Introduction to the Volume Shadow Copy Service

Exploration of Windows 7
Advanced Forensic Topics – Day 2

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Data Integrity in Windows 7

- Volume Shadow Copy Service
- Expanded feature set in Vista:
  - Backup and Restore Center
  - System Restore
  - Previous Versions
  - System Image Backup

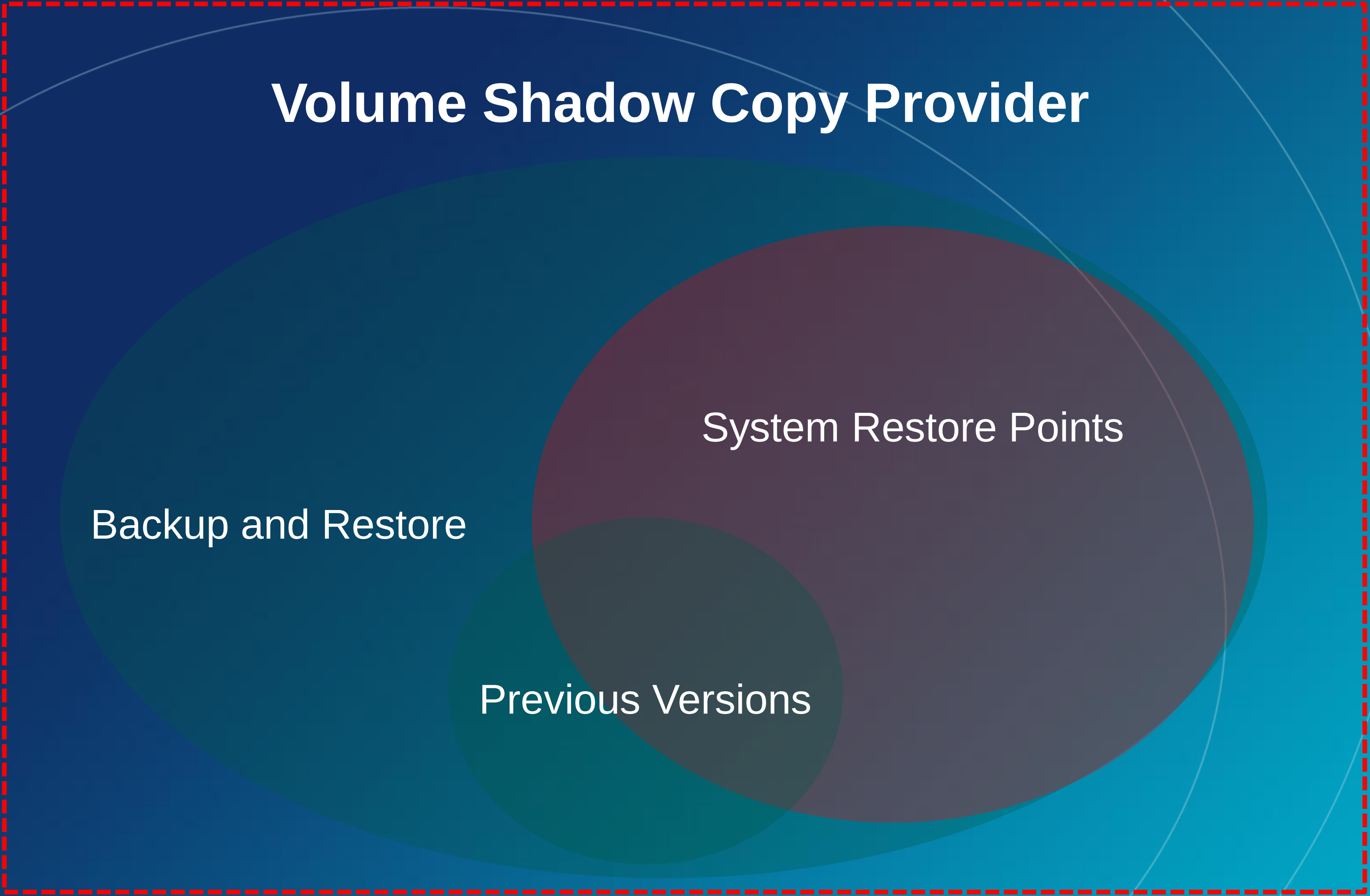
Data Integrity in Windows 7

- Shadow Copy can be used in conjunction with the Windows Recovery Environment (WinRE) to “restore” a non-bootable system to a bootable state

