
--	---

See also

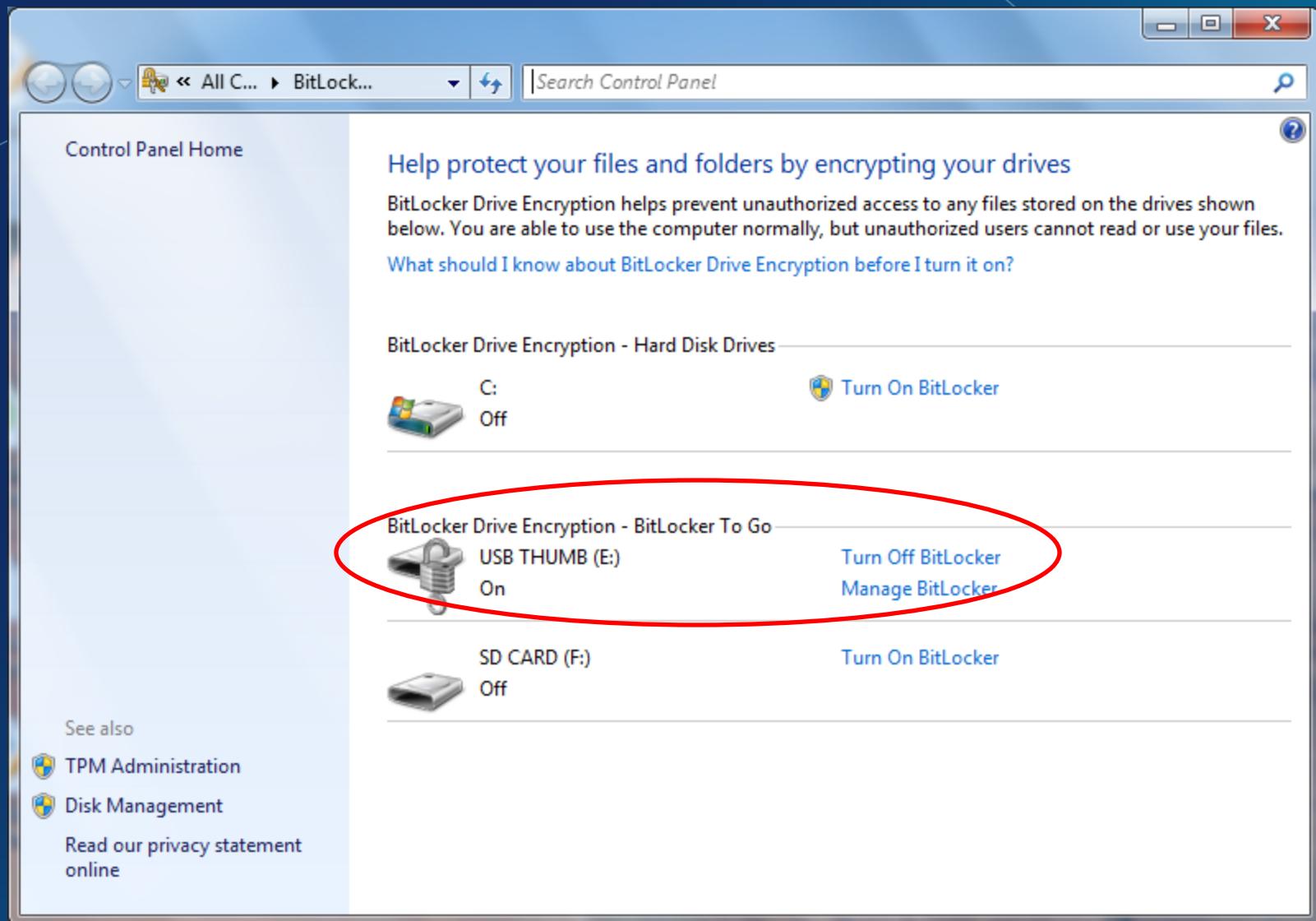
-  TPM Administration
-  Disk Management
- Read our privacy statement online

A red circle highlights the "Encrypting" status of drive C. A red oval highlights a tooltip window titled "Encryption in progress" which states: "Encryption of C: by BitLocker Drive Encryption has started. Click for more information."

LAW ENFO
©2007 Micro

9:54 AM
4/1/2009

Enabling BitLocker - OS



Questions?



Enabling BitLocker “To Go”



