



Introduction to Windows 7

Exploration of Windows 7



Who Am I?

- Chris Ard
- Investigative Consultant
- 10 years at Microsoft
- Dallas, TX
- Multiple Certs, MBA, CISSP, MCSE, XYZ, etc
- chrisard@microsoft.com

Available SKUs



- Windows Vista Starter
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate

- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate

Windows 7 SKU Descriptions

All Windows 7 versions are a super set of the version below with no trade off on features when you upgrade from one version to the next

Windows® 7 Enterprise
Windows® Ultimate

Windows® 7
Professional

Windows® 7 Home
Premium

Windows® 7
Home Basic

Windows® 7
Starter

- “Enterprise” provides advanced data protection & information access for businesses that use IT as a strategy asset
- “Ultimate” is the no-compromise SKU for technical enthusiasts
- “Professional” is the business-focused SKU for small and lower mid-market companies and users who have networking, backup, and security needs and multiple PCs or servers
- “Home Premium” is the standard consumer SKU, providing full functionality on the latest hardware, easy ways to connect, and a visually rich environment
- “Home Basic” is the SKU for value PCs in emerging markets, meant for accessing the internet and running basic productivity applications
- “Starter” is an entry-level OEM SKU for small form factor PCs in all markets

SKU / Features



- **Windows 7 Starter**

Entry-level OEM SKU in all markets for cost-conscious consumers. "Starter" PC.

- **Broad application and device compatibility**
- **Safe, reliable, and supported**
- **Ability to join a HomeGroup**



SKU / Features

- **Windows 7 Home Basic** - Emerging market customers of value PCs who might otherwise choose Starter will choose Home Basic because...
 - Live Thumbnail Previews & enhanced visual experience
 - Advanced networking support (ad-hoc wireless networks and internet connection sharing)
 - No hardware restrictions

SKU / Features



- **Windows 7 Home Premium**
- All features of Home Basic Plus:
 - Aero® Glass & advanced windows navigation
 - Easy networking & sharing across all your PCs & devices
 - **Enhancements to Windows Media Center and media streaming, including Play To, and improved media format support**
 - Multi-touch and improved handwriting recognition

SKU / Features



- **Windows 7 Professional**
 - Ability to join a managed network with Domain Join
 - Protect data with advanced network backup and Encrypted File System
 - Print to the right printer at home or work with Location Aware Printing

SKU / Features



- **Windows 7 Enterprise**
 - BitLocker™ data protection on internal and external drives
 - DirectAccess provides seamless connectivity to your corporate network.
 - Decrease time branch office workers wait to open file across the network with BranchCache™.
 - Prevent unauthorized software from running with AppLocker™.

SKU / Features

- **Windows Vista Ultimate**
- Ultimate gives users everything Windows 7 has to offer by combining all of the features of Home Premium and Enterprise.
- Media Center
- Bitlocker
- EFS
- Backup/Restore
- DirectAccess Support
- Multi-Touch

Windows 7 Security

Building upon the security foundations of Windows Vista.

Fundamentally Secure Platform



- Streamlined User Account Control
- Enhanced Auditing

Securing Anywhere Access



- Network Access Protection
- DirectAccess™

Protect Users & Infrastructure



- AppLocker™
- Internet Explorer 8
- Data Recovery

Protect Data from Unauthorized Viewing



- RMS
- EFS
- BitLocker

Desktop Auditing

Windows Vista

- New XML based events
- Fine grained support for audit of administrative privilege
- Simplified filtering of “noise” to find the event you’re looking for
- Tasks tied to events

Challenges

- Granular auditing complex to configure
- Auditing access and privilege use for a group of users

Windows 7

Enhanced Auditing

- Demonstrate why a person has access to specific information
- Understand why a person has been denied access to specific information
- Track all changes made by specific people or groups



Remote Access for Mobile Workers

Access Information Anywhere

Situation Today



- Difficult for users to access corporate resources from outside the office
- Challenging for IT to manage, update, patch mobile PCs while disconnected from company network

Windows 7 Solution

DirectAccess™



- Same experience accessing corporate resources inside and outside the office
- Seamless connection increases productivity of mobile users
- Easy to service mobile PCs and distribute updates and policies

Protect Users & Infrastructure



AppLocker™



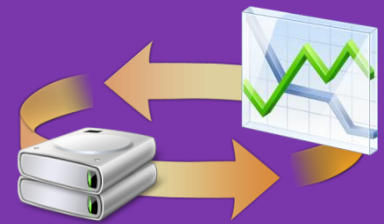
- Enables application standardization within an organization without increasing TCO
- Increase security to safeguard against data and privacy loss
- Support compliance enforcement

Internet Explorer 8



- Protect users against social engineering and privacy exploits
- Protect users against browser based exploits
- Protect users against web server exploits

Data Recovery



- File back up and restore
- CompletePC™ image-based backup
- System Restore
- Volume Shadow Copies

Microsoft | Services

IE8 Security Enhancements



Protection against Social Engineering Attacks

- **Phishing Filter** evolves to **SmartScreen™ Filter** to encompass malware threats
- **Domain Name Identification** highlights the real domain you're browsing on



Protection against Browser Attacks

- **Per-user ActiveX** contains risk to single user account.
- **Per-site ActiveX** allows developer restrict control to only their site/app



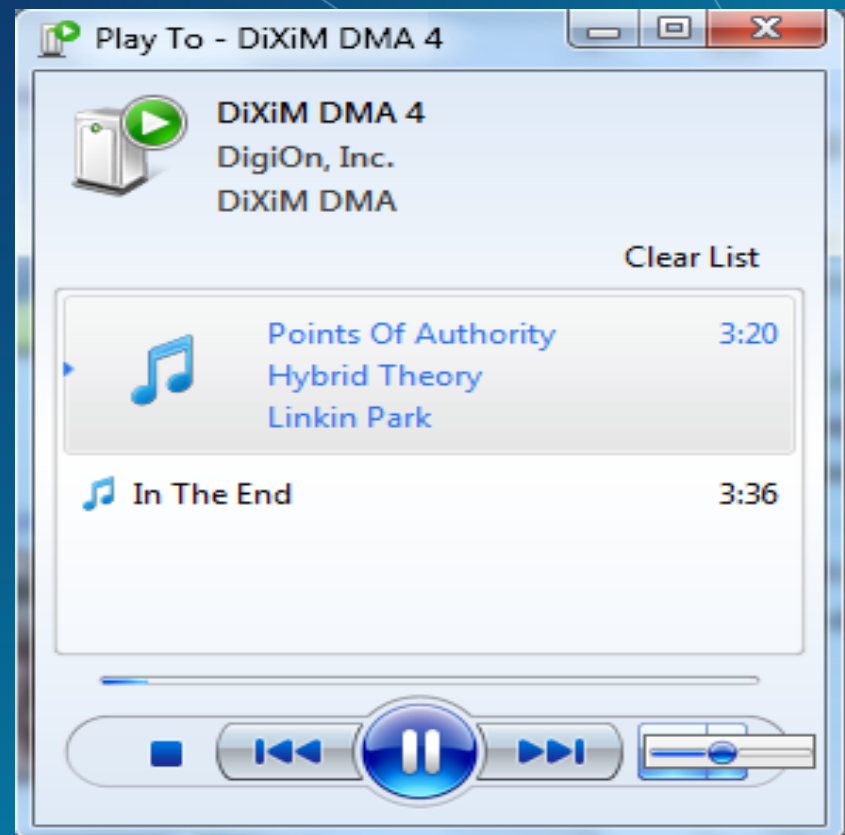
Protection against Web site exploits

- **Cross Domain Requests** object ensures data is only shared after a mutual validation of identity
- **Cross-Site Scripting Filter** helps protect users against a compromised site

Powerful Multimedia Capabilities



- Enhanced organizing and SHARING of media
 - Indexing
 - Media Library
 - Device Support



Device Stage

“Share Media”



- Photo-realistic image of device on taskbar
- Access device details and tasks directly from the icon
- Sync data effortlessly between media



Protect Data from Unauthorized Viewing



Windows 7

RMS



- Policy definition and enforcement
- Protects information wherever it travels
- Integrated RMS Client
- Policy-based protection of document libraries in SharePoint

EFS



- User-based file and folder encryption
- Ability to store EFS keys on a smart card

BitLocker



- Easier to configure and deploy
- Roam protected data between work and home
- Share protected data with co-workers, clients, partners, etc.
- Improve compliance and data security

Microsoft Services

Data Protection Scenarios

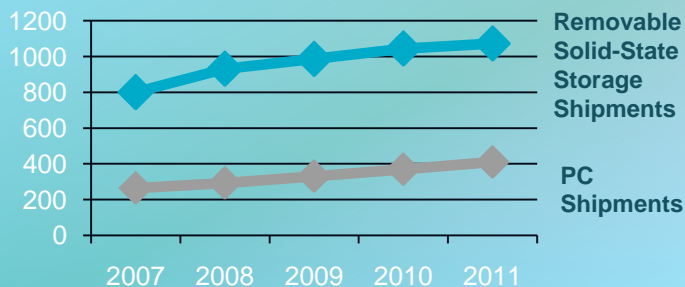
Scenario	RMS	EFS	BitLocker™
Remote document policy enforcement	✓		
Protect content in transit	✓		
Protect content during collaboration	✓		
Local multi-user file & folder protection on a shared machine		✓	
Remote file & folder protection		✓	
Untrusted network administrator		✓	
Laptop protection			✓
Branch office server			✓
Local single-user file & folder protection			✓

BitLocker

Situation Today



Worldwide Shipments (000s)



- Gartner "Forecast: USB Flash Drives, Worldwide, 2001-2011" 24 September 2007, Joseph Unsworth
- Gartner "Dataquest Insight: PC Forecast Analysis, Worldwide, 1H08" 18 April 2008, Mikako Kitagawa, George Shiffler III

Windows 7 Solution

BitLocker To Go™



- Extend BitLocker™ drive encryption to removable devices
- Create group policies to mandate the use of encryption and block unencrypted drives
- Simplify BitLocker setup and configuration of primary hard drive

BitLocker

Technical Details

- BitLocker Enhancements

- Automatic 500 Mb hidden boot partition
- New Key Protectors
 - Domain Recovery Agent (DRA)
 - Smart card – data volumes only



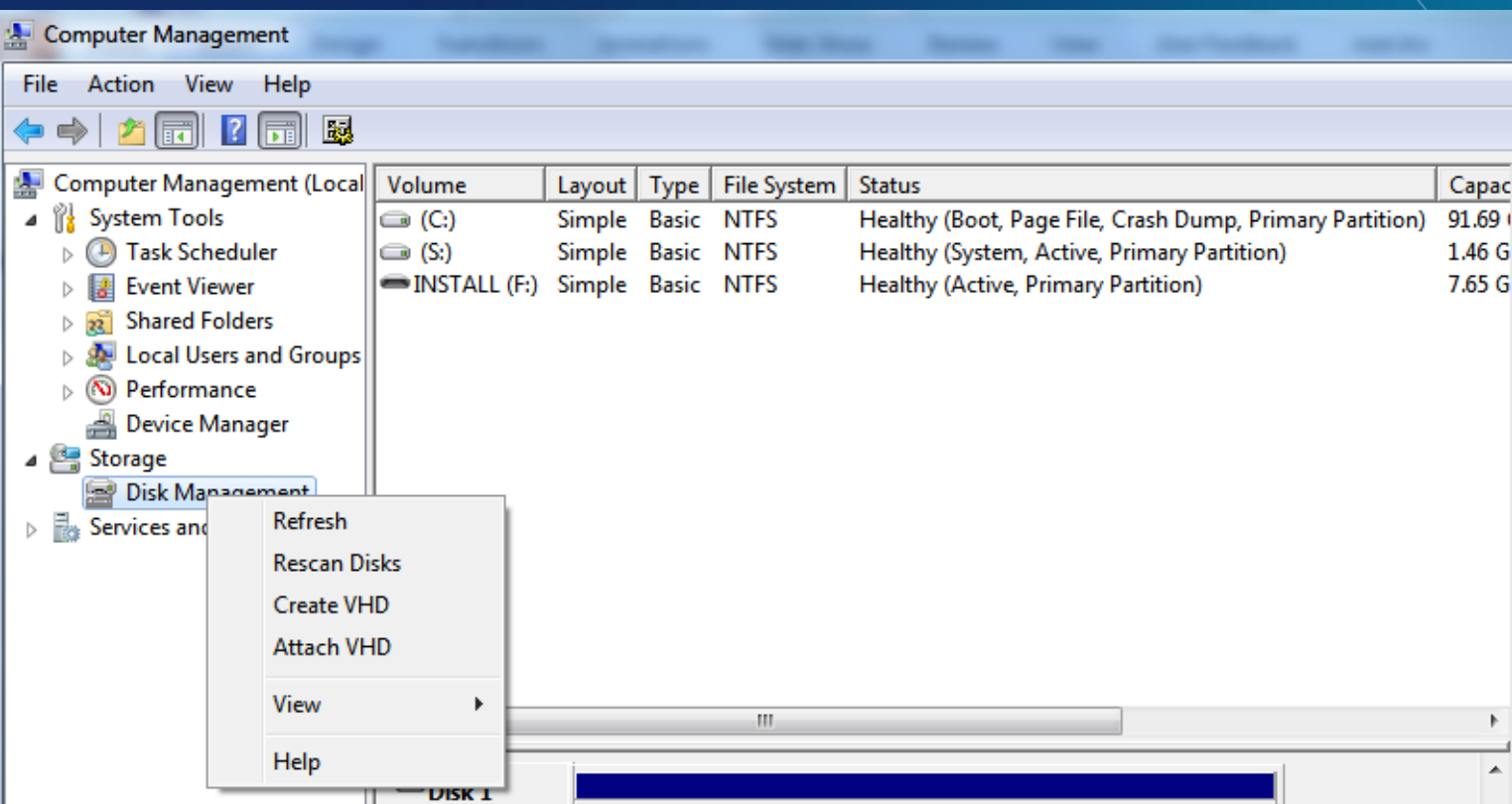
- BitLocker To Go™

- Support for FAT*
- Protectors: DRA, passphrase, smart card and/or auto-unlock
- Management: protector configuration, encryption enforcement
- SKU Availability
 - Encrypting – Enterprise, Ultimate
 - Unlocking – All



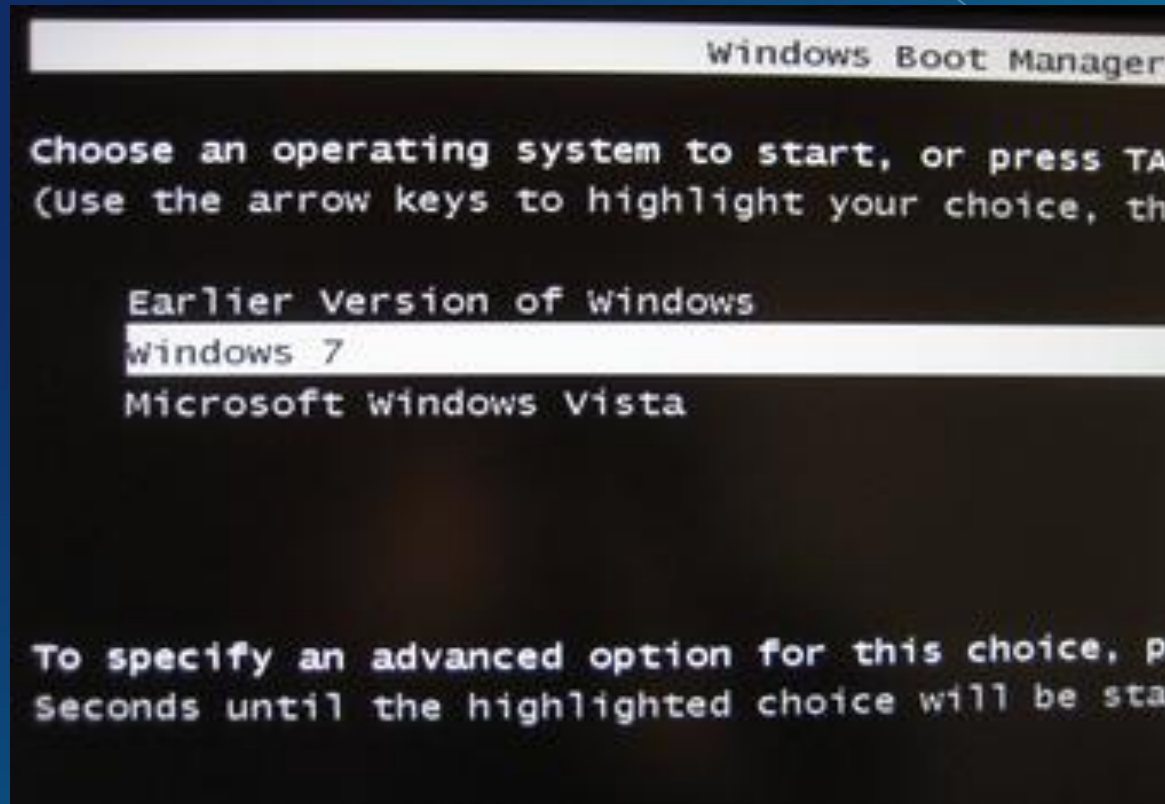
Virtual Hard Drive (VHD) Support

- Mount VHD files as drives
 - Mount existing VHD files as drive letter
 - Create VHD files



Virtual Hard Drive (VHD) Support

- Boot from VHD
 - Create multi-boot scenarios between OS on real hard drive and an alternate OS on VHD file



Everyday Tasks Are Faster & Easier

Simpler Home Networking

“Creating a home network and sharing between home PCs and devices is too hard”

HomeGroup

Easier set-up

Easier file & media sharing

across multiple PCs

One step printer sharing

Simple security control



Security - EFS



- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate



- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate

Security - BitLocker



- Windows Vista Enterprise
- Windows Vista Ultimate



- Windows Seven Enterprise
- Windows Seven Ultimate

Data Recovery

Scenario	Vista All	Vista Business/Enterprise/Ultimate	Win 7 All	Win 7 Professional/Enterprise/Ultimate
Basic File Backup	✓	✓	✓	✓
Network Backup				✓
Complete PC Backup		✓		
System Image				✓
System Restore	✓	✓	✓	✓
Previous Version		✓		✓



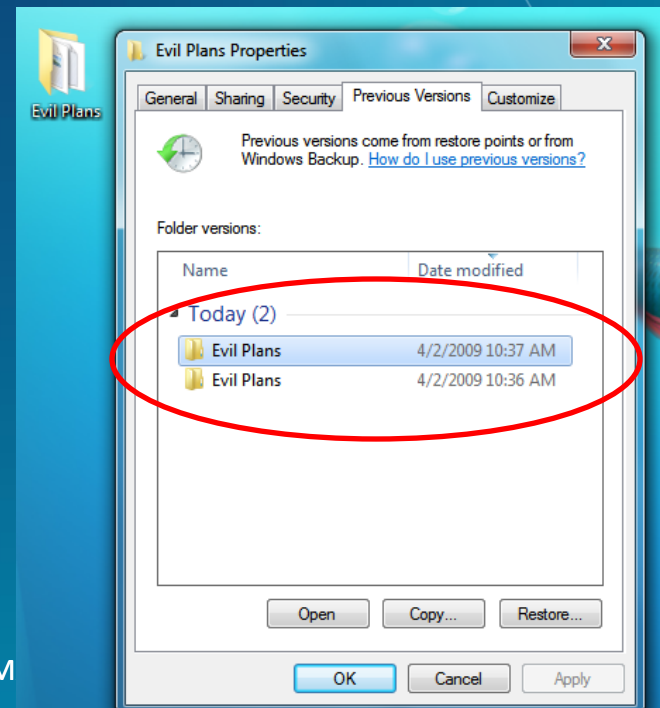
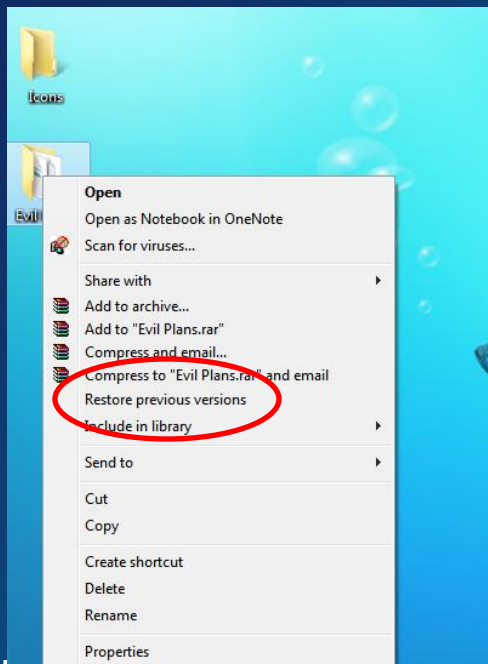
Windows VSS

- Introduced in Server 2003, now called “Previous Versions” this feature is available in Windows Vista:
 - Business
 - Enterprise
 - Ultimate
- On by Default!!*
- A user can track back through previous versions of a document and even recover deleted documents from the system



Previous Version

- Recovers USER data as well as ANY other file
- Exposed in GUI
- Enabled by default

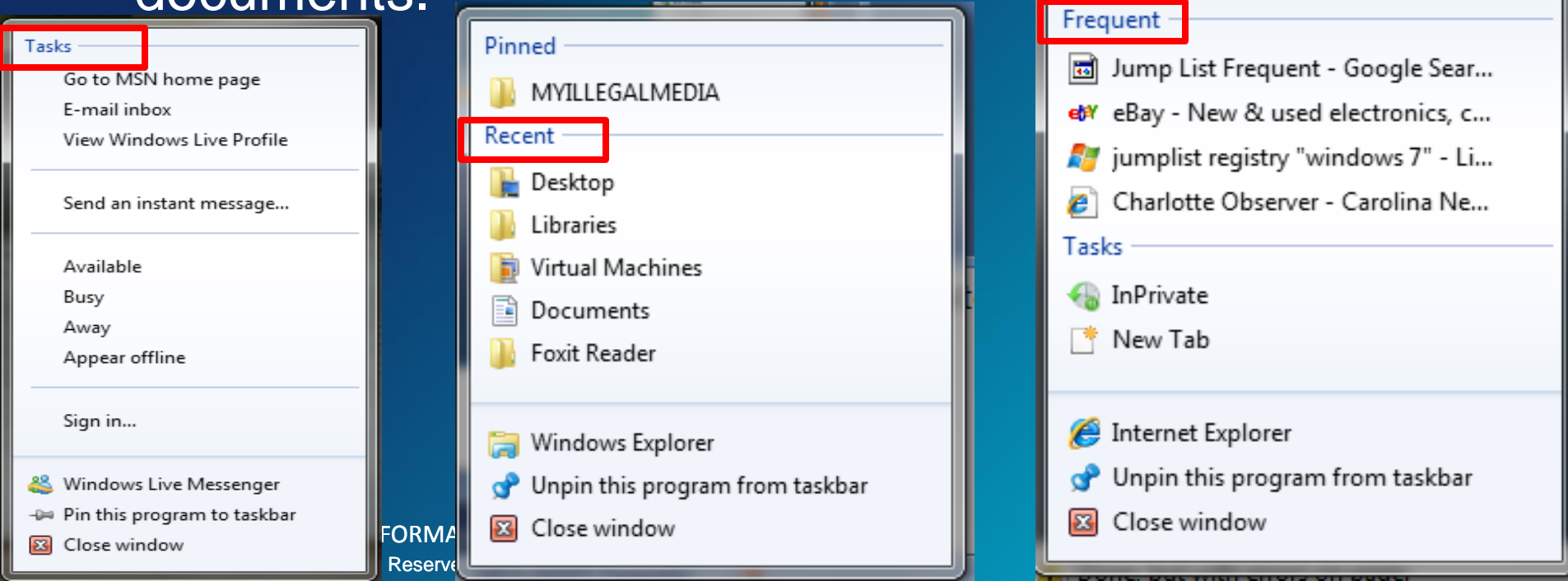


Windows 7 Forensic Artifacts of Interest

Exploration of Windows 7

New File System Features – Jump Lists

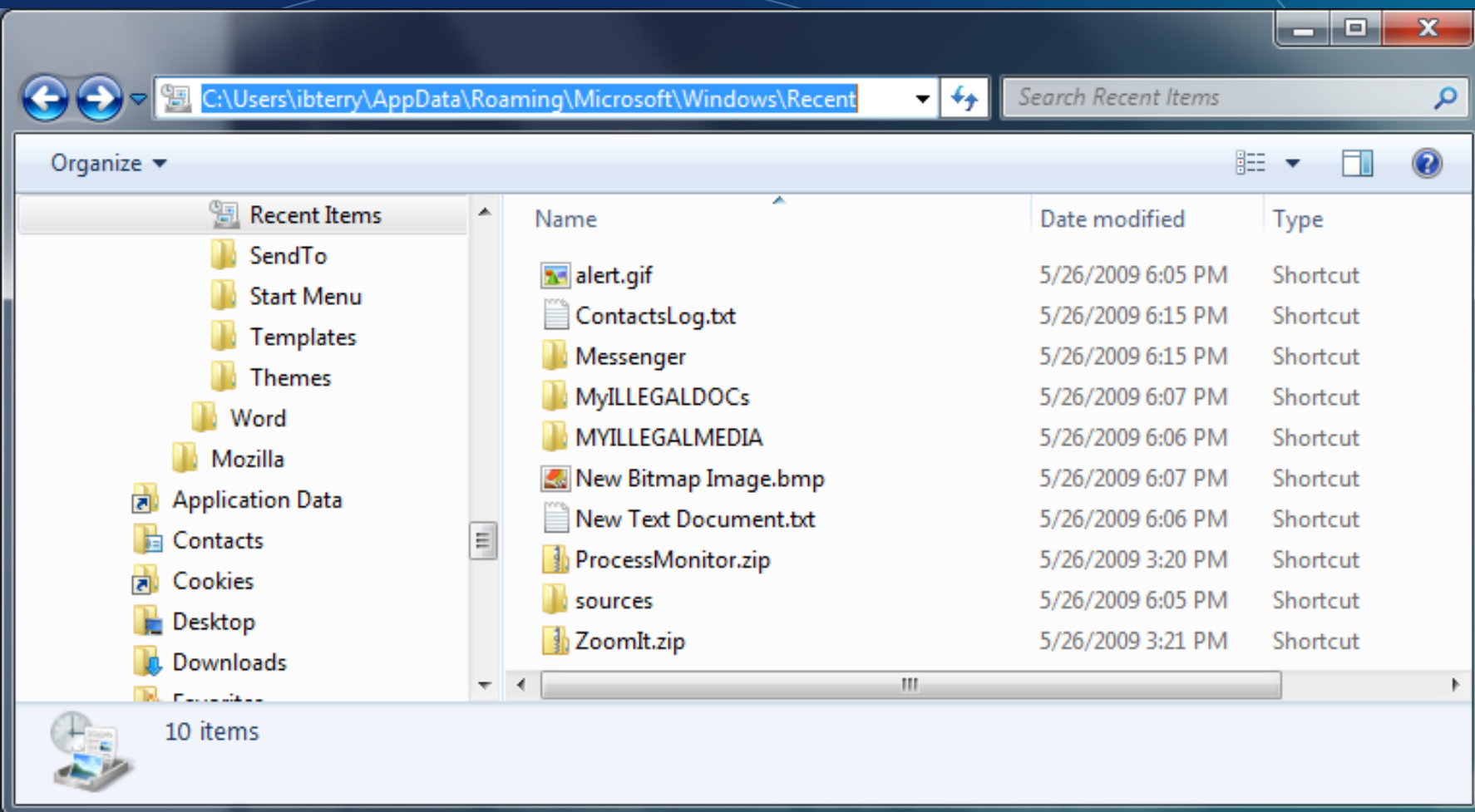
- Jump Lists - You can think of Jump Lists as miniature Start menus for program icons on the Taskbar. Each Jump List can contain tasks, links to recent and frequently used documents, and links to pinned documents.



New File System Features – Jump Lists

- Jump List data for all applications are stored centrally in the users profile.
 - C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Recent
- When viewed in explorer this looks like any other Windows folder.

New File System Features – Jump Lists Explorer



New File System Features – Jump Lists FTK

AccessData FTK Imager

File View Mode Help

Evidence Tree

- Libraries
 - C:\Users\vbtery\AppData\Roaming\Microsoft\Windows\Libraries
- Recent
 - C:\Users\vbtery\AppData\Roaming\Microsoft\Windows\Recent
 - AutomaticDestinations
 - CustomDestinations

File List

Name	Size	Type	Date Modified
AutomaticDestinations	4 KB	Directory	5/26/2009 1
CustomDestinations	4 KB	Directory	5/27/2009 2
alert.gif.Ink	1 KB	Regular File	5/26/2009 1
ContactsLog.txt.Ink	2 KB	Regular File	5/26/2009 1
desktop.ini	1 KB	Regular File	4/29/2009 1
Messenger.Ink	1 KB	Regular File	5/26/2009 1
MyILLEGALDOCs.Ink	1 KB	Regular File	5/26/2009 1
MYILLEGALMEDIA.Ink	1 KB	Regular File	5/26/2009 1
New Bitmap Image.bmp.Ink	1 KB	Regular File	5/26/2009 1
New Text Document.txt.Ink	1 KB	Regular File	5/26/2009 1
ProcessMonitor.zip.Ink	1 KB	Regular File	5/26/2009 7
sources.Ink	1 KB	Regular File	5/26/2009 1
ZoomIt.zip.Ink	1 KB	Regular File	5/26/2009 7

Custom Content Sources

Evidence: File System | Path | File | Options

New Edit Remove Remove All Create Image

Properties Hex Value Interpreter Custom Content Sources

For Help, press F1

These do not appear in explorer view!!!

AccessData FTK Imager

File View Mode Help

Evidence Tree

- Libraries
 - C:\Users\ibtery\AppData\Roaming\Microsoft\Windows\Libraries
- Recent
 - C:\Users\ibtery\AppData\Roaming\Microsoft\Windows\Recent
 - AutomaticDestinations
 - CustomDestinations

Custom Content Sources

Evidence:File System Path File	Options

File List

Name	Size	Type	Date Modified
1b4dd6f29cb1962.automaticDestinations-ms	23 KB	Regular File	5/26/2009
2177a2ffffe4fecda2b95ca27b6c33d9.automaticDestinations-ms	10 KB	Regular File	5/22/2009
28c8b86deab549a1.automaticDestinations-ms	3 KB	Regular File	5/13/2009
74d7f43c1561fc1e.automaticDestinations-ms	13 KB	Regular File	5/27/2009
7e4dca80246863e3.automaticDestinations-ms	19 KB	Regular File	5/26/2009
9b9cdc69c1c24e2b.automaticDestinations-ms	84 KB	Regular File	5/26/2009
a2b95ca27b6c33d9.automaticDestinations-ms	3 KB	Regular File	5/26/2009
adecfb853d77462a.automaticDestinations-ms	5 KB	Regular File	5/22/2009
bc03160ee1a59fc1.automaticDestinations-ms	6 KB	Regular File	5/21/2009
f5ac5390b9115fdb.automaticDestinations-ms	26 KB	Regular File	5/22/2009
f8f810d971d3f8bb.automaticDestinations-ms	4 KB	Regular File	5/18/2009

Hex View

3510	32 00 37 b2 7b 00 b4 3a-bd bb 20 00 41 44 56 53	2-7*{':%\$ -ADVS
3520	4f 43 7e 31 2e 50 50 54-00 00 6c 00 08 00 04 00	OC~1.PPT~1....
3530	ef be b4 3a bd bb b4 3a-bd bb 2a 00 00 00 9e 34	i%':%\$':%\$*....4
3540	01 00 00 00 10 00 00 00-00 00 00 00 00 00 00	
3550	00 00 00 00 41 00 64 00-76 00 20 00 53 00 6f 00	...A.d.v- .S-o-
3560	63 00 69 00 61 00 6c 00-20 00 4e 00 65 00 69 00	c-i-a-l- .N-e-t-
3570	77 00 6f 00 72 00 6b 00-69 00 6e 00 67 00 20 00	w-o-r-k-i-n-g- .
3580	32 00 30 00 20 00 2e 00-70 00 70 00 74 00 00 00	2-0-0-9-.ppt
3590	78 00 00 00 1c 00 32 00-00 00 1a 00 ef be 02 00	x....2....i%..
35a0	50 00 6f 00 77 00 65 00-72 00 50 00 6f 00 69 00	P-o-w-e-r-P-o-i-
35b0	6e 00 74 00 2e 00 53 00-68 00 6f 00 77 00 2e 00	n-t- .S-h-o-w- .
35c0	31 00 32 00 00 00 1c 00-00 00 67 00 00 00 1c 00	1-2-.....g....
35d0	00 00 01 00 00 00 1c 00-00 00 2d 00 00 00 00 00	
35e0	00 00 66 00 00 00 11 00-00 00 03 00 00 00 ce 07	..f.....i-
35f0	18 40 10 00 00 00 00 00-43-3a 5c 55 73 65 72 73 5c	@.....C:\Users\
3600	69 62 74 65 72 72 79 5c-44 65 73 6b 74 6f 70 5c	ibtery\Desktop\
3610	41 64 76 20 53 6f 63 69-61 6c 20 4e 65 74 77 6f	Adv Social Netwo
3620	72 6b 69 6e 67 20 30-30 39 2e 70 70 74 78 00	rking 2009.pptx-
3630	00 39 00 00 00 09 00 00-a0 2d 00 00 00 31 53 50	9-.....-...1SP

Reference to a PPT

Cursor pos = 0

Recent/C:\Users\ibtery\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\f5ac5390b9115fdb.automaticDestinations-ms

3560	63 00	69 00	61 00	6c 00	-2 00
3570	77 00	6f 00	72 00	6b 00	-69 00
3580	32 00	30 00	00 00	00 00	-2e 00
3590	78 00	00 00	1c 00	32 00	-00 00

Name	Size	Type	Date Modified
1b4dd67f29cb1962.automaticDestinations-ms	23 KB	Regular File	5/26/2009 1
2177a2ffffe4fecd.automaticDestinations-ms	10 KB	Regular File	5/22/2009 2
28c8b86deab549a1.automaticDestinations-ms	3 KB	Regular File	5/13/2009 2
74d7f43c1561fc1e.automaticDestinations-ms	13 KB	Regular File	5/27/2009 1
7e4dca80246863e3.automaticDestinations-ms	19 KB	Regular File	5/26/2009 6
9b9cdc69c1c24e2b.automaticDestinations-ms	84 KB	Regular File	5/26/2009 1
a2b95ca27b6c33d9.automaticDestinations-ms	3 KB	Regular File	5/26/2009 1
adecfb853d77462a.automaticDestinations-ms	5 KB	Regular File	5/22/2009 3
bc03160ee1a59fc1.automaticDestinations-ms	6 KB	Regular File	5/21/2009 1
f5ac5390b9115fdb.automaticDestinations-ms	26 KB	Regular File	5/22/2009 8
f8f810d971d3f8bb.automaticDestinations-ms	4 KB	Regular File	5/18/2009 9

3510	32 00 37 b2 7b 00 b4 3a-bd bb 20 00 41 44 56 53	2-7*{':;%} -ADVS
3520	4f 43 7e 31 2e 50 50 54-00 00 6c 00 08 00 04 00	OC~1.PPT~1.....
3530	ef be b4 3a bd bb b4 3a-bd bb 2a 00 00 00 9e 34	1%':;%}':;%}*....4
3540	01 00 00 00 10 10 00 00-00 00 00 00 00 00 00	
3550	00 00 00 00 00 41 00 64 00-76 00 20 00 53 00 6f 00	...A-d-v- S-o
3560	63 00 69 00 61 00 6c 00-20 00 4e 00 65 00 74 00	c-i-a-l- N-e-t-
3570	77 00 6f 00 72 00 6b 00-69 00 6e 00 67 00 20 00	w-o-r-k-i-n-g-
3580	32 00 30 00 00 00 00 00-2e 00 70 00 70 00 74 00	2-0-0-9-. p-p-t-
3590	78 00 00 00 00 1c 00 32 00-00 00 1a 00 ef be 02 00	x-...2-...i%..
35a0	50 00 6f 00 77 00 65 00-72 00 50 00 6f 00 69 00	P-o-w-e-r-P-o-i-
35b0	6e 00 74 00 2e 00 53 00-68 00 6f 00 77 00 2e 00	n-t-. S-h-o-w-.
35c0	31 00 32 00 00 00 1c 00-00 00 67 00 00 00 1c 00	1-2-.....g.....
35d0	00 00 01 00 00 00 1c 00-00 00 2d 00 00 00 00 00	
35e0	00 00 66 00 00 00 11 00-00 00 03 00 00 00 ce 07	..f.....î.
35f0	18 40 10 00 00 00 00 43-3a 5c 55 73 65 72 73 5c	@.....C:\Users\
3600	69 62 74 65 72 72 79 5c-44 65 73 6b 74 6f 70 5c	ibterry\Desktop\
3610	41 64 76 20 53 6f 63 69-61 6c 20 4e 65 74 77 6f	Adv Social Netwo
3620	72 6b 69 6e 67 20 32 30-30 39 2e 70 70 74 78 00	rking 2009.pptx-
3630	00 39 00 00 00 00 09 00-00 a0 2d 00 00 00 31 53 50	-9-.....1SP

Cursor pos = 0

Recent/C:\Users\ibterry\AppData\Roaming\Microsoft\Windows\Recent/AutomaticDestinations/f5ac5390b9115fdb.automaticDestinations-ms

New File System Features – Jump Lists












- Automatic Jump lists collect and store usage data on what items are used (i.e. the # of times a particular item is opened)
 - Algorithms generate a recent and/or frequent list of items from this data.
 - Usage data comes both indirectly and directly from the application.
 - >Example, if the app uses the common file open dialog, we get the usage indirectly. But if the app uses their own UI to open a file, they would need to tell us about that file directly through an API.