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

Data Integrity in Vista



Volume Shadow Copy Provider

Backup and Restore

System Restore Points

Previous Versions

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

Microsoft | Services

Forensic Investigation Topics for Windows 7

Volume Shadow Copy Implementations in Windows 7

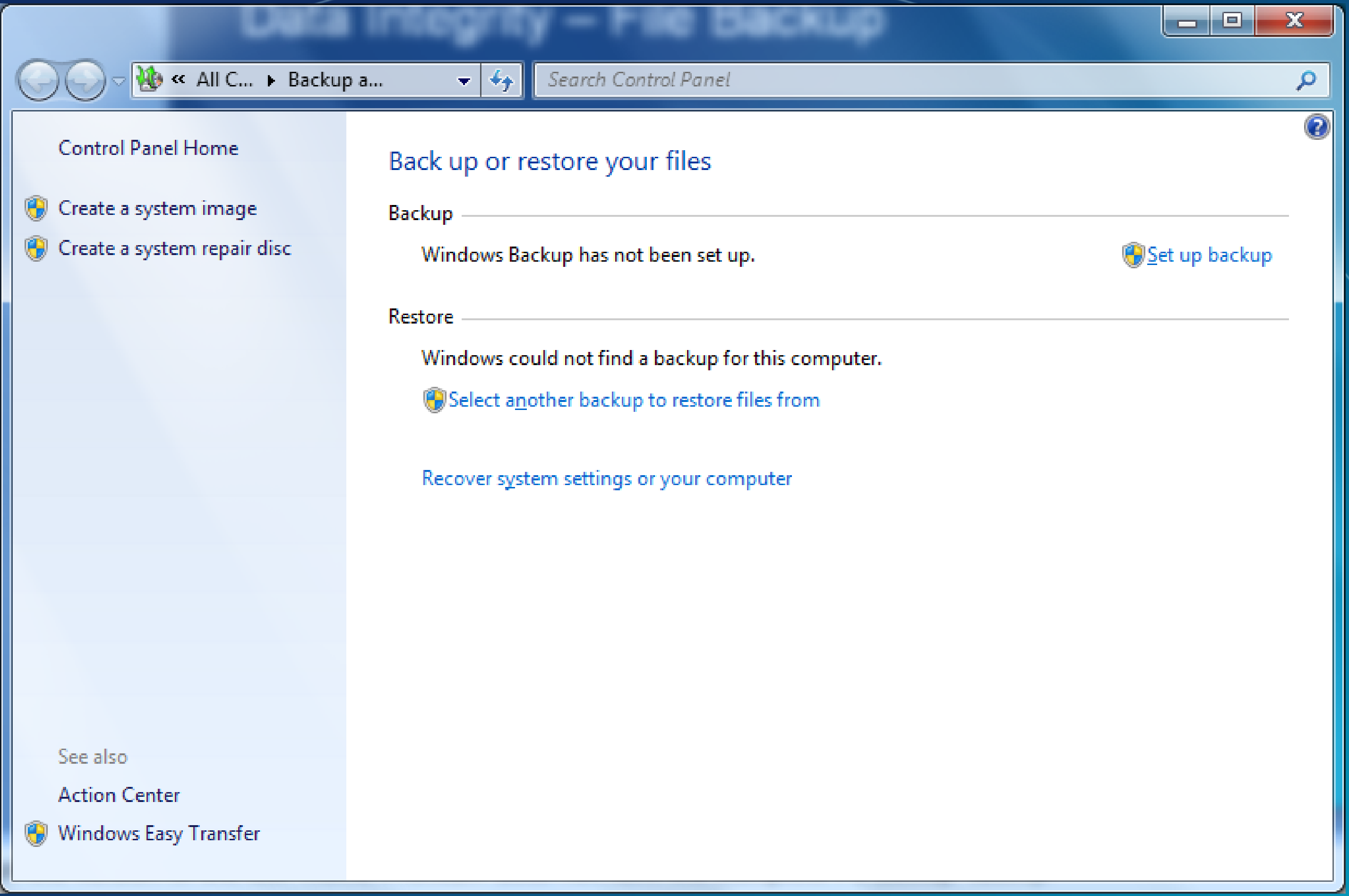
LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

Forensic Investigation Topics for Windows 7

File Backup Using Volume Shadow Copy

Data Integrity – File Backup



Control Panel Home

Create a system image

Create a system repair disc

See also

Action Center

Windows Easy Transfer

Back up or restore your files

Backup

Windows Backup has not been set up.

Set up backup

Restore

Windows could not find a backup for this computer.

Select another backup to restore files from

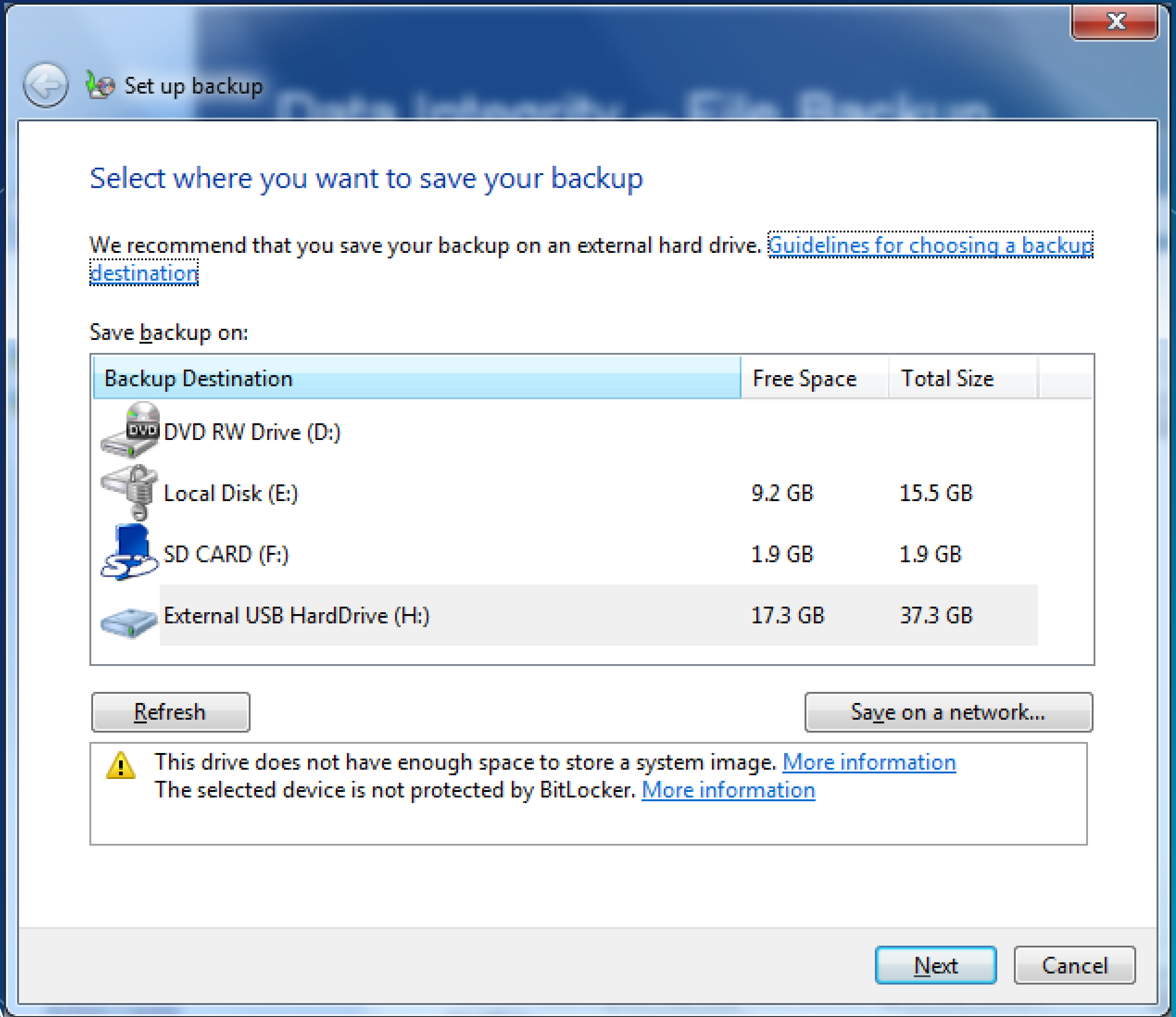
Recover system settings or your computer