Enabling BitLocker of USB Stick



Enabling BitLocker of USB Stick

All C... BitLock... Search Control Panel

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: Turn On BitLocker

BitLocker Drive Encryption - BitLocker To Go

USB THUMB (E): Turn On BitLocker

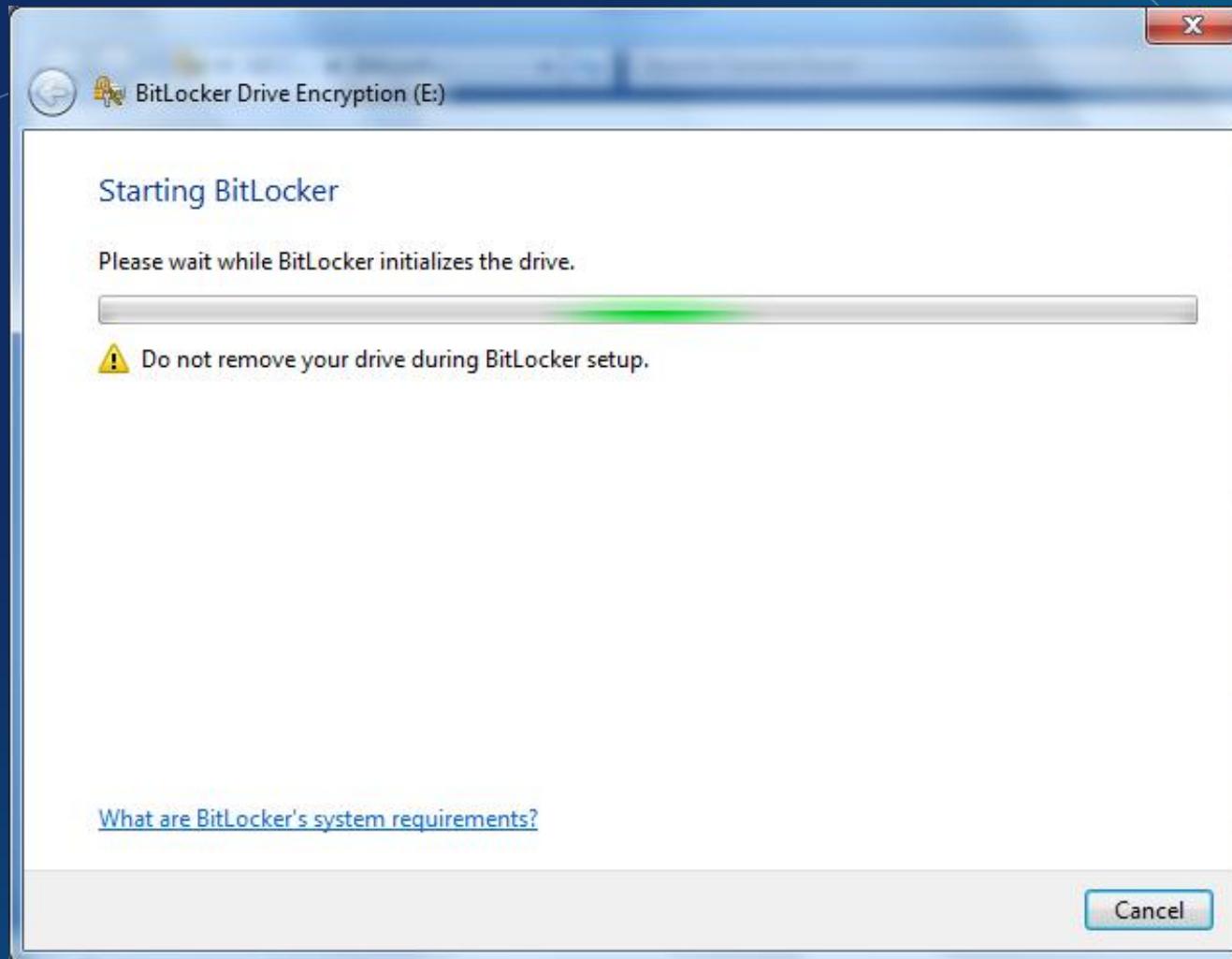
SD CARD (F): Turn On BitLocker

See also

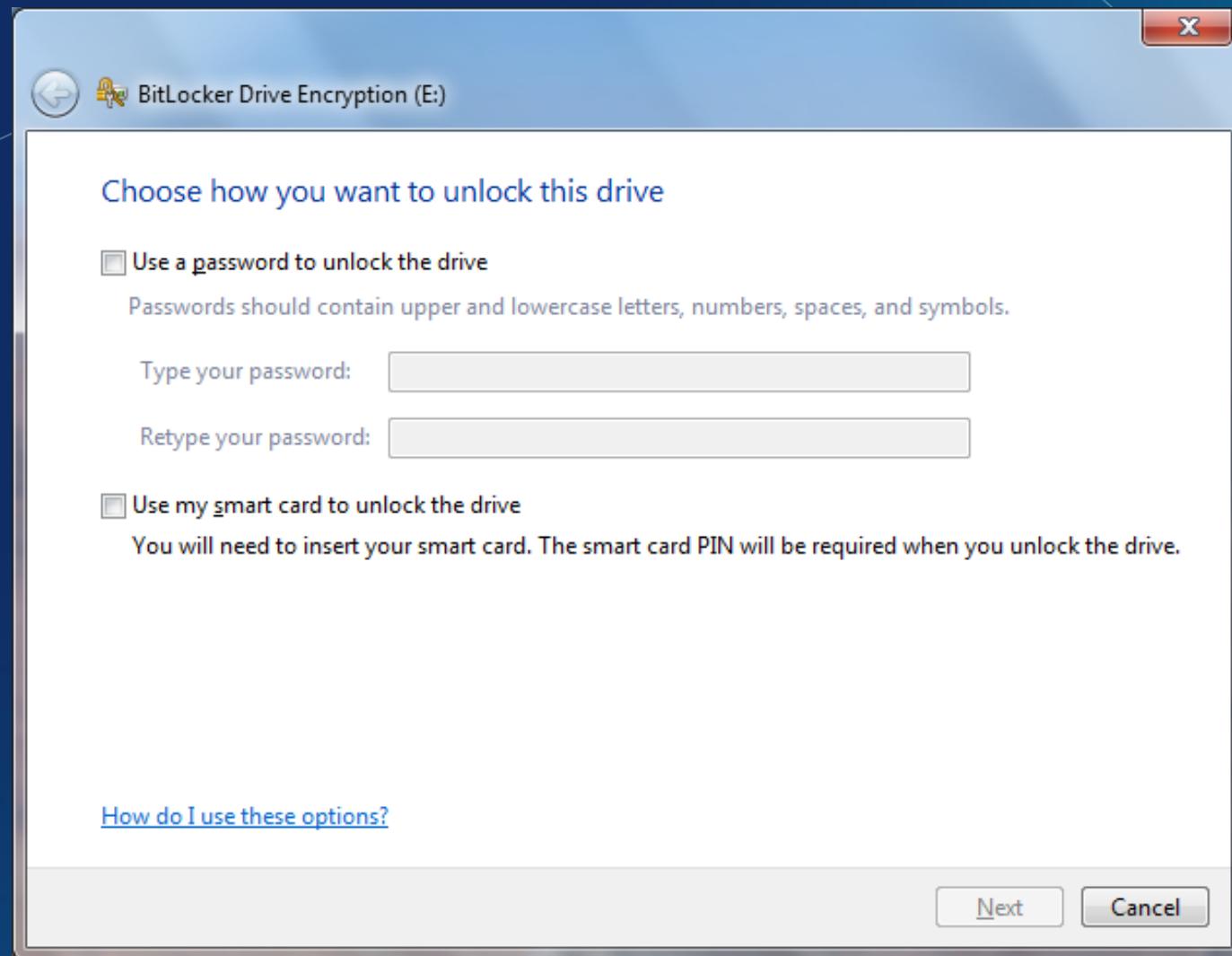
- TPM Administration
- Disk Management

Read our privacy statement online

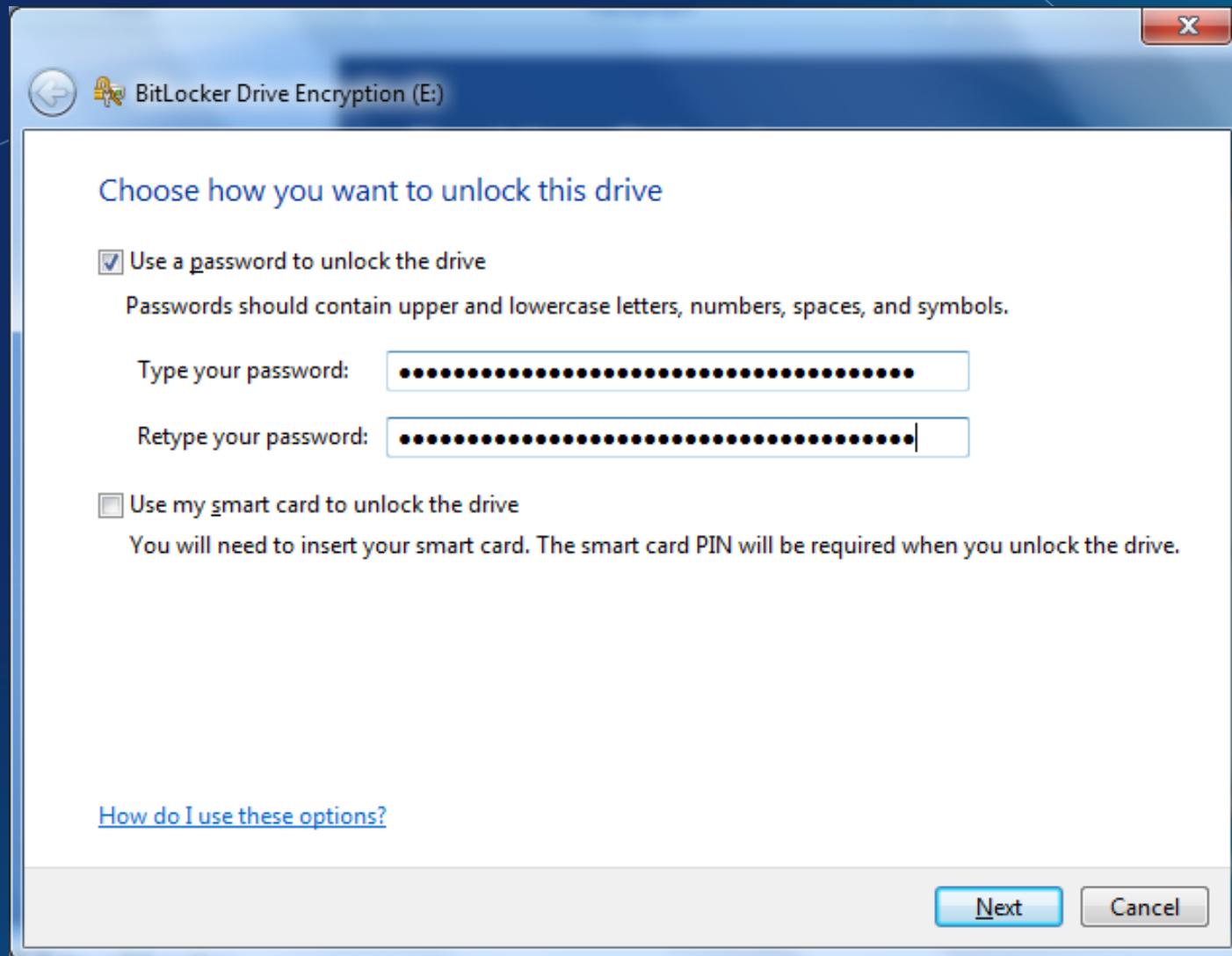
Enabling BitLocker of USB Stick



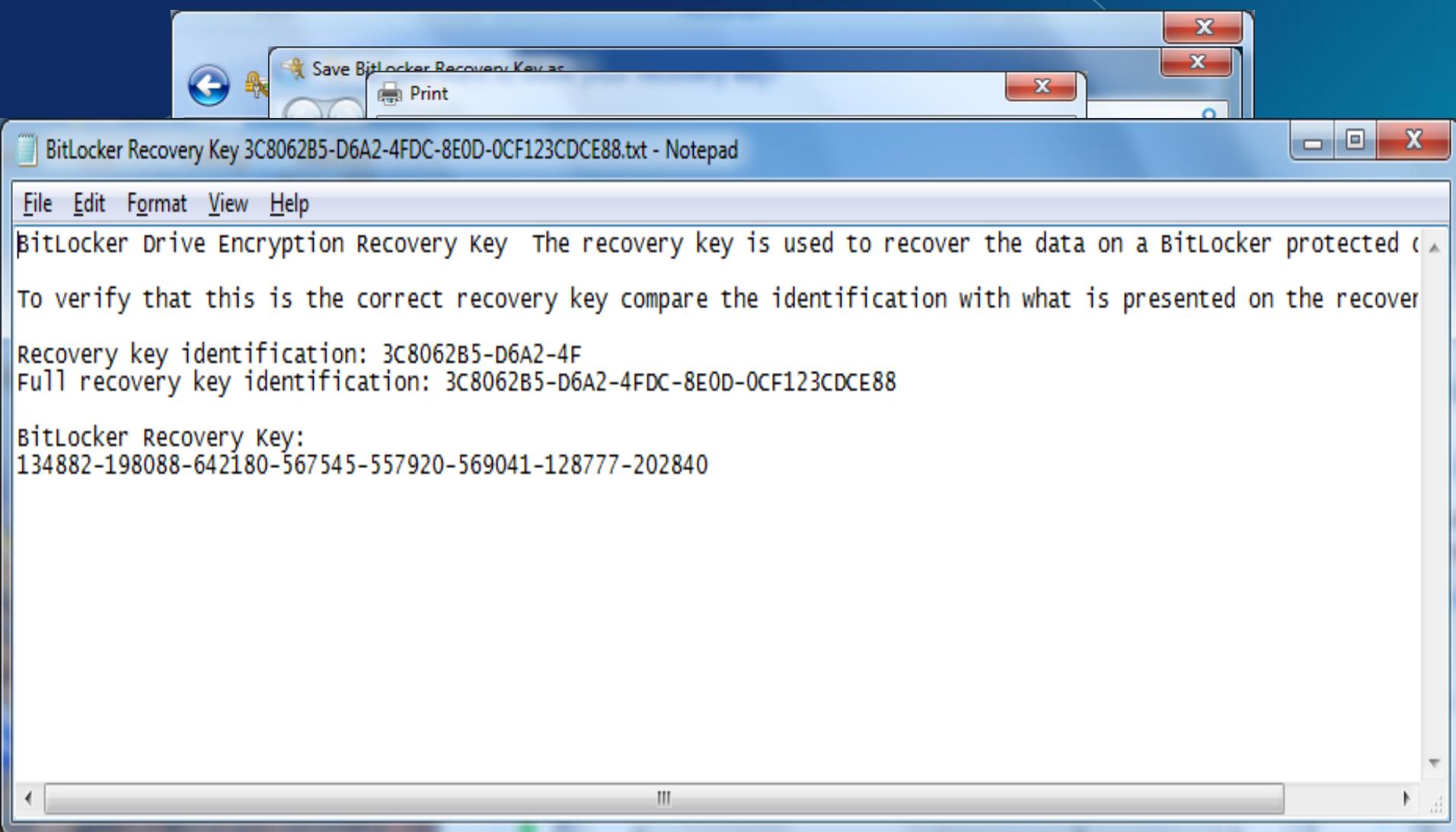