New File System Features – Jump Lists

- Custom Jump List applications can provide their own list of items to show in the menu, along with custom-named categories. They can also choose to display tasks. However, when using the custom list, the app is responsible for keeping track of usage and any algorithms that determine what to show in the list and in what order.

New File System Features – Jump Lists

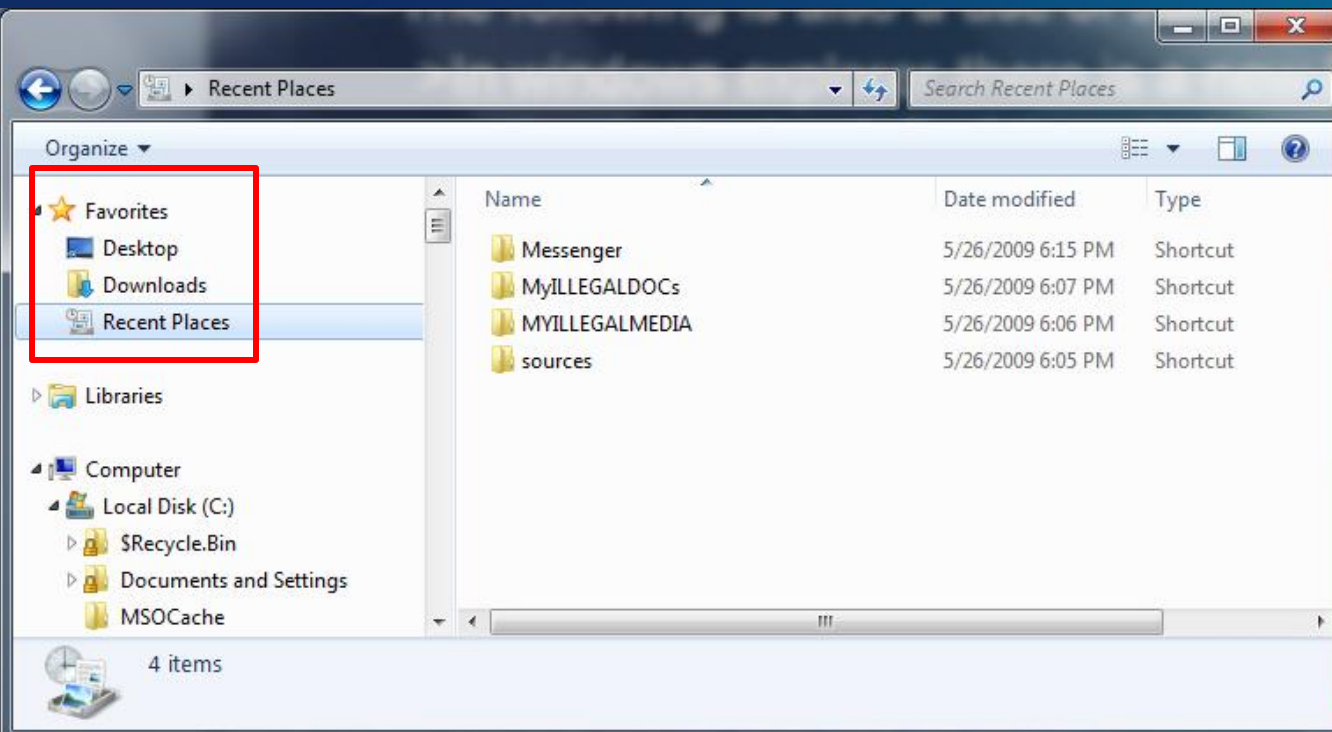
- Files are application specific – each file is for a particular application. Some applications may have both a custom and an automatic file; this would happen if the app customizes their list, but we also collect automatic usage data for that app's files (e.g. through Explorer or the common file open dialog).

File List				
Name				
 1b4dd67f29cb1962.automaticDestinations-ms				
 2177a2ffffe4fecdc.automaticDestinations-ms				
 28c8b86deab549a1.automaticDestinations-ms				
 74d7f43c1561fc1e.automaticDestinations-ms				
 7e4dca80246863e3.automaticDestinations-ms				
 9b9cdc69c1c24e2b.automaticDestinations-ms				
 a2b95ca27b6c33d9.automaticDestinations-ms				
 adefcb853d77462a.automaticDestinations-ms				
 bc03160ee1a59fc1.automaticDestinations-ms				
 f5ac5390b9115fdb.automaticDestinations-ms				
 f8f810d971d3f8bb.automaticDestinations-ms				

File List				
Name	Size	Type	Date Modified	
 2177a2ffffe4fecdc.customDestinations-ms	4 KB	Regular File	5/22/2009 2:39:19 PM	
 28c8b86deab549a1.customDestinations-ms	5 KB	Regular File	5/27/2009 2:23:57 PM	
 5afe4de1b92fc382.customDestinations-ms	19 KB	Regular File	5/12/2009 7:32:20 PM	
 74d7f43c1561fc1e.customDestinations-ms	4 KB	Regular File	5/27/2009 2:00:55 PM	
 b06a975b62567622.customDestinations-ms	11 KB	Regular File	5/26/2009 6:51:33 PM	

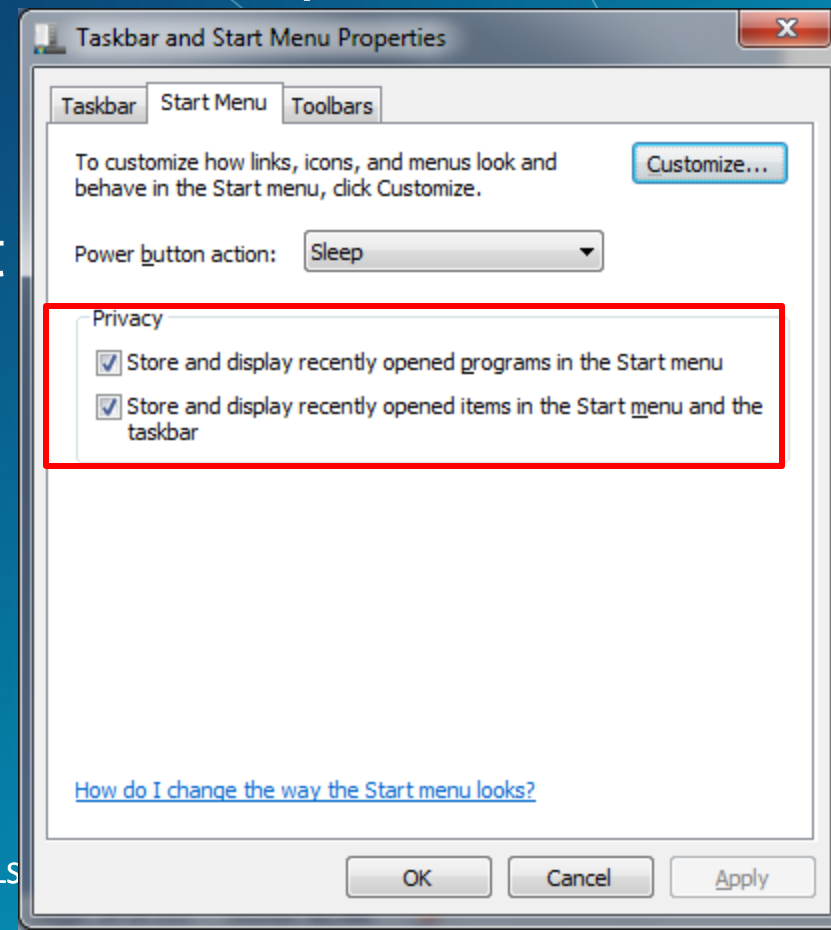
New File System Features – Jump Lists

- The following is also a use of Jump Lists
 - > In windows explorer there is a new Favorites option in the top left of the window.



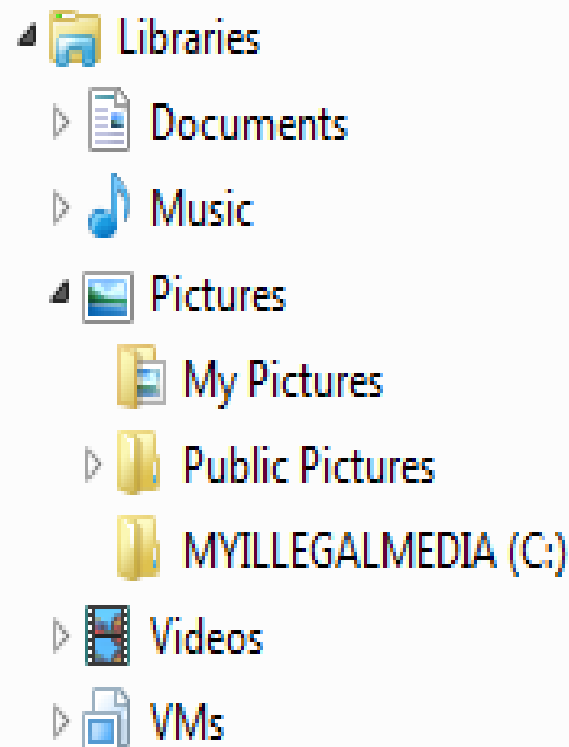
New File System Features – Jump Lists

- The following setting can affect not only the start menu, but various apps that use Jump Lists
- Unselecting this option will prevent application history from appearing on the start menu and clear some application history.



New File System Features - Libraries

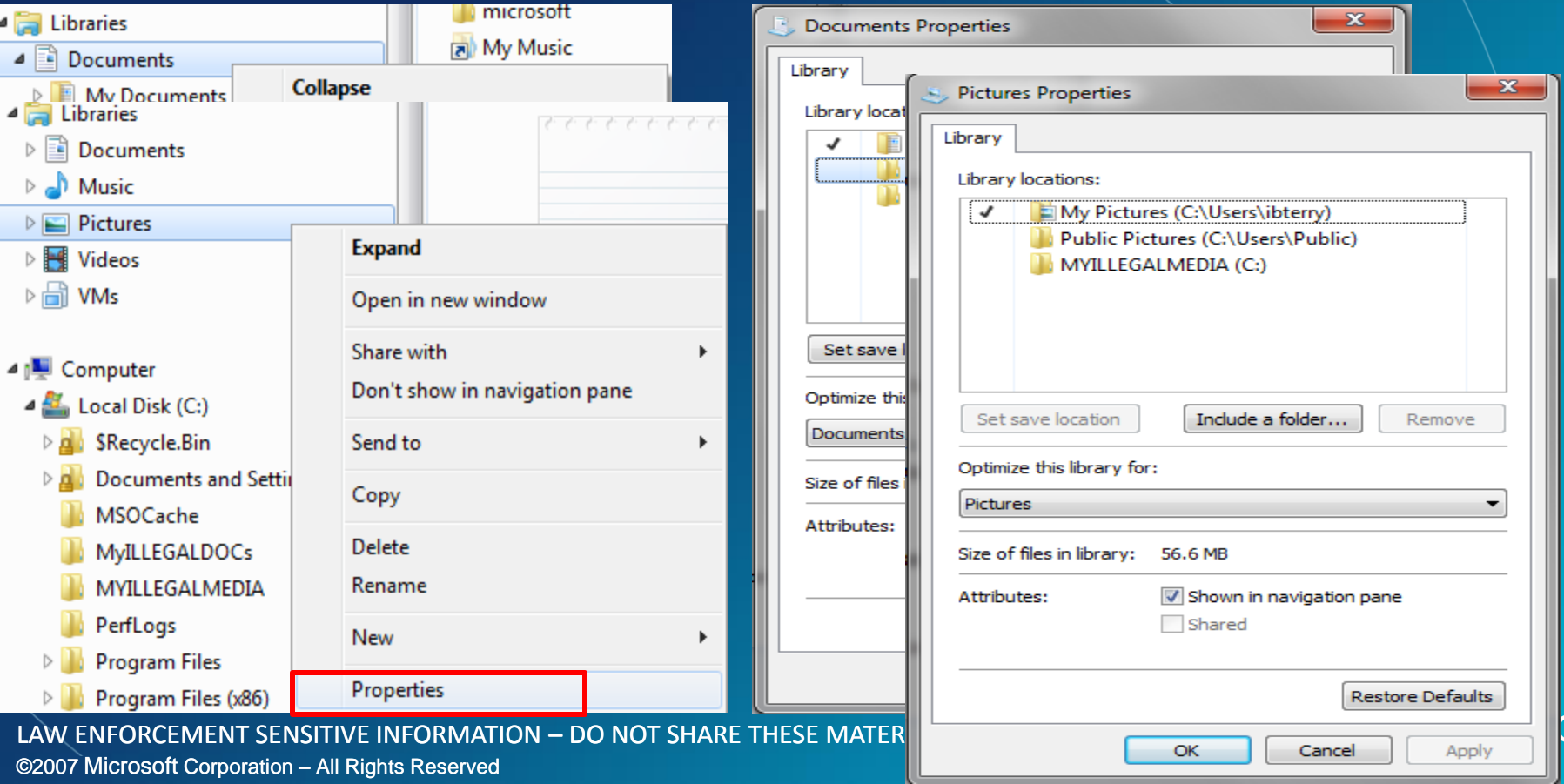
- Libraries – added to assist users with finding and organizing their media. User defined collections of content.



- Default locations
 - Documents
 - Pictures
 - Videos
 - Music
- Custom locations can be added

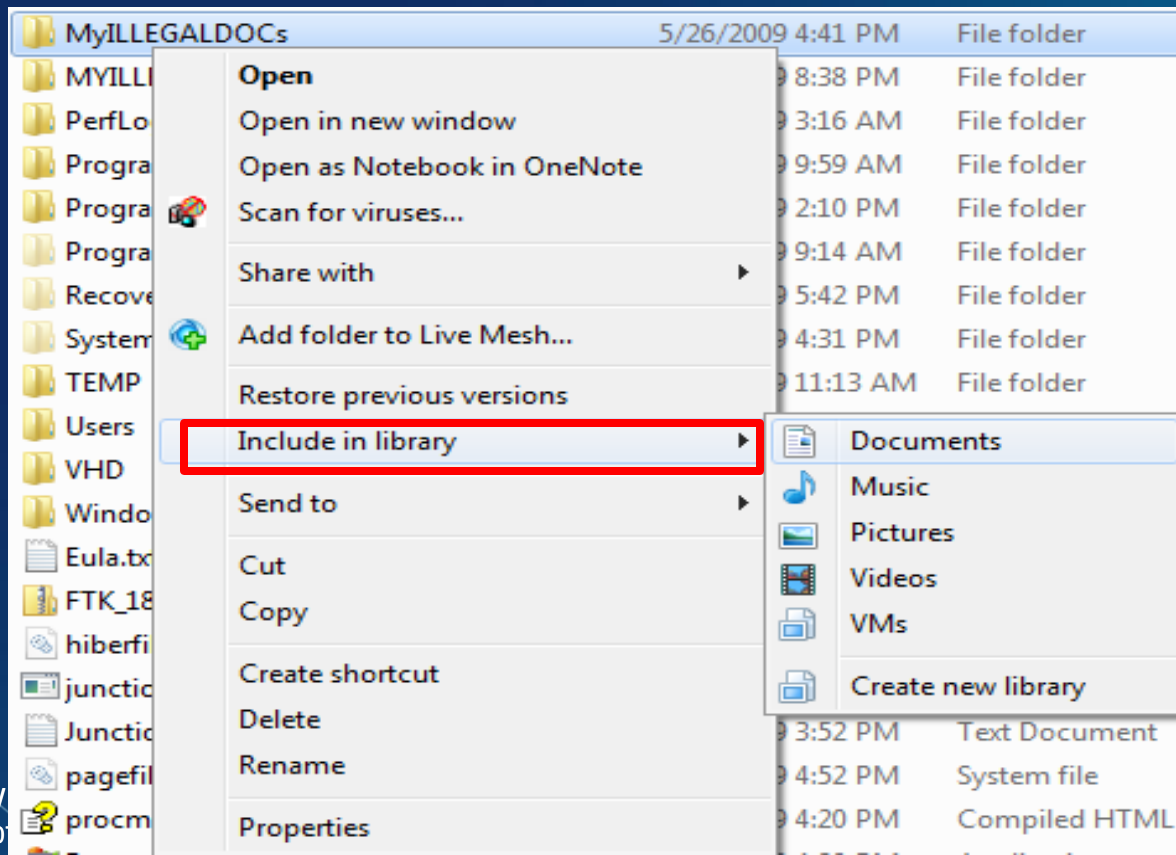
New File System Features - Libraries

- New folders can be added via right clicking on the desired library and choosing properties.



New File System Features - Libraries

- Folders can also be linked to a Library by right clicking on the desired folder and choosing the Include in Library option



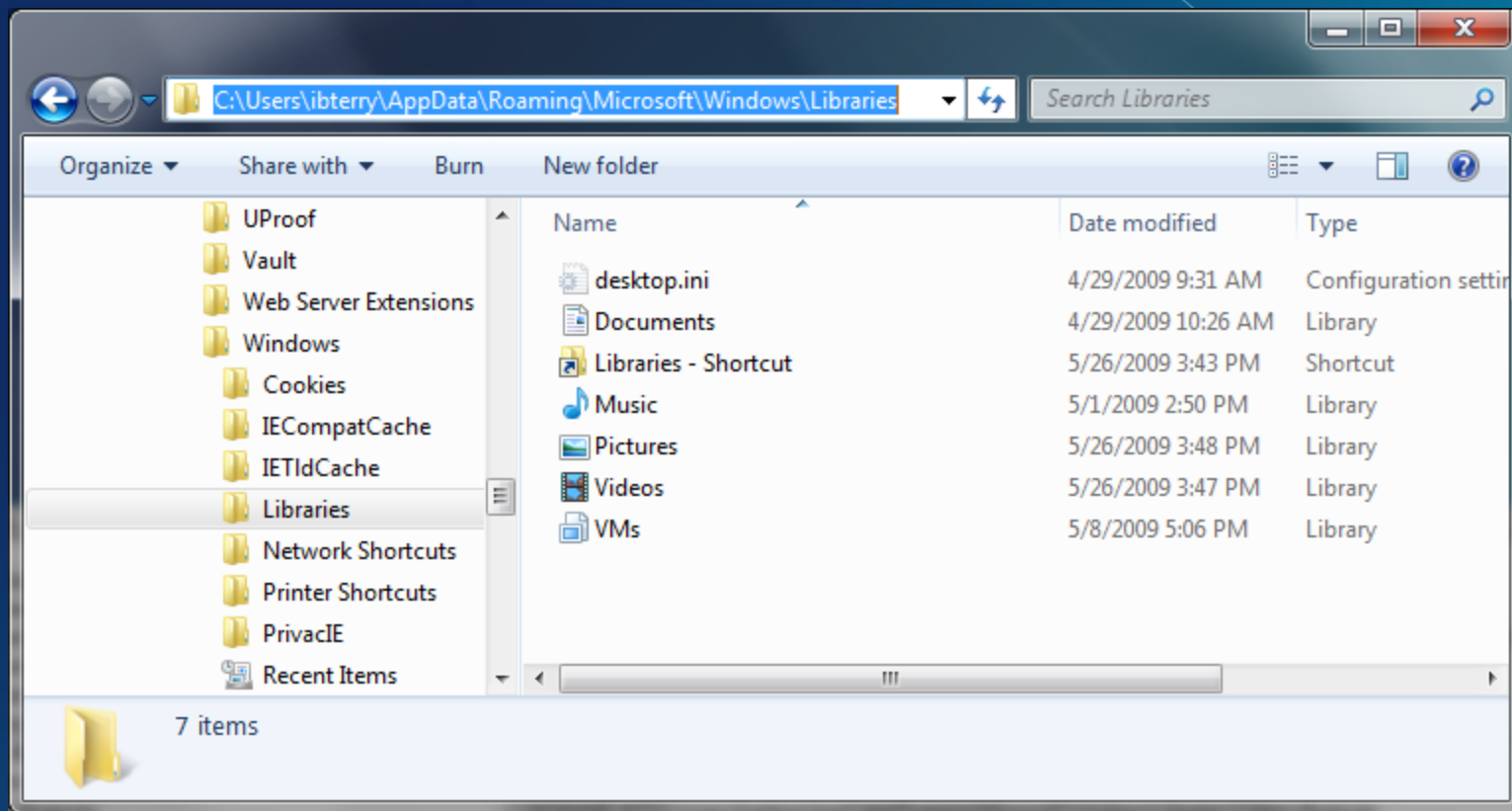
New File System Features - Libraries

- So... What is a Library... Exactly?
 - It is not a folder
 - It is not a symbolic link
 - Libraries don't actually store files

The library is a list of Monitored folders that are defined in configuration files located in
C:\Users\<usersprofile>\AppData\Roaming\
Microsoft\Windows\Libraries

New File System Features - Libraries

- In Windows Explorer... It looks like any other windows folder.



New File System Features - Libraries

- When viewed via FTK... we see that the Library files are XML based files named with the library-ms extension.

File Name	Full Path
<input type="checkbox"/> ? \$!30	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\!\$!30
<input type="checkbox"/> ? desktop.ini	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini
<input type="checkbox"/> Documents.library-ms	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms
<input type="checkbox"/> FileSlack	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Documents.library-ms>>FileSlack
<input type="checkbox"/> FileSlack	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms>>FileSlack
<input type="checkbox"/> FileSlack	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms>>FileSlack
<input type="checkbox"/> FileSlack	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms>>FileSlack
<input type="checkbox"/> Music.library-ms	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Music.library-ms
<input type="checkbox"/> Pictures.library-ms	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Pictures.library-ms
<input type="checkbox"/> Videos.library-ms	J:\NNAME-NTFS\Users\badguy\AppData\Roaming\Microsoft\Windows\Libraries\Videos.library-ms

New File System Features - Libraries

- It is possible to view the file via Notepad once they have been exported by a tool like FTK Imager



Pictures.library-ms.copy0 - Notepad

```
File Edit Format View Help
<?xml version="1.0" encoding="UTF-8"?>
<libraryDescription xmlns="http://schemas.microsoft.com/windows/2009/library">
  <name>@shell32.dll,-34595</name>
  <ownerSID>S-1-5-21-124525095
  <version>7</version>
  <isLibraryPinned>true</isLib
  <iconReference>imageres.dll,
  <templateInfo>
    <folderType>{b3690e58-e961
  </templateInfo>
  <propertyStore>
    <property name="HasModifie
  </propertyStore>
  <searchConnectorDescriptionL
  <searchConnectorDescriptio
    <description>@shell32.dl
    <isDefaultSaveLocation>t
    <isSupported>true</isSup
    <simpleLocation>
      <url>knownFolder:{33E2
      <serialized>MBAAAEAFCA
    </simpleLocation>
  </searchConnectorDescripti
  <searchConnectorDescription publisher="Microsoft" product="windows">
    <description>@shell32.dll,-34599</description>
    <isDefaultNonOwnerSaveLocation>true</isDefaultNonOwnerSaveLocation>
    <isSupported>true</isSupported>
    <simpleLocation>
      <url>knownFolder:{B6EBFB86-6907-413C-AF7-4FC2ABF07CC5}</url>
      <serialized>MBAAAEAFCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAkZAUAWHQB+TQDi66kGEiINcAS
      AAWAAAAAYBAAAAAAAAAZmXxcq1wy3lmb30ccjBAAM1Y5NQF1JkqkLg4cNSD3QLTITTV04de7qLAcYy1PDvZZoweDURZCpk5CIXD7wt6yEy0UFNeHxu6CAHmc9zWDAAAAA</serialized>
    </simpleLocation>
  </searchConnectorDescription>
  <searchConnectorDescription>
    <isSupported>true</isSupported>
    <simpleLocation>
      <url>C:\MYILLEGALMEDIA</url>
    </simpleLocation>
  </searchConnectorDescription>
</searchConnectorDescriptionList>
</libraryDescription>
```



Internet Explorer 8

Features in IE8 for
Windows 7



Tabbed Browsing

- Tabbed Browsing: In a single instance of Internet Explorer a user can have multiple pages opened in tabs



- Each tab represents a new page...but a separate process. This is new to Windows 7

Tabbed Browsing - Processes

The image displays two side-by-side screenshots of the Windows Task Manager application, illustrating the process list and system resource usage. Both screenshots show the 'Processes' tab selected, with a list of running processes and their associated user, CPU usage, and memory consumption.

Left Screenshot (Windows Task Manager):

Image Name	User Name	CPU	Memory (K)	Description
POWERPNT.EXE *32	iberry	00	31,700 K	Micro
explore.exe *32	iberry	00	27,820 K	Inter
OUTLOOK.EXE *32	iberry	01	25,264 K	Micro
explorer.exe	iberry	00	24,624 K	Wind
Moe.exe *32	iberry	00	23,068 K	Mesh
dwm.exe	iberry	00	22,320 K	Desk
GROOVE.EXE *32	iberry	00	16,564 K	Micro
msnmsgr.exe *32	iberry	00	10,292 K	Wind
MoeMonitor.exe	iberry	00	8,696 K	MOE
ieexplore.exe *32	iberry	00	7,512 K	Inter
ipoint.exe	iberry	00	7,108 K	IPoin
Realmon.exe	iberry	00	3,516 K	Real
taskmgr.exe	iberry	01	2,352 K	Wind
rundll32.exe		00	2,132 K	

Processes: 74 CPU Usage: 14% Physical Memory: 37%

Right Screenshot (Windows Task Manager):






Image Name	User Name	CPU	Memory (K)	Description
csrss.exe		00	1,744 K	
dwm.exe	iberry	00	23,644 K	Desk
explorer.exe	iberry	00	24,580 K	Wind
FlashUtil10b.exe *32	iberry	00	1,196 K	Adob
GROOVE.EXE *32	iberry	00	6,500 K	Micro
explore.exe *32	iberry	00	24,900 K	Inter
ieexplore.exe *32	iberry	00	38,068 K	Inter
ieexplore.exe *32	iberry	00	23,768 K	Inter
ieexplore.exe *32	iberry	00	7,872 K	Inter
ipoint.exe	iberry	00	7,108 K	IPoin
Moe.exe *32	iberry	00	23,032 K	Mesh
MoeMonitor.exe	iberry	00	8,696 K	MOE
msnmsgr.exe *32	iberry	00	10,256 K	Wind
ONENOTEM.EXE *32	iberry	00	1,124 K	Micro

Processes: 75 CPU Usage: 1% Physical Memory: 40%

Instant Search

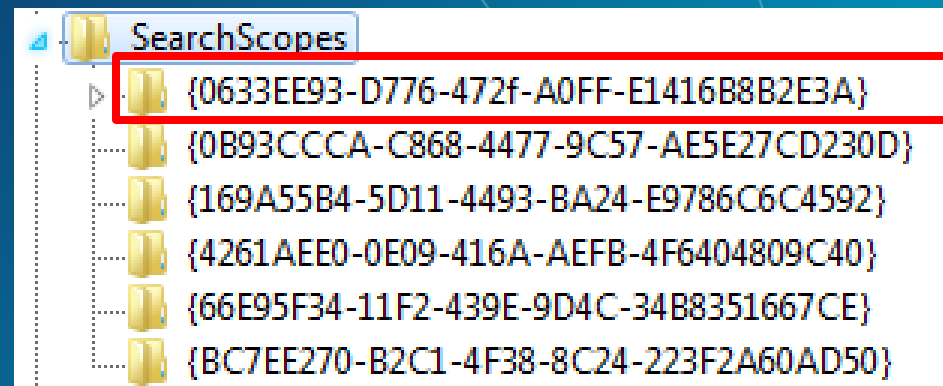
- You can view the currently selected default search provider for Internet Explorer in the following location

HKU\<USER GUID>\Software\Microsoft\Internet Explorer\SearchScopes
-DefaultScope Identified the scope by a GUID

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 DefaultScope	REG_SZ	{0633EE93-D776-472f-A0FF-E1416B8B2E3A}
 DownloadUpdates	REG_DWORD	0x00000001 (1)
 UpgradeTime	REG_BINARY	7d 93 32 30 d3 c8 c9 01
 Version	REG_DWORD	0x00000002 (2)

Instant Search

- You can view all of the available search providers in the keys below the SearchScopes key...
- Within each GUID subkey there are items of interest
 - DisplayName
 - URL



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	Live Search
FaviconPath	REG_SZ	C:\Users\iberry\AppData\LocalLow\Microsoft\Internet Explorer\Services\search_{0633EE93-D776-...
FaviconURL	REG_SZ	http://search.live.com/favicon.ico
FaviconURLFallback	REG_SZ	http://www.live.com/favicon.ico
OSDFileURL	REG_SZ	http://www.ieaddons.com/en/DownloadHandler.ashx?ResourceId=790
ShowSearchSuggestions	REG_DWORD	0x00000001 (1)
SuggestionsURL	REG_SZ	http://api.search.live.com/qsml.aspx?query={searchTerms}&MARKET={Language}&FORM=IE8SSC
SuggestionsURLFallback	REG_SZ	http://api.search.live.com/qsml.aspx?query={searchTerms}&src=IE-SearchBox&maxwidth={ie:max...
URL	REG_SZ	http://search.live.com/results.aspx?q={searchTerms}&Form=IE8SRC&src={referrer:source}