Backup and Restore Center in the Control Panel

Data Integrity – File Backup

- Backup Files Settings
  - Backup Files
    - >Backups up all files on the system
    - >Media supported: CD, DVD, Hard Disk, Network
  - Files that are not backup up include:
    - >EFS encrypted files
    - >System files
    - >Program files
    - >Recycle bin
    - >Temporary files

Data Integrity – File Backup



Select where you want to save your backup

We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

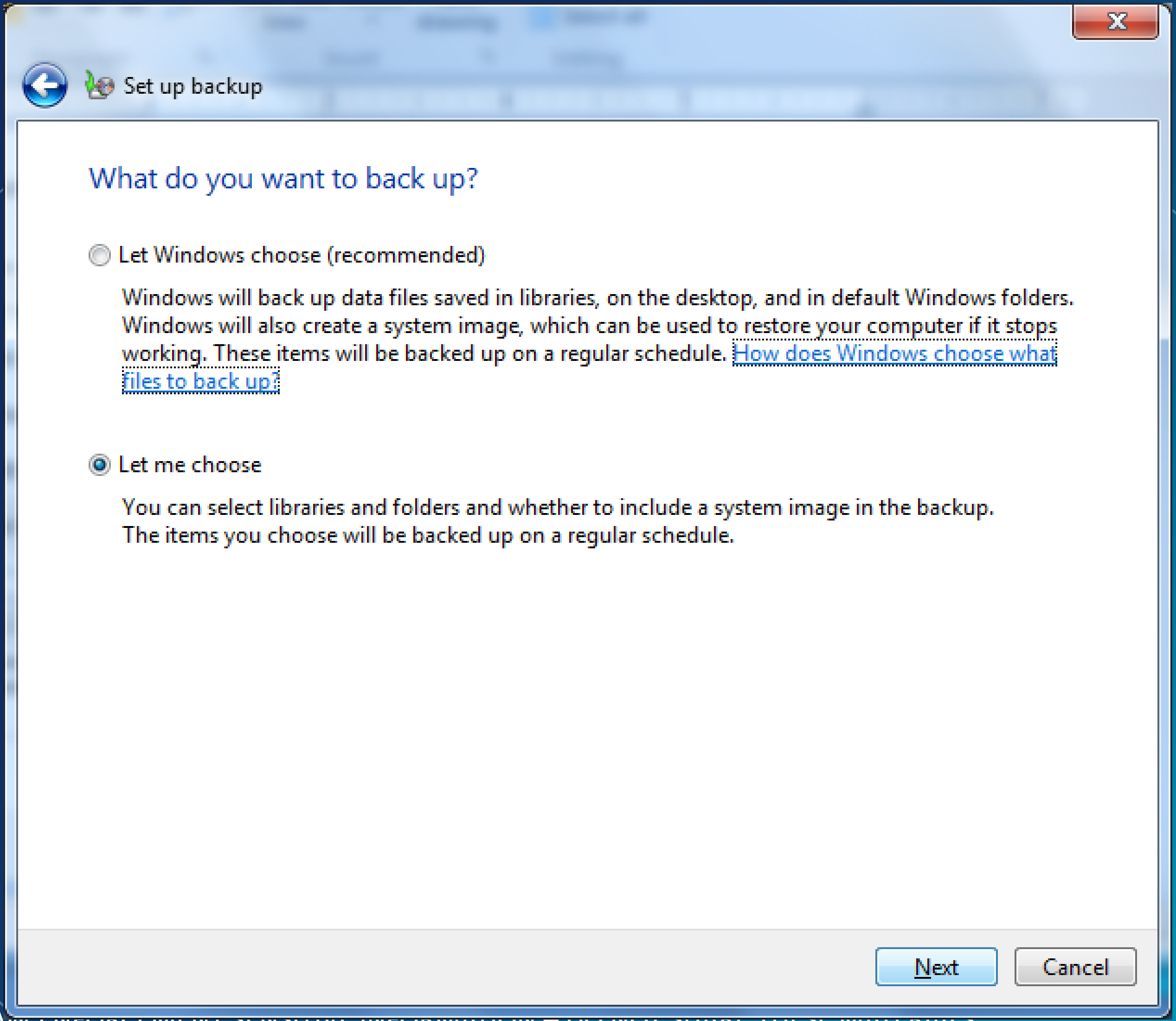
Save backup on:

Backup Destination	Free Space	Total Size
DVD RW Drive (D:)		
Local Disk (E:)	9.2 GB	15.5 GB
SD CARD (F:)	1.9 GB	1.9 GB
External USB HardDrive (H:)	17.3 GB	37.3 GB

⚠ This drive does not have enough space to store a system image. More information
The selected device is not protected by BitLocker. More information

- The Backup file wizards starts with the selection of the backup destination.