Enabling BitLocker of USB Stick



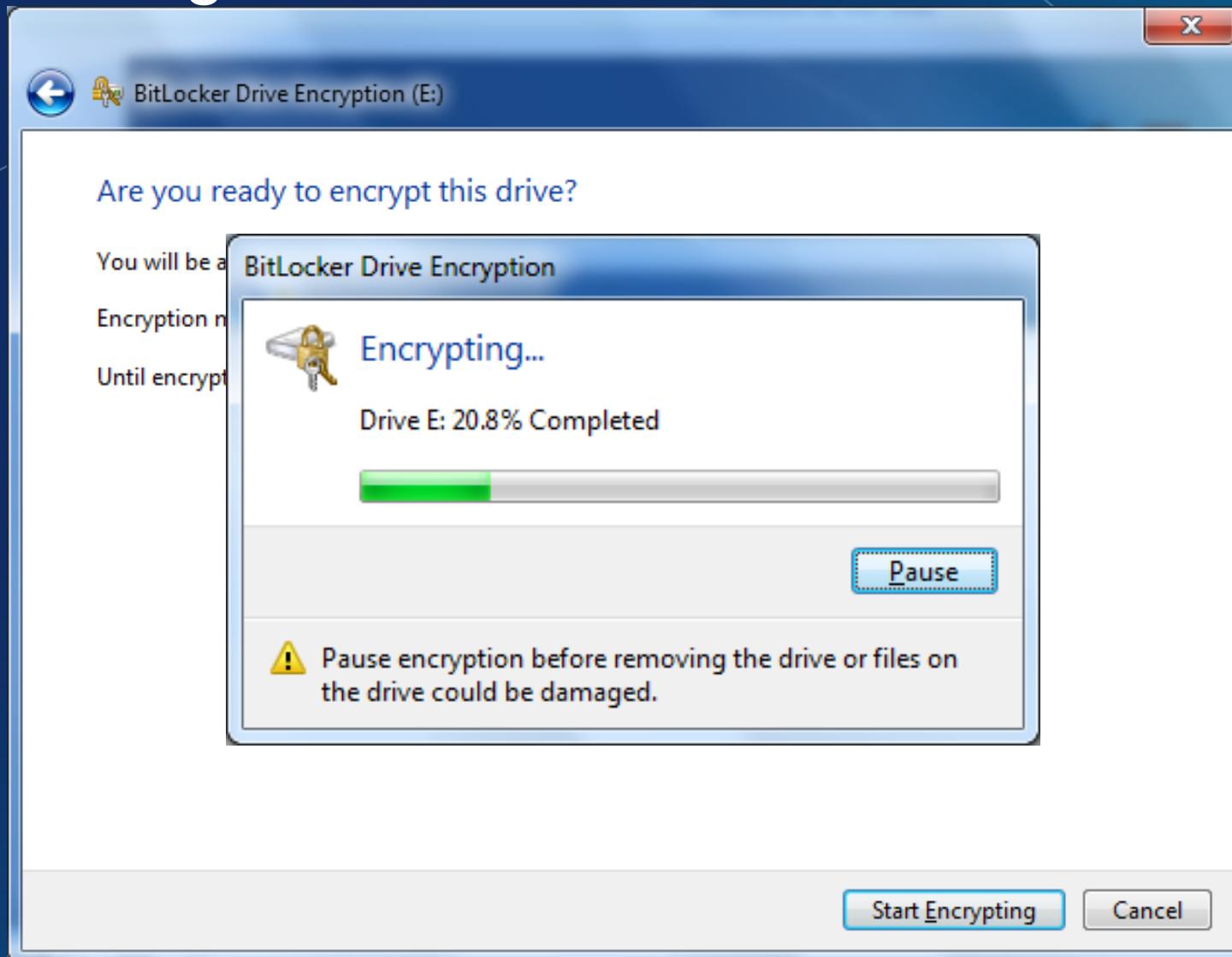
Enabling BitLocker of USB Stick



Enabling BitLocker of USB Stick

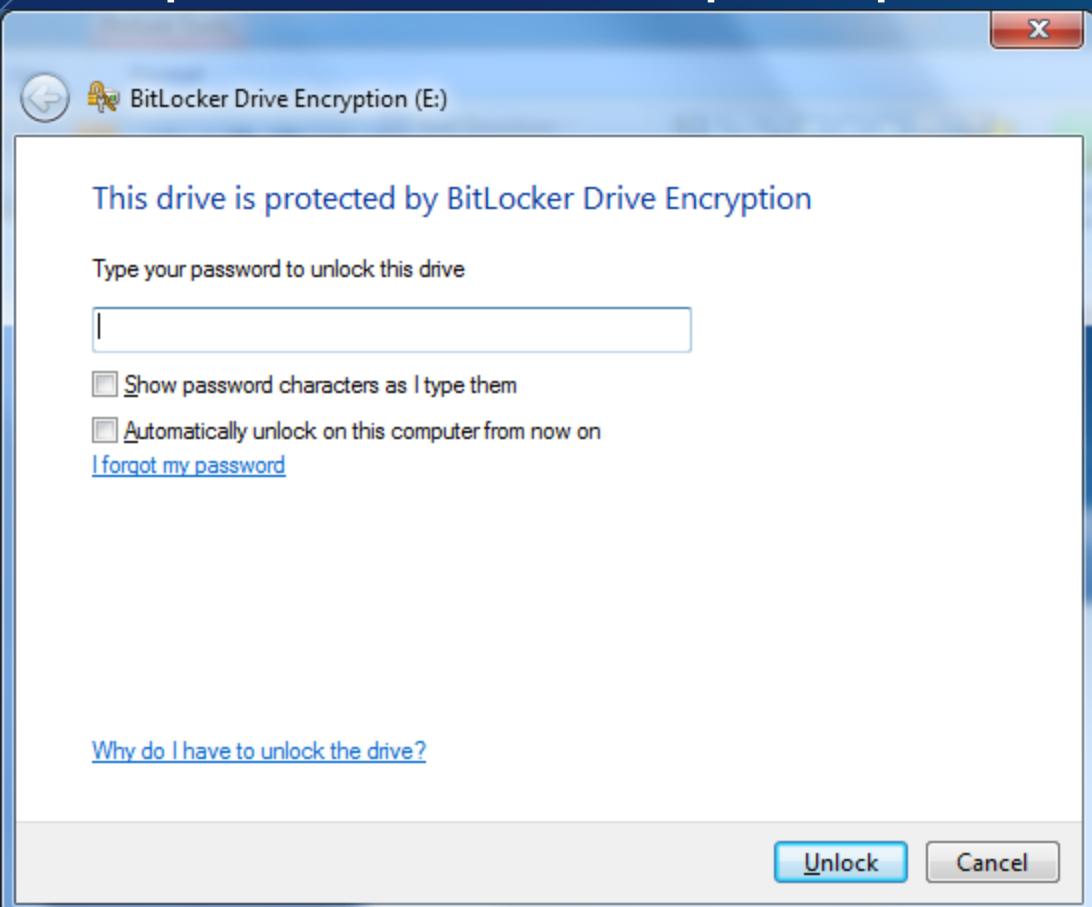


Enabling BitLocker of USB Stick



Unlocking your BitLocker enabled USB

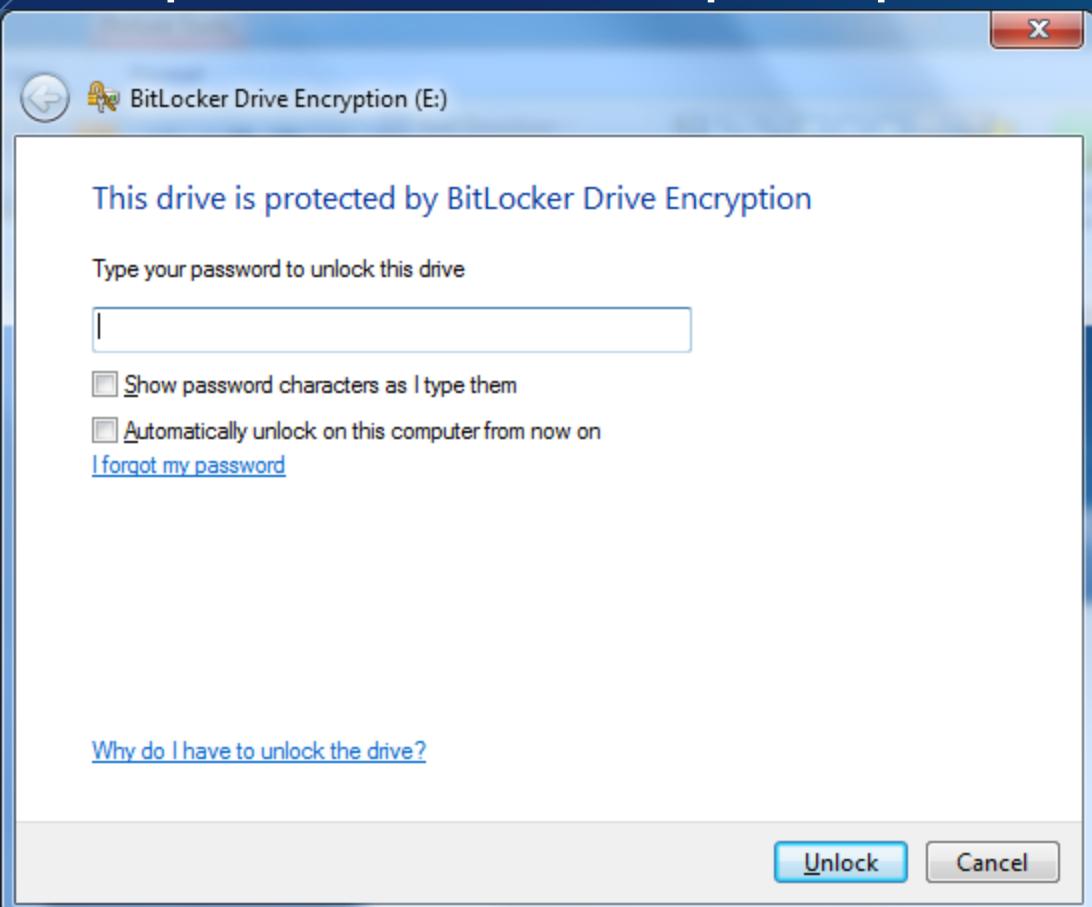
- Insert USB device into PC and type your password when prompted



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

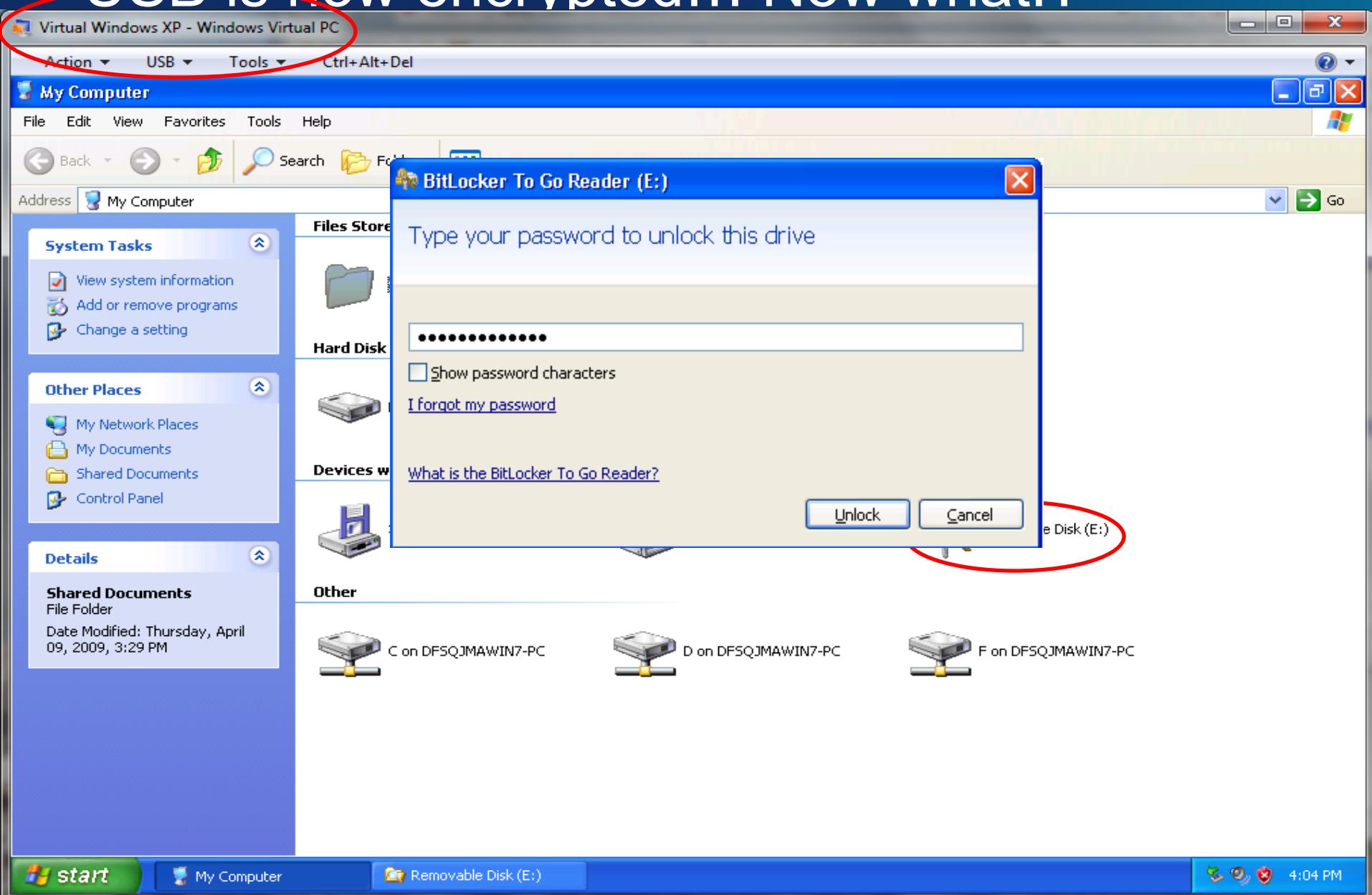


NOTE: The device can be unlocked on any Bitlocker To Go capable PC if you know the password

USB is now encrypted... Now what!?