Instant Search

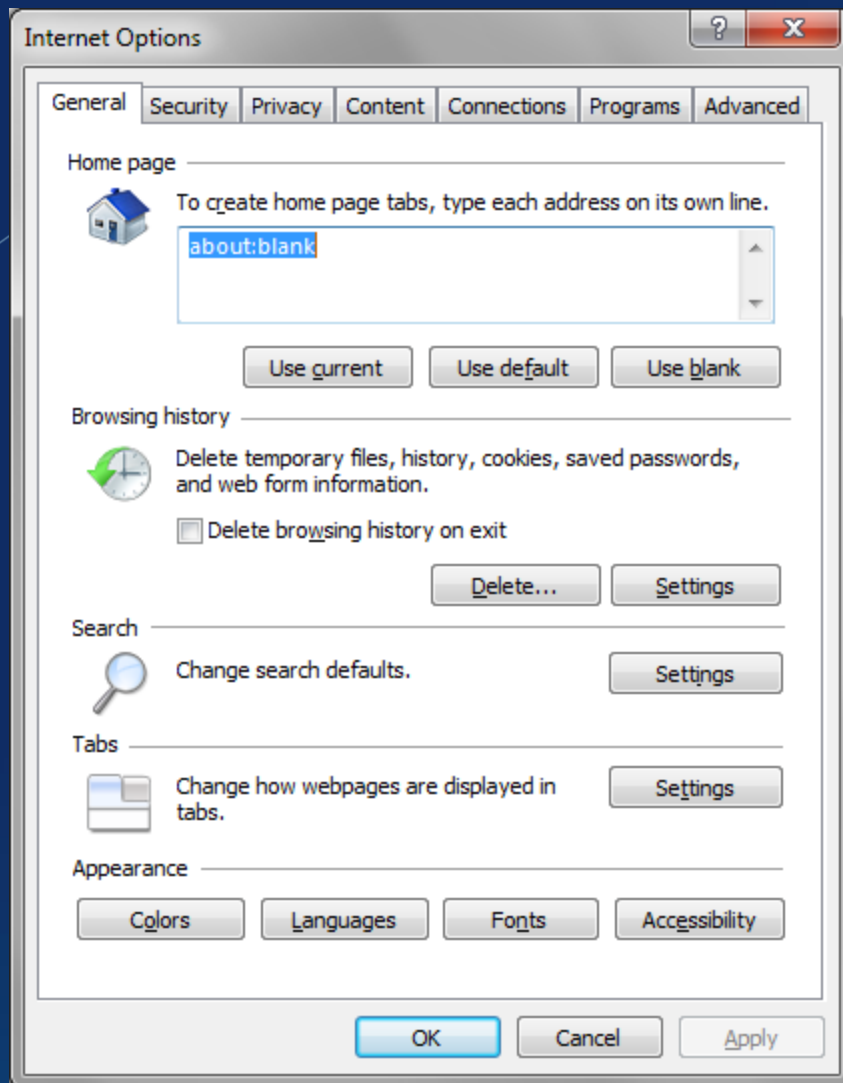
- Instant Search is not a function of the integrated search capabilities in Windows.
- Settings for what has been searched using Instant Search is not recorded in the registry....the only data available would be in the Index.dat file for the user

C:\users\<username>\AppData\Local\Microsoft\Windows\Temporary Internet Files\low\content.IE5\index.dat

“Cover Your Tracks”

- Internet Explorer 8 has a feature that will protect users data more when they choose to delete browsing history
- Traditionally the index.dat file was somewhat recoverable forensically even after the “Delete History” operation
- In addition, the clearing of personal data experience has been enhanced

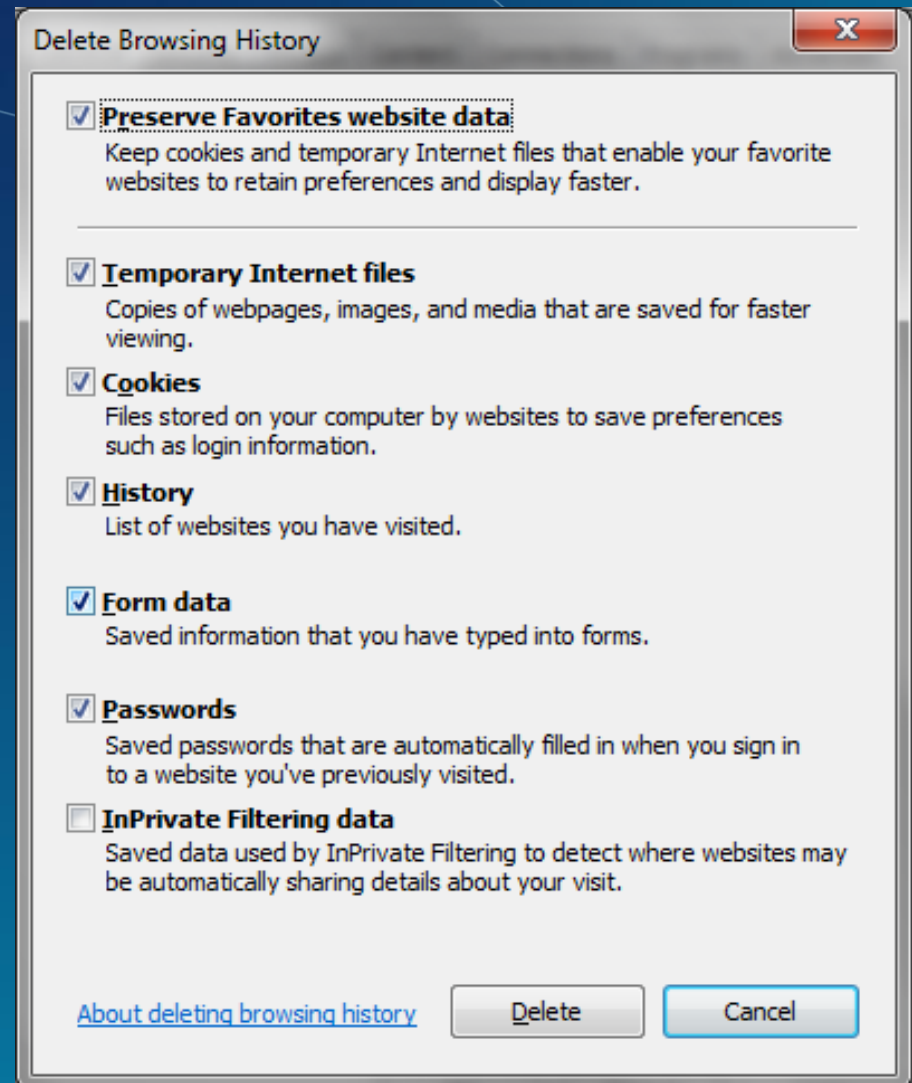
“Cover Your Tracks”



- The “Internet Option” interface looks pretty much the same
- We have the “Delete...” button in the middle of the frame

“Cover Your Tracks”

- We can choose what items are to be deleted.



“Cover Your Tracks”

- What does “Delete” really delete?
 - Temporary Internet Files
 - Cookies
 - History of the Websites Visited (index.dat)
 - Saved Passwords
 - Temporary Information Stored by Browser Add-ons

“Cover Your Tracks”

- Index.dat is not really deleted....it is overwritten with zeros to erase data.
- The initial size of the index.dat file on a newly installed system is around 32KB
- When the “Delete All” operation occurs, the file is zeroed out meaning that the file will never get smaller.

“Cover Your Tracks”

- The header of the file seems to be the same every time
- Below is an example of a new index.dat file viewed through FTK

43 6c 69 65 6e 74 20 55-72 6c 43 61 63 68 65 20	Client UrlCache
4d 4d 46 20 56 65 72 20-35 2e 32 00 00 80 00 00	MMF Ver 5.2.....
00 00 00 00 80 00 00 00-20 00 00 00 00 00 00
00 00 20 03 00 00 00 00-00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-04 00 00 00 00 00 00
44 36 42 42 5a 4e 52 57-00 00 00 00 4e 37 4b 5a	D6BBZNRW...N7KZ
50 4f 32 50 00 00 00 00-4f 31 4e 49 54 55 33 44	P02P...01NITU3D
00 00 00 00 4e 56 4a 44-4e 54 49 46 00 00 00 00	...NVJDNTIF....
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00	

“Cover Your Tracks”

- Browse any 4 websites to populate data in the users index.dat file... The file size will change at this point.

“Cover Your Tracks”

URL	http://www.torproject.org/
Filename	R8WBZQYO\torproject_org[1].htm
User name	badguy
Content info	HTTP/1.1 200 OK Content-Location: index.html.en Vary: negotiate,accept-language TCN: choice ETag: "11825b-2597-46ae349602200" Content-Length: 9623 Keep-Alive: timeout=15, max=100 Content-Type: text/html Content-Language: en
Last Accessed (UTC)	5/28/2009 3:33:17 AM
Last Modified (UTC)	5/27/2009 11:38:48 AM
Last Checked (UTC)	5/28/2009 3:33:18 AM
Expires (UTC)	Not specified
Hits	1
Use Count	0

Data in Index.dat
can be verified
with various
forensic tools.

“Cover Your Tracks”

- When a user evokes the “Delete Browsing History” function, IE8 overwrites the data in the index.dat file
- The file size remains the same....but now everything after the header data is zeroed out.

33ED0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33EEC	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33F08	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33F24	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
33F40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

“Cover Your Tracks”

- All of the supporting cache locations identified in the header information in index.dat have been cleaned out as well.
- This amounts to a more secure cleanup of Internet browsing history on the system

“Cover Your Tracks”



Preserve Favorites website data

Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

- This type of cleanup process has been in place since IE7 in Windows Vista.
- There is one area that may be a bit better for forensic examinations.
 - “Preserve Favorites website data” is a default setting in IE 8.
 - In my testing sites that were in the favorites did not have their data removed from Index.dat. It also appears that some of the supporting data related to ad tracking etc may stay as well

“Cover Your Tracks Part2”

- IE8 has a continued focus on security and privacy
- Most notable feature is the InPrivate browsing mode

When InPrivate Browsing is turned on, you will see this indicator



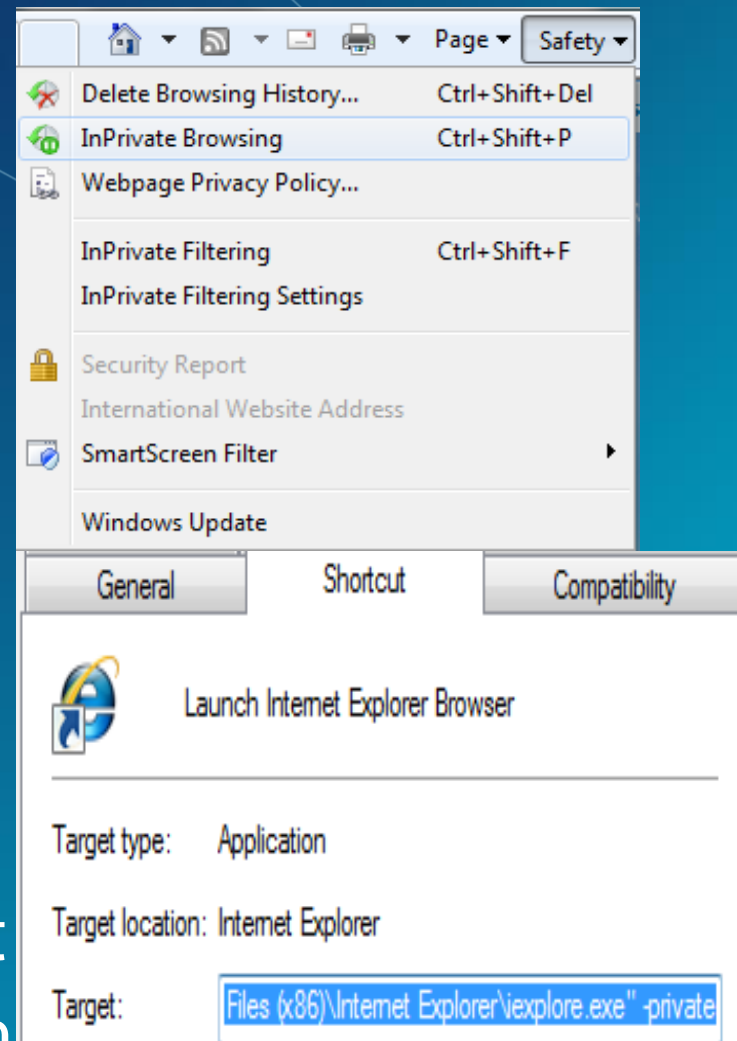
InPrivate Browsing prevents Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data.

“Cover Your Tracks Part2” - InPrivate

- Why is there an InPrivate mode?
 - Product Group Scenarios
 - Checking e-mail at an Internet café
 - Shopping for a gift on a family PC
- **InPrivate Browsing:** lets you control whether or not IE saves browsing history, cookies, and other data
- **InPrivate Filtering:** informs you about content that is in a position to observe your browsing history, and allows you to block it
- **InPrivate Subscriptions:** subscribe to lists of websites that are auto blocked or allowed.

“Cover Your Tracks Part 2” InPrivate Browsing

- InPrivate Browsing can be activated in the following ways
 - Navigating to the new Safety dropdown box and choosing InPrivate Browsing.
 - Using Ctrl+Shift+P as a hotkey
 - Modifying your IE shortcut to use the –private switch



“Cover Your Tracks Part2” – InPrivate Browsing

–How does InPrivate Browsing potentially affect your investigations?

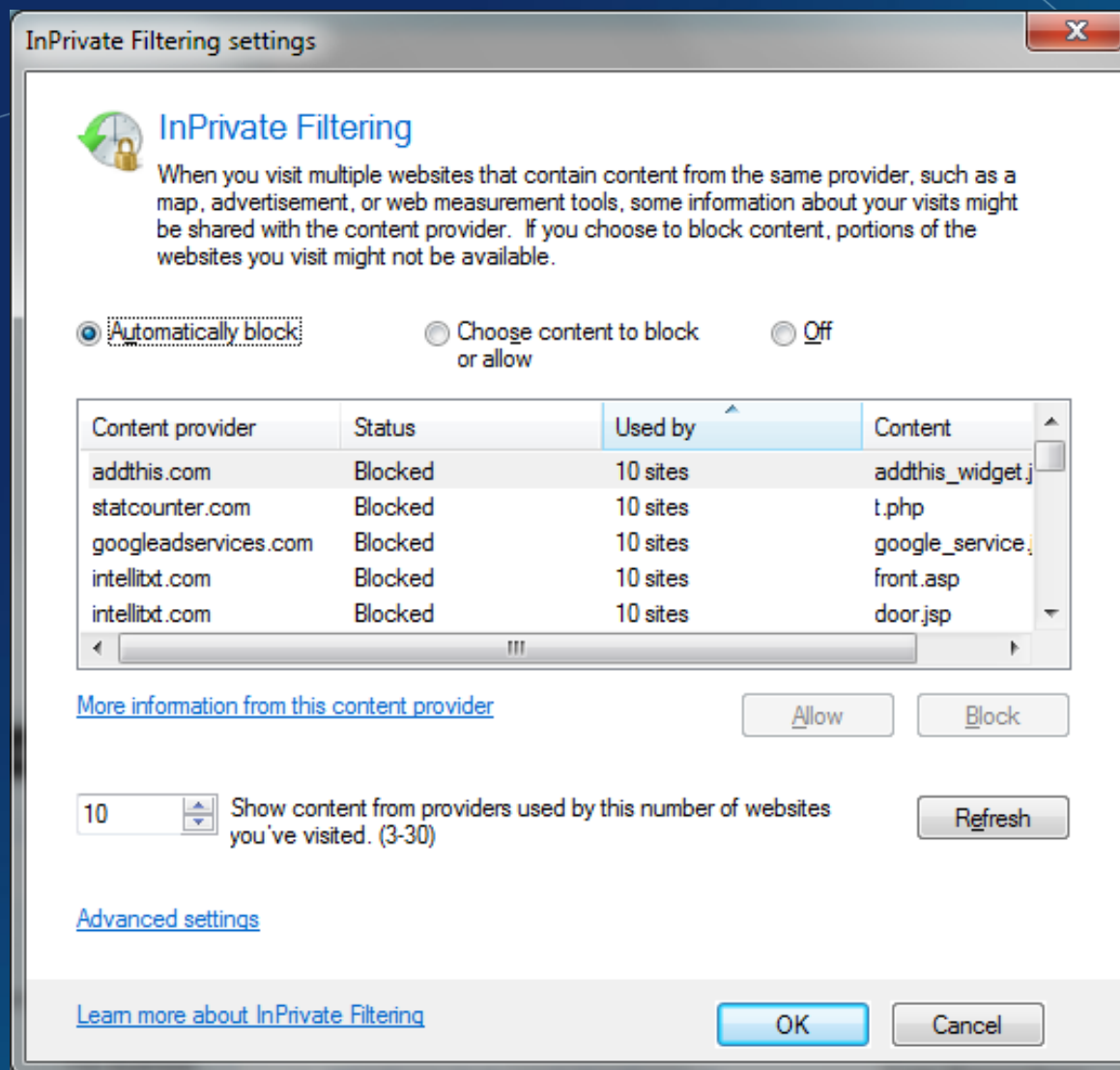
- New cookies are not stored
- New history entries will not be recorded
- New temporary Internet files will be deleted after the Private Browsing window is closed
- Form data, Passwords, and Typed Addresses will not be stored
- Visited links will not be stored
- Queries entered into the search box are not stored

“Cover Your Tracks Part2” - InPrivate Filtering

–What is InPrivate Filtering?

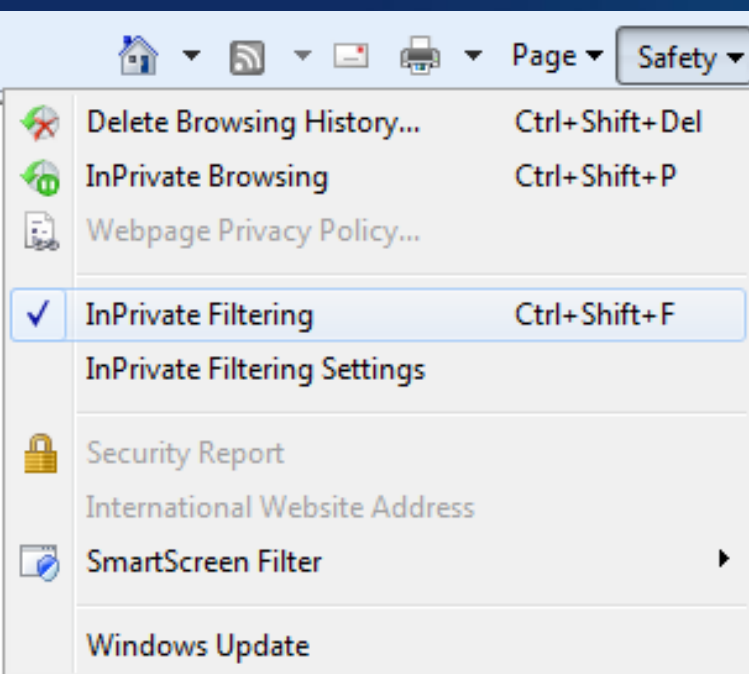
- InPrivate Filtering helps protect privacy by offering the user the ability to block content coming from third parties that are in a position to track and aggregate their online behavior.
- Internet Explorer will only record data for InPrivate Filtering when you are in “regular” browsing mode, as no browsing history is retained while browsing InPrivate.

“Cover Your Tracks Part2” - InPrivate Filtering



“Cover Your Tracks Part2” - InPrivate Filtering

- InPrivate Filtering is not enabled by default and once enabled is only on for one browsing session.



[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Safety\Privacy]

"StartMode"=dword:00000001

0 - off

1 - auto

2 - manual


This setting enables InPrivate Filtering for all IE Sessions

IE 8 - InPrivate Subscriptions

–What are InPrivate Subscriptions?

- InPrivate Filtering subscriptions are periodically updated lists of websites that are known to share private information. When you subscribe to a list, Internet Explorer checks automatically for updates.

Add-on Types

 Toolbars and Extensions

 Search Providers

 Accelerators

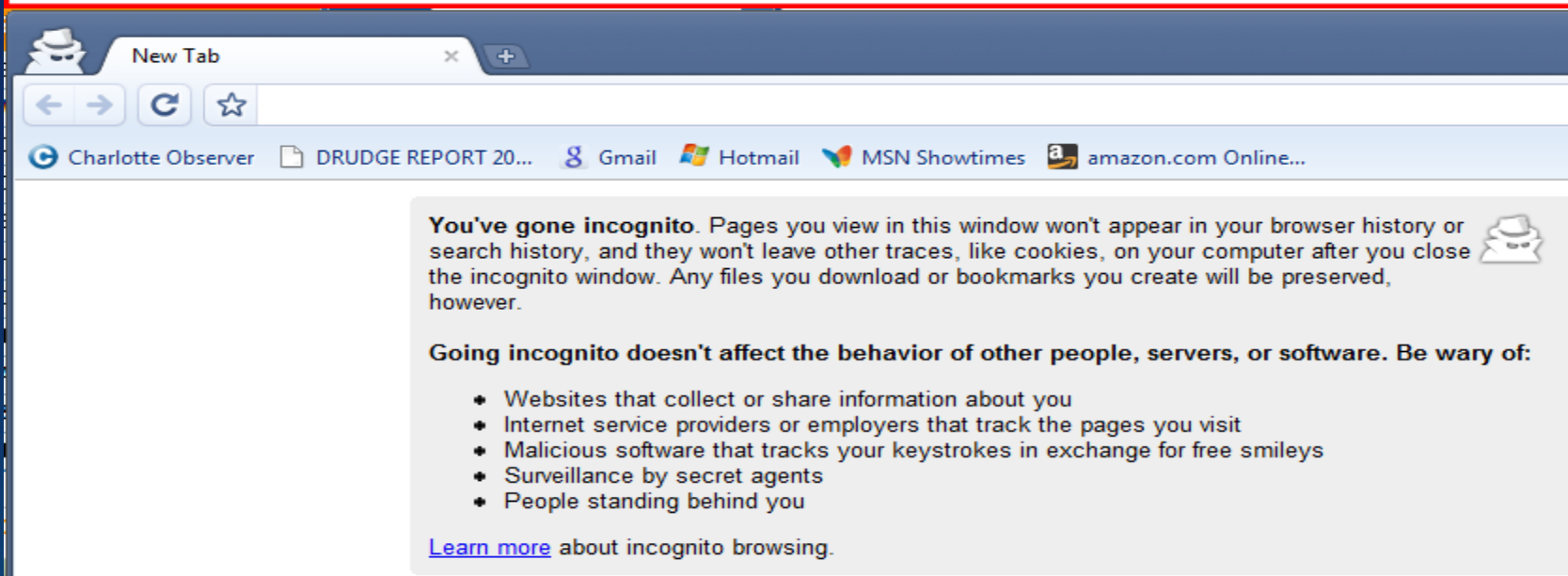
 InPrivate Filtering

“Cover Your Tracks Part2” – InPrivate Summary

- Don't shoot the messenger!!! Please. Microsoft is not the only one doing this...

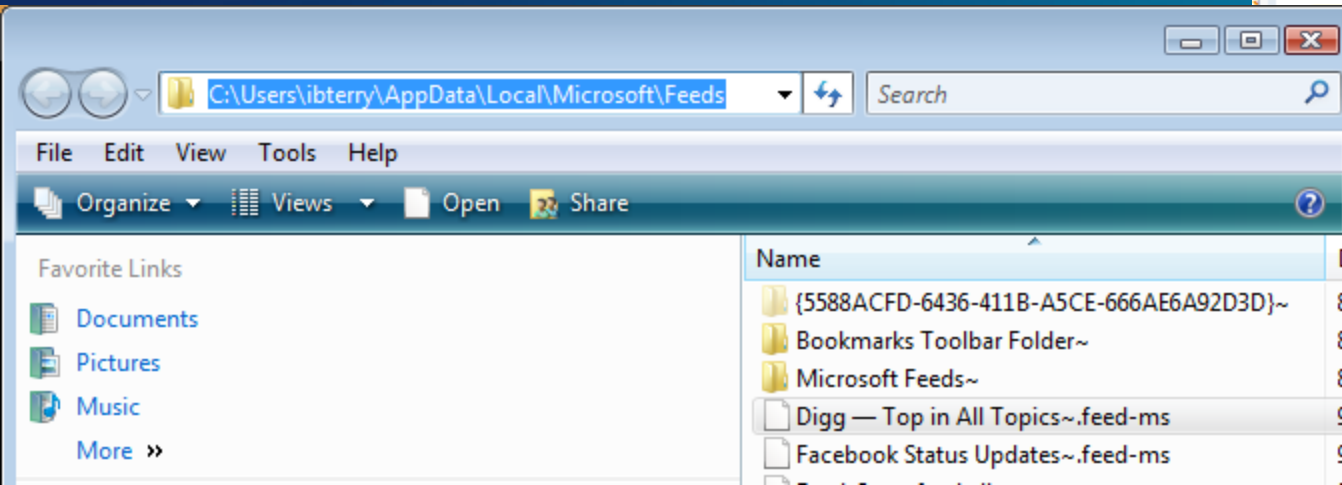
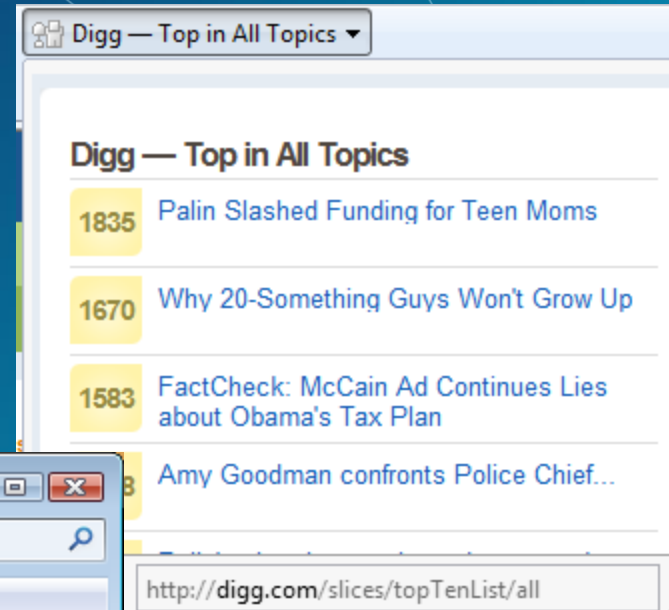
Firefox 3 Beta 2 Update Highlights Private Browsing Mode

The update also features enhancements to the Clear Private Data tool, which helps make it easier to remove data related to online activities.



IE8 – Web Slices

- A Web Slice is a specific portion of a webpage that you can subscribe to, and which enables you to see when content is updated.
- The service is very similar to RSS Feeds functionality.





Windows 7 Virtualization Technologies

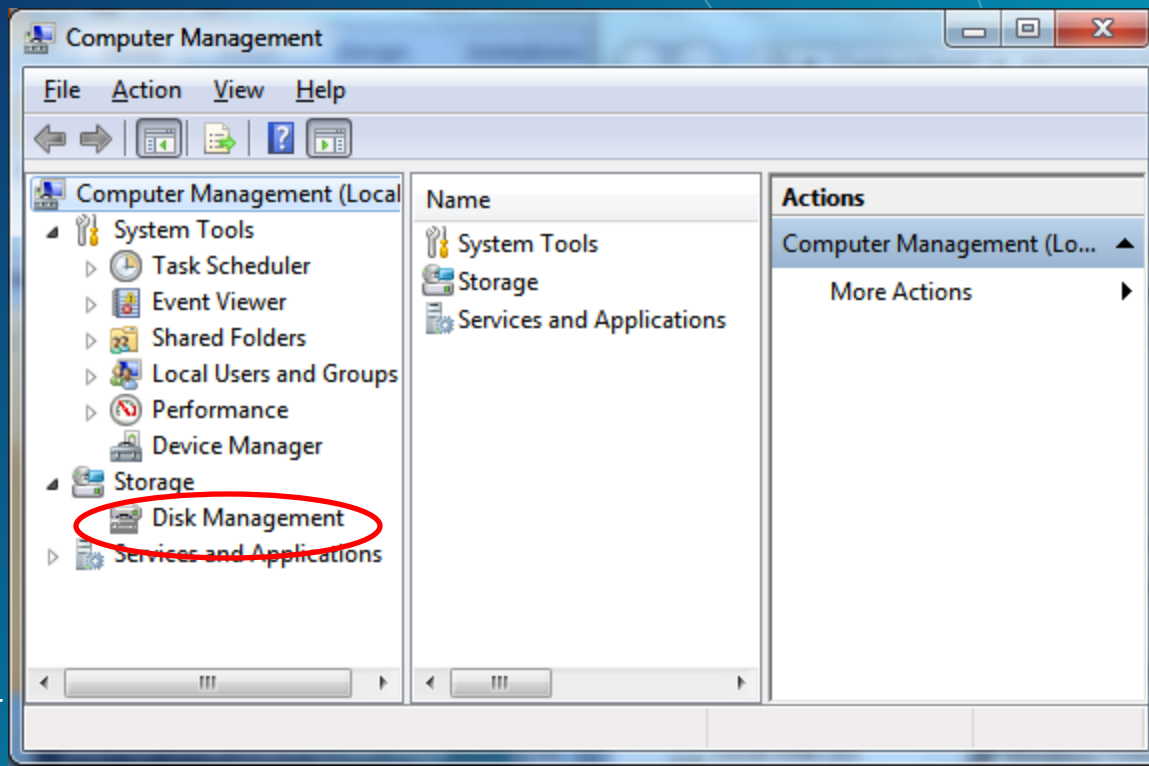


Virtualization Technologies

- Integrated Virtual Hard Drive (VHD) Creation and Mounting
- Boot to Virtual Hard Drive (VHD)
- VHD File Use in System Image Backup
- Virtual PC 7 Technologies
 - Windows XP Compatibility Mode
 - Undo Disks

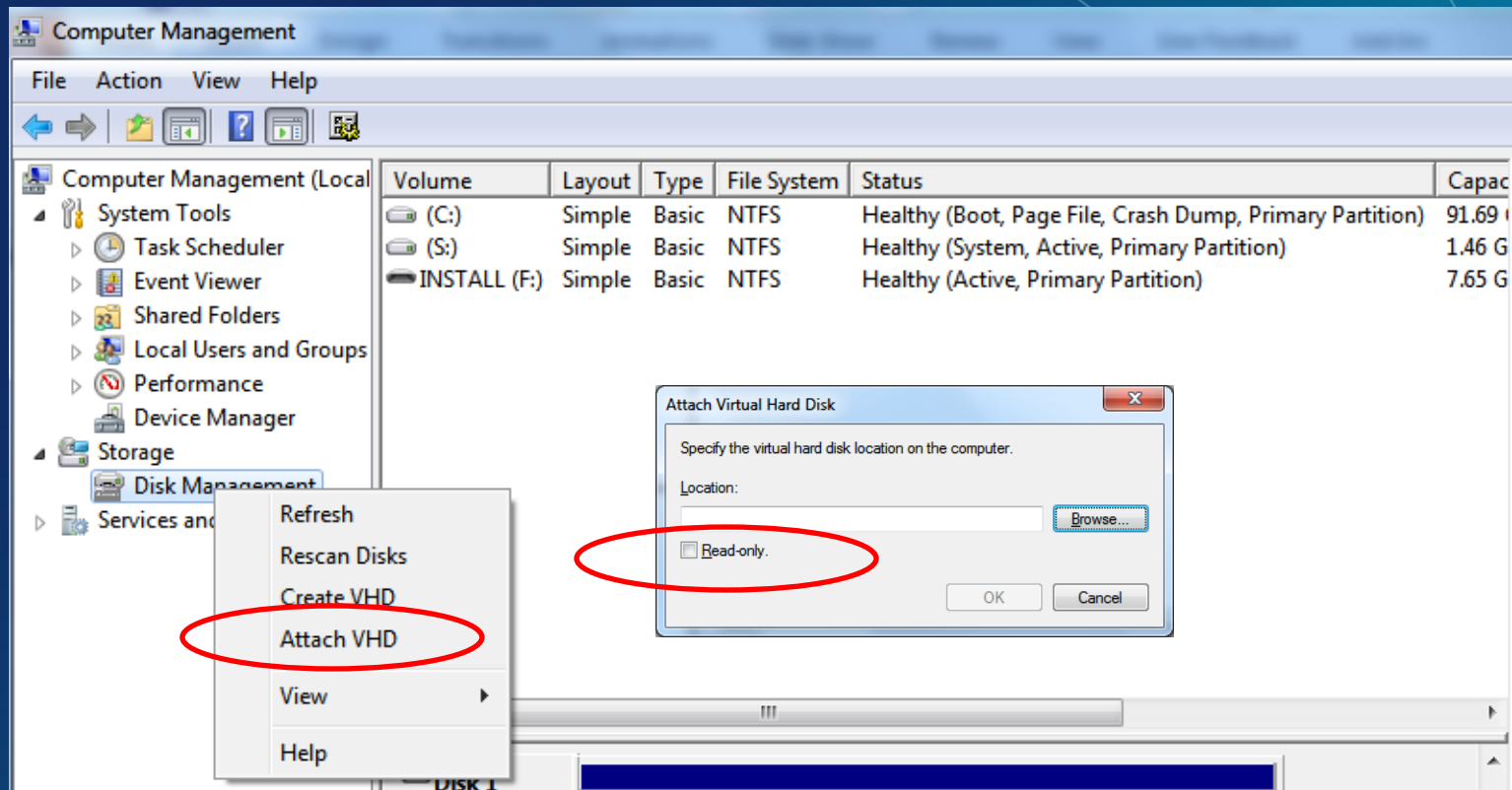
Integrated VHD Creation and Mounting

- Native in file system
- Accessed through Control Panel\AdministrativeTools\Computer Management