Data Integrity – File Backup



Set up backup

What do you want to back up?

○ Let Windows choose (recommended)

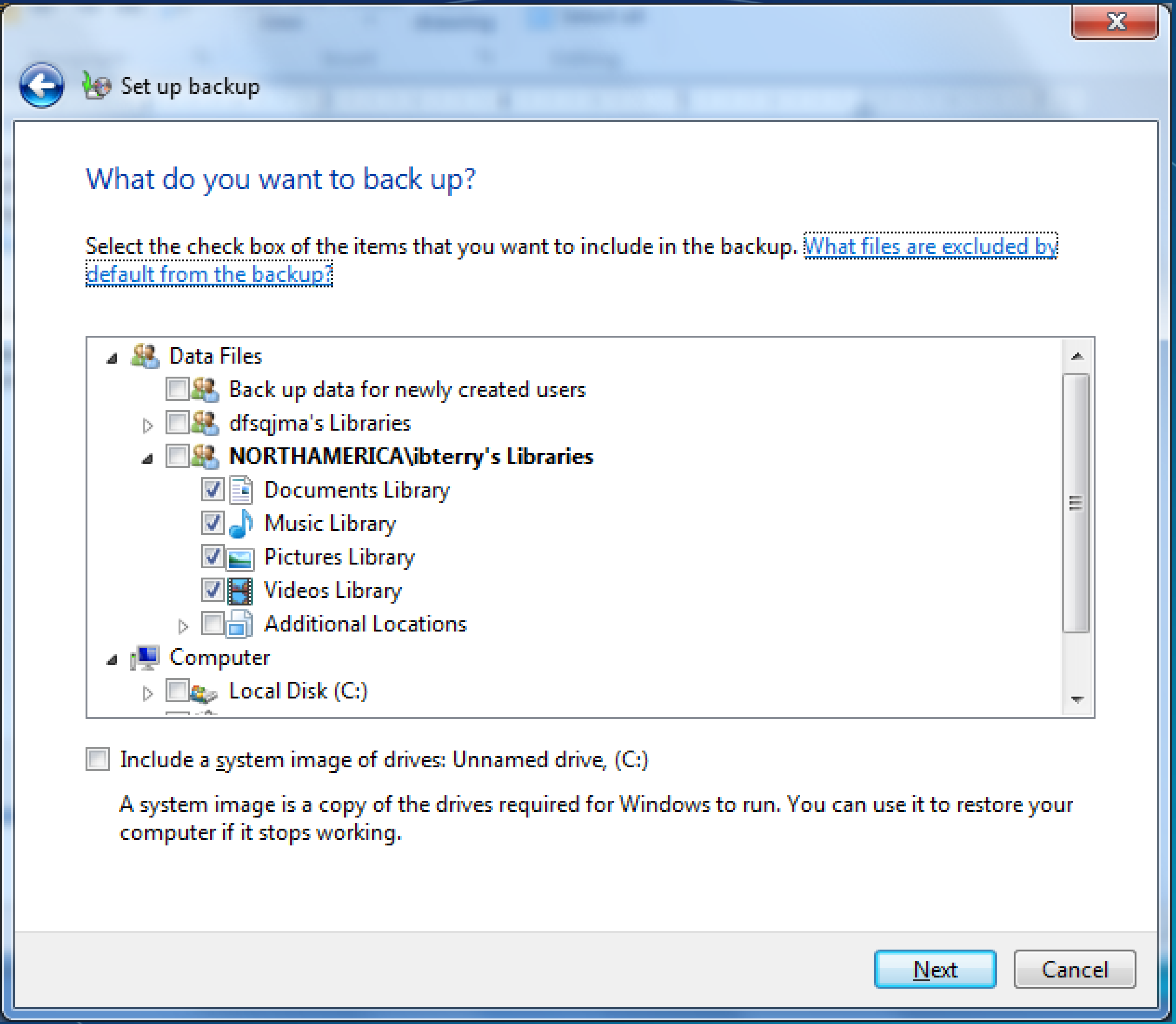
Windows will back up data files saved in libraries, on the desktop, and in default Windows folders. Windows will also create a system image, which can be used to restore your computer if it stops working. These items will be backed up on a regular schedule. How does Windows choose what files to back up?

● Let me choose

You can select libraries and folders and whether to include a system image in the backup. The items you choose will be backed up on a regular schedule.

- Notice you can allow Windows to choose what to backup or you can manually select what should be backed up.

Data Integrity – File Backup



What do you want to back up?

Select the check box of the items that you want to include in the backup. What files are excluded by default from the backup?