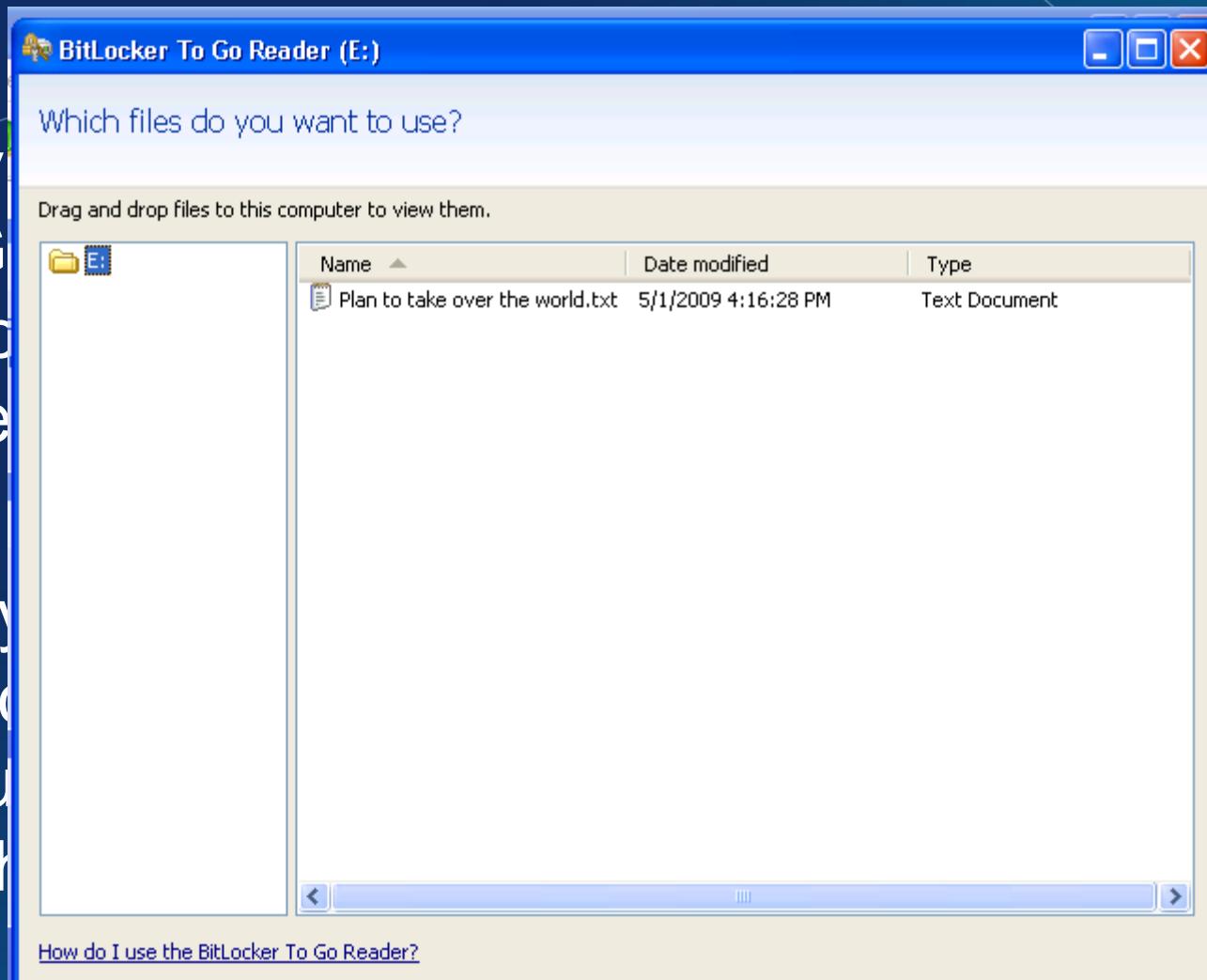
- If the encrypted USB is formatted with FAT then it can be used on down level Operating Systems
 - Win XP
 - Windows Vista
- How is this possible? These Operating Systems did not have Bitlocker to go functionality.

USB is now encrypted... Now what!?



USB is now encrypted... Now what!?

- Previous slide
To Go
BitLocker
drive
- This slide
encrypts
and
features
machines



45
Minutes



Enabling BitLocker with a Thumb drive as a startup key

Exercise

25
Minutes



Enabling BitLocker Encryption of a Thumb drive **Exercise**



BitLocker Technical Details

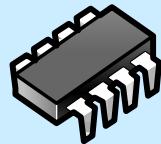
Exploration of Windows 7 Advanced Forensic Topics – Day 3

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

Ease of Use



TPM Only

"What it is."

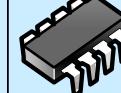
Protects against:
SW-only attacks
Vulnerable to: HW attacks (including potentially "easy" HW attacks)



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

Security

BitLocker in Windows Vista

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

*Introduced in Windows Vista SP1

BitLocker in Windows 7

Operating system drive overview

Drive Type	Unlock Methods	Recovery Methods	Management	Other requirements
Operating System Drives	TPM TPM+PIN TPM+Startup key TPM+PIN+Startup Key Startup key	Recovery password Recovery Key Active Directory backup of recovery password Data Recovery Agent	Robust and consistent Group Policy enforcement Minimum Pin Length	Drive preparation fully integrated in BitLocker setup. System partition size: 200MB without WinRE 400MB with WinRE 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

Windows RE
250 MB
NTFS

System Partition
200 MB
NTFS

OS
Remaining Disk
NTFS

Note: An additional 50MB is required on the recovery partition for volume snapshots during Complete PC backups

System Partition/Windows RE
400 MB
NTFS

OS
Remaining Disk
NTFS

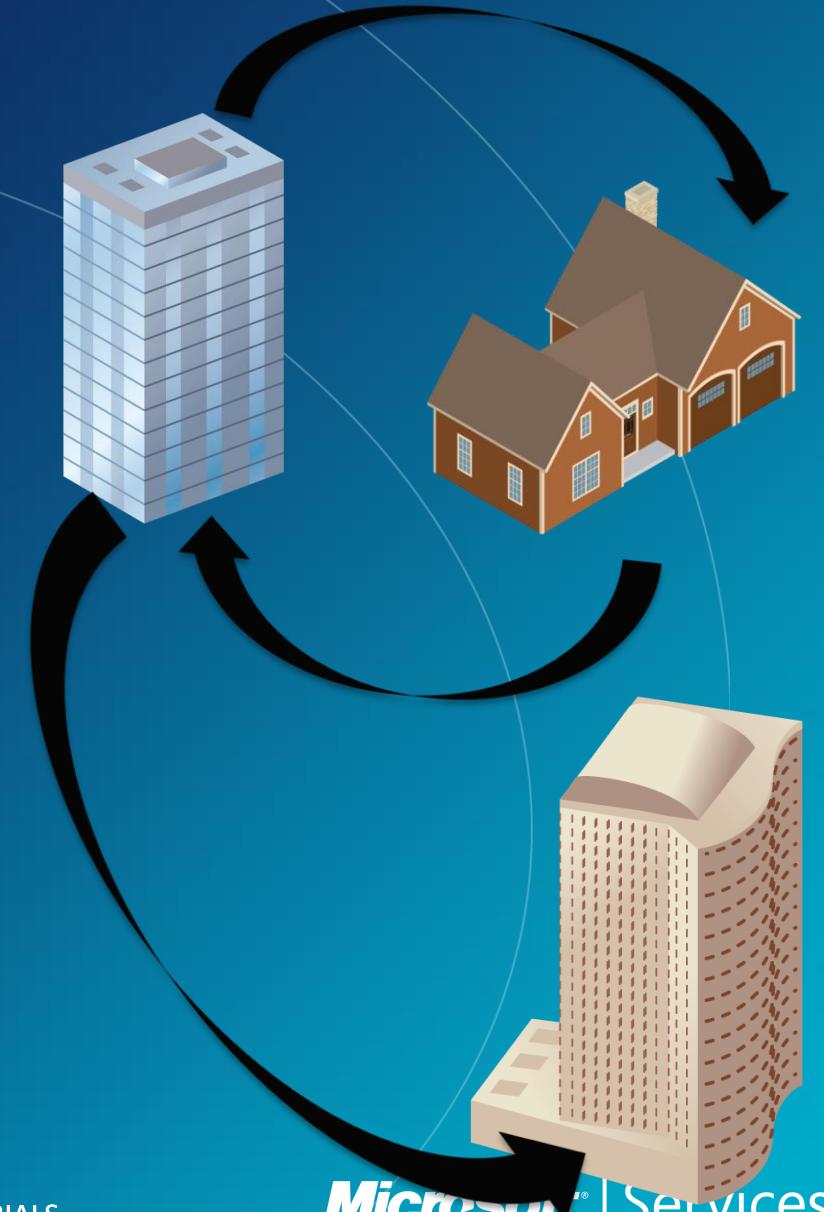
Windows 7 BitLocker To Go

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

Windows 7 BitLocker To Go

New unlock methods

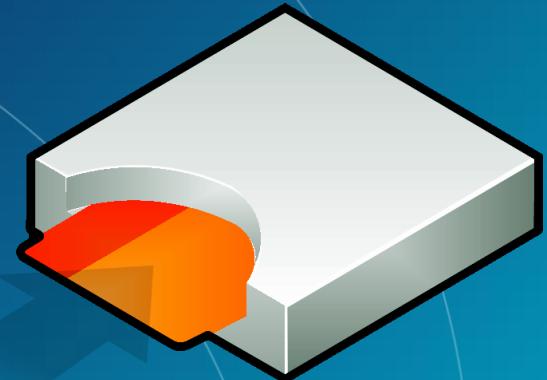
- Roaming using a Passphrase
 - No specific hardware requirement
 - Easily roam inside and outside domains/organizations
 - Complexity and length requirements managed by Group Policy