Integrated VHD Creation and Mounting

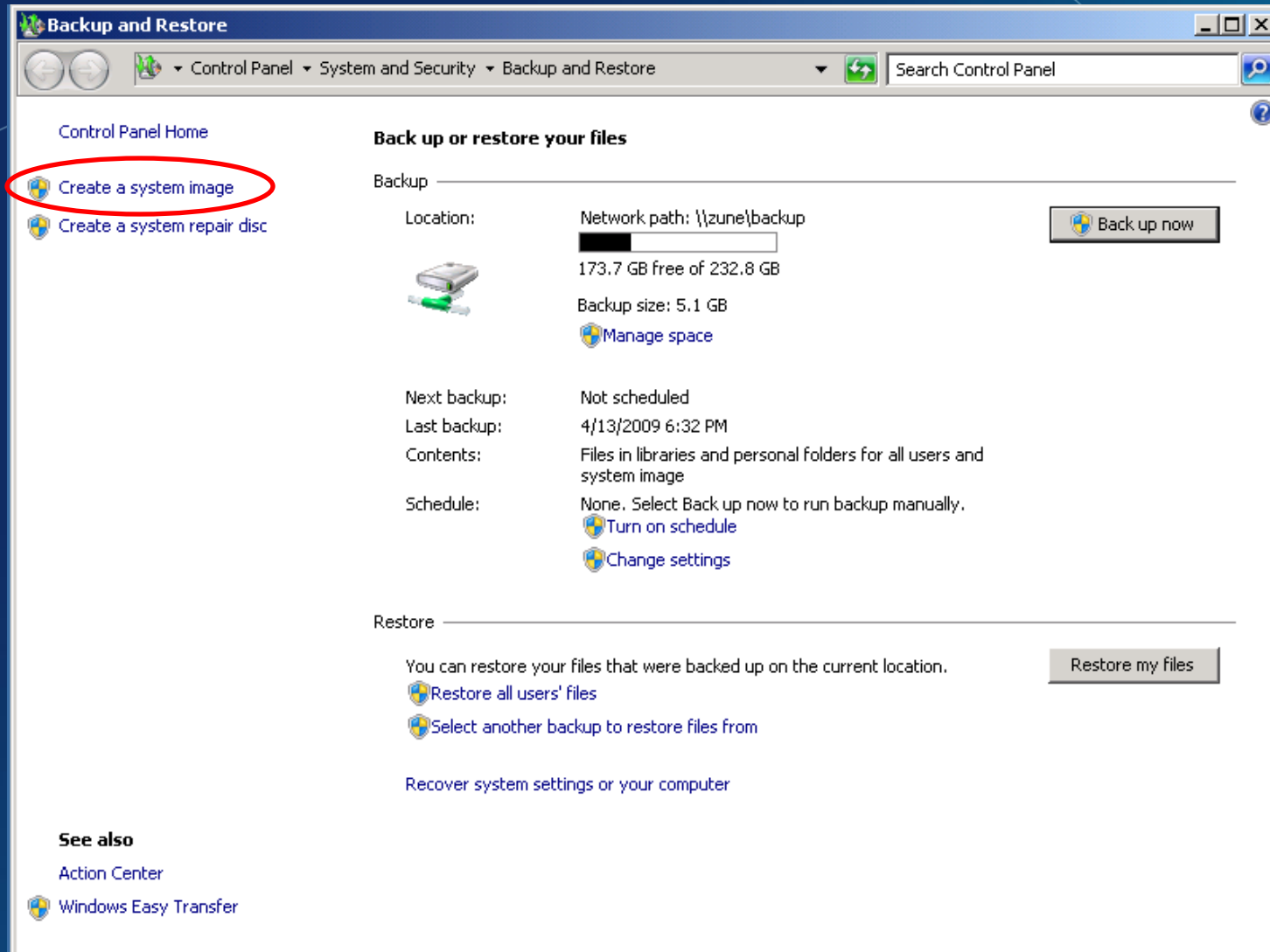
- When mounting, can select “Read Only”
















VHD File Format Used in System Image Backup

- System Image Backup (formerly Complete PC Backup in Vista)
- Backs up full hard drive, not just files and folders
- VHD can be stored on local USB drive or over network
- Can be mounted natively on a Windows 7 Forensic Workstation for examination

System Image Backup



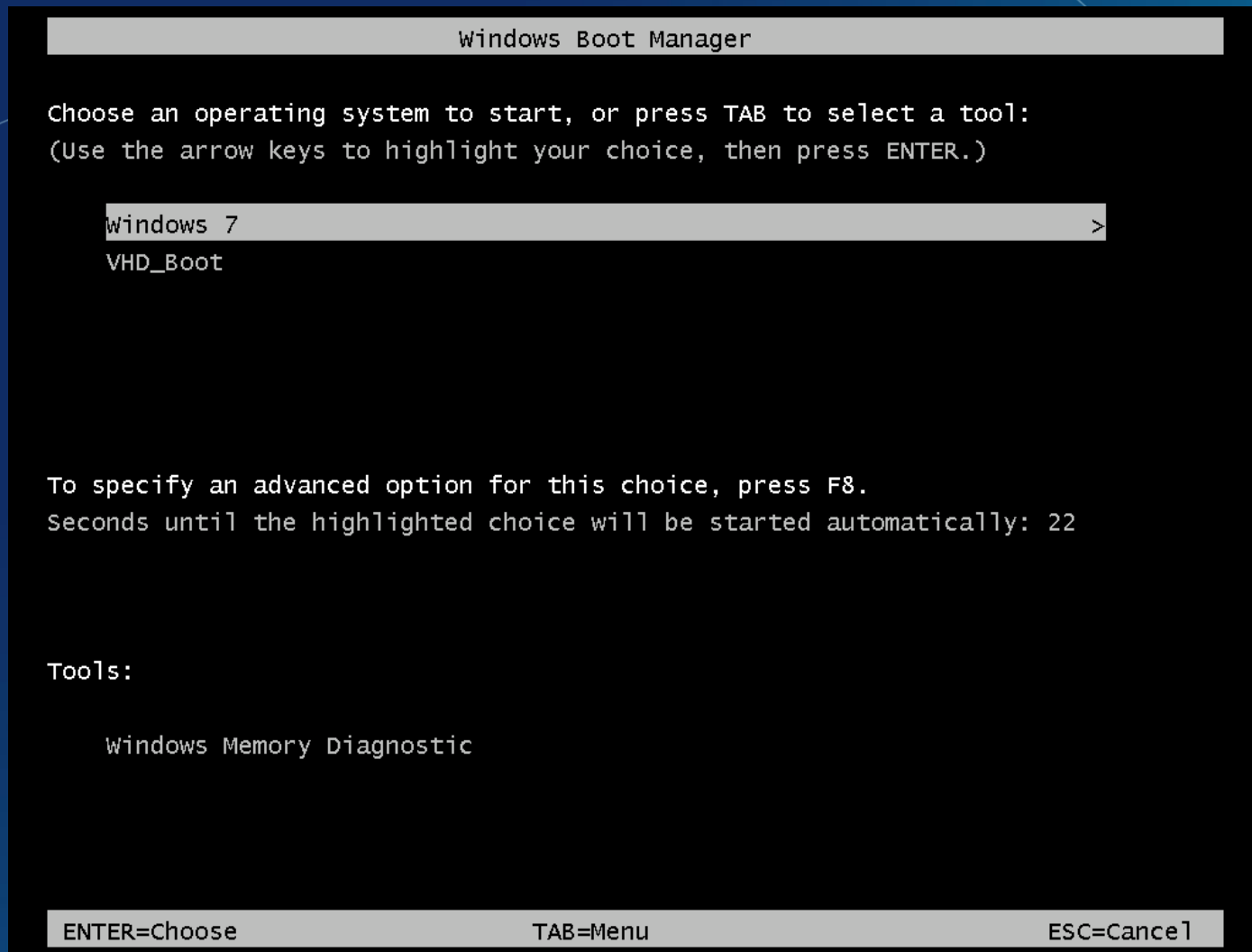
System Image Backup

Name	Date modified	Type	Size
 8d39ed38-20ab-11de-b2f5-806e6f6e6963.vhd	4/13/2009 6:29 PM	VHD File	36,876 KB
 8d39ed39-20ab-11de-b2f5-806e6f6e6963.vhd	4/13/2009 6:32 PM	VHD File	5,289,261 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_AdditionalFilesc3b9f3c...	4/13/2009 6:32 PM	XML Document	2 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Components.xml	4/13/2009 6:32 PM	XML Document	10 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_RegistryExcludes.xml	4/13/2009 6:32 PM	XML Document	7 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writer4dc3bdd4-ab48-...	4/13/2009 6:32 PM	XML Document	3 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writer542da469-d3e1-4...	4/13/2009 6:32 PM	XML Document	2 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writer6ad56c2-b509-4...	4/13/2009 6:32 PM	XML Document	2 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writerafb4a2-367d-4...	4/13/2009 6:32 PM	XML Document	4 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writerbe000cbe-11fe-4...	4/13/2009 6:32 PM	XML Document	4 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writercd3f2362-8bef-46...	4/13/2009 6:32 PM	XML Document	7 KB
 20df5e68-40ad-4e60-a5db-9e334544bfea_Writer8132975-6f93-44...	4/13/2009 6:32 PM	XML Document	2,350 KB
 BackupSpecs.xml	4/13/2009 6:32 PM	XML Document	2 KB

Boot to VHD

- Can configure Windows 7 to boot to the hard drive, OR VHD on the hard drive
- Only supported to boot **Windows 7 VHD** files
- Creates a boot list to select OS during system startup

Boot to a VHD



VHD Disk Investigative Impact

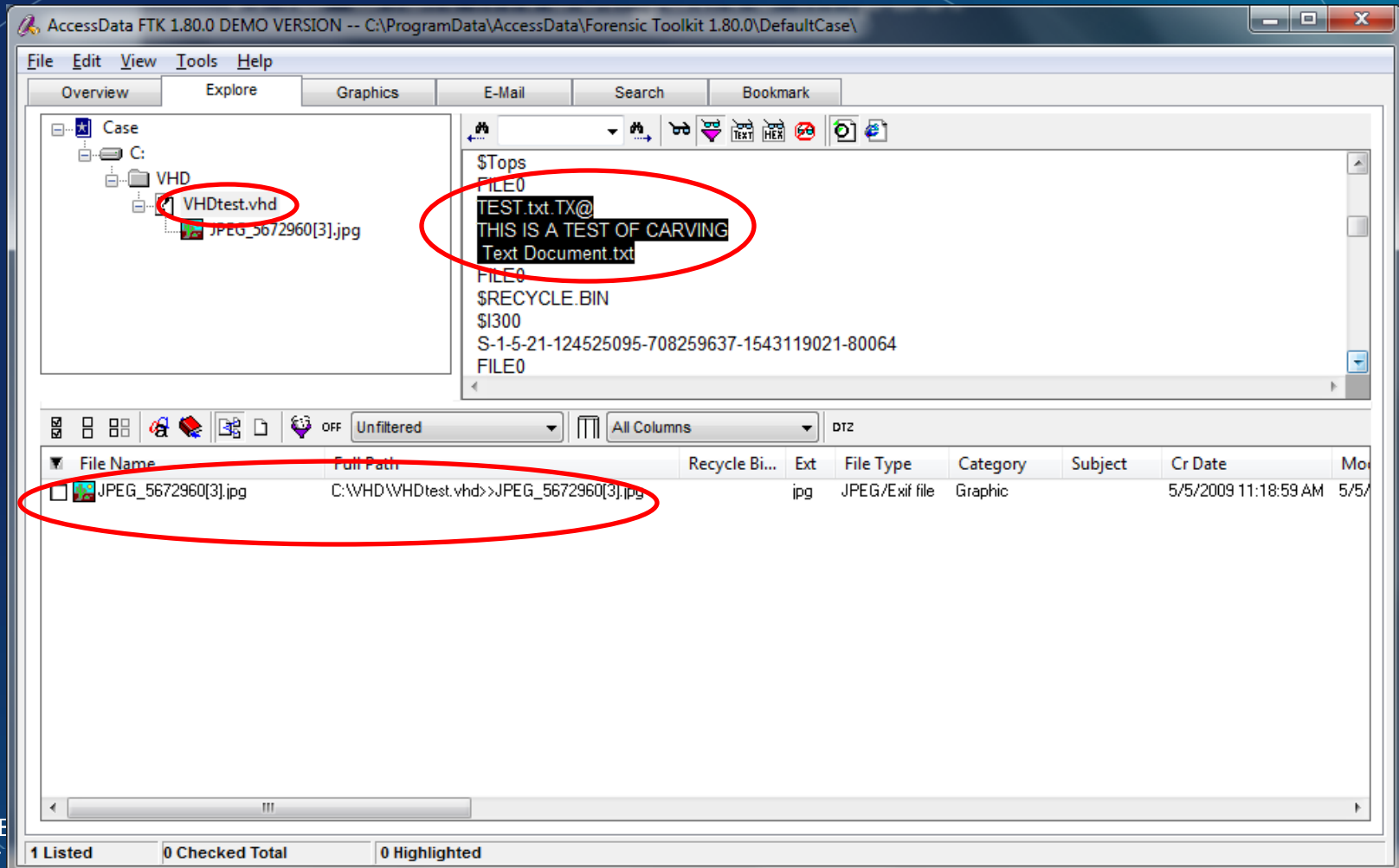
- Win7 machines may have several VHD files – backups, user created HDs, other bootable Operating systems. These may contain files critical to your case.
- Some of this data maybe auto carved via your forensic tools during examination.
- It some situations it might be useful to use the built in ability of Win7 to mount a VHD read only to get a full view into the Virtual Hard Disk.

VHD Disk Investigative Impact

- Three methods to view data in a VHD
 - Add VHD file into FTK to be examined
 - Use built in VHD mount feature of Win7 to image the VHD after you have given it a drive letter
 - Add it into FTK as an acquired image!

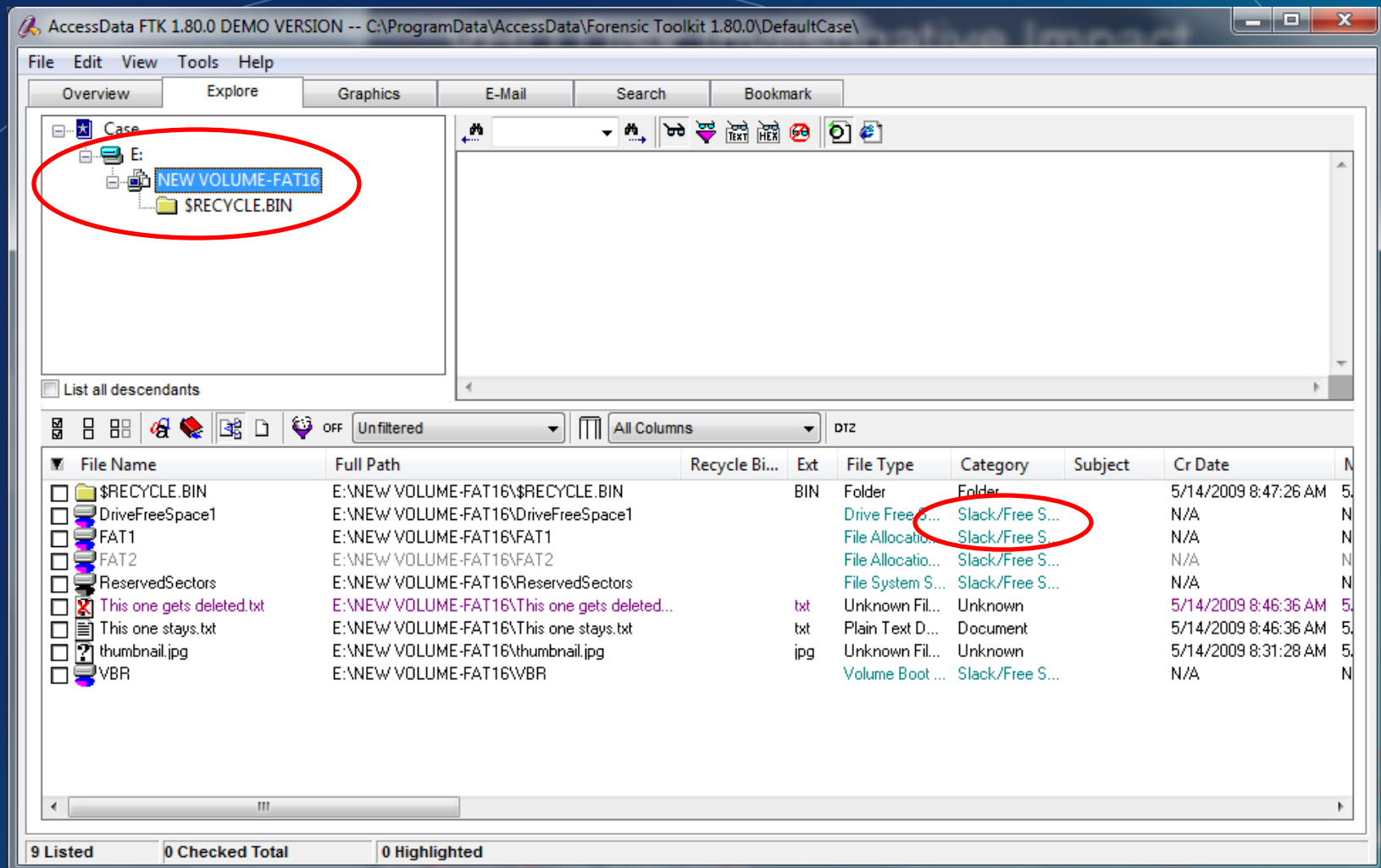
VHD Disk Investigative Impact

VHD added directly into FTK



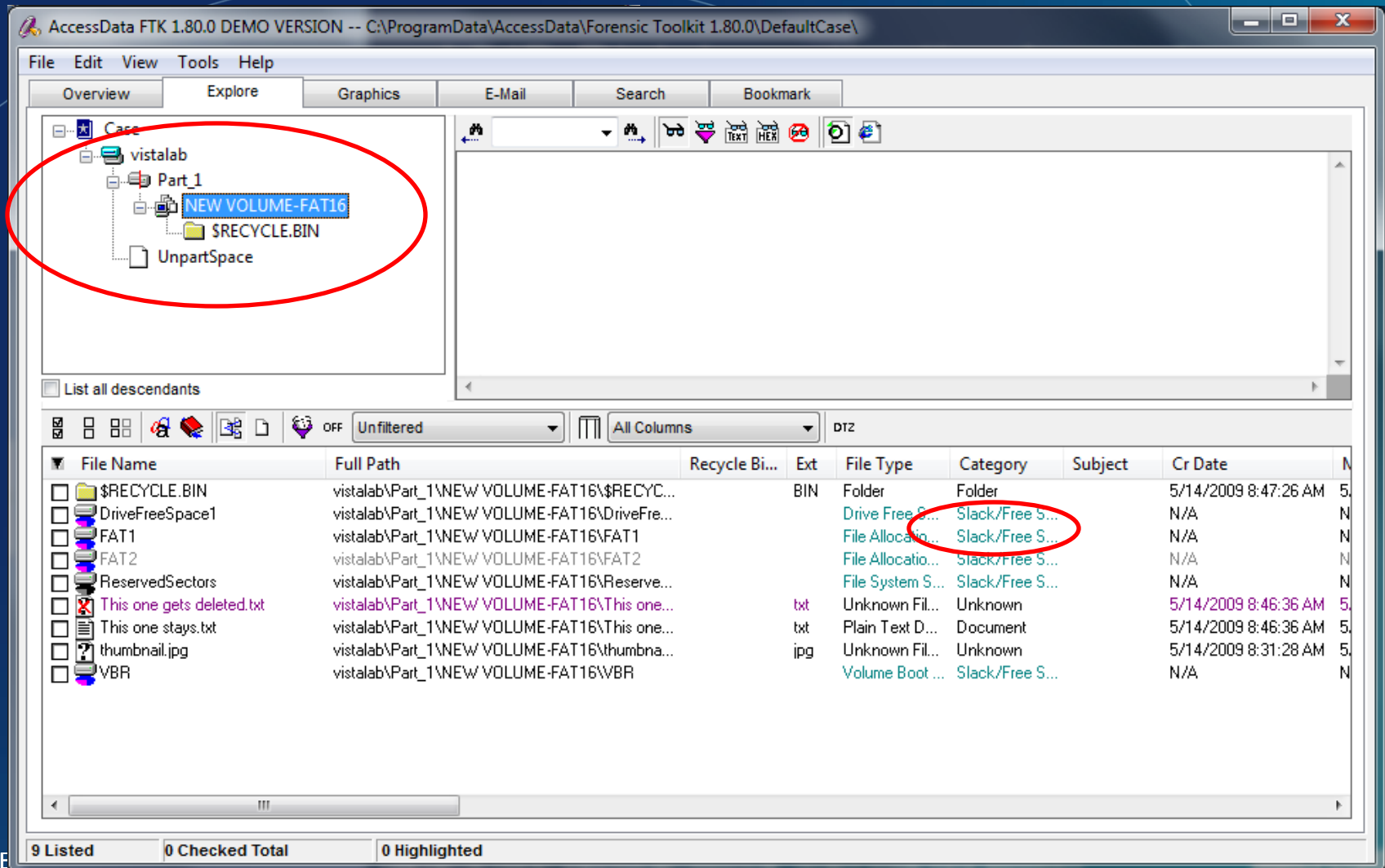
VHD Disk Investigative Impact

VHD mounted as a drive letter



VHD Disk Investigative Impact

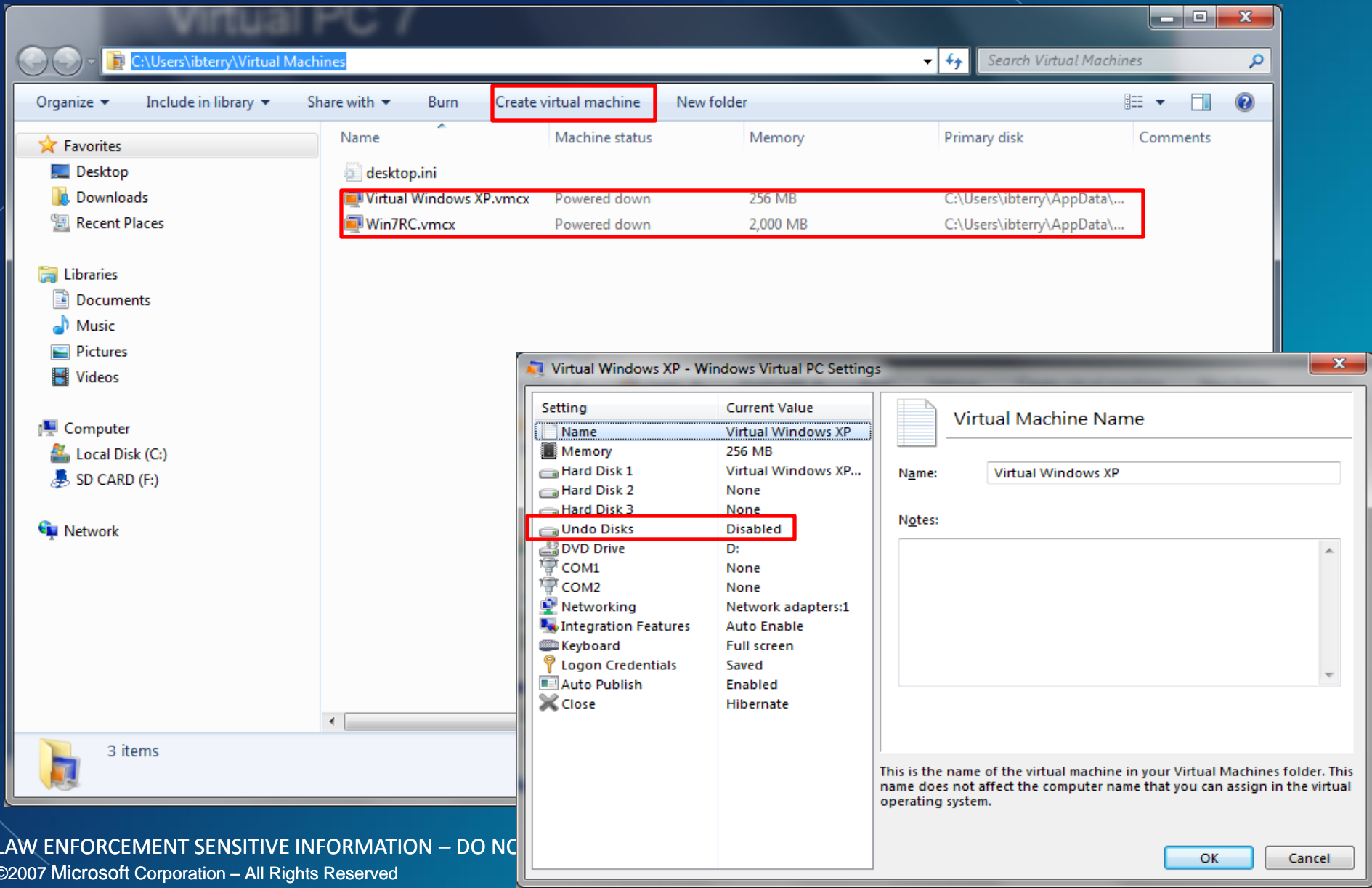
VHD added as acquired image in FTK



Virtual PC 7

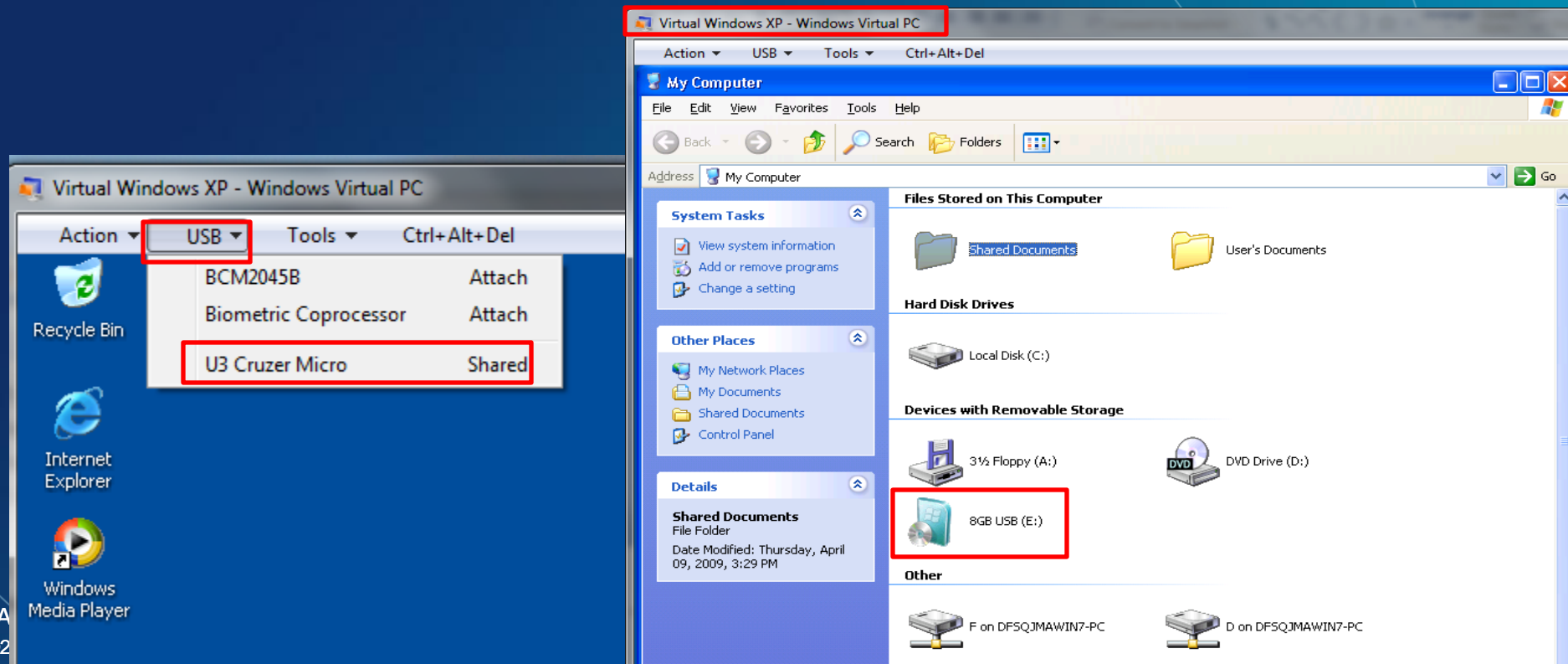
- Comes as separate download
- Windows 7 ONLY as host
 - Home Basic, Home Premium, Professional, Enterprise and Ultimate
- Supported GUEST operating systems
 - Windows XP, Vista and Windows 7
- Intel or AMD processor with Hardware Assisted Virtualization support required

Virtual PC 7 – User Interface



Virtual PC 7

- Allows running of multiple operating systems on host computer for testing, and compatibility
- USB Support in guest operating system!



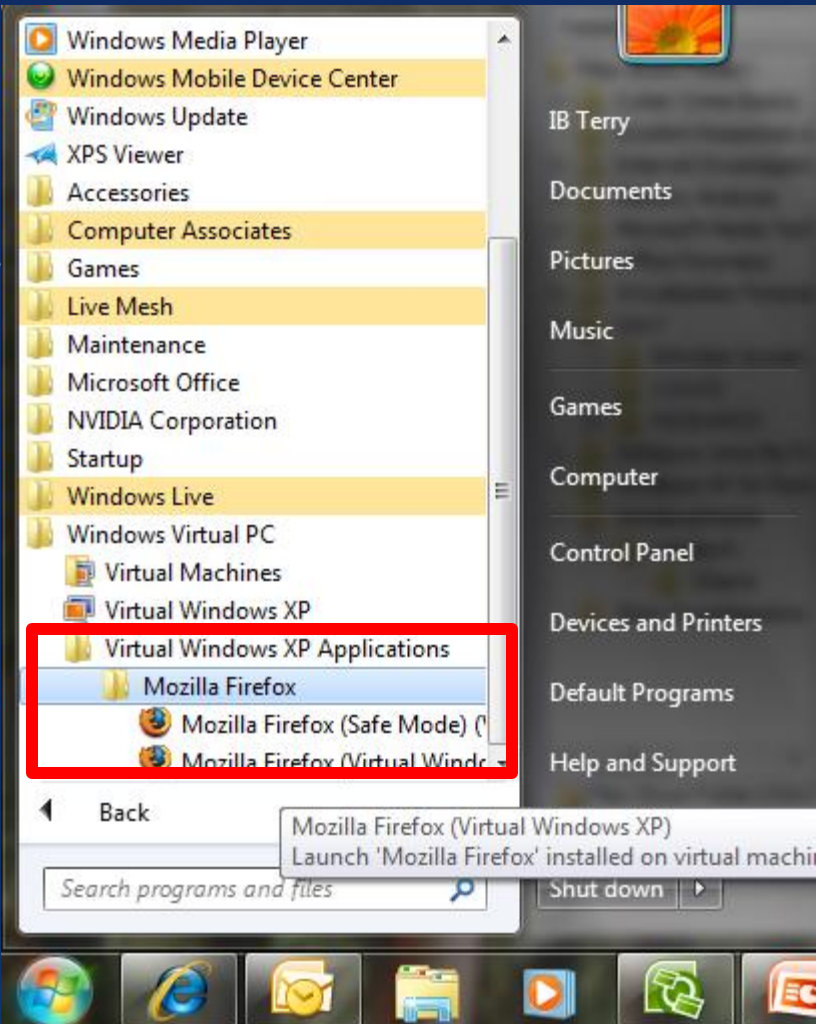
Windows XP Compatibility Mode

- Feature of Virtual PC
- Only available on Windows 7 Professional, Enterprise and Ultimate
- Guest must be Windows XP Professional SP 3