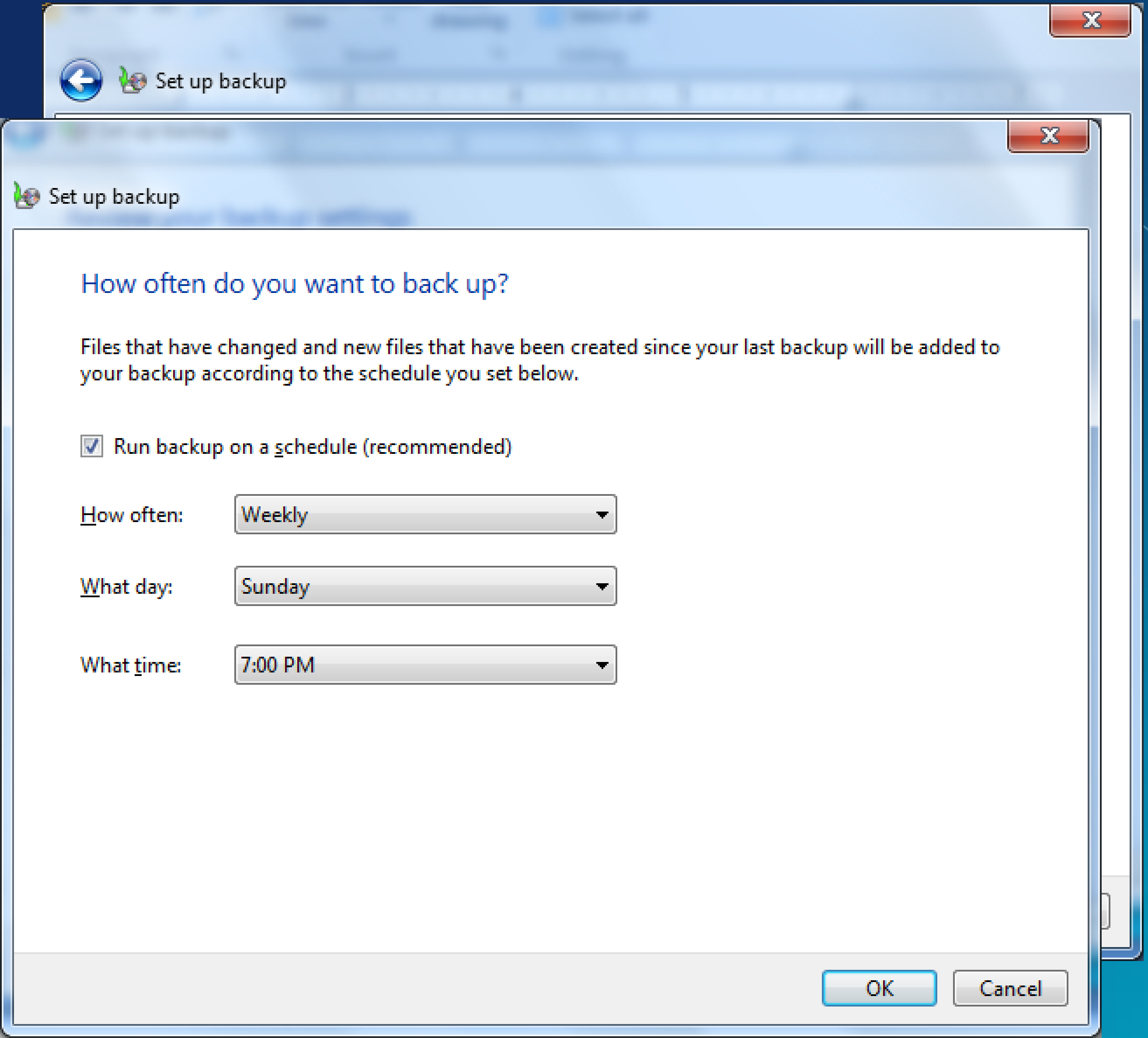
- Data Files
  - □ Back up data for newly created users
  - □ dfsqjma's Libraries
  - □ **NORTHAMERICA\ibterry's Libraries**
    - ☑ Documents Library
    - ☑ Music Library
    - ☑ Pictures Library
    - ☑ Videos Library
    - □ Additional Locations
- Computer
  - □ Local Disk (C:)

□ Include a system image of drives: Unnamed drive, (C:)

A system image is a copy of the drives required for Windows to run. You can use it to restore your computer if it stops working.

- The wizard makes it easy to backup data in user profiles or select data in other locations on the PC.

Data Integrity – File Backup



How often do you want to back up?

Files that have changed and new files that have been created since your last backup will be added to your backup according to the schedule you set below.

☑ Run backup on a schedule (recommended)