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

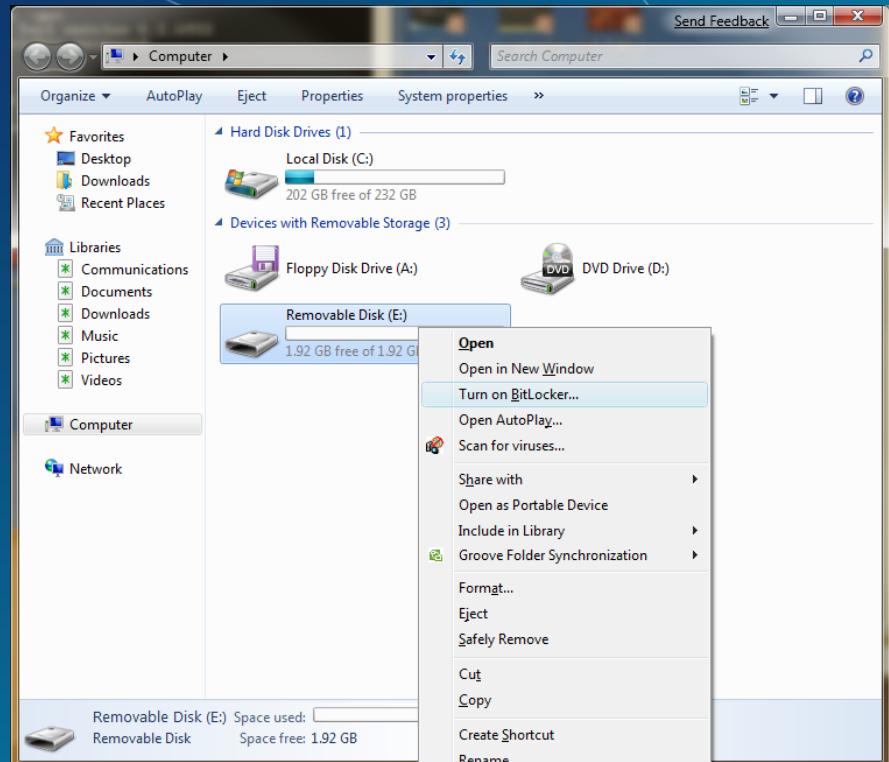
New recovery mechanism

- 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

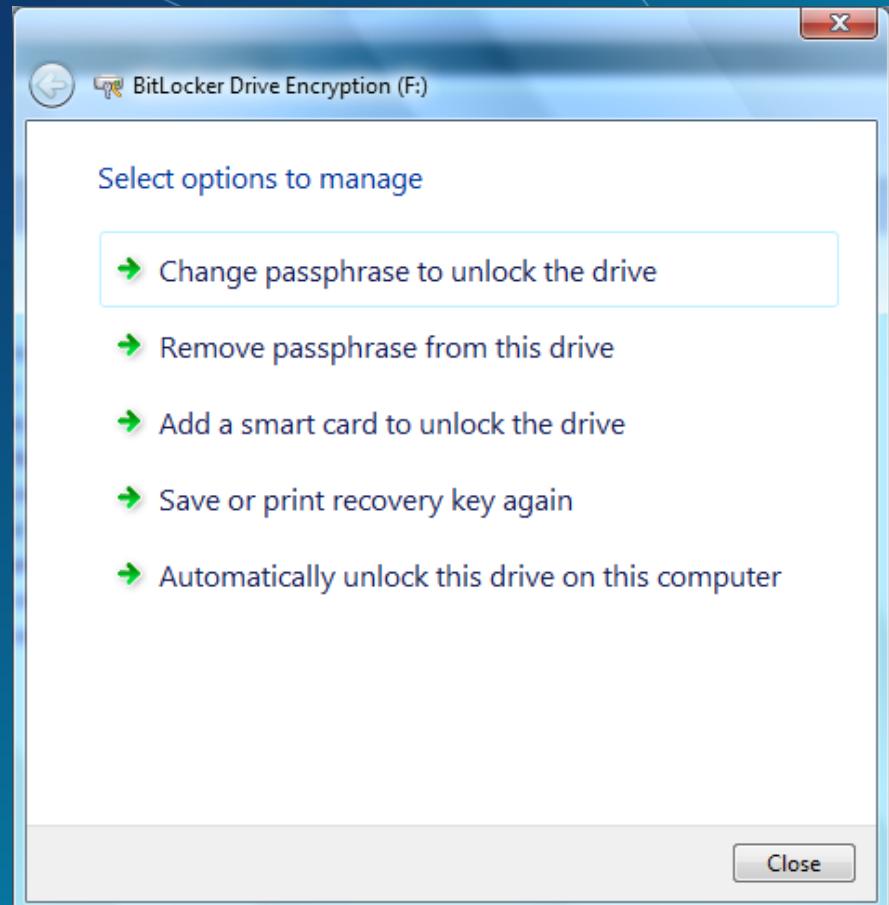
- BitLocker from Windows Explorer
- Right click drives in Windows Explorer to:
 - Turn on BitLocker
 - Unlock a drive
 - Manage BitLocker



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

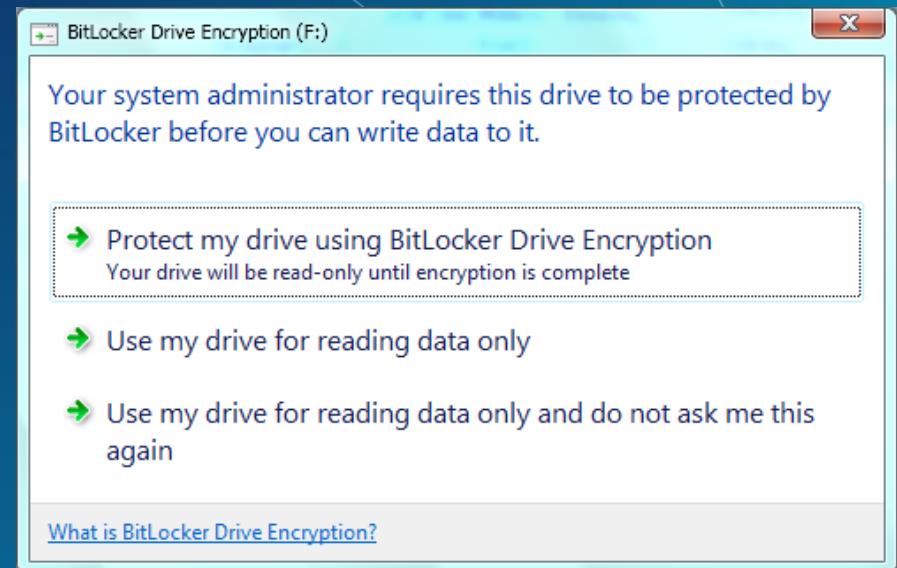
Mandating BitLocker on removable drives

- 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





Microsoft | Services

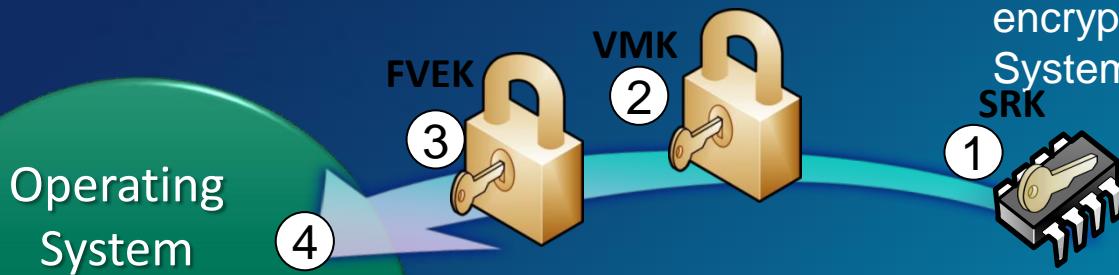
Disk Layout and Key Storage

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

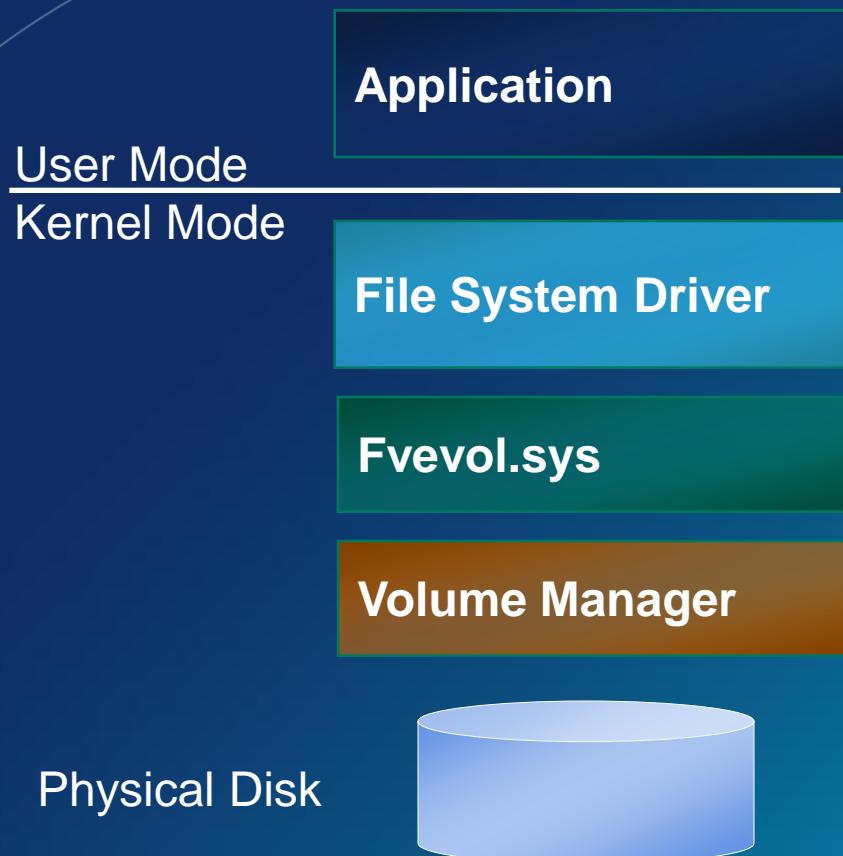
Drive Encryption Specifics

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

Offset (h)	Offset (d)	Size	Field	Required Value for BitLocker
0x003	3	8	Signature	'-','F','V','E','-','F','S','-'
0x00B	11	2	BytesPerSector	
0x00D	13	1	SectorsPerCluster	One of 0x01, 0x02, 0x04, 0x08, 0x10, 0x20, 0x40 or 0x80
0x00E	14	2	ReservedClusters	0x0000
0x010	16	1	FatCount	0x00
0x011	17	2	RootEntries	0x0000
0x013	19	2	Sectors	0x0000
0x016	22	2	SectorsPerFat	0x0000
0x020	32	4	LargeSectors	0x00000000
0x038	56	8	MetadataLcn	

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:

MetadataLCN * SectorsPerCluster * BytesPerSector

Examination of Physical Image

Offset (h)	Offset (d)	Size	Field	Content
0x000	0	8	Signature	'-','F','V','E','-','F','S','-'
0x008	8	2	Size	Size of structure. Validation data follows this structure.
0x002	2	10	Version	0x0001 for current version.
0x004	4	12		Version specific content.

- Additionally a text string search for –FVE-FS- to find this location and verify the calculation

Examination of Physical Image - VISTA

00000000	eb	52	90	2d	46	56	45	2d-46	53	2d	00	02	08	00	00	ëR--FVE-FS-----
00000016	00	00	00	00	00	f8	00	00-3f	00	ff	00	00	e8	2e	00ø..?..ÿ..è..
00000032	00	00	00	00	80	00	80	00-ff	37	25	02	00	00	00	00ÿ7%-----
00000048	00	00	0c	00	00	00	00	00-26	17	00	00	00	00	00	00&-----
00000064	f6	00	00	00	01	00	00	00-9b	3a	85	90	6b	85	90	6e	ö.....:..k..n

- 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

0000000000	eb	58	90	2d	46	56	45	2d-46	53	2d	00	02	08	00	00	ex --FVE-FS-----
0000000010	00	00	00	00	00	f8	00	00-3f	00	ff	00	00	28	03	00	-----ø---?---ý---(---
0000000020	00	00	00	00	e0	1f	00	00-00	00	00	00	00	00	00	00	-----à-----
0000000030	01	00	06	00	00	00	00	00-00	00	00	00	00	00	00	00	-----.....-----

- 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?