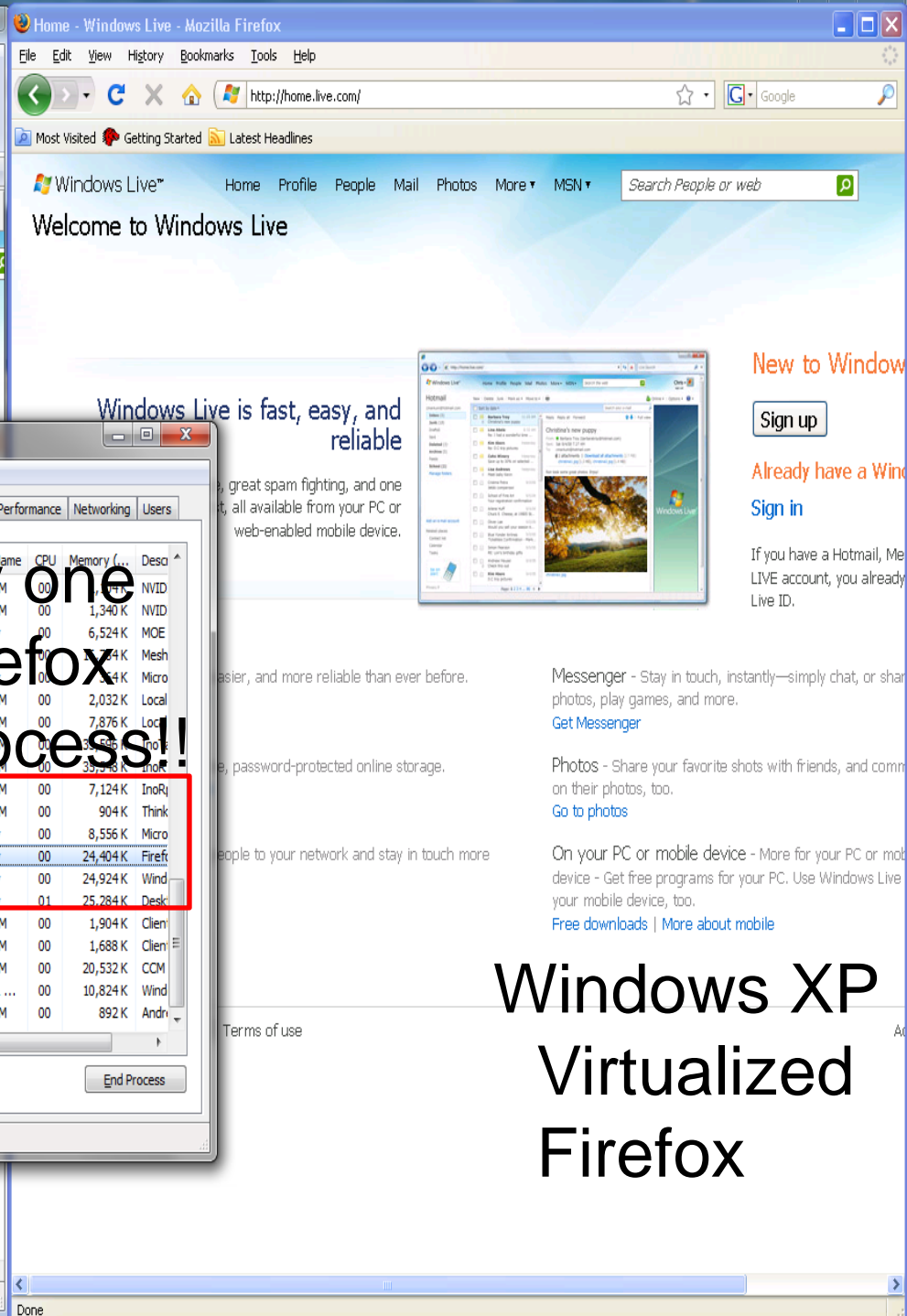
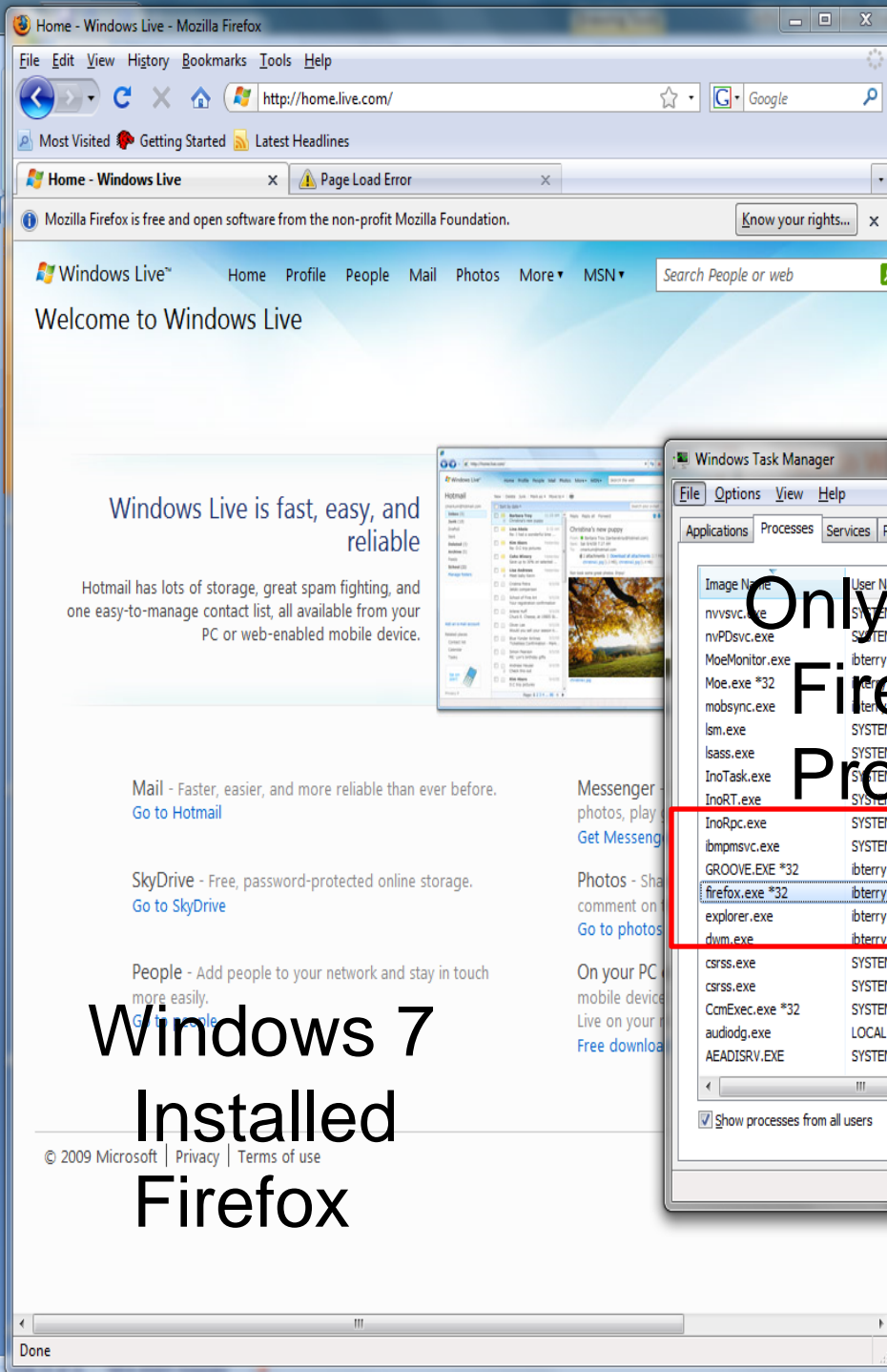
Windows XP Compatibility Mode

- Runs under Virtual PC 7
- Windows XP VHD you install applications into
- Application is published in the Windows 7 Start Menu
- When you run application it is running in XP VHD, BUT it appears to you to just be an application running in your Windows 7
- Allows you to run applications not compatible with Windows 7, in Windows 7

Windows XP Compatibility Mode

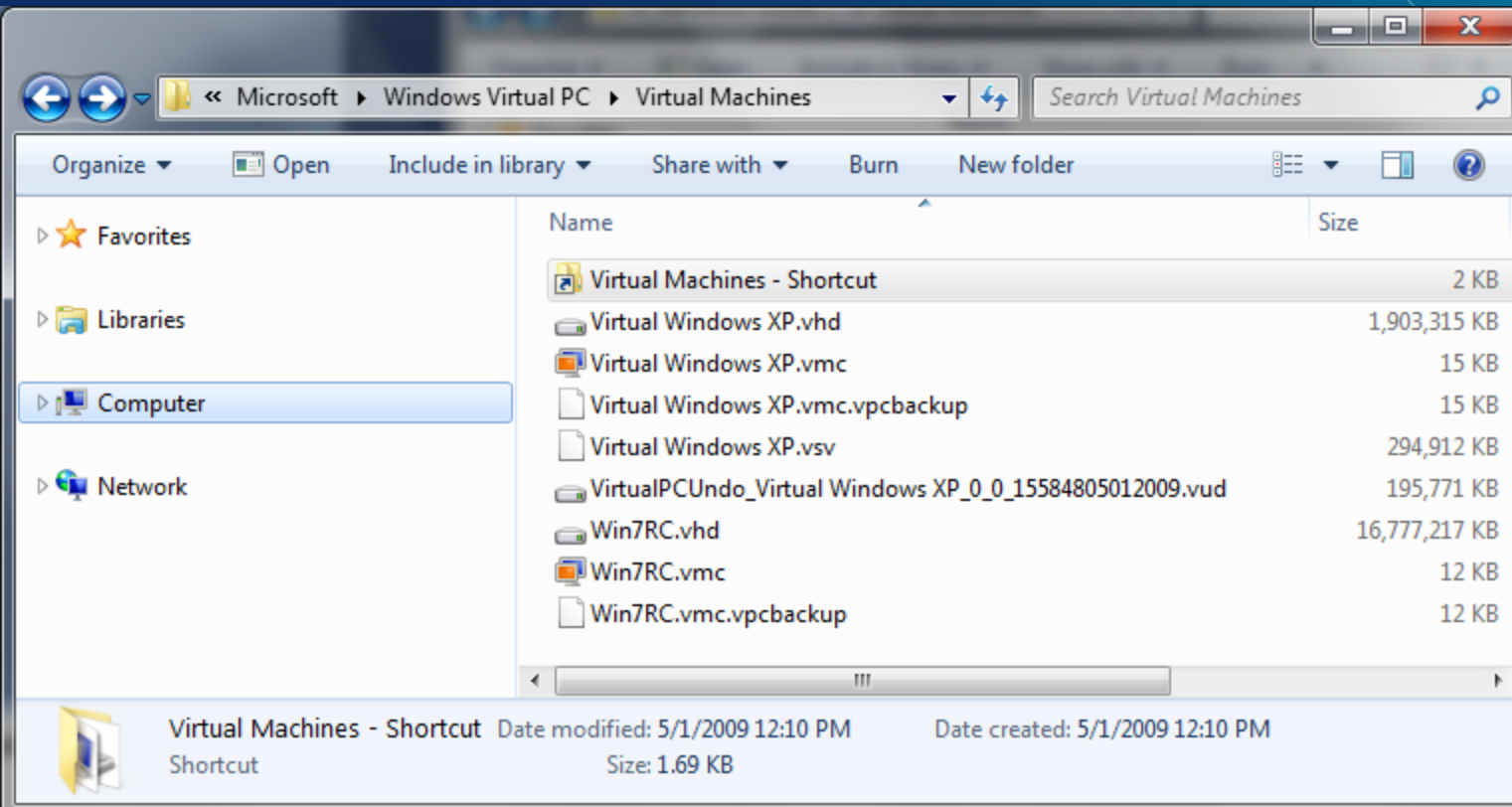


- Firefox web browser was installed in guest XP virtual machine.
- Shortcut to Firefox was automatically added to the host Windows 7 machine running Virtual PC.
- Once running it looks like any other execution of Firefox



Windows XP Compatibility Mode

- Default location for Virtual machines is
 - C:\Users\<username>\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines



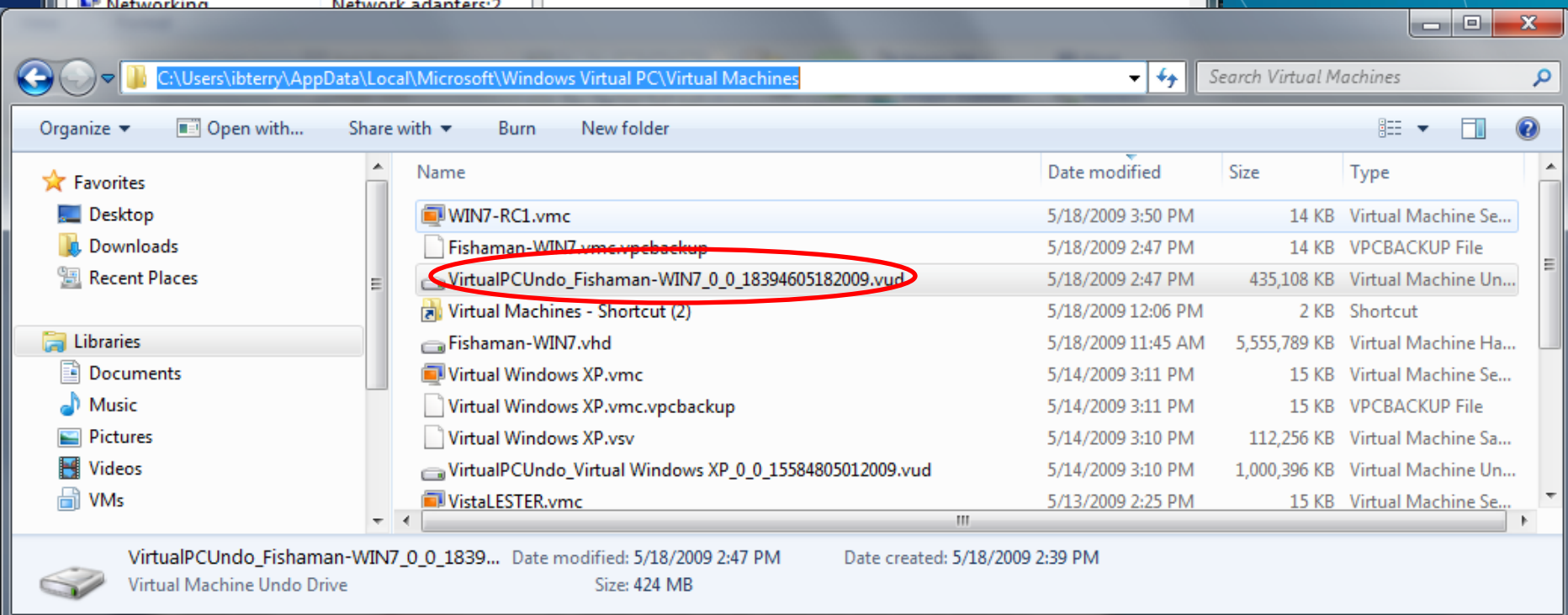
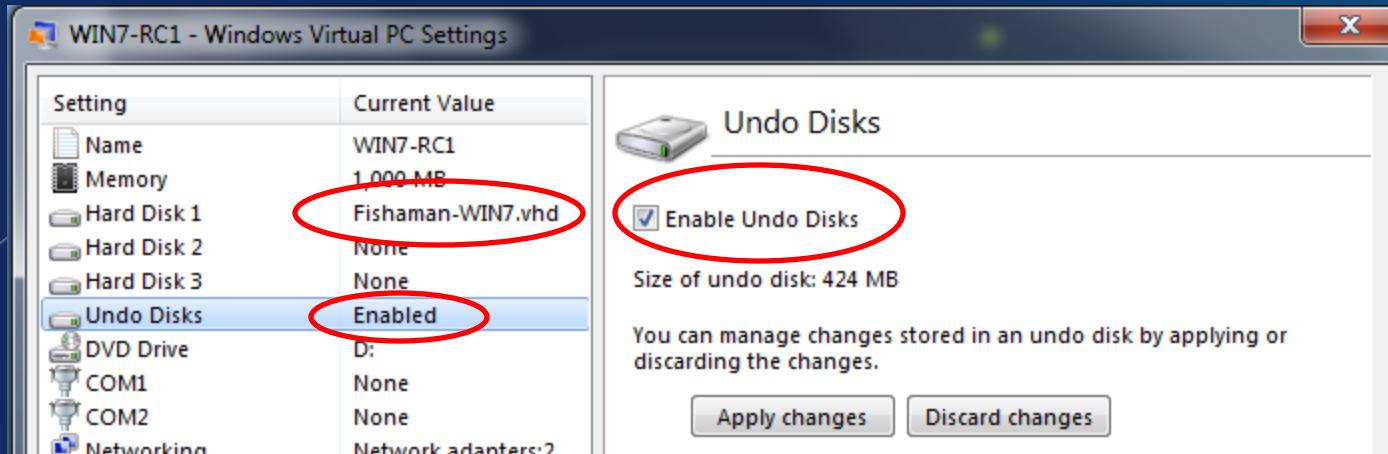
Virtual PC Undo Disks

- **UNDO - to make of no effect or as if not done : make null : reverse.** Merriam-Webster
- This is a great feature for Information Technology professionals – aids in testing and deployment of new services and applications
- Could potentially cause difficulties for forensic examiners.

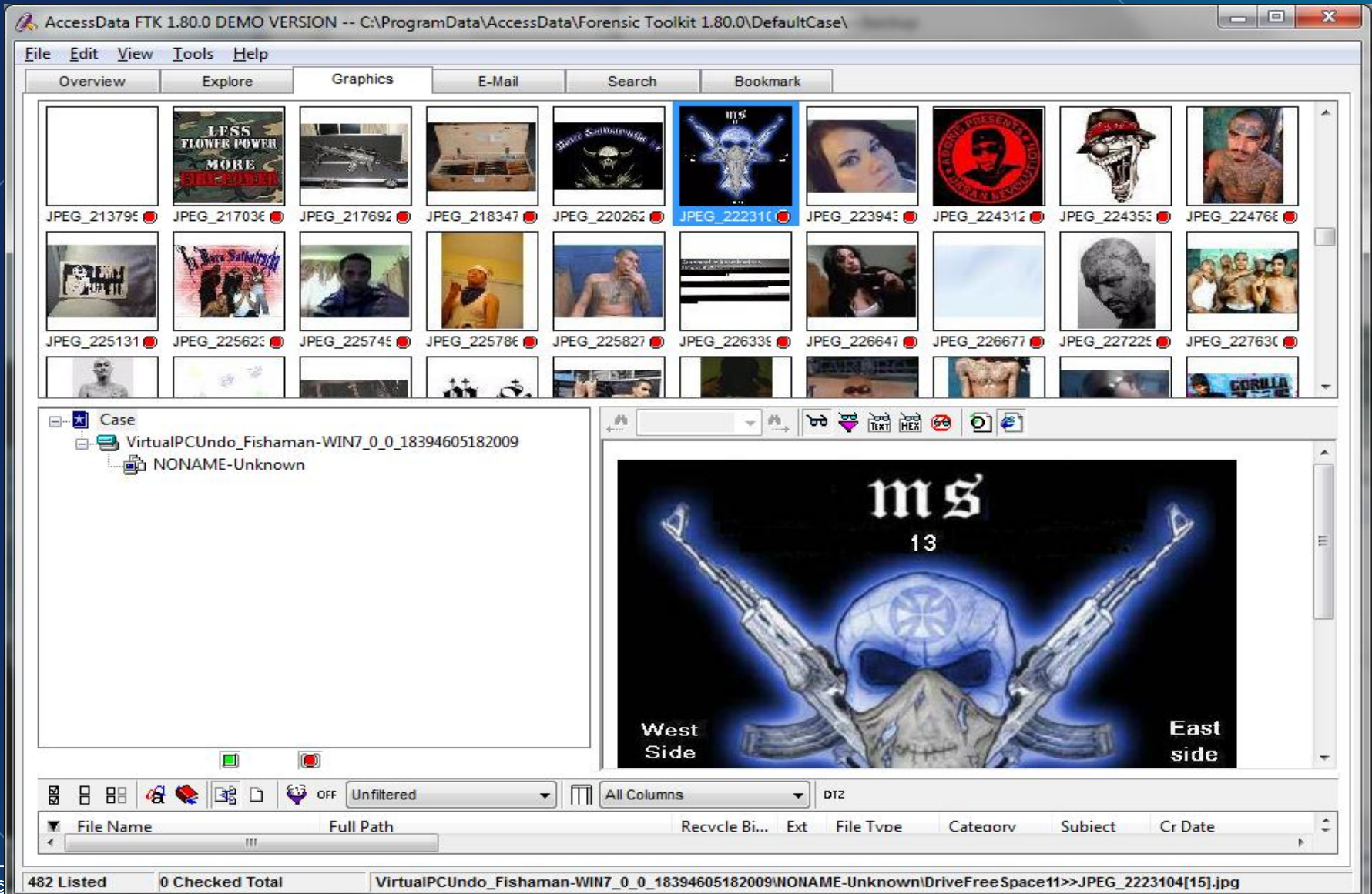
Virtual PC Undo Disks

- If the Enable undo disks option is selected for a virtual machine, any changes made during a virtual machine session are saved to an undo disk (.vud) file. An undo disk file is a temporary file and is separate from the virtual hard disk. When the virtual machine is closed, the changes stored in the undo disk can be deleted, committed to the virtual hard disk file, or saved until a later time.

Virtual PC Undo Disks



Virtual PC Undo Disks – Carved in FTK



Virtual PC Undo Disks

- How can you tell if a Virtual Machine has undo disk enabled?
 - Each virtual machine has a .VMC configuration file. – Located in folder with VHD usually
 - This file contains the setting for the machine such as
 - >Memory Allocated
 - >Hard Drive, Path to the VHD file
 - > Network setting
 - >Undo Disks!

Virtual PC Undo Disks

- How can you tell if a Virtual Machine has undo disk enabled?
 - Each virtual machine has a .VMC configuration file. – Located in folder with VHD usually
 - This file contains the setting for the machine such as
 - >Memory Allocated
 - >Hard Drive, Path to the VHD file
 - > Network setting
 - >Undo Disks!

Virtual PC Undo Disks – VMC edited in notepad

```
<ide_adapter>
  <ide_controller id="0">
    <location id="0">
      <drive_type type="integer">1</drive_type>
      <pathname>
        <absolute type="string">C:\Users\ibterry\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines\Fishaman-WIN7.vhd</absolute>
        <relative type="string">.\Fishaman-WIN7.vhd</relative>
      </pathname>
      <undo_pathname>
        <absolute type="string">C:\Users\ibterry\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines\VirtualPCUndo_WIN7-RC1_0_0_21014905182000.vud</absolute>
        <relative type="string">.\VirtualPCUndo_WIN7-RC1_0_0_21014905182000.vud</relative>
      </undo_pathname>
    </location>
  </ide_controller>
  <ide_controller id="1">
    <location id="0">
      <drive_type type="integer">2</drive_type>
      <pathname>
        <absolute type="string">D</absolute>
        <relative type="string" />
      </pathname>
    </location>
  </ide_controller>
</ide_adapter>
```

Virtual PC Memory of hibernated virtual machines

- One feature of VPC is to allow for the state of a Virtual machine to be saved
- When the Virtual Machine is in the saved state the status information(memory) is written to a .VSV file
- These VSV files *MAY* contain information about programs that were executing when the machine was put into the saved state.



Introduction to the Volume Shadow Copy Service

Exploration of Windows 7



Data Integrity in Windows 7

- Volume Shadow Copy is involved in every transaction with disks that are being monitored – System is monitored by default
- Only the changes between snapshots are recorded in the snapshot dataset

Vista - Volume Snapshot Creation

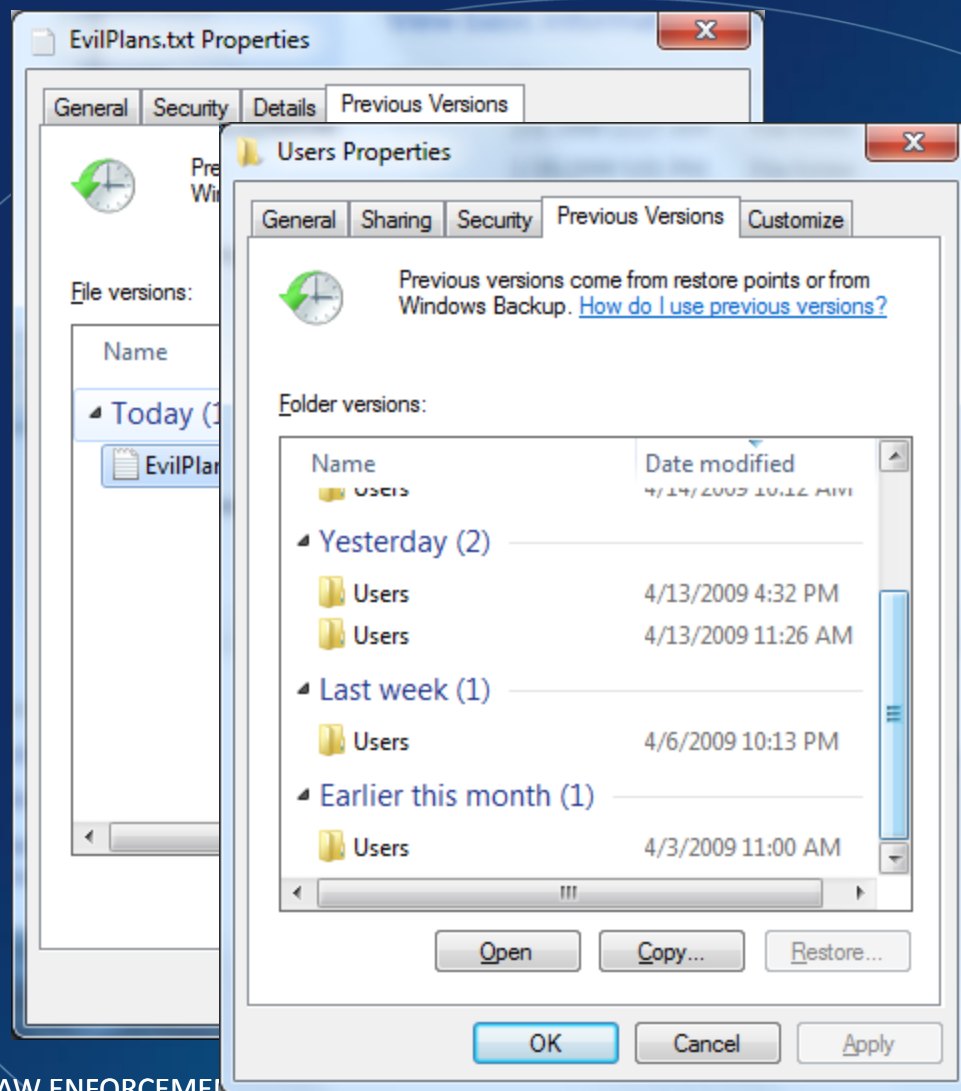
- When are volume snapshots created?
 - Manually
 - Every 24 hours
 - Before a Windows Update
 - Unsigned Driver Installation
 - An application that calls the Snapshot API

Win 7 - Volume Snapshot Creation

- When are volume snapshots created?
 - Manually
 - **Every 7 days**
 - Before a Windows Update
 - Unsigned Driver Installation
 - An application that calls the Snapshot API

Data Integrity - Previous Versions

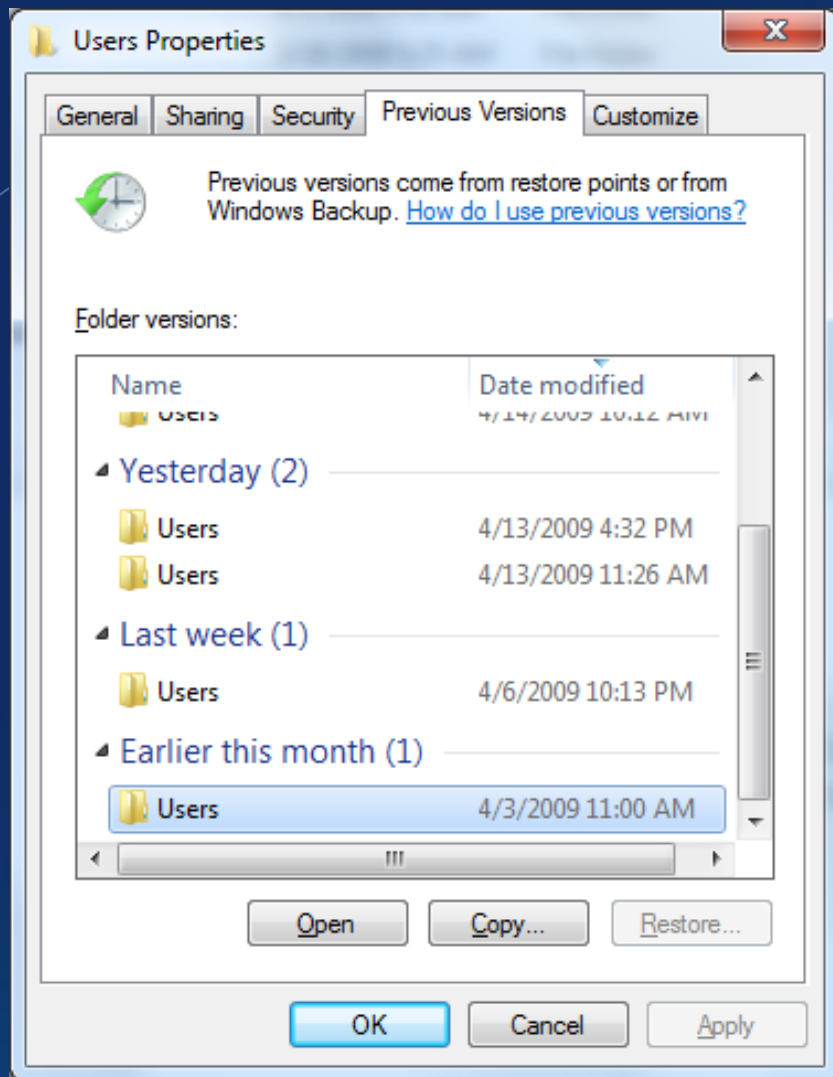
- Previous Versions
 - Restore previous versions of folders and files



Data Integrity - Previous Versions

- Previous Versions is a component of the Volume Shadow Copy Service
- Previous Versions of a file or folder are available if a changed version of that file or folder was captured during creation of a volume snapshot

Data Integrity - Previous Versions

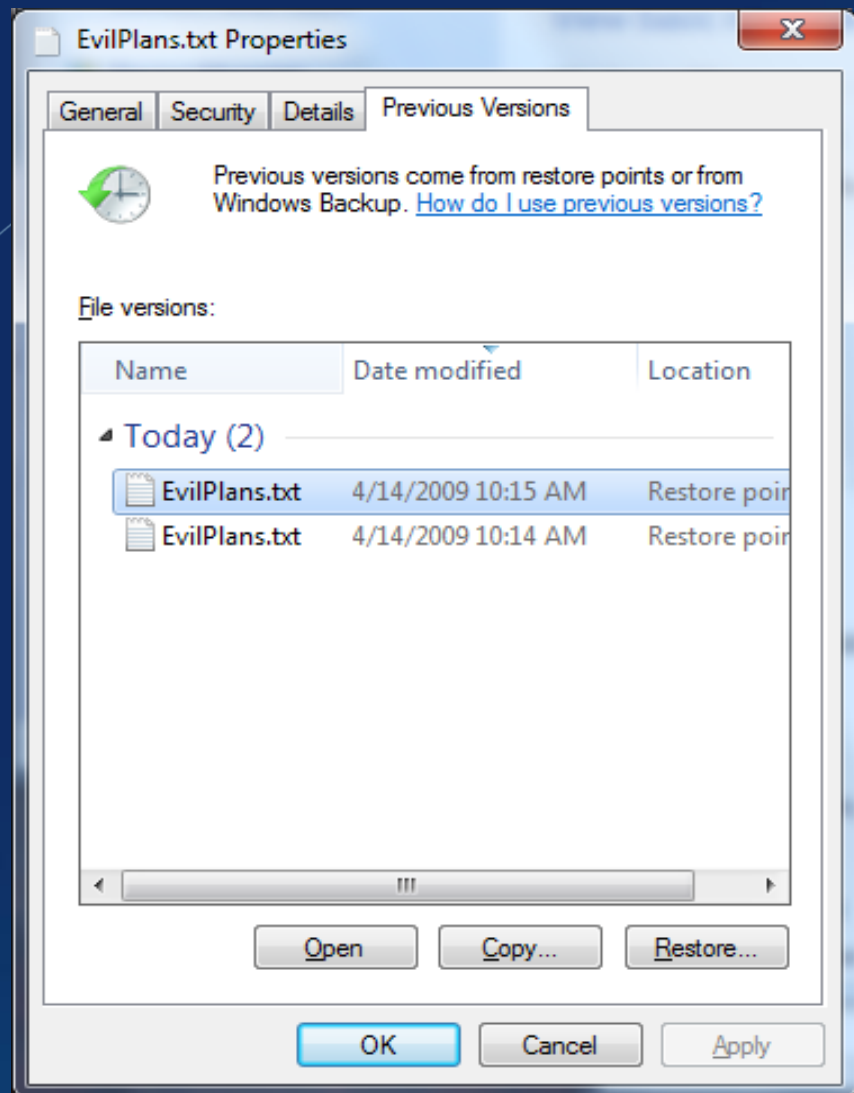


- You will be presented with all previous versions of the resource to:
 - Open
 - Copy
 - Restore

Data Integrity - Previous Versions

- You can save off copies of the document throughout its lifespan within the volume snapshot data available on the system
- If you restore the file...you lose all other snapshot data for that file
- Recovering any of the files may result in file metadata not being complete

Data Integrity - Previous Versions

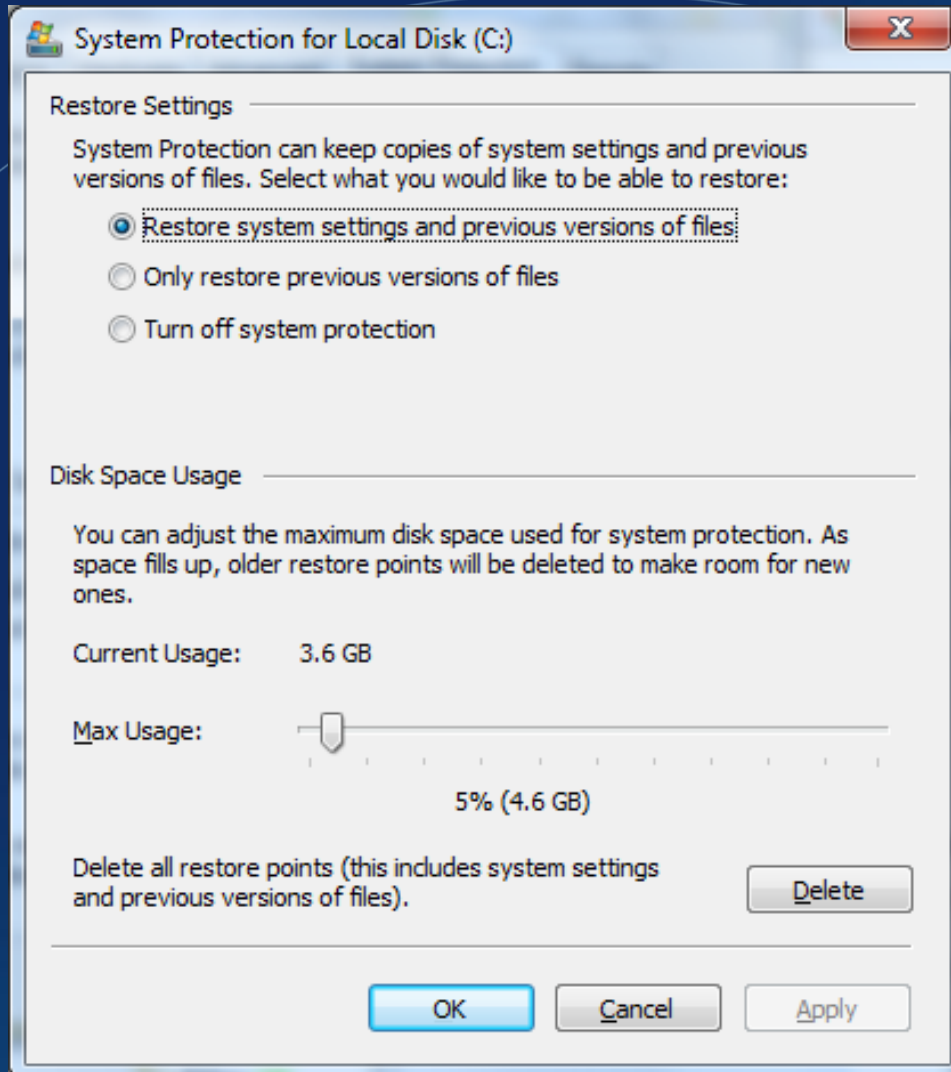


- The data needed to successfully restore a file is:
 - The original file
 - +
 - The change data
- Defragmentation may affect recoverability