How often: Weekly

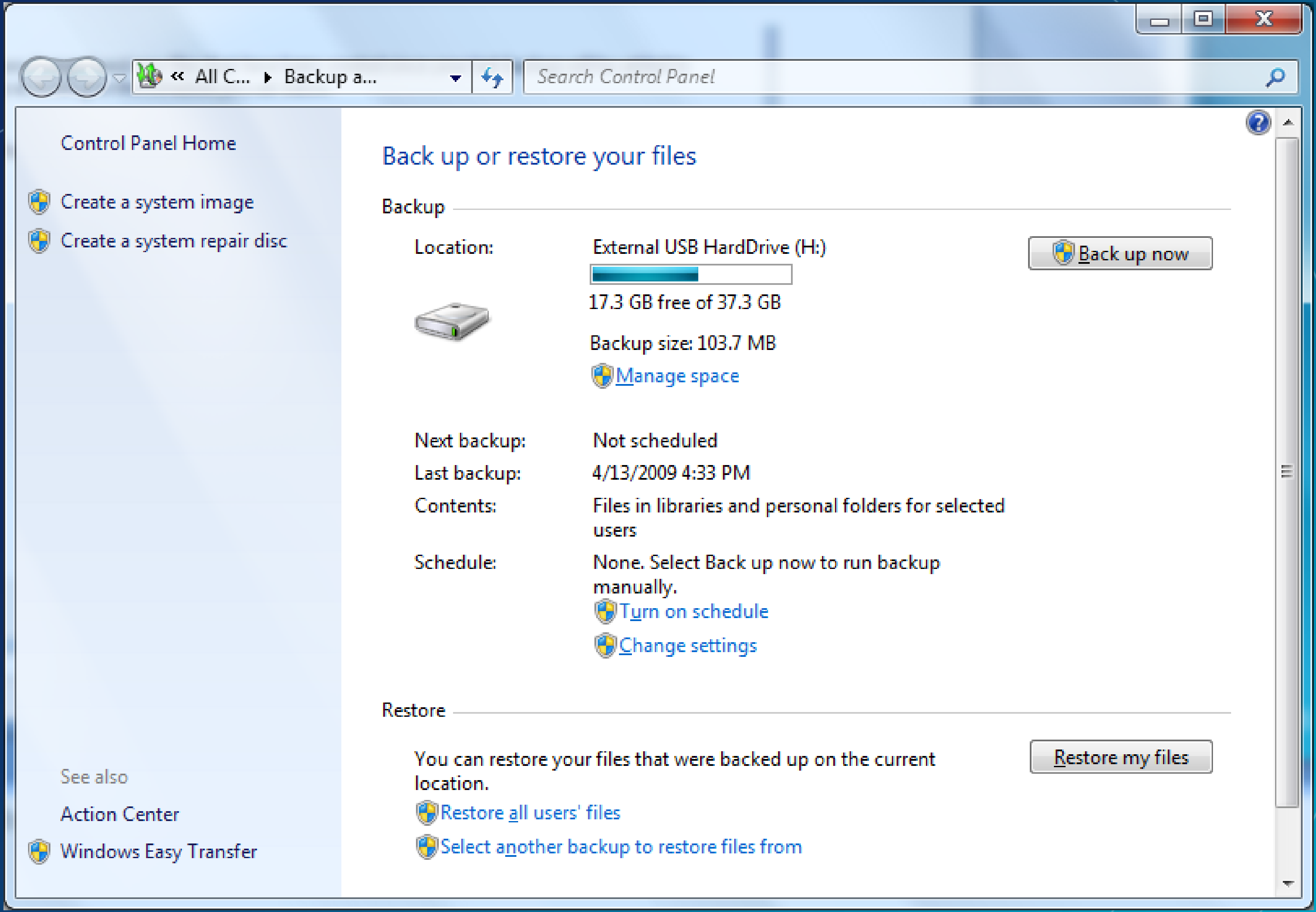
What day: Sunday

What time: 7:00 PM

- Shows what will be included in the backup. Also there is an option to create a reoccuring schedule for the backup.

Microsoft Services

Data Integrity – File Backup



Back up or restore your files

Backup

Location: External USB HardDrive (H:)

17.3 GB free of 37.3 GB

Backup size: 103.7 MB

Manage space

Next backup: Not scheduled

Last backup: 4/13/2009 4:33 PM

Contents: Files in libraries and personal folders for selected users

Schedule: None. Select Back up now to run backup manually.

Turn on schedule

Change settings

Restore

You can restore your files that were backed up on the current location.

Restore all users' files

Select another backup to restore files from

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft Services

Data Integrity – File Backup

- The file system is scanned for the required files that should be included in the backup set
- The files identified in the scan are backed up to the target media
- The backup is saved to a folder on the backup media in the name of the machine.

Data Integrity – File Backup

- Within the backup folder name after the machine there are additional folders
  - Backup files <year>-<month>-<day>-<HHMMSS>
    - >Backup files x.zip (where x is a simple integer)
    - >Each file contains a set of the actual backup up files
    - >Catalogs Folder
      - >There is a Backup files catalog associated with each zip file in the backup set
  - Catalogs
    - >Contains the Global Windows Backup Catalog file for this job

File Backup Investigative Impact

- File Backups are GUI driven
- “Schedulable”
- Multiple types of common media are now supported for the backup
- Investigators should:
  - Look for backup data on all applicable devices
  - Be aware of the folder naming conventions and format of the new backup implementation