000000000	33 c0 8e d0 bc 00 7c fb-50 07 50 1f fc be 1b 7c	3À-B¾- ûP-P-Û¾-
000000010	bf 1b 06 50 57 b9 e5 01-f3 a4 cb bd be 07 b1 04	z -·PW¹å -ó¾E¾-±-
000000020	38 6e 00 7c 09 75 13 83-c5 10 e2 f4 cd 18 8b f5	8n - -u -·À -åöí -·ö
000000030	83 c6 10 49 74 19 38 2c-74 f6 a0 b5 07 b4 07 8b	-·È -It -8 ,tö u -·-
000000040	f0 ac 3c 00 74 fc bb 07-00 b4 0e cd 10 eb f2 88	8-<-tü» -· -í -ëö -
000000050	4e 10 e8 46 00 73 2a fe-46 10 80 7e 04 0b 74 0b	N -èF -s *pF - - - -t -
000000060	80 7e 04 0c 74 05 a0 b6-07 75 d2 80 46 02 06 83	- - - t - ¶ -uò -F - - -
000000070	46 08 06 83 56 0a 00 e8-21 00 73 05 a0 b6 07 eb	F - - V - - è! -s - ¶ -ë
000000080	bc 81 3e fe 7d 55 aa 74-0b 80 7e 10 00 74 c8 a0	¾ -> p } U - t - - - -t È
000000090	b7 07 eb a9 8b fc 1e 57-8b f5 cb bf 05 00 8a 56	- - èö -ü -W -öÈz - - - V
0000000a0	00 b4 08 cd 13 72 23 8a-c1 24 3f 98 8a de 8a fc	- - í -r # - Á\$? - - P -ü
0000000b0	43 f7 e3 8b d1 86 d6 b1-06 d2 ee 42 f7 e2 39 56	C - à - Ñ - Ö ± - ÒiB - à9V
0000000c0	0a 77 23 72 05 39 46 08-73 1c b8 01 02 bb 00 7c	- w # r - 9F - s - , - - » -
0000000d0	8b 4e 02 8b 56 00 cd 13-73 51 4f 74 4e 32 e4 8a	- N - - V - Í - sQOtN2ä -
0000000e0	56 00 cd 13 eb e4 8a 56-00 60 bb aa 55 b4 41 cd	V - í - éä - V - - » - U - Áí

- 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

000000000	eb	58	90	2d	46	56	45	2d-46	53	2d	00	02	08	00	00	éX--FVE-FS-----
00000010	00	00	00	00	00	f8	00	00-3f	00	ff	00	20	00	00	00	-----ø---?---ÿ-----
00000020	00	00	00	00	e0	1f	00	00-00	00	00	00	00	00	00	00	-----à-----
00000030	01	00	06	00	00	00	00	00-00	00	00	00	00	00	00	00	-----
00000040	80	00	29	00	00	00	00	4e-4f	20	4e	41	4d	45	20	20	-->)-----NO NAME
00000050	20	20	46	41	54	33	32	20-20	20	33	c9	8e	d1	bc	f4	FAT32 3É·Ñ¾ô
00000060	7b	8e	c1	8e	d9	bd	00	7c-a0	fb	7d	b4	7d	8b	f0	ac	{·Á·Ù%· ·û}·}·ë-
00000070	98	40	74	0c	48	74	0e	b4-0e	bb	07	00	cd	10	eb	ef	·@t·Ht··»·í·ëí
00000080	a0	fd	7d	eb	e6	cd	16	cd-19	00	00	00	00	00	00	00	ý}ëí·í-----
00000090	00	00	00	00	00	00	00	00-00	00	00	00	00	00	00	00	-----
000000a0	3b	d6	67	49	29	2e	d8	4a-83	99	f6	a3	39	e3	d0	01	;ÖgI).ØJ·ö£9åD-
000000b0	00	00	10	02	00	00	00	00-00	e0	47	29	00	00	00	00	-----àG)-----

- 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

000	9c	00	00	00	01	00	00	00-30	00	00	00	9c	00	00	000.....0.....
016	75	39	c1	de	46	02	87	44-8b	55	b5	9f	f4	1e	b0	2e	u9ÀPF..-D-Uµ-ô-º.	u9ÀPF..-D-Uµ-ô-º.
032	01	00	00	00	00	00	00	00-c0	97	7b	0e	d9	a3	c7	01À-{.Ù£Ç-À-{.Ù£Ç-
048	6c	00	06	00	09	00	01	00-b3	a4	6c	7c	30	f6	e2	4b	1.....'ñl 0öåK	1.....'ñl 0öåK
064	a2	3e	5c	f7	9b	ad	a1	60-80	2e	34	0e	d9	a3	c7	01	»>\÷--í..4-Ù£Ç-	»>\÷--í..4-Ù£Ç-
080	20	00	00	00	02	00	01	00-45	00	78	00	74	00	65	00E-x-t-e-E-x-t-e-
096	72	00	6e	00	61	00	6c	00-4b	00	65	00	79	00	00	00	r-n-a-l-K-e-y--	r-n-a-l-K-e-y--
112	2c	00	00	00	01	00	01	00-02	20	00	00	f8	1a	b4	18	,.....ø--'	,.....ø--'
128	71	fe	50	98	8d	66	42	5e-94	a0	66	92	d9	1d	65	5b	qþP..fB^..f-Ù-e[qþP..fB^..f-Ù-e[
144	d4	64	f8	eb	72	a2	06	52-de	fc	02	81					Ödøero·RPü..	Ödøero·RPü..

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?



30
Minutes



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

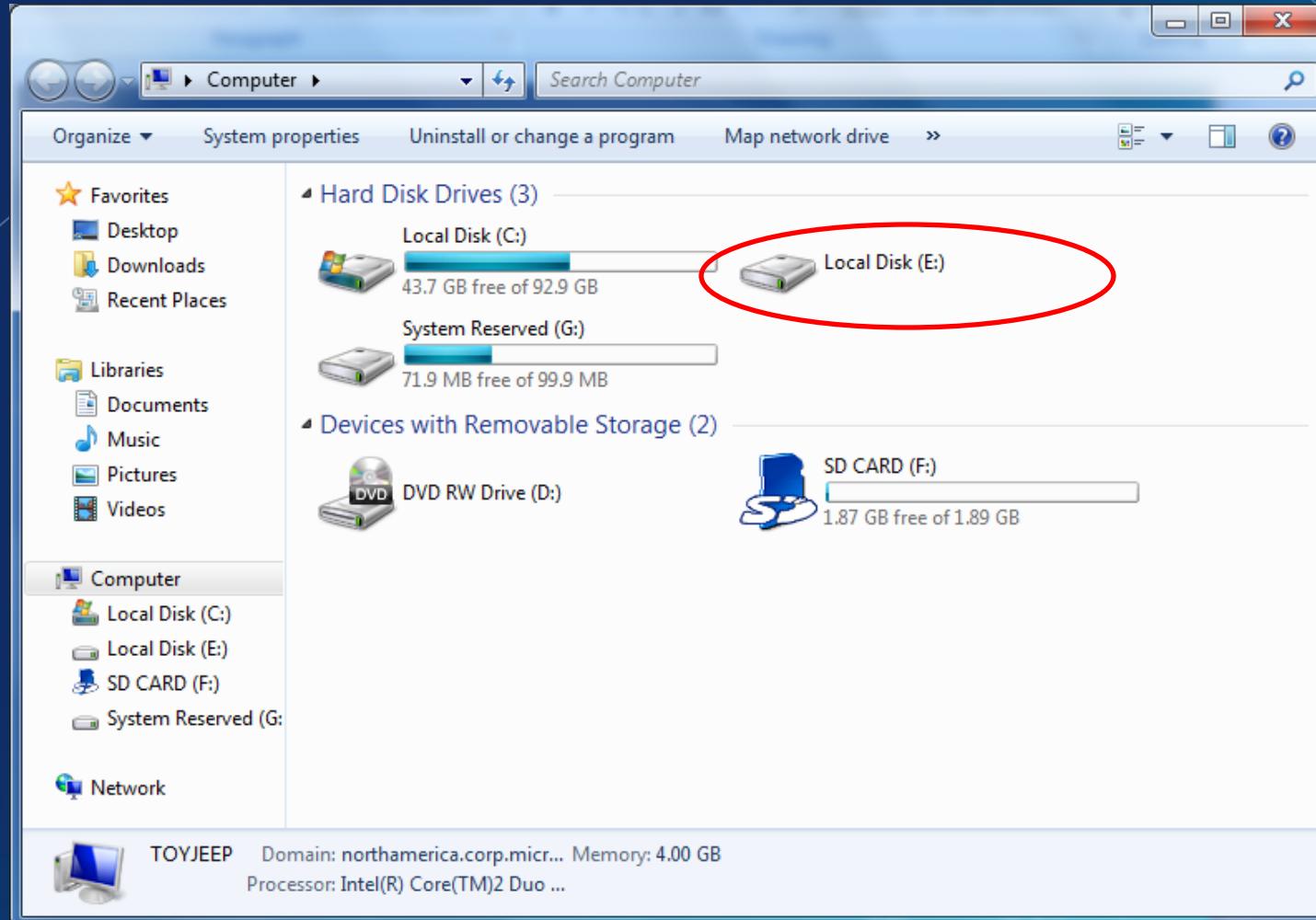
- Investigators can use the recovery mechanisms built into the BitLocker mechanism to access the protected drive
- Just like EFS
-

WE STILL NEED THE PASSWORD!!!