Accessing and Mounting Volume Shadow Copy Stores

- Vista VSS consumed 15% regardless of drive size and was not configurable
- Win 7 VSS disk consumption will vary depending on drive size and is configurable.
- 5% for volumes > 64GB
- 3% for volumes <= 64GB

Accessing and Mounting Volume Shadow Copy Stores



- Disk space usage can be customized
- Restore options allow only previous versions or System restore and Previous Versions

Introduction to BitLocker FVE

(Understanding the Steps Required to enable BitLocker and
BitLocker ToGo)

Exploration of Windows Vista

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

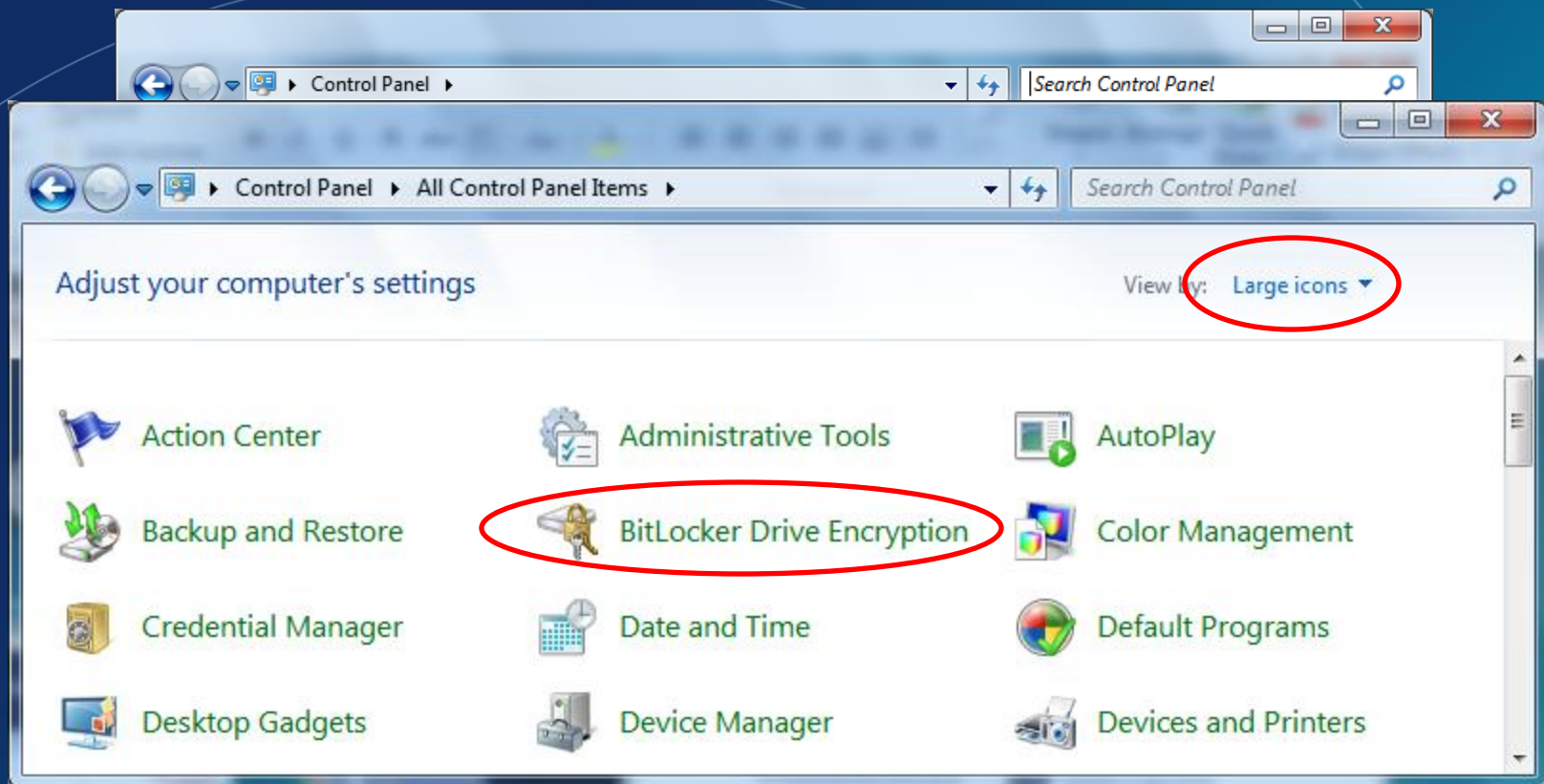
BitLocker Requirements

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

Enabling OS BitLocker via USB Key



Enabling BitLocker - OS



Enabling BitLocker - OS



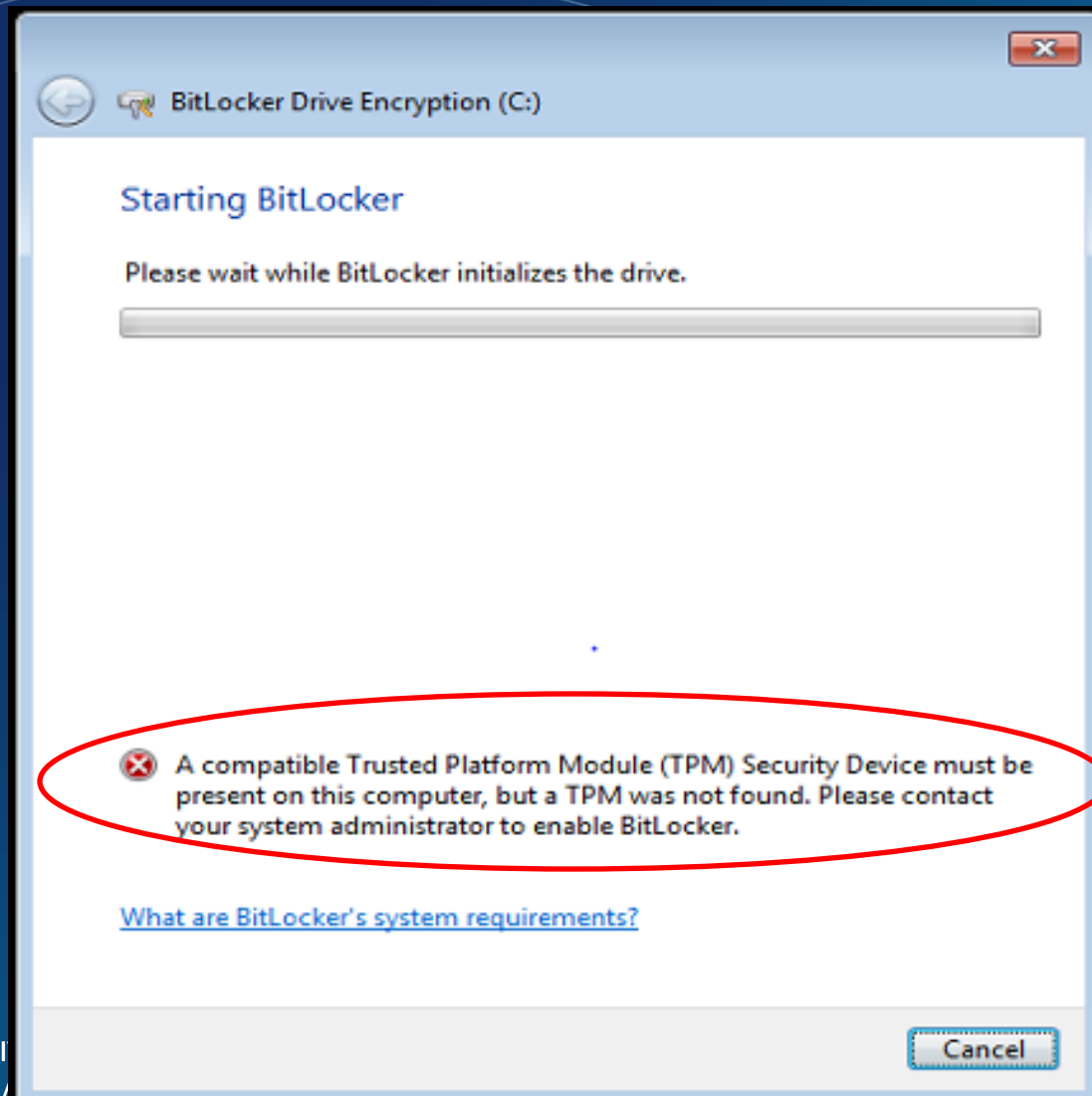
See also

 TPM Administration

 Disk Management

[Read our privacy statement online](#)

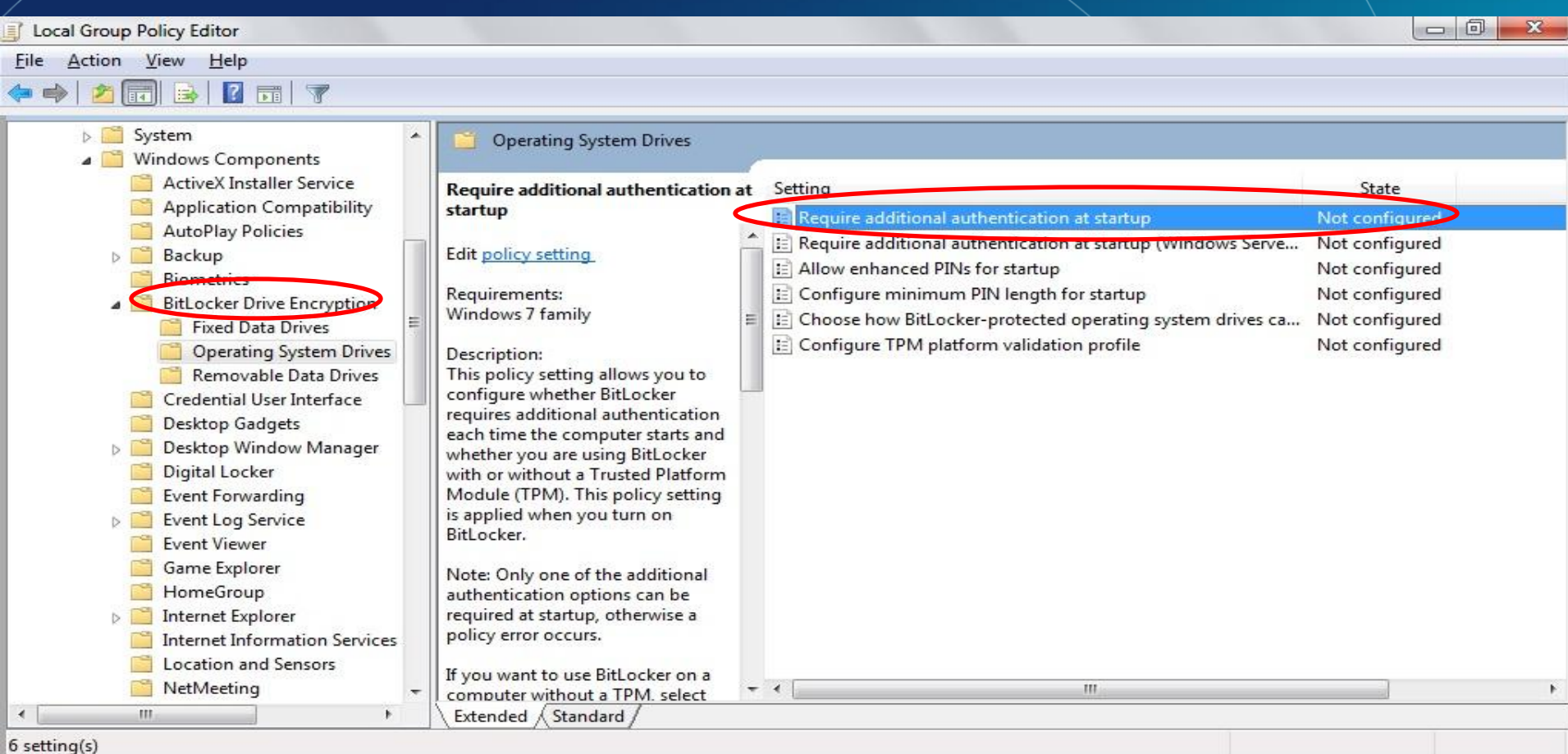
Enabling BitLocker - OS



Enabling BitLocker - OS

Execute: gpedit.msc

Navigate: Computer Configuration\Administrative Templates\Windows Components



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



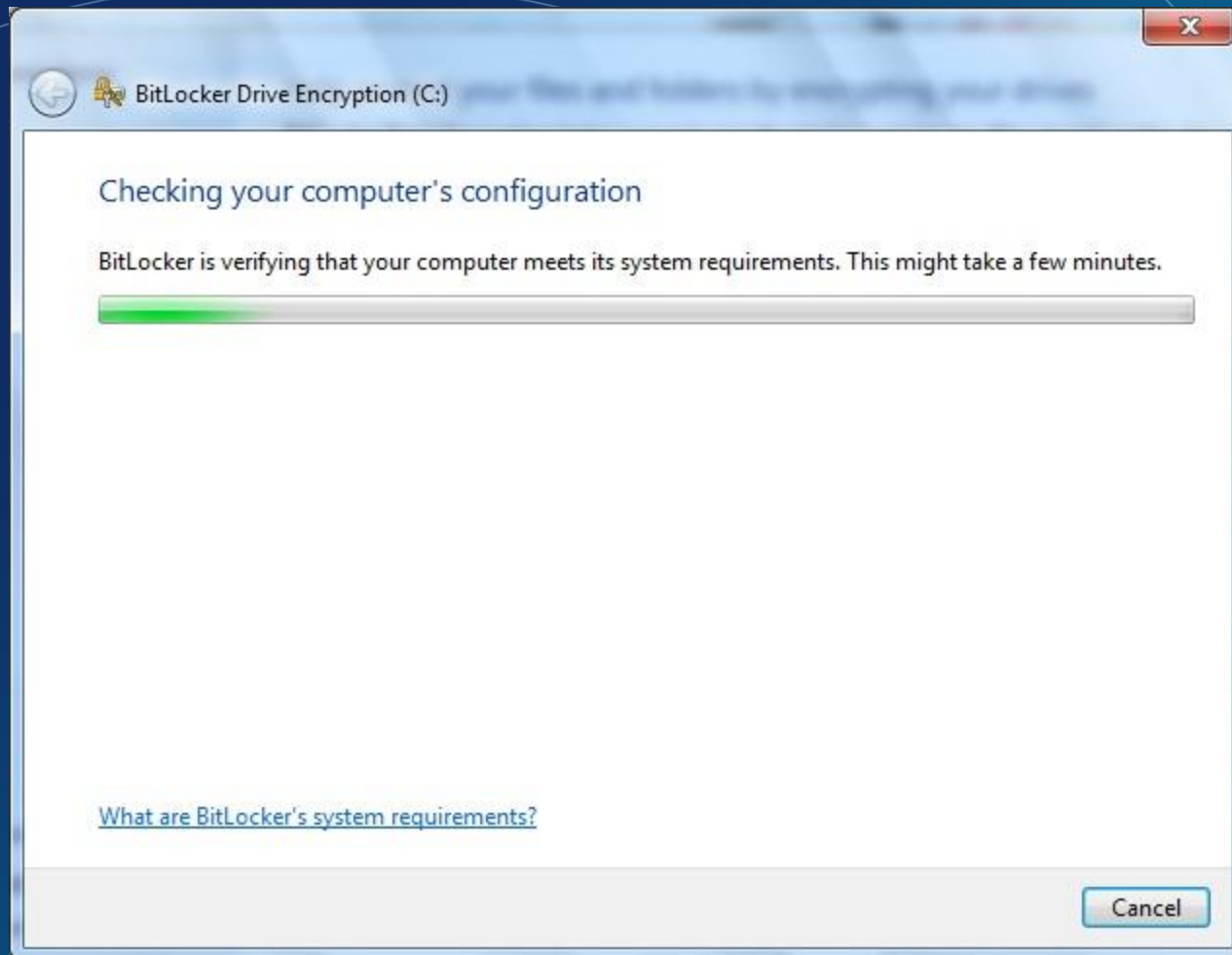
See also

 TPM Administration

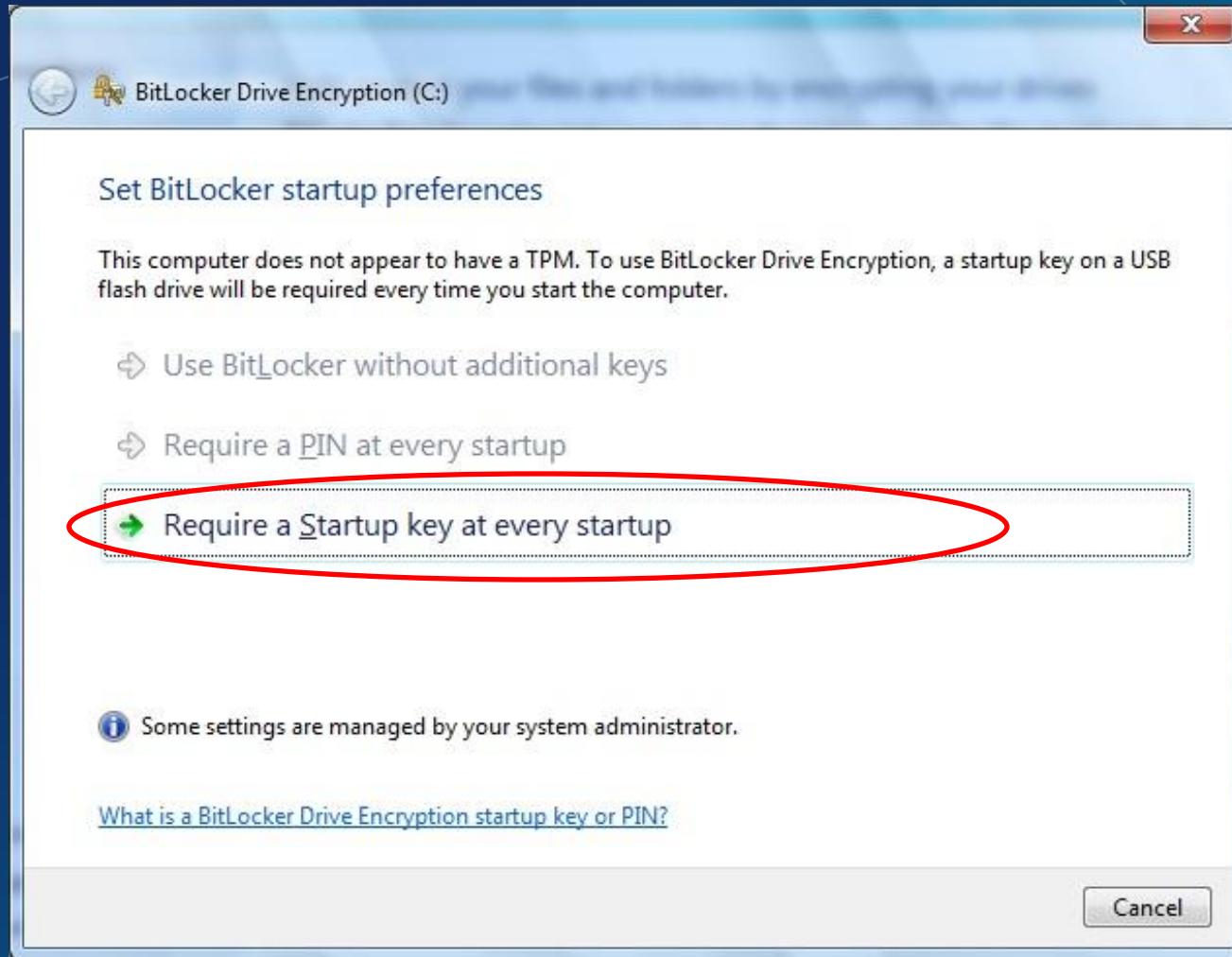
 Disk Management

[Read our privacy statement online](#)