Forensic Investigation Topics for Windows 7

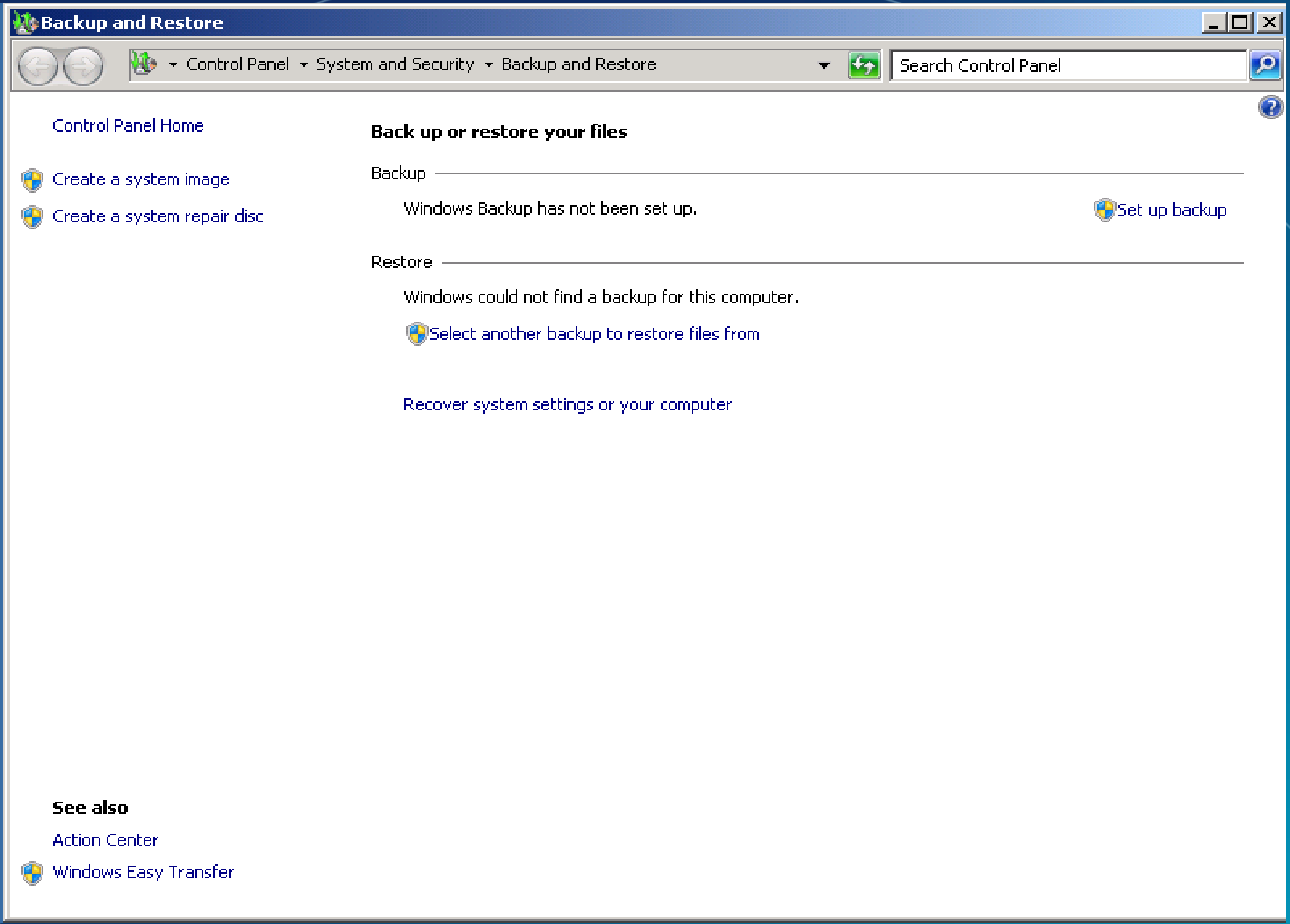
Complete System Image Backup

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Data Integrity – System Image Backup

- Complete System Image Backup Settings
  - Complete PC Backup
    - >Provides a full backup of the entire system including files not captured in the File Backup scenario
    - >Media supported: One or More DVD, Hard Disk, or network location
    - >Target drive MUST NOT BE compressed
    - >The volume Windows is installed on will always be included (Including system partition w/BitLocker)

Data Integrity – System Image Backup



Backup and Restore

Control Panel ▸ System and Security ▸ Backup and Restore

Search Control Panel

Control Panel Home

Create a system image

Create a system repair disc

See also

Action Center

Windows Easy Transfer

Back up or restore your files

Backup

Windows Backup has not been set up. Set up backup

Restore

Windows could not find a backup for this computer.

Select another backup to restore files from

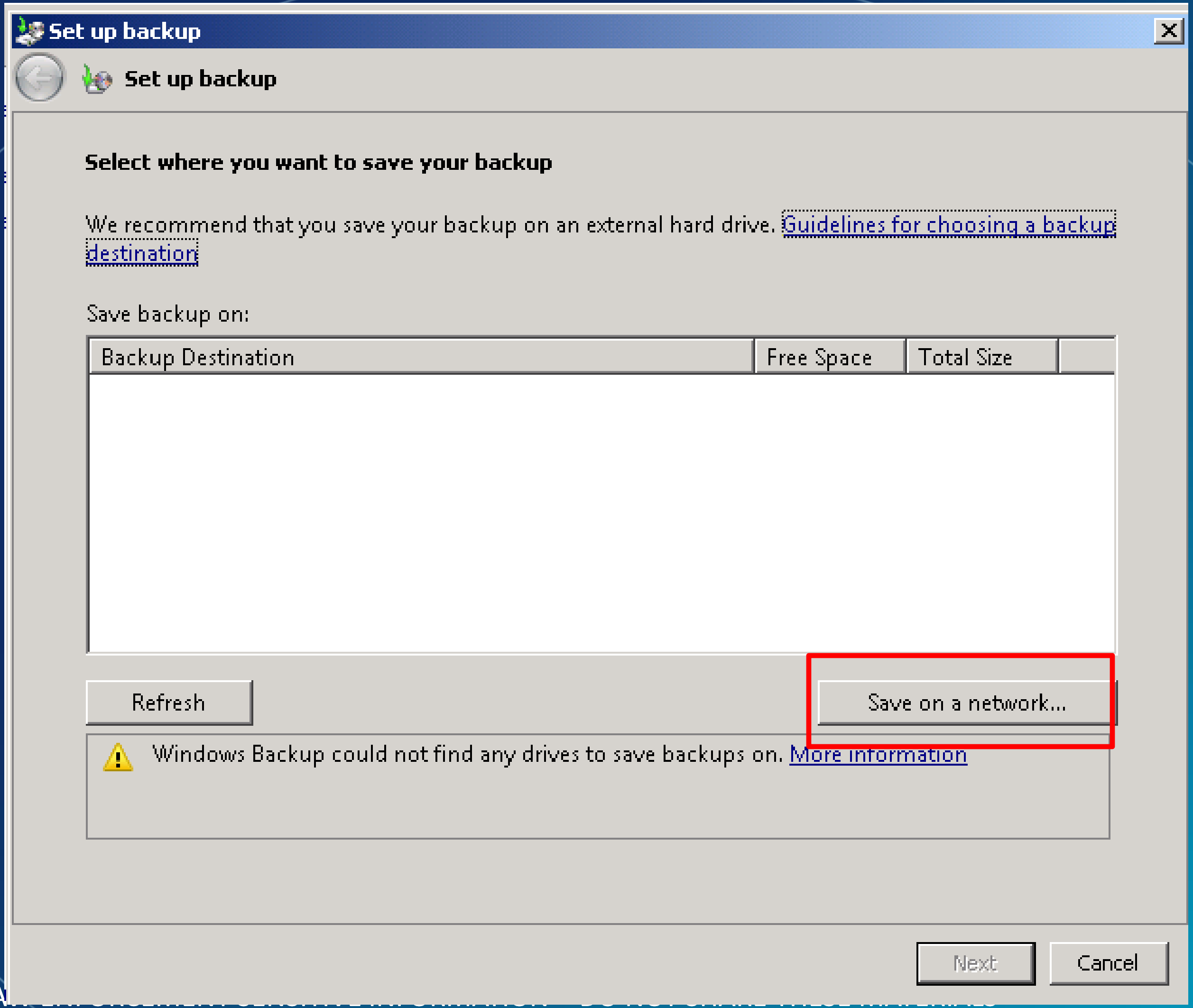
Recover system settings or your computer