Mounting a BitLocker Drive

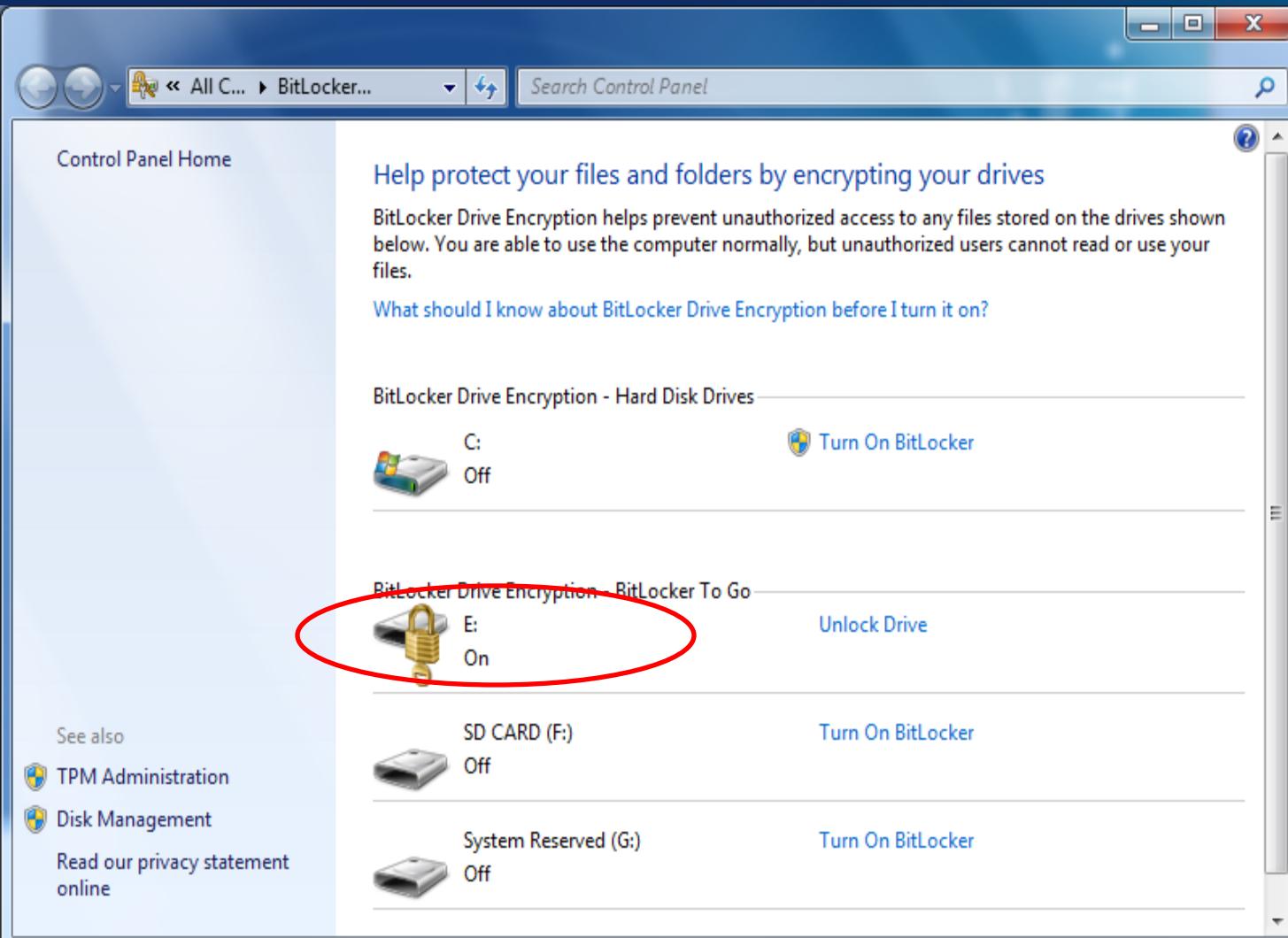
- Physical Mount
 - Install the “suspect” drive as a secondary drive through a write blocker
 - Boot to a BitLocker capable version of Win 7
 - Access the BitLocker MMC
 - You should see the “suspect” drive
 - Use the BitLocker recovery process to temporarily access the data

Mounting a BitLocker Drive



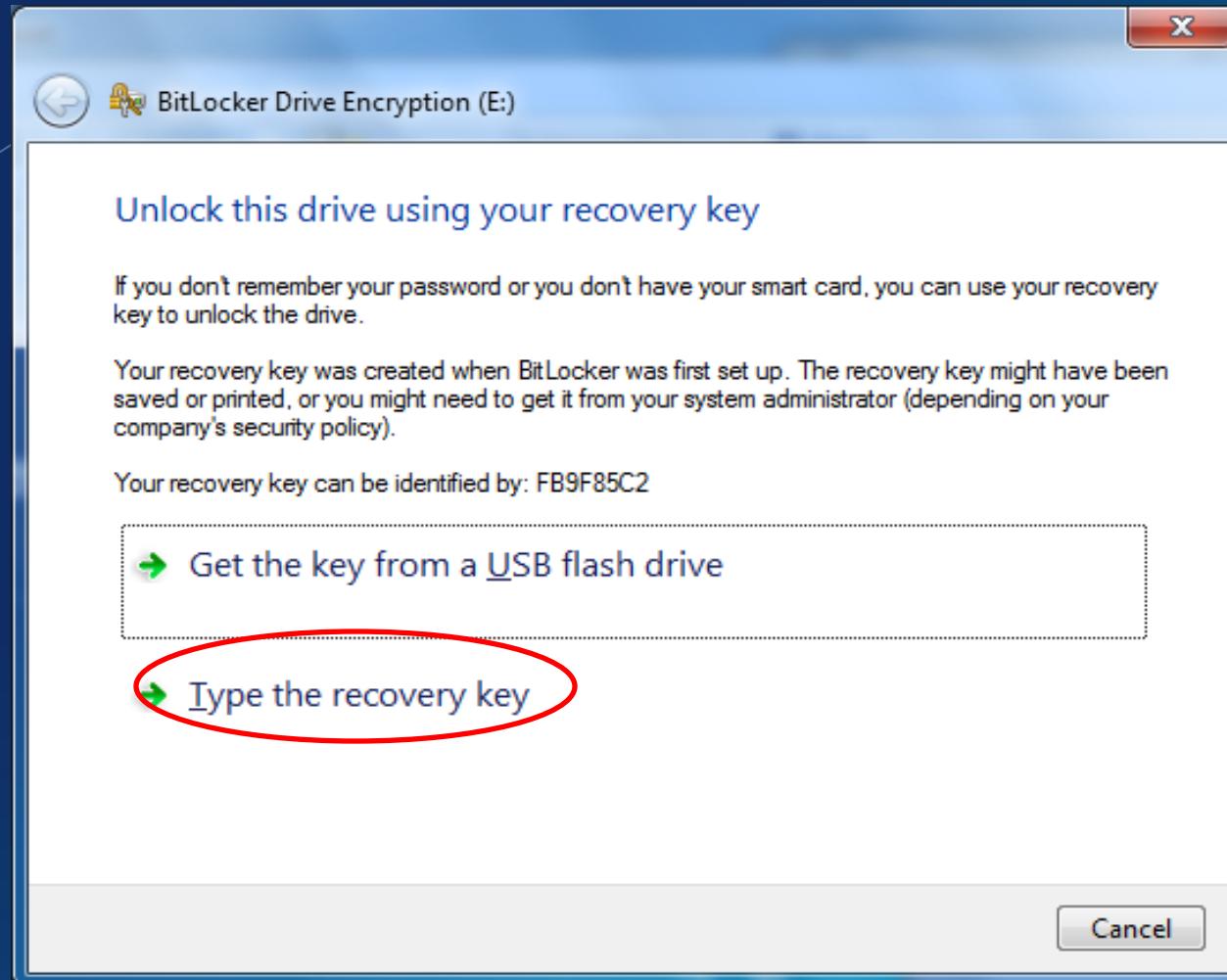
- The drive is recognized but it can not be read
- Details are unavailable

Mounting a BitLocker Drive



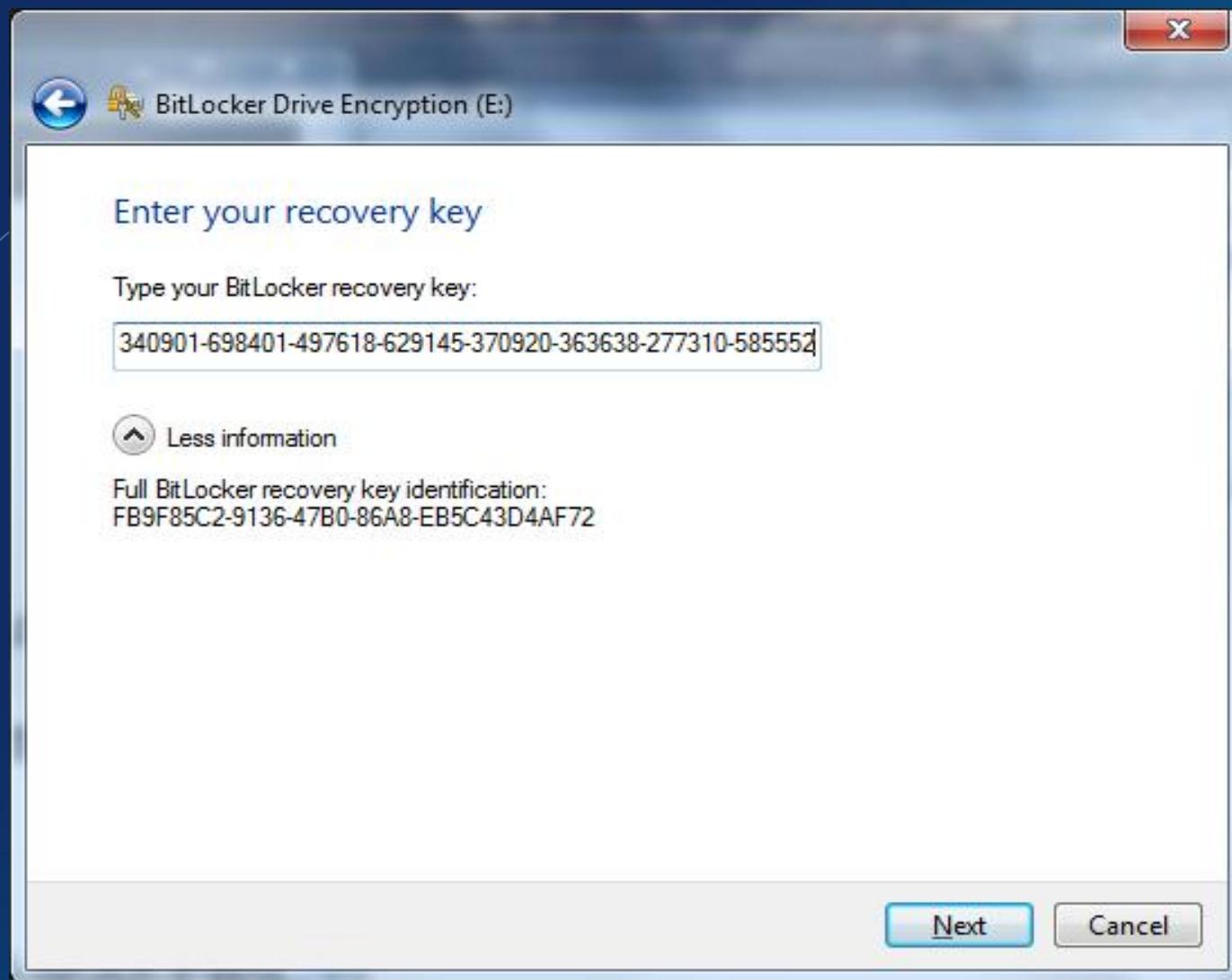
- The BitLocker MMC is sees the drive as protected – “Unlock”