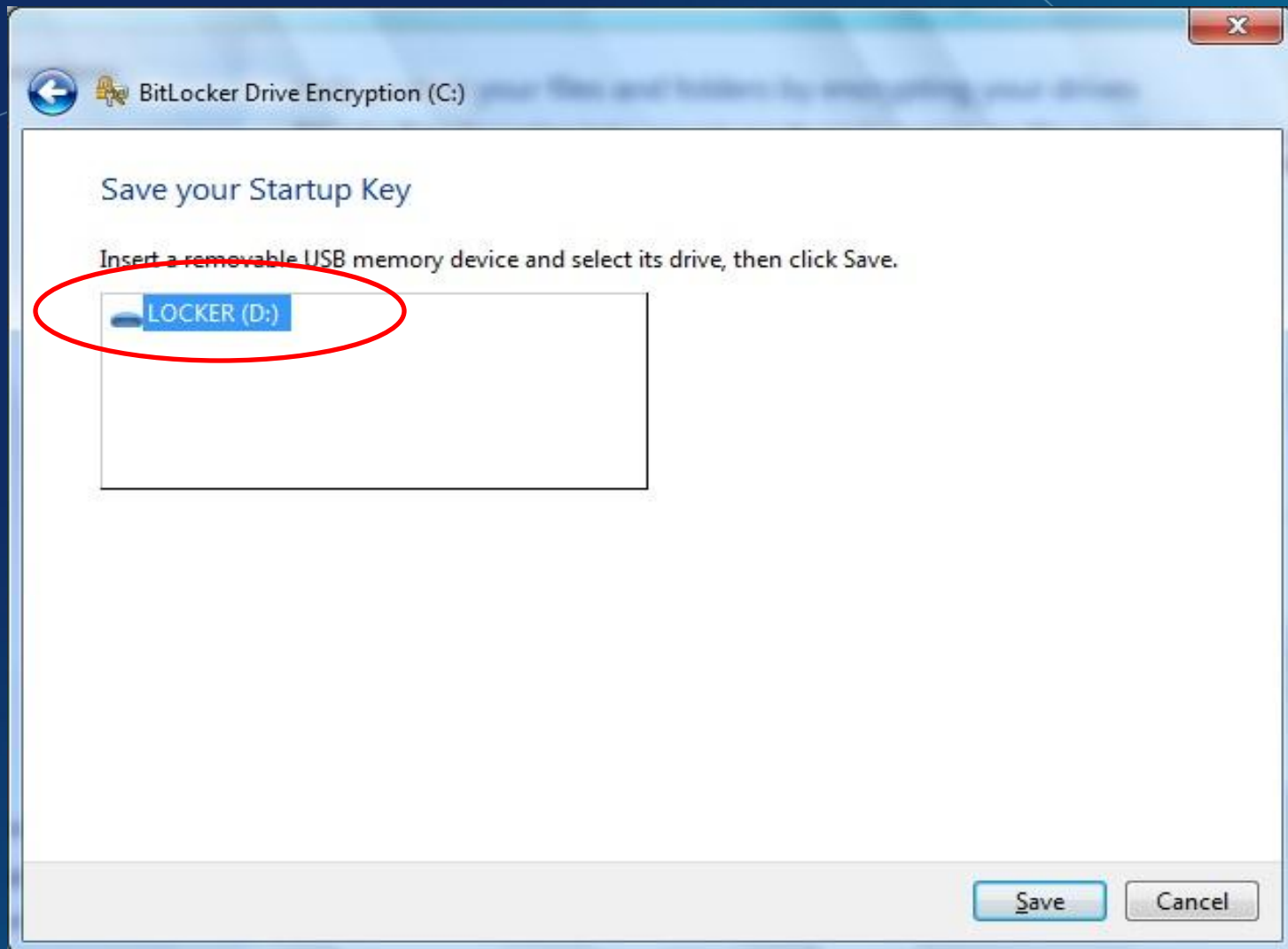
Enabling BitLocker - OS



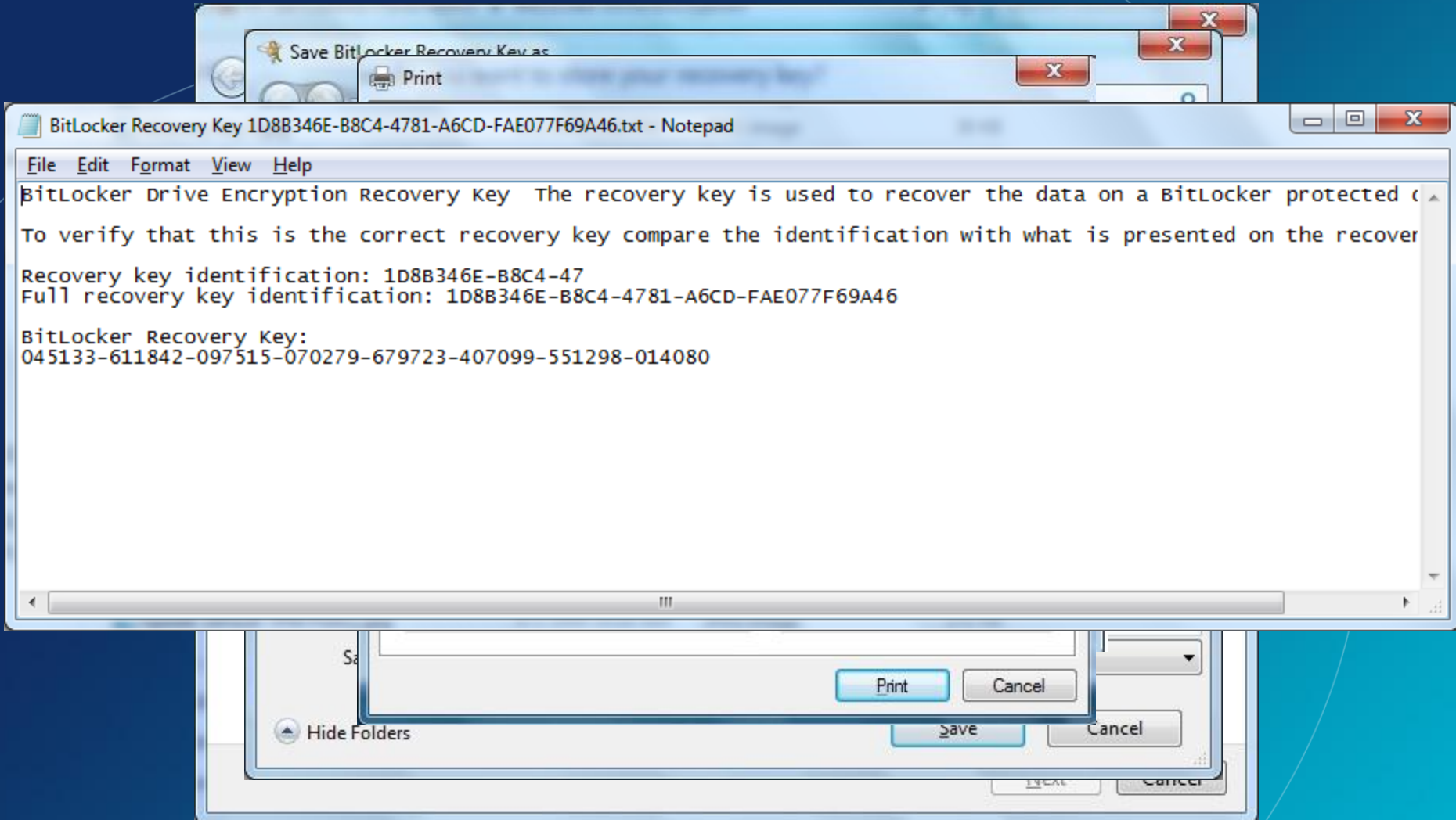
Enabling BitLocker - OS



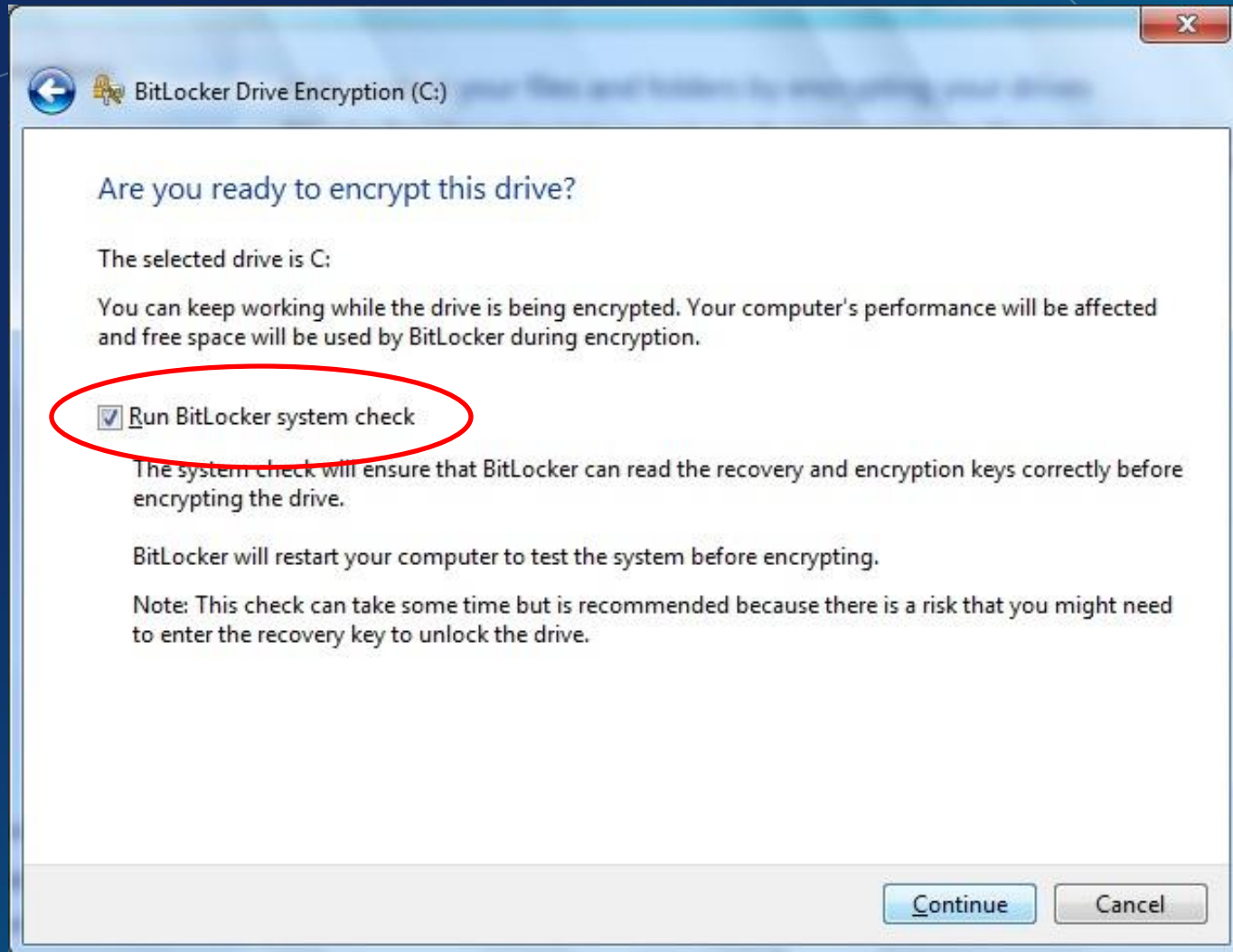
Enabling BitLocker - OS



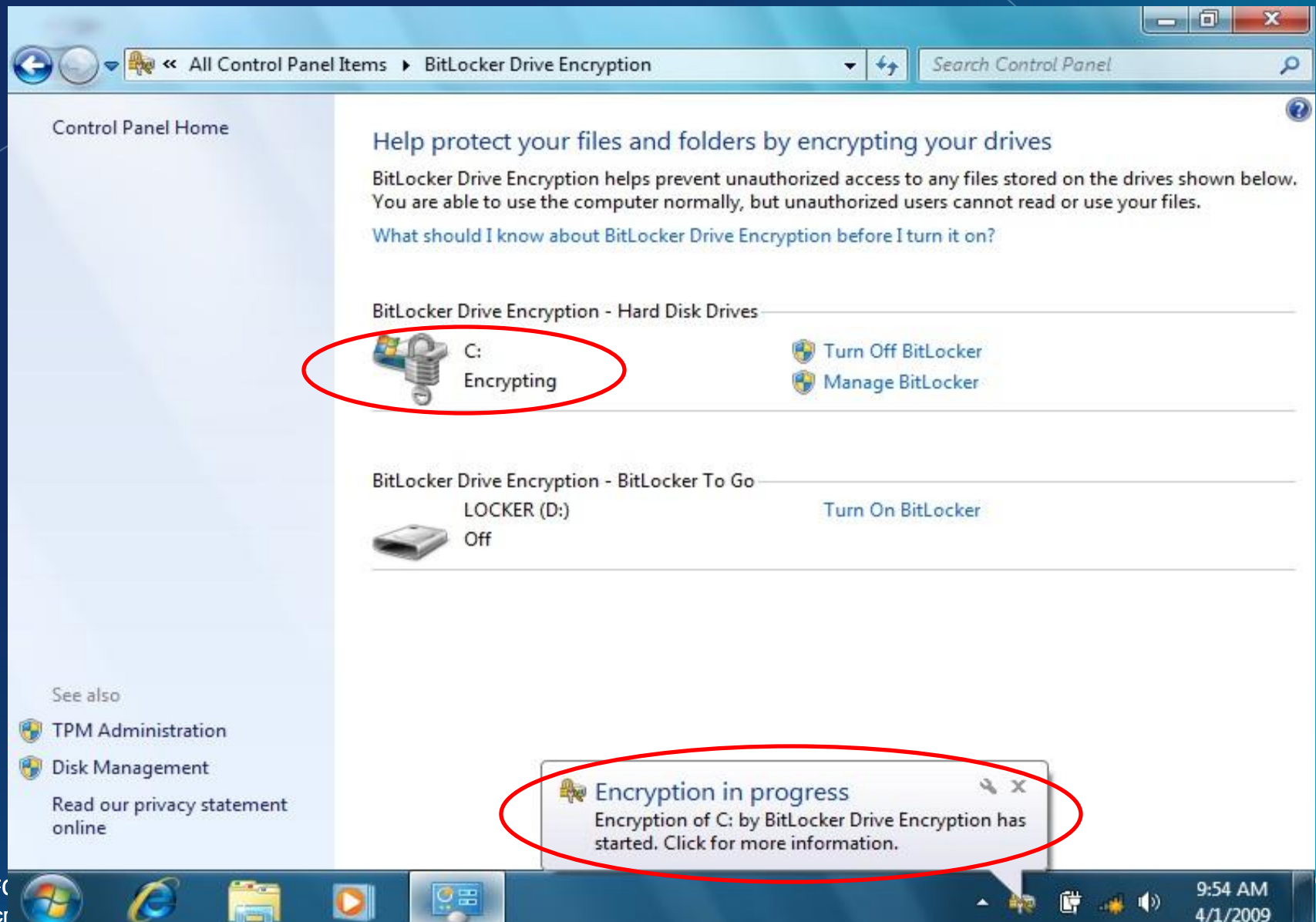
Enabling BitLocker - OS



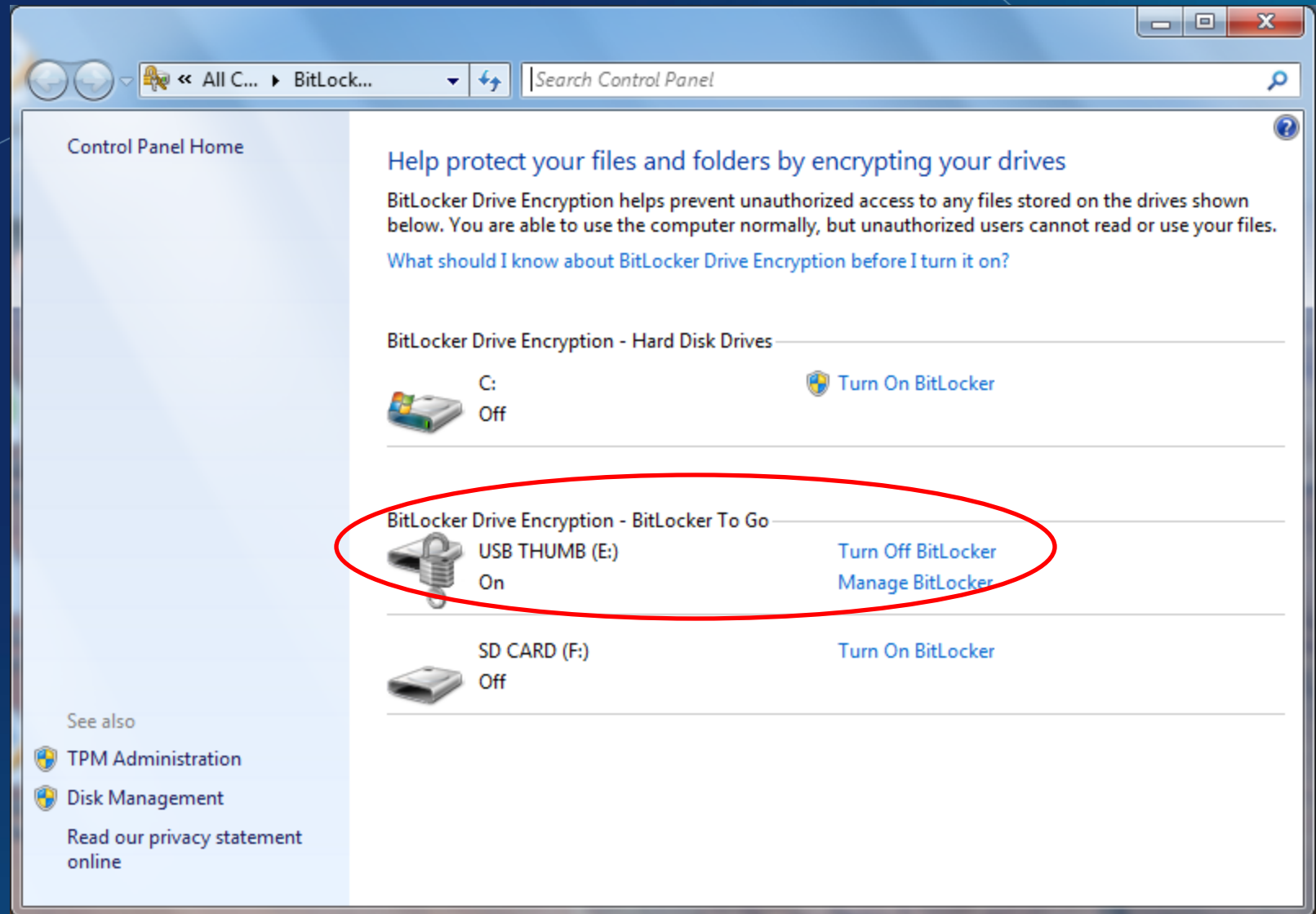
Enabling BitLocker - OS



Enabling BitLocker



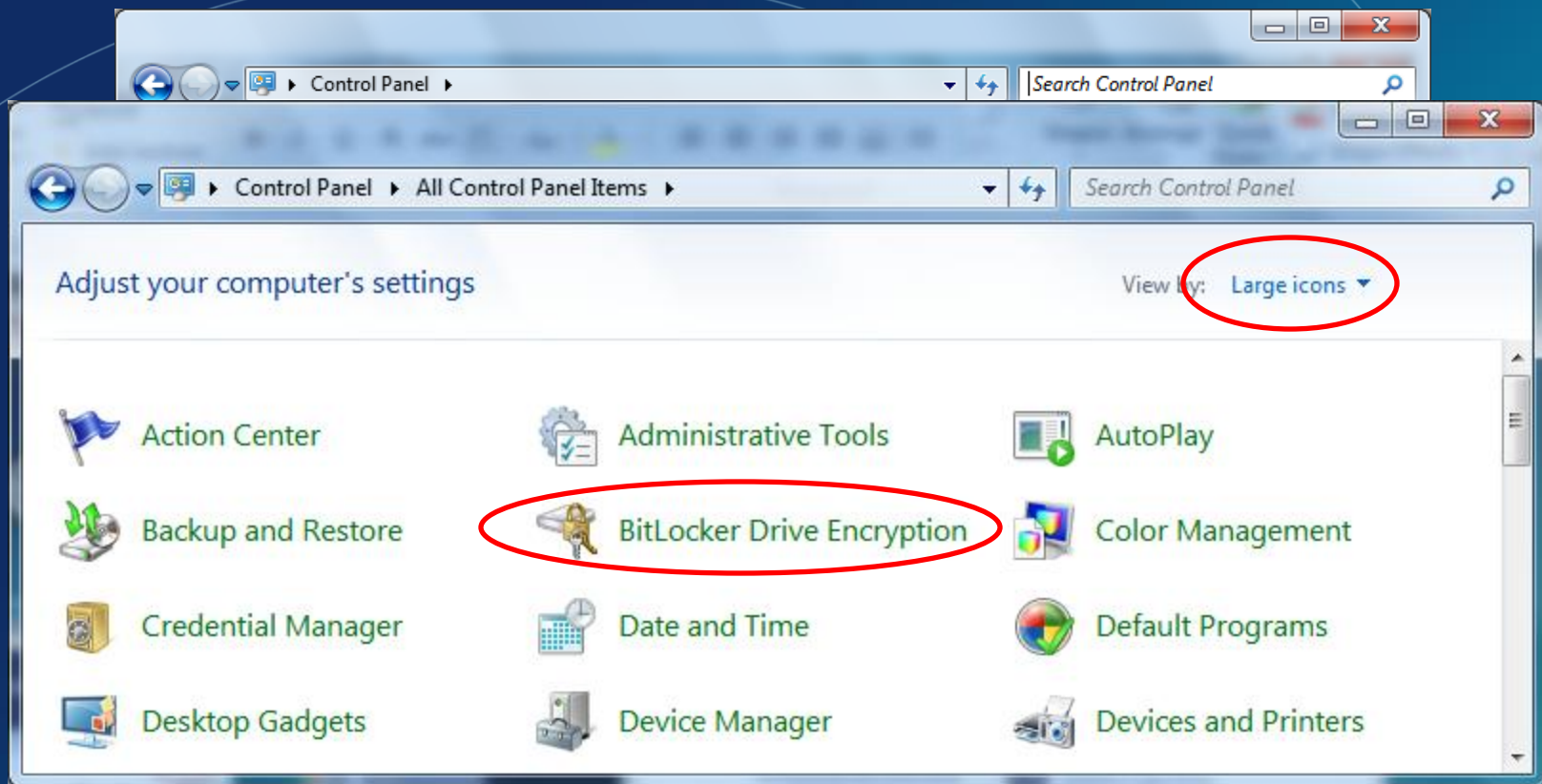
Enabling BitLocker - OS



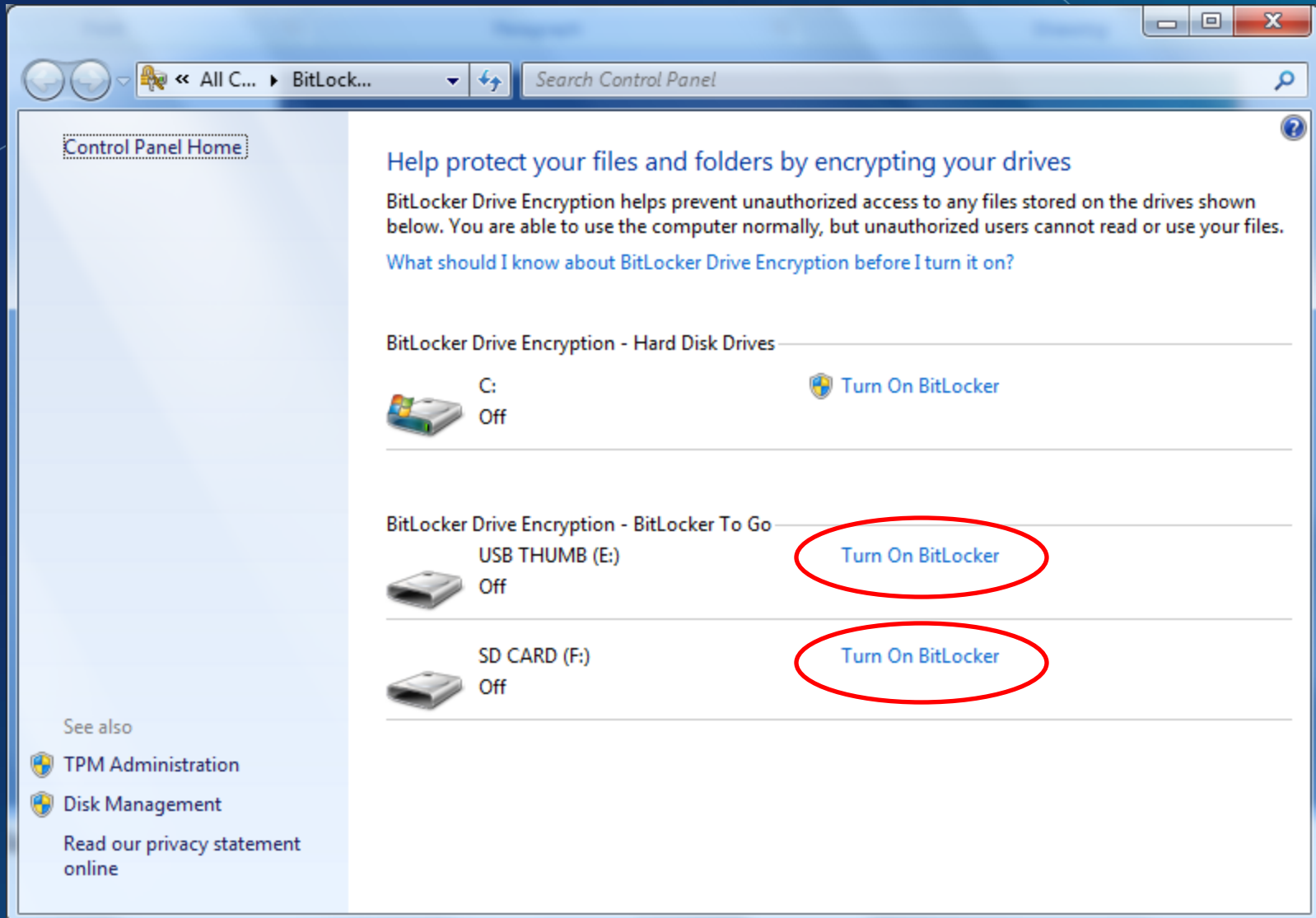
Enabling BitLocker “To Go”



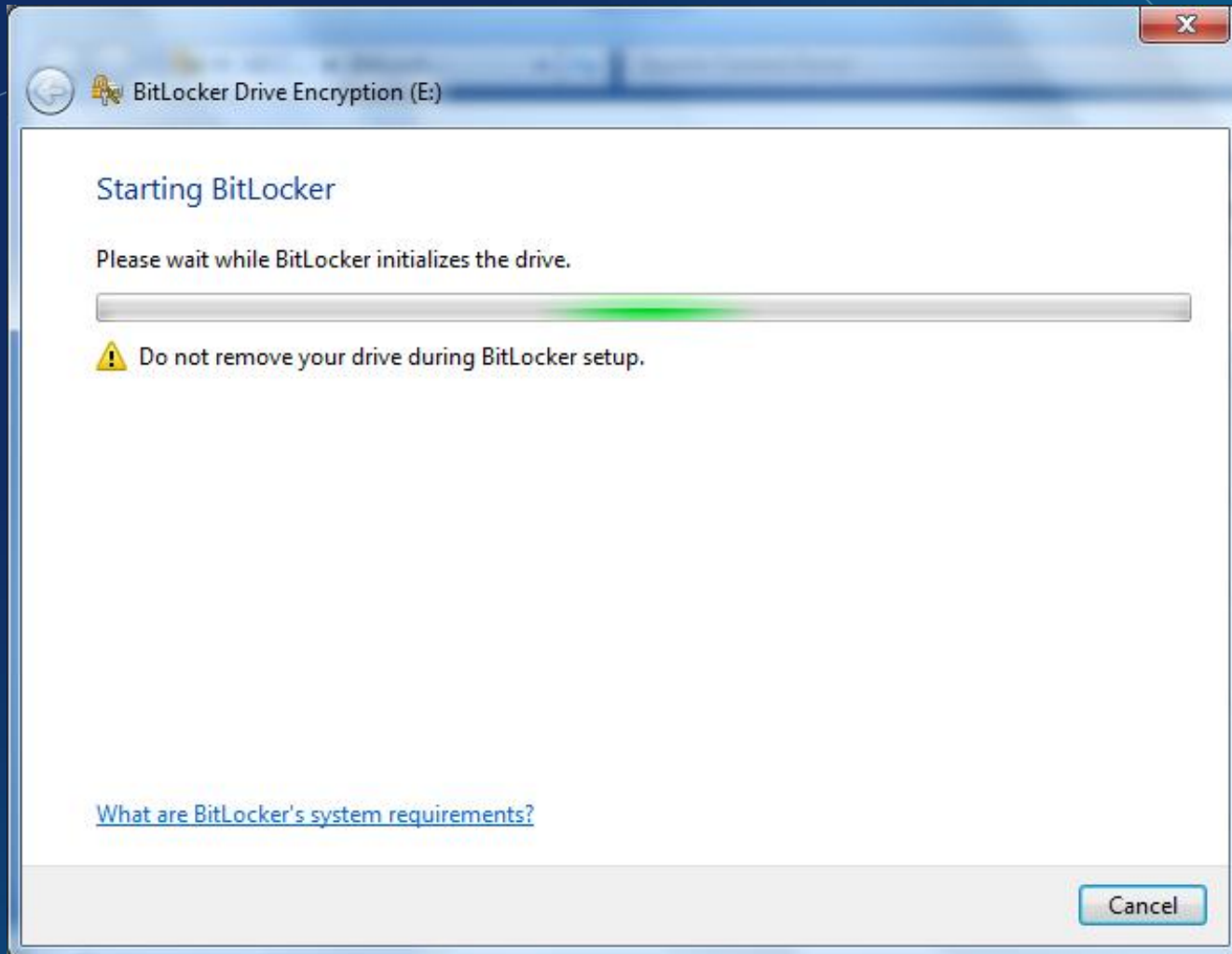
Enabling BitLocker of USB Stick



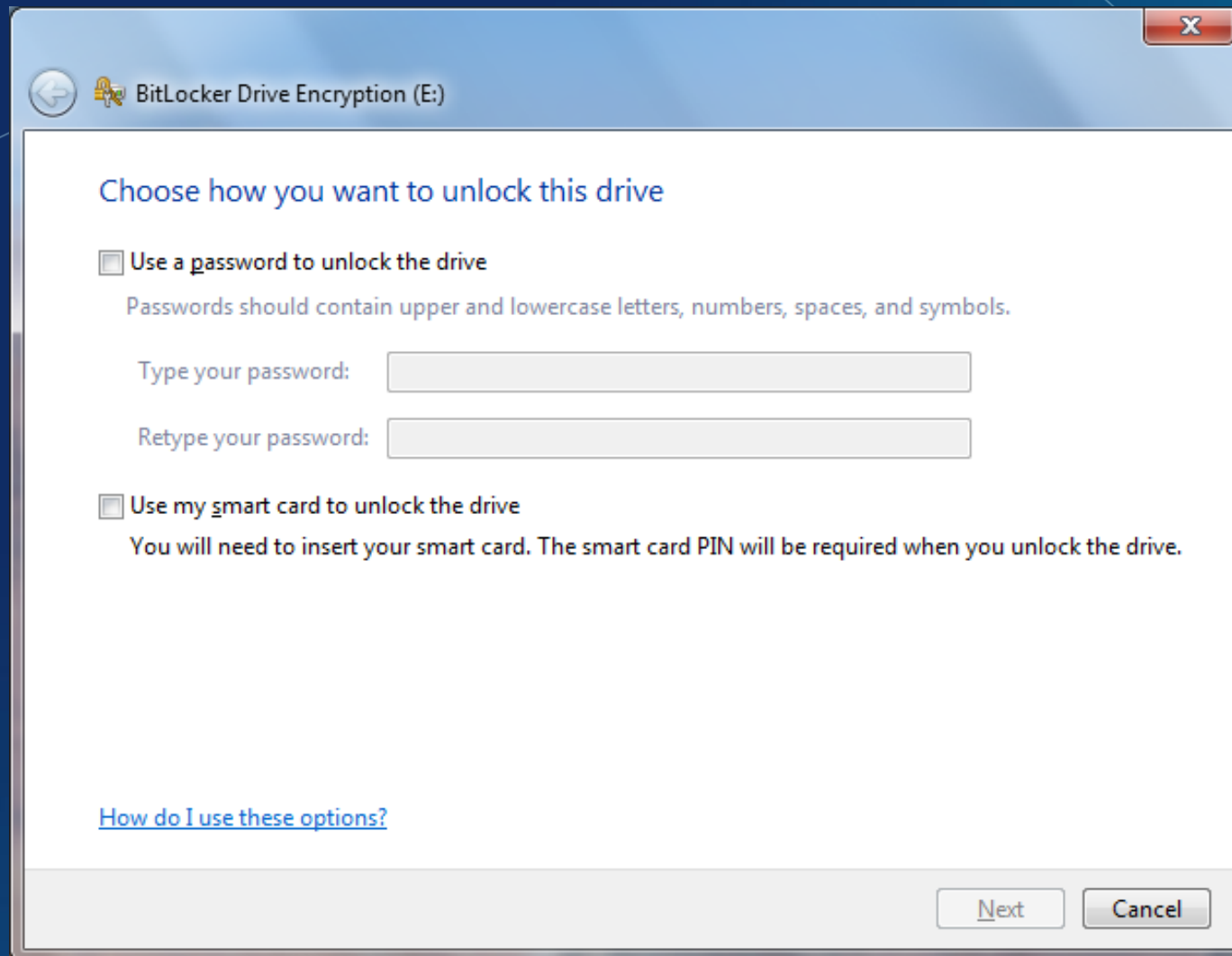
Enabling BitLocker of USB Stick



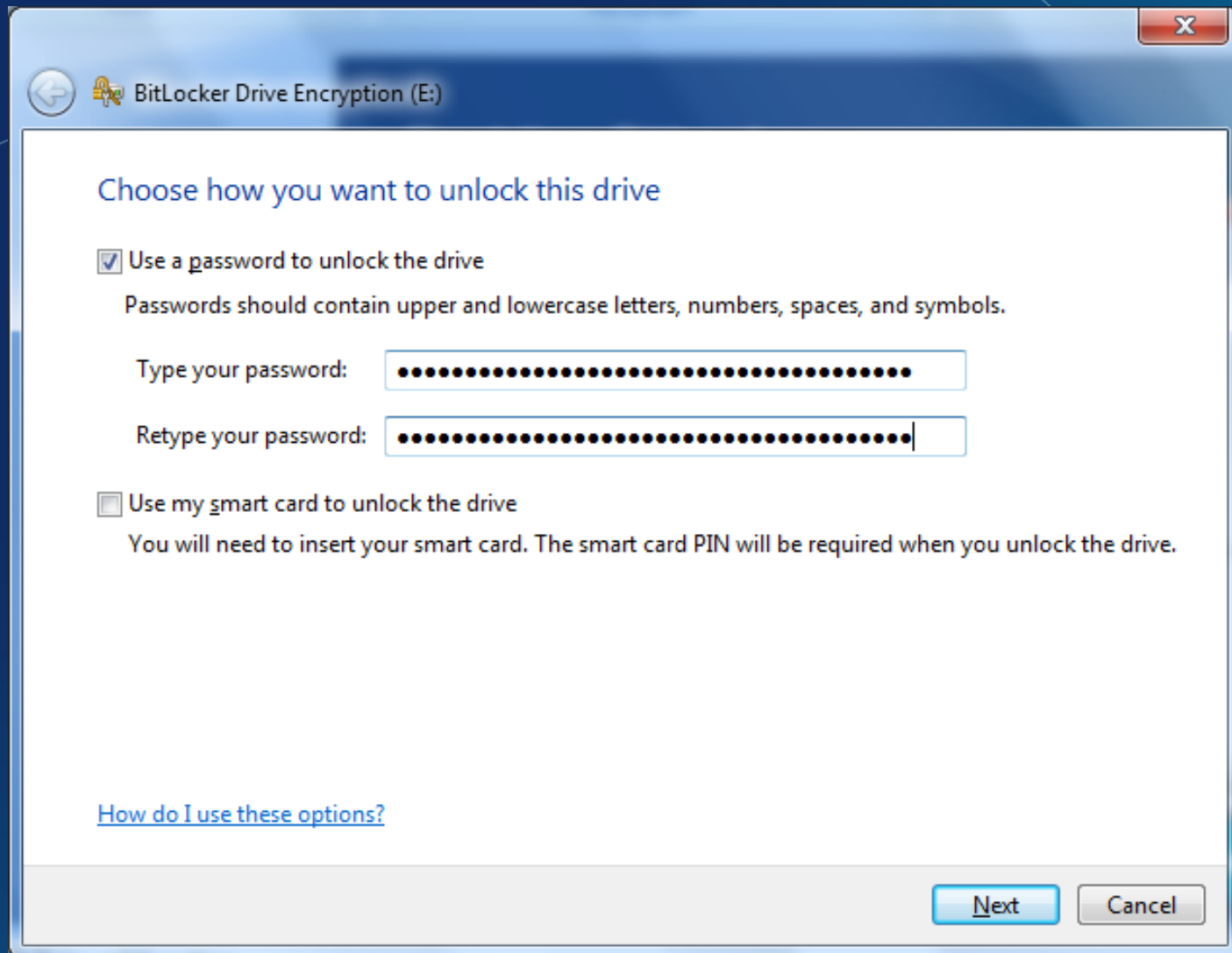
Enabling BitLocker of USB Stick



Enabling BitLocker of USB Stick



Enabling BitLocker of USB Stick



BitLocker Drive Encryption (E:)

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:

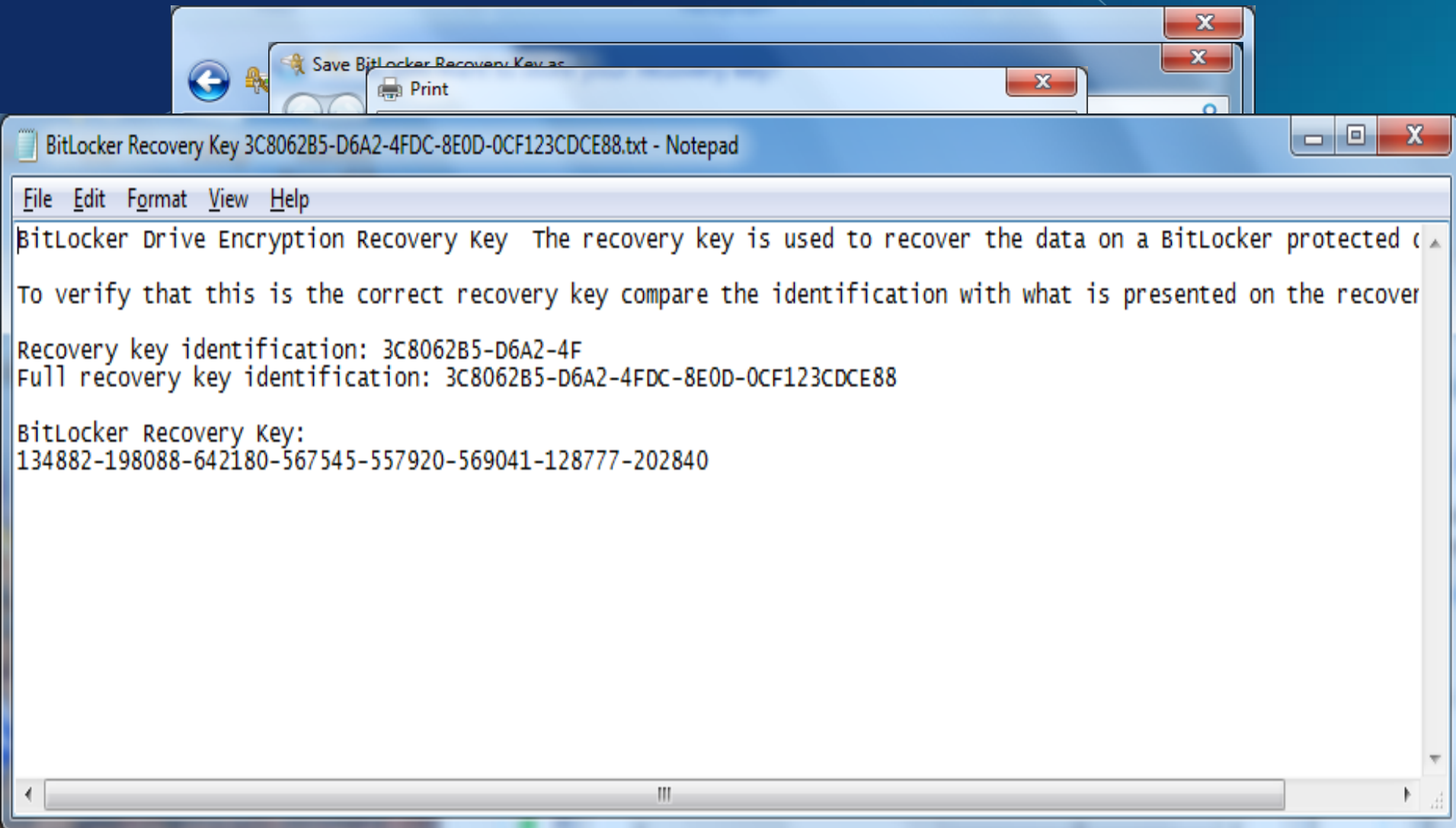
☐ Use my smart card to unlock the drive

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

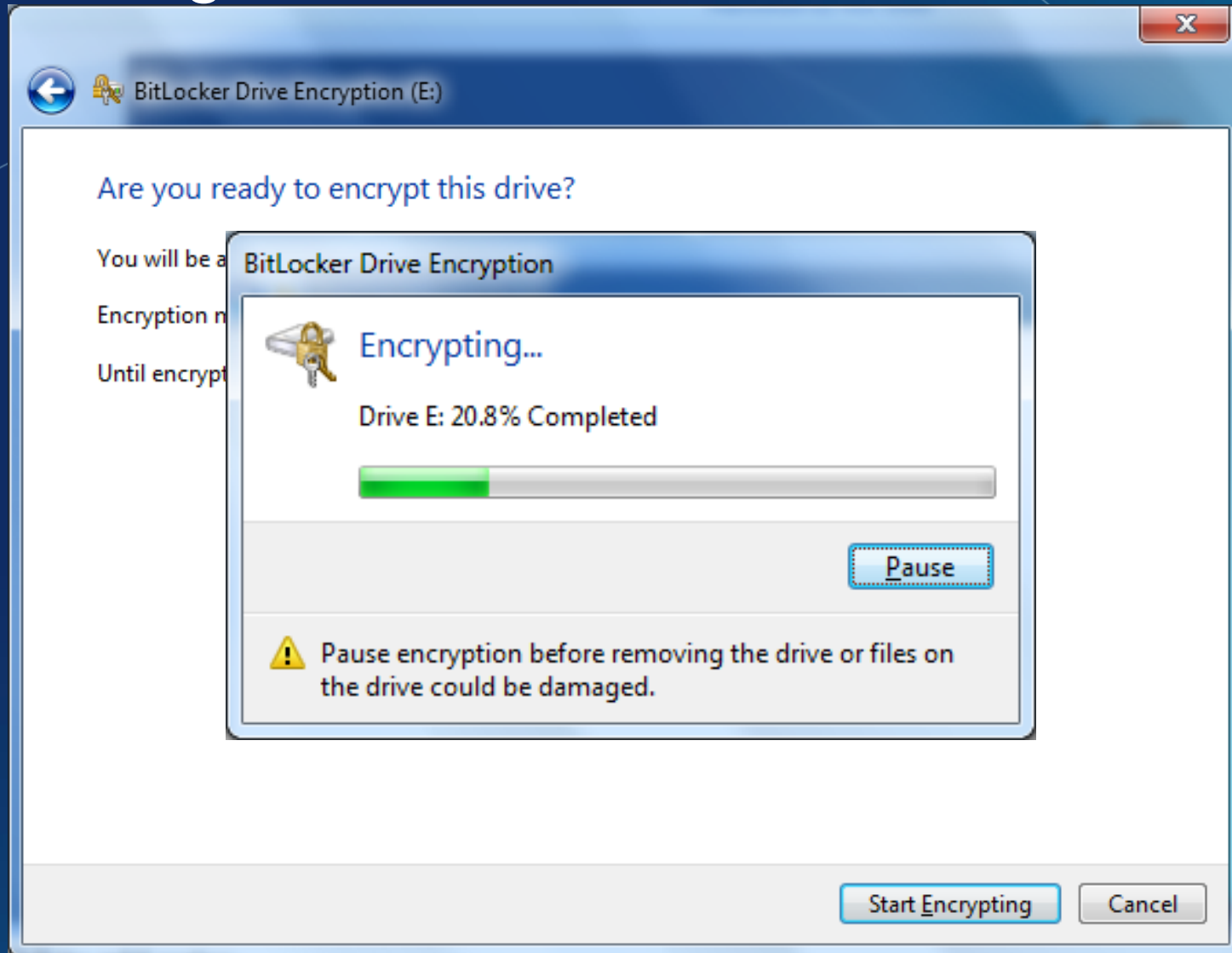
[How do I use these options?](#)

Next Cancel

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

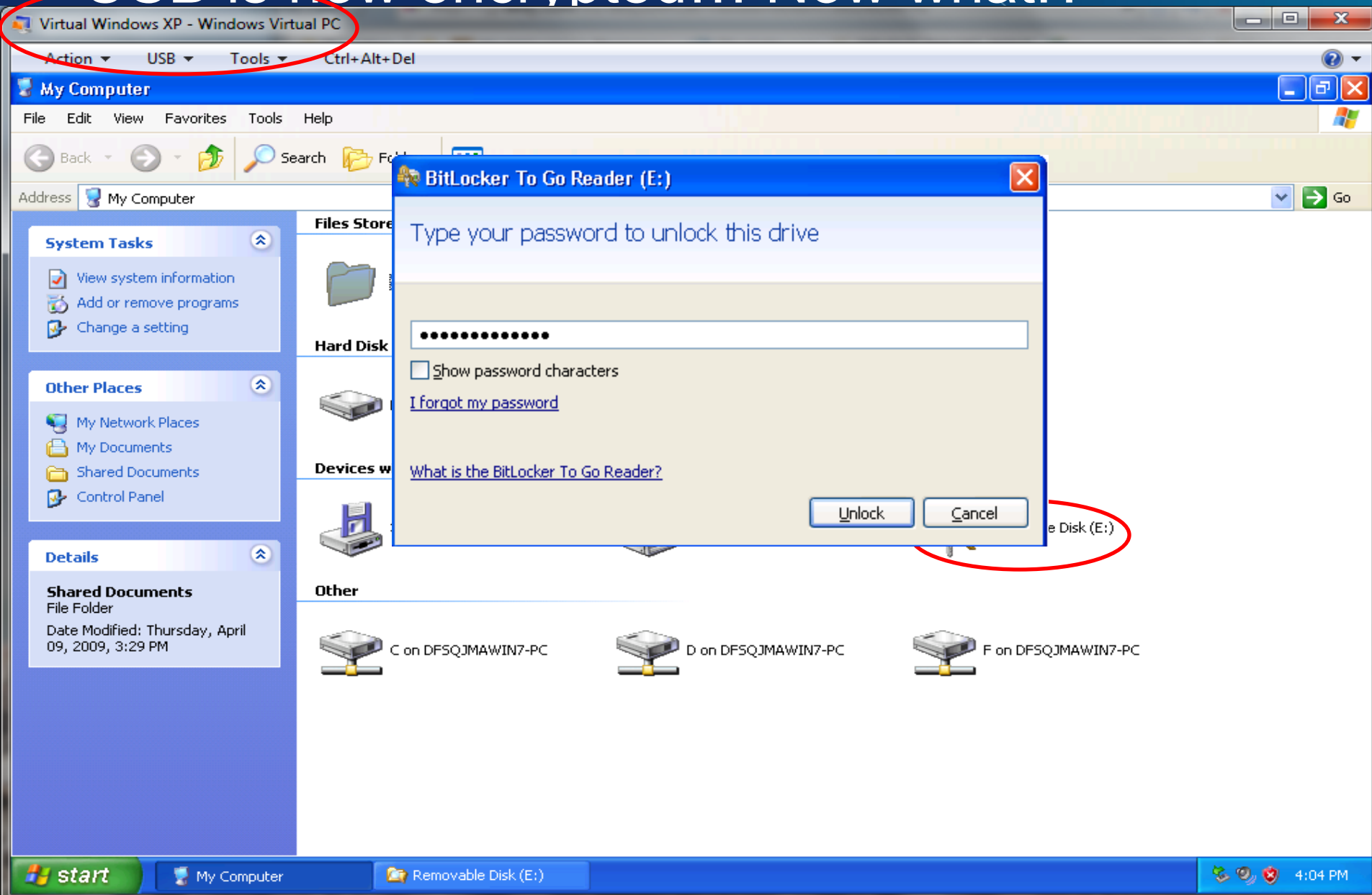


NOTE: The device can be unlocked on any Bitlocker To Go capable PC if you know the password

USB is now encrypted... Now what!?