Similar look and feel to File Backup operations

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Microsoft | Services

Data Integrity – System Image Backup



Set up backup

Set up backup

Select where you want to save your backup

We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

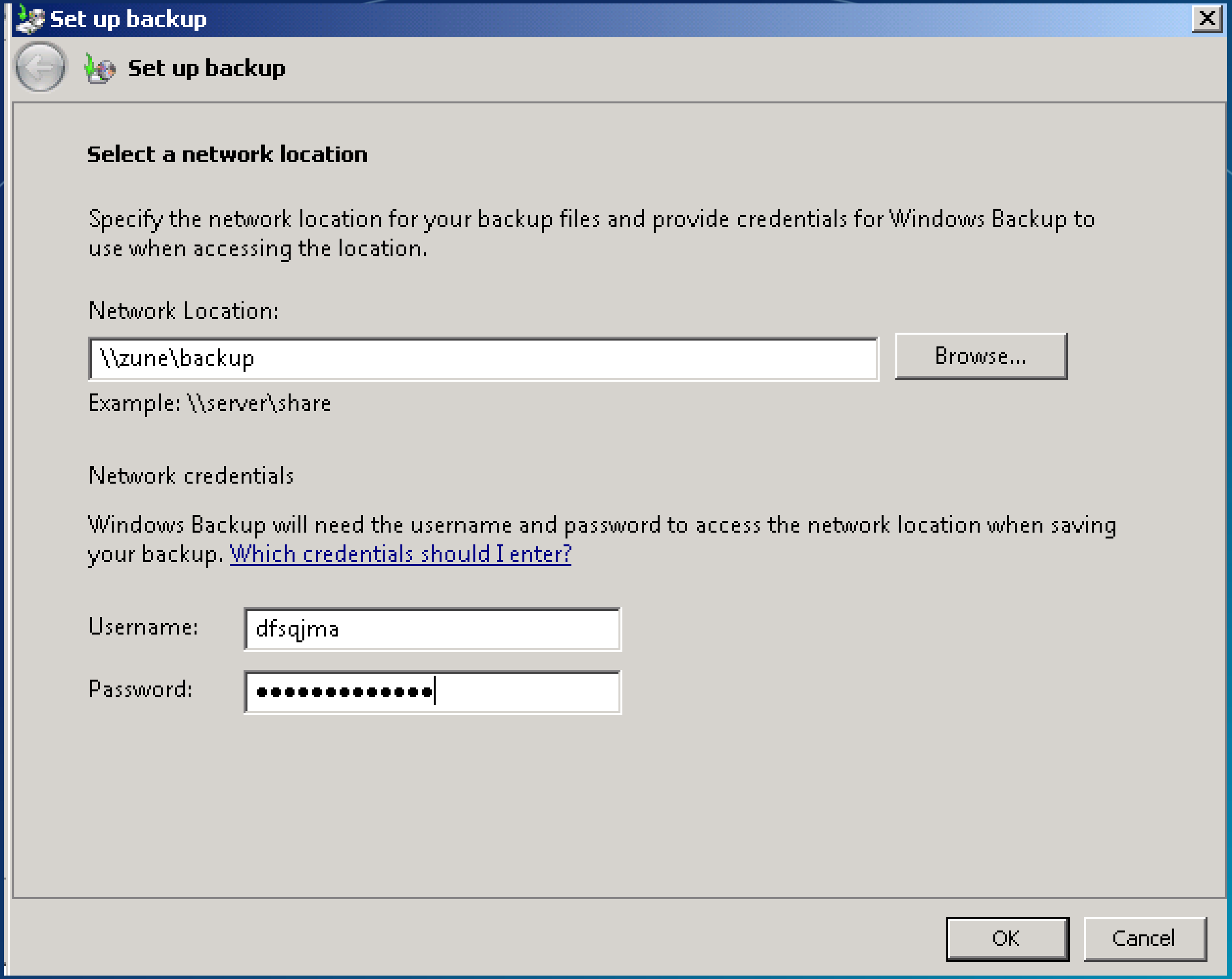
Save backup on:

Backup Destination	Free Space	Total Size

Windows Backup could not find any drives to save backups on. More information

- All connected drives are displayed
- In the event that no drives are present the backup can be sent to a network location.

Data Integrity – System Image Backup



Select a network location

Specify the network location for your backup files and provide credentials for Windows Backup to use when accessing the location.

Network Location: \\zune\backup

Example: \\server\share

Network credentials