Mounting a BitLocker Drive



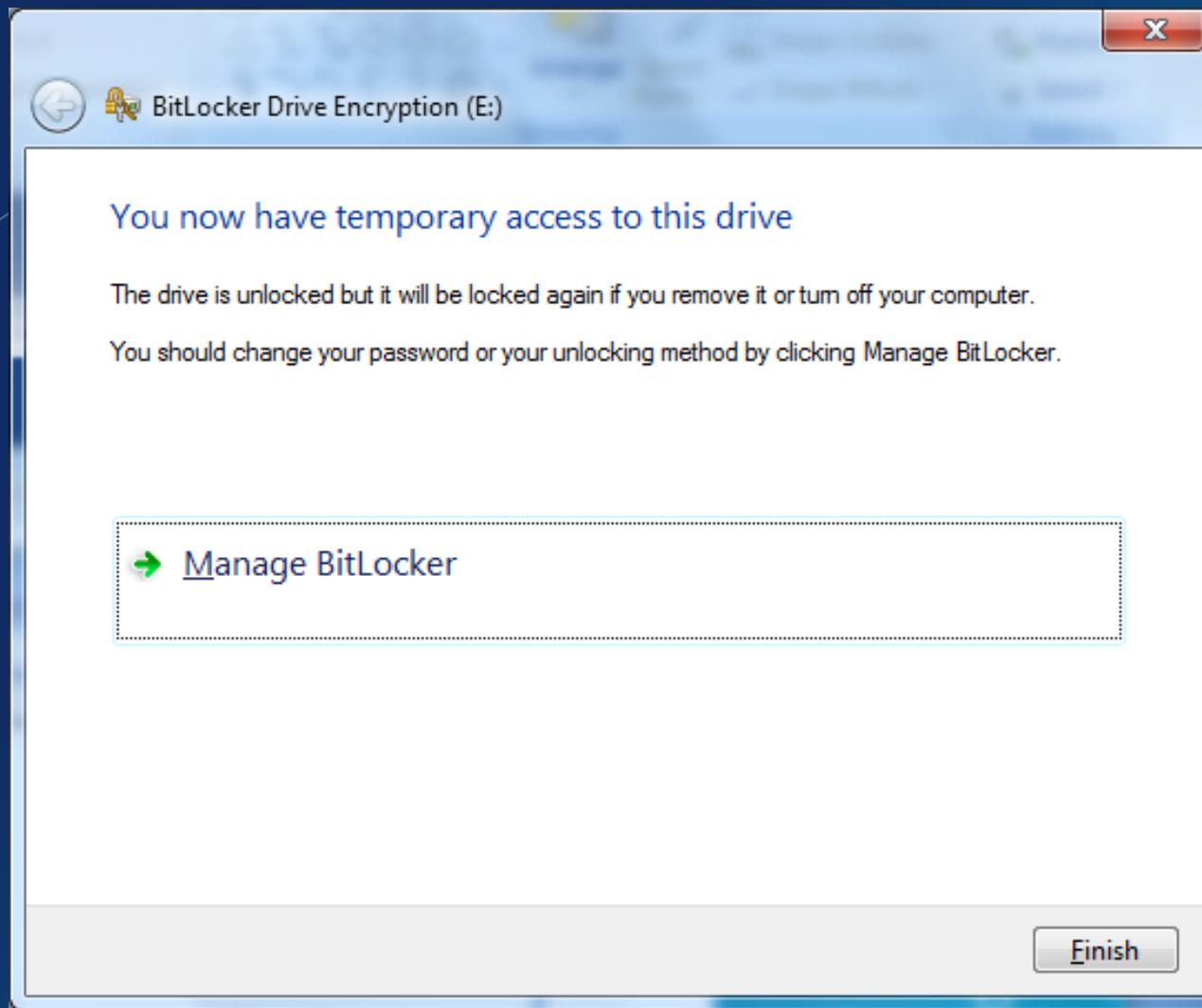
- Choose password format – “USB Key” or “Manually”

Mounting a BitLocker Drive



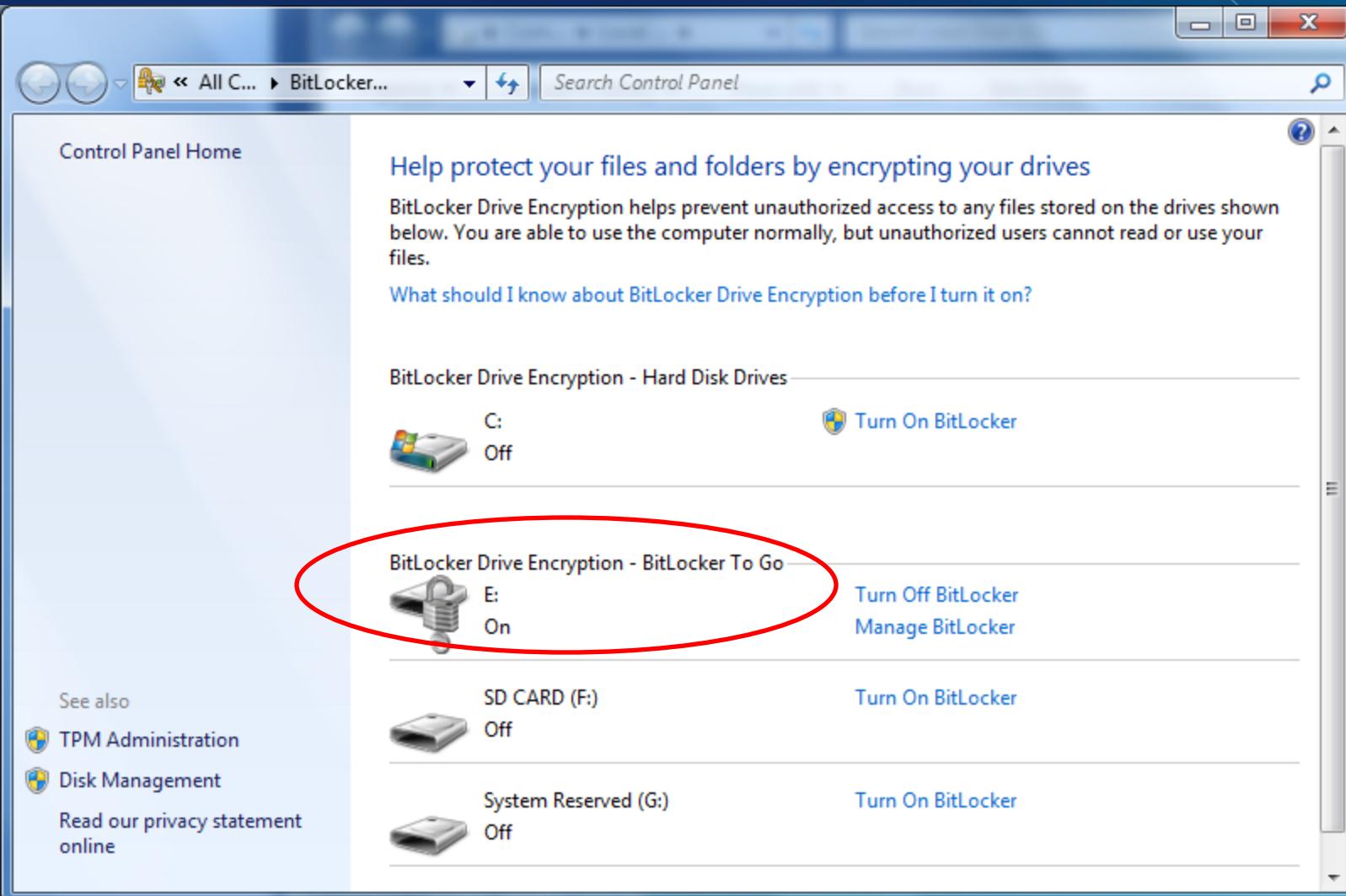
- We have the Recovery Key
Password so we type it in

Mounting a BitLocker Drive



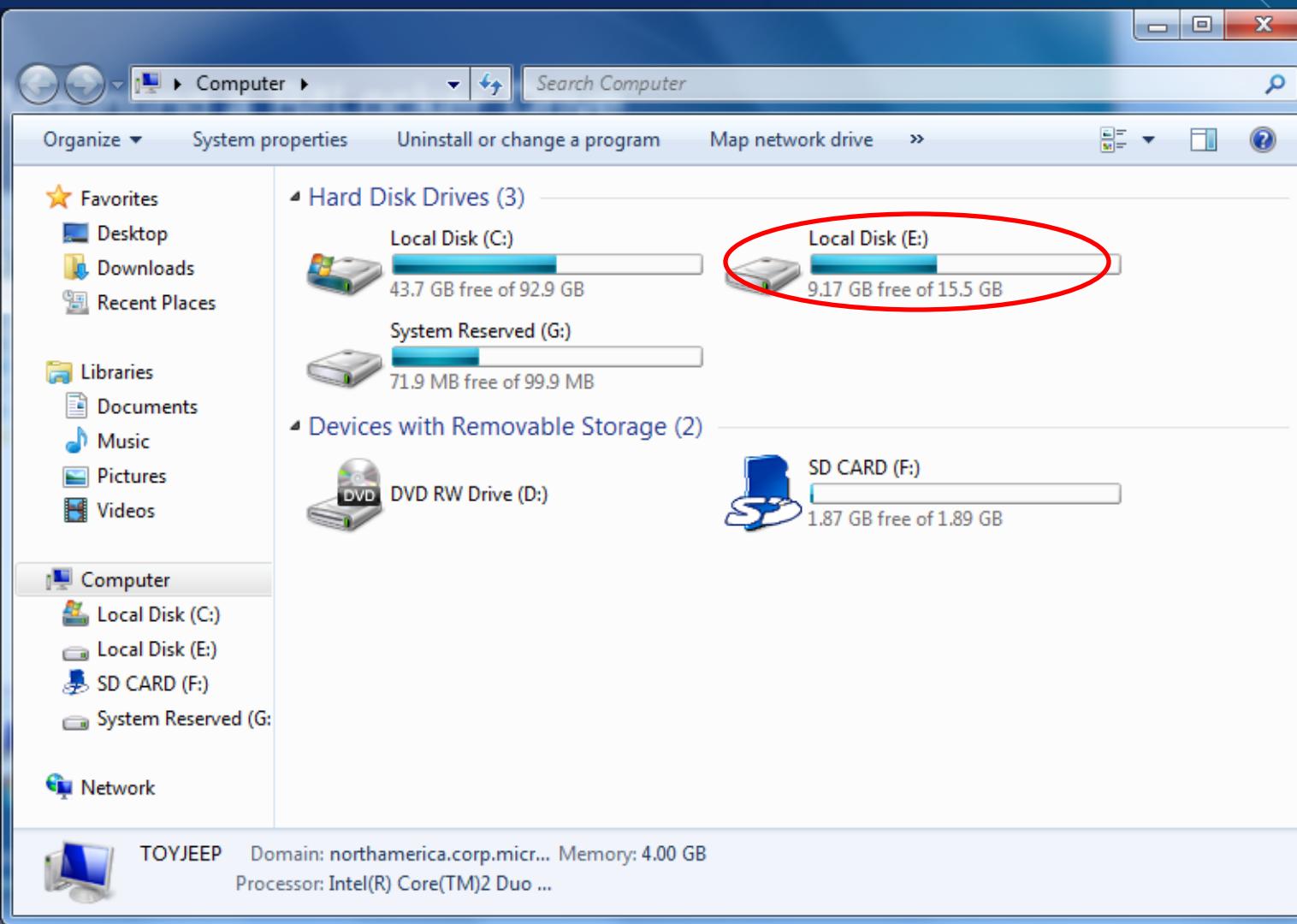
- "You can now temporarily access this drive"

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?

Prevent memory overwrite on restart

Prevent memory overwrite on restart

Not Configured Comment:

Enabled

Disabled

Supported on: At least Windows Vista

Options:

Help:

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.

OK Cancel Apply

The screenshot shows the Windows Group Policy Management Editor interface. The title bar says "Prevent memory overwrite on restart". The main pane displays the policy settings. The "Not Configured" radio button is selected. The "Comment" field is empty. The "Supported on" field says "At least Windows Vista". In the "Help" section, there is a detailed description of the policy's function. A red oval highlights the last sentence of the help text: "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`

Manage-BDE

```
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

Volume

Encryption State

Encryption Used

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?



30
Minutes



Mounting BitLocker Protected Volumes for Preview

Exercise

30
Minutes



Imaging Implications for BitLocker Protected Drives

Exercise

30
Minutes



Examining File system Signatures of BitLocker Protected Volumes

Exercise

BitLocker in Win7 at a Glance

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