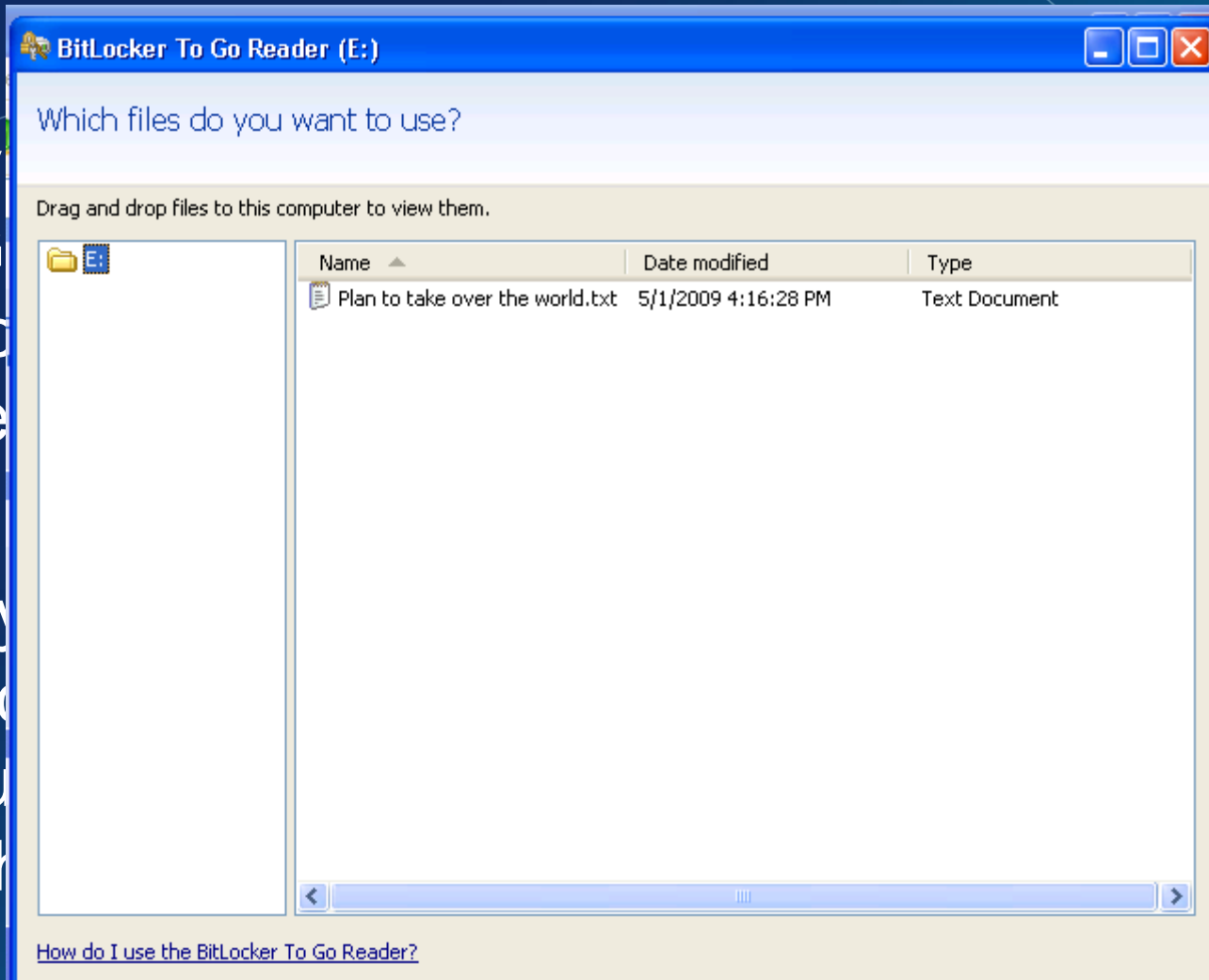
- If the encrypted USB is formatted with FAT then it can be used on down level Operating Systems
 - Win XP
 - Windows Vista
- How is this possible? These Operating Systems did not have Bitlocker to go functionality.

USB is now encrypted... Now what!?



USB is now encrypted... Now what!?

- Previous To Go BitLocker drive
- This encryption and feature machine



BitLocker

ed

Back the

ad

ill

7

BitLocker Technical Details

Exploration of Windows 7

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?

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

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

Mounting BitLocker Protected Volumes

Exploration of Windows 7

Requirements

- 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

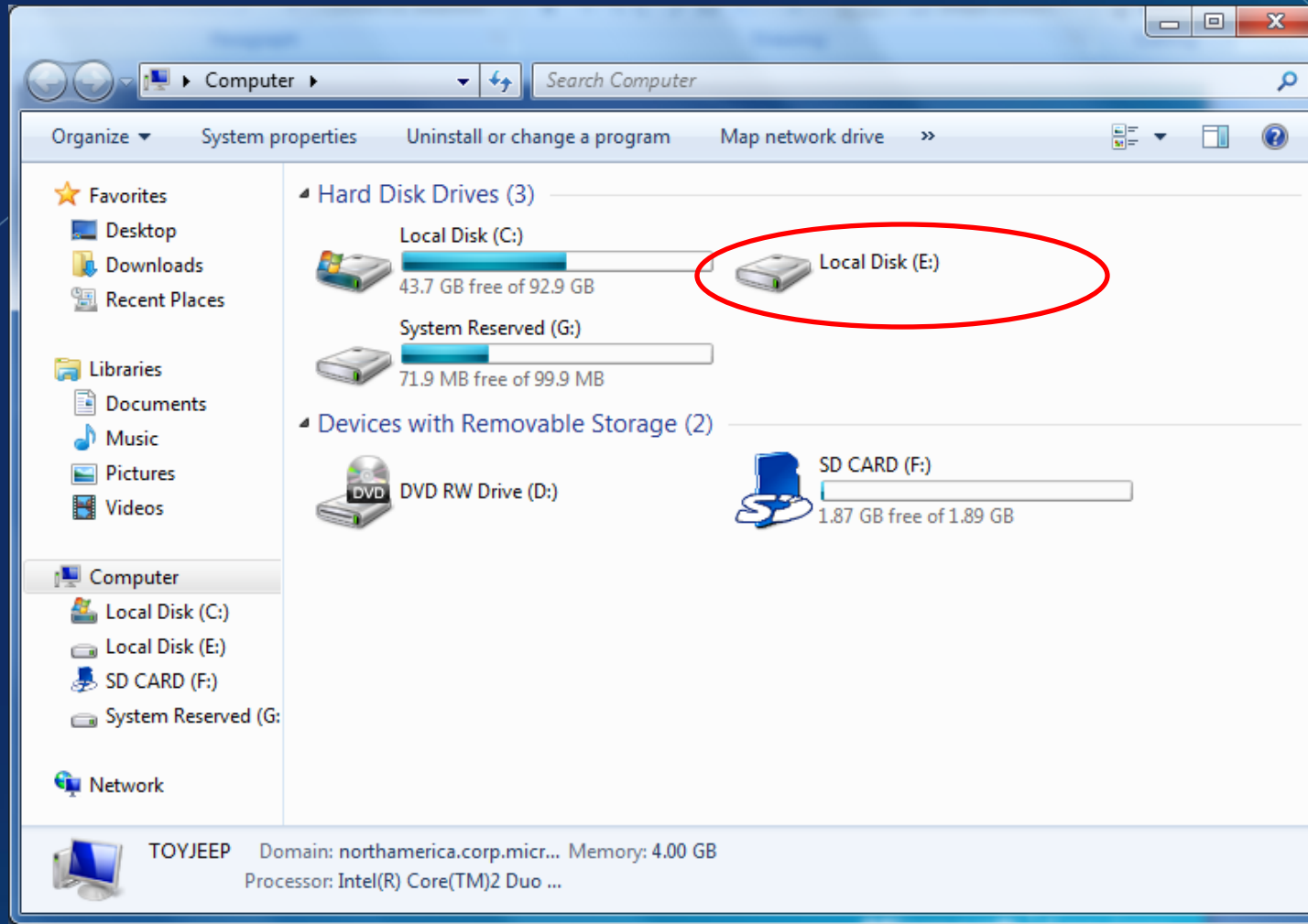
- Investigators can use the recovery mechanisms built into the BitLocker mechanism to access the protected drive
- Just like EFS

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

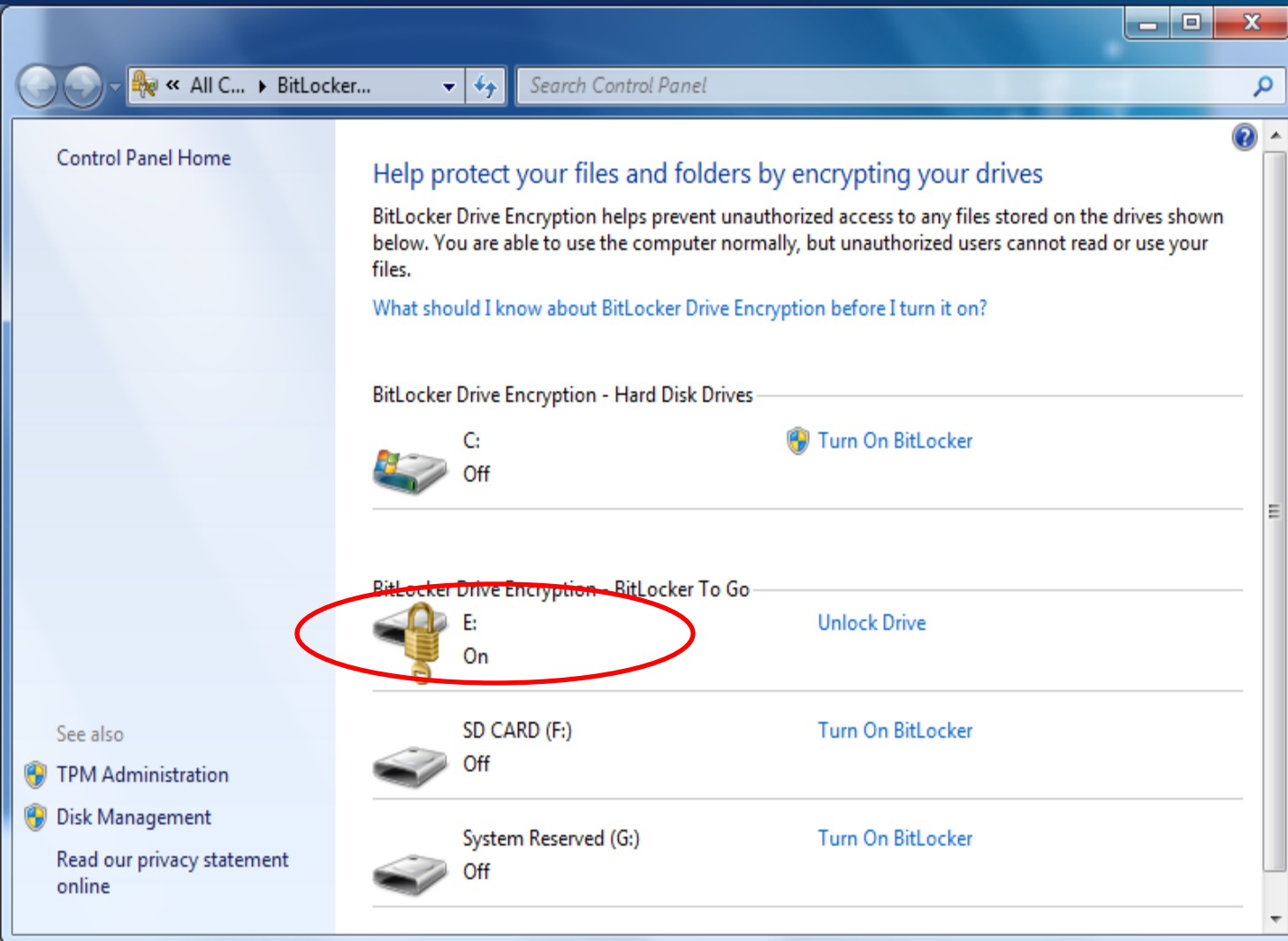
Mounting a BitLocker Drive



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

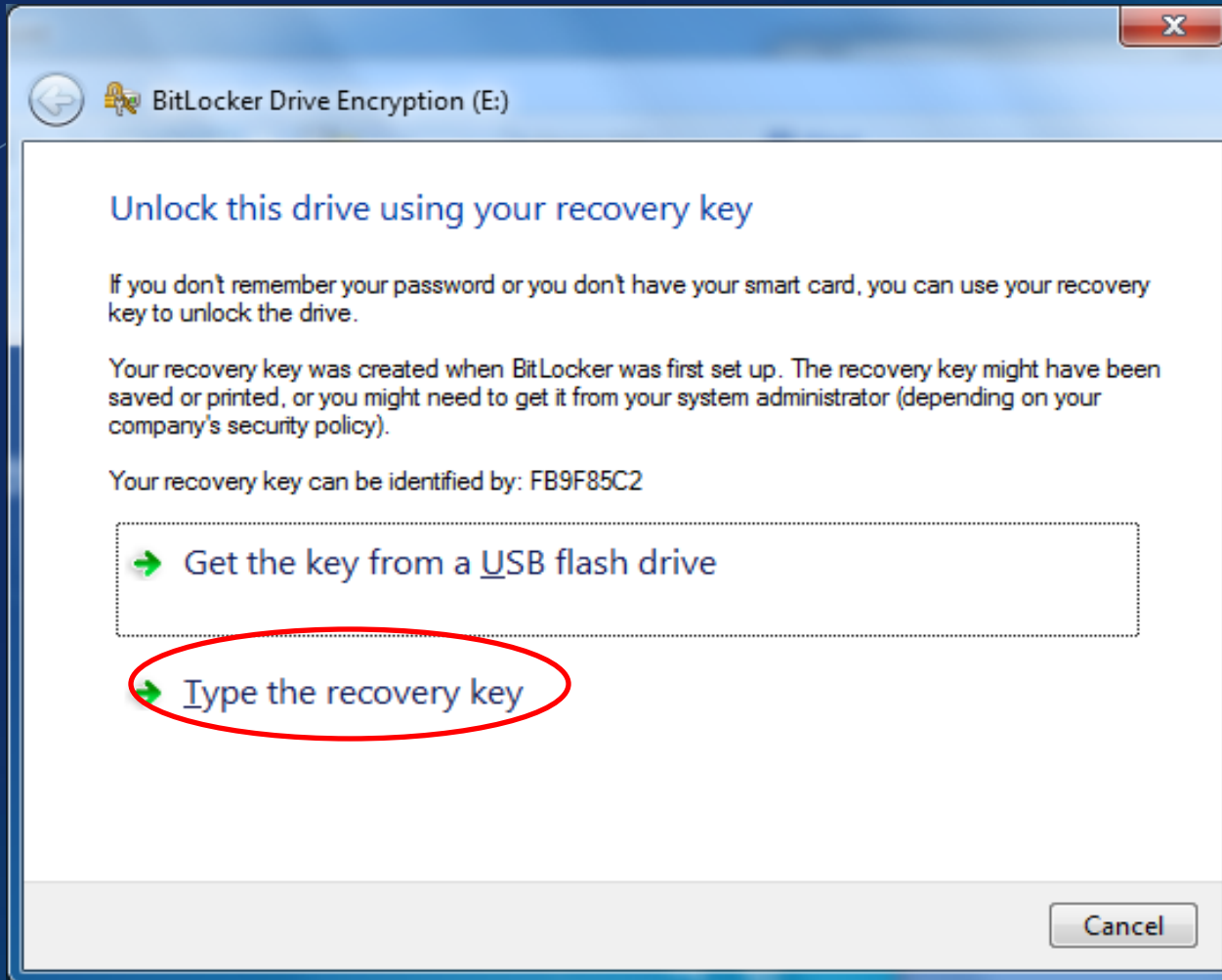
Mounting a BitLocker Drive

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

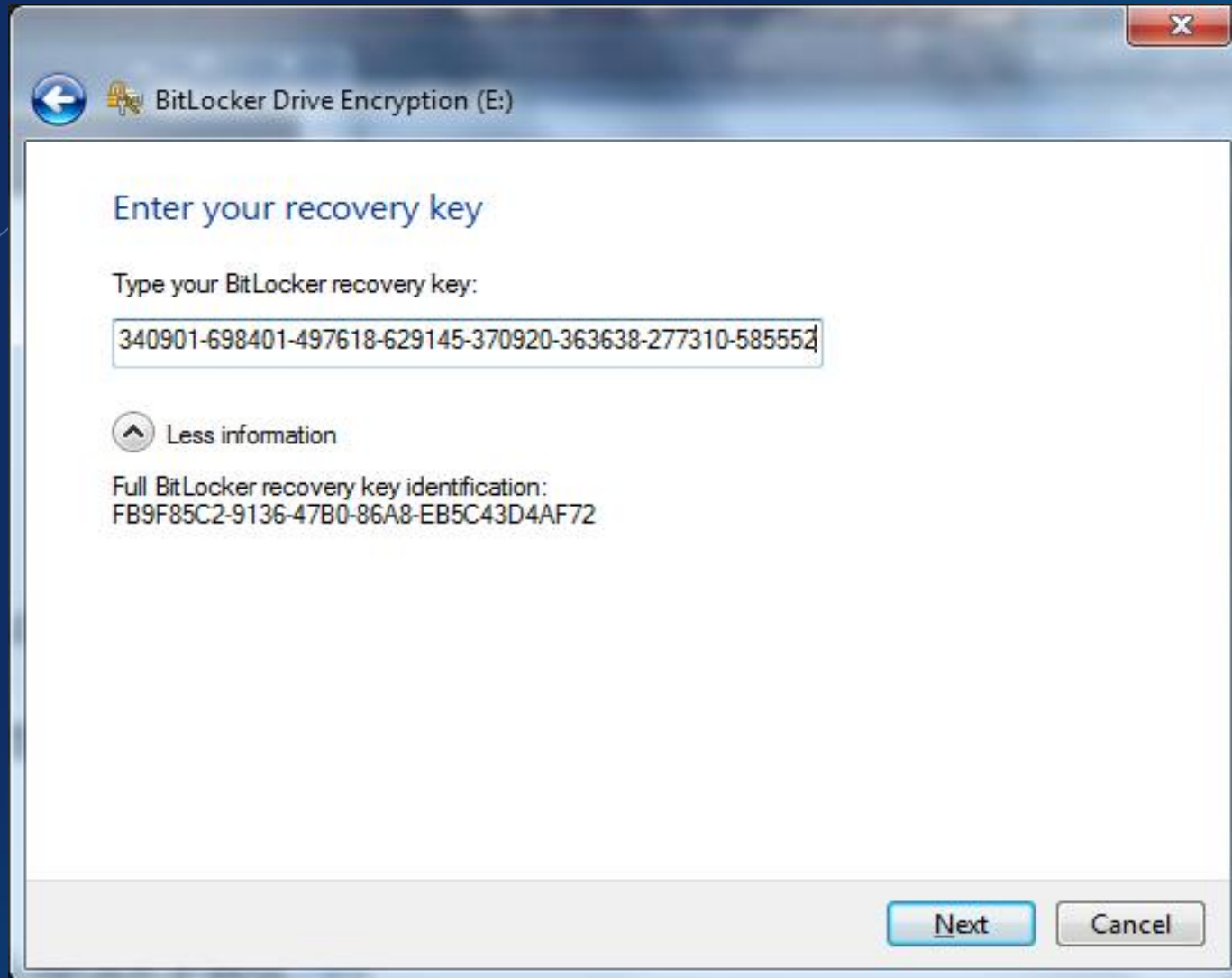


Mounting a BitLocker Drive

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



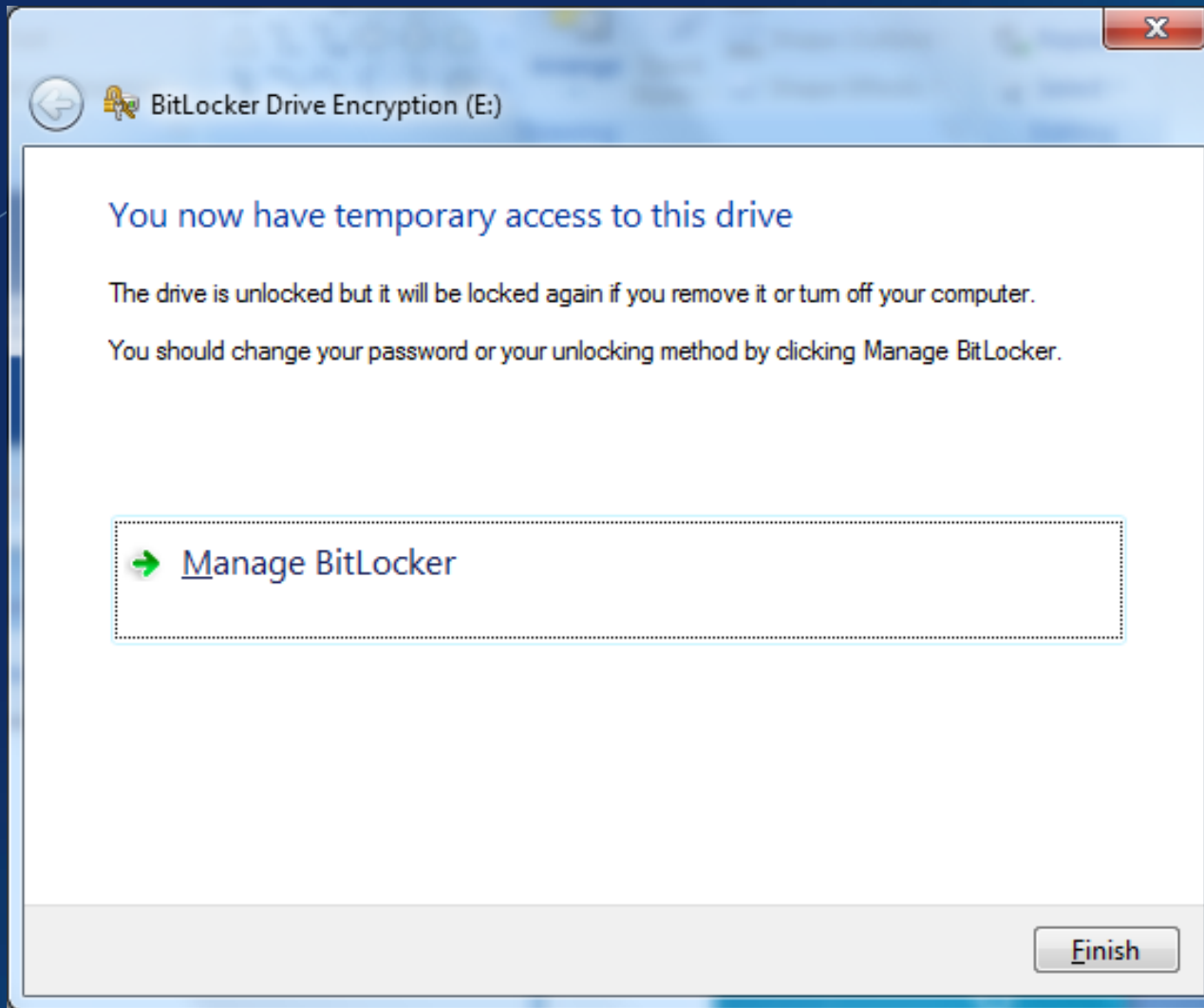
Mounting a BitLocker Drive



The screenshot shows a Windows dialog box titled "BitLocker Drive Encryption (E:)". Inside the dialog, the text "Enter your recovery key" is displayed. Below this, a label reads "Type your BitLocker recovery key:". A text input field contains the recovery key: "340901-698401-497618-629145-370920-363638-277310-585552". Below the input field, there is a link that says "Less information" with an upward-pointing arrow icon. At the bottom of the dialog, there are two buttons: "Next" and "Cancel".

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

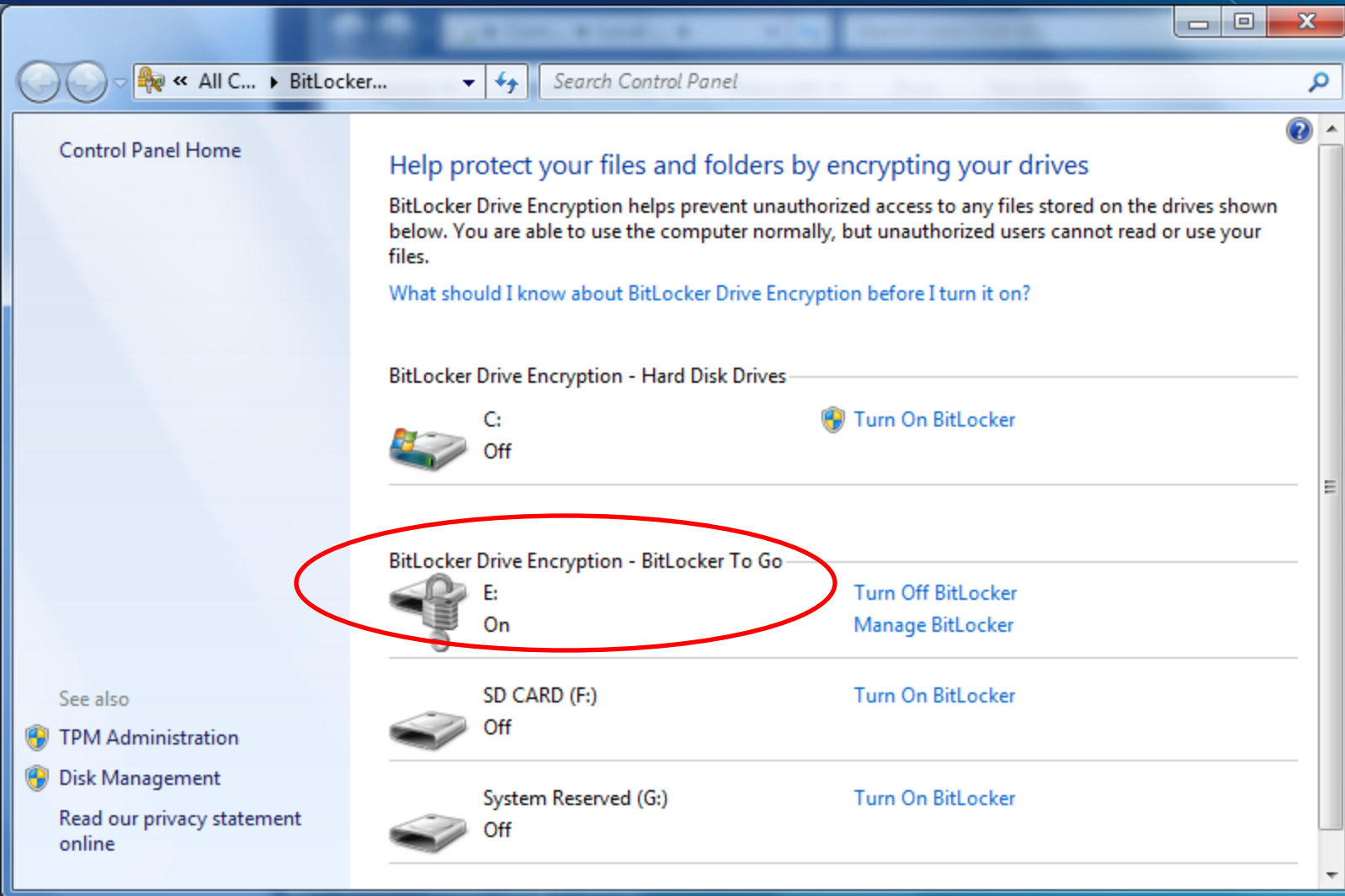
Mounting a BitLocker Drive



- “You can now temporarily access this drive”

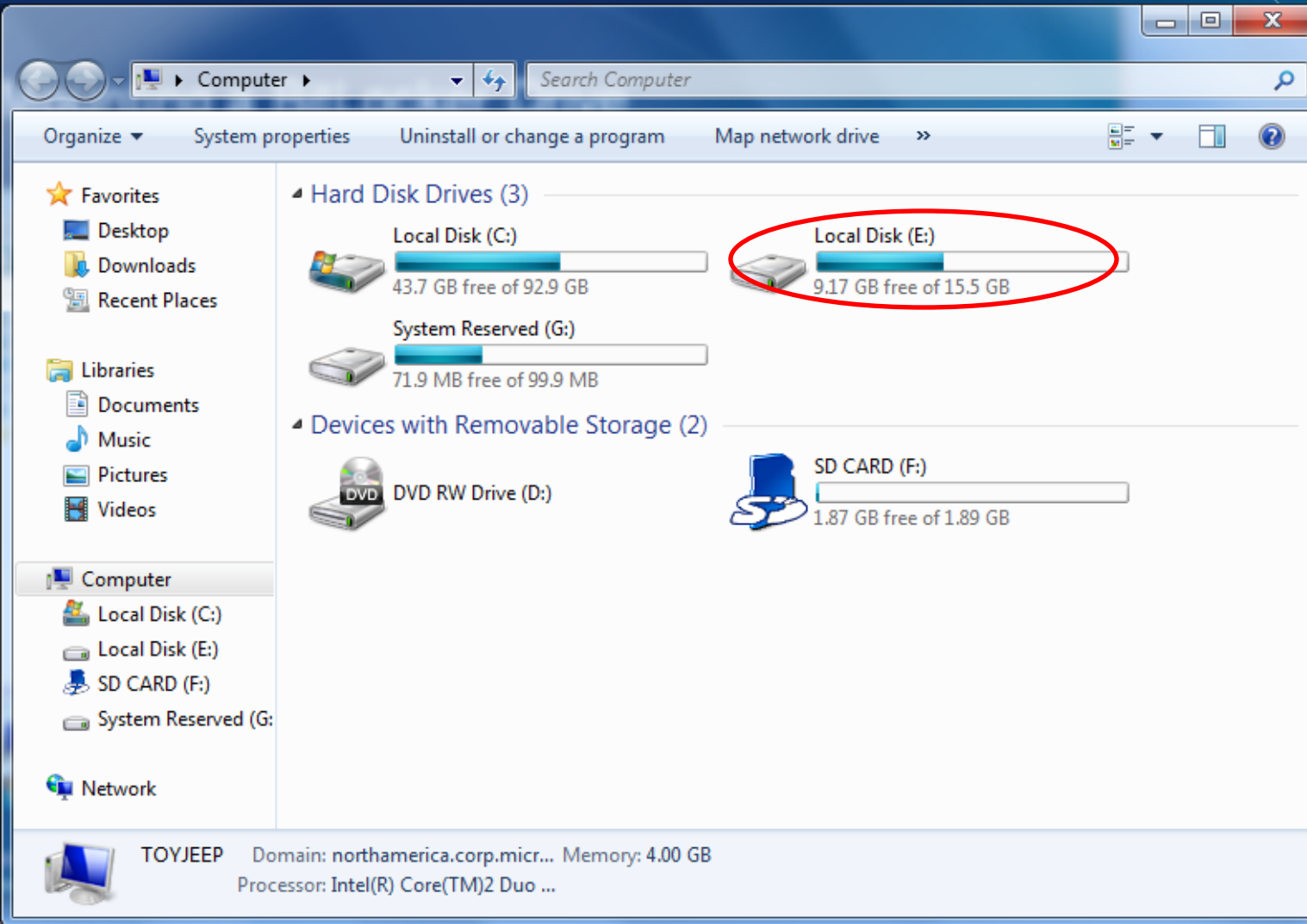
Mounting a BitLocker Drive

- Granted access to a BitLocker protected drive!



Mounting a BitLocker Drive

- Drive details are now available and we can process the drive



Dealing with BitLocker on a Live System

Exploration of Windows 7

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
```

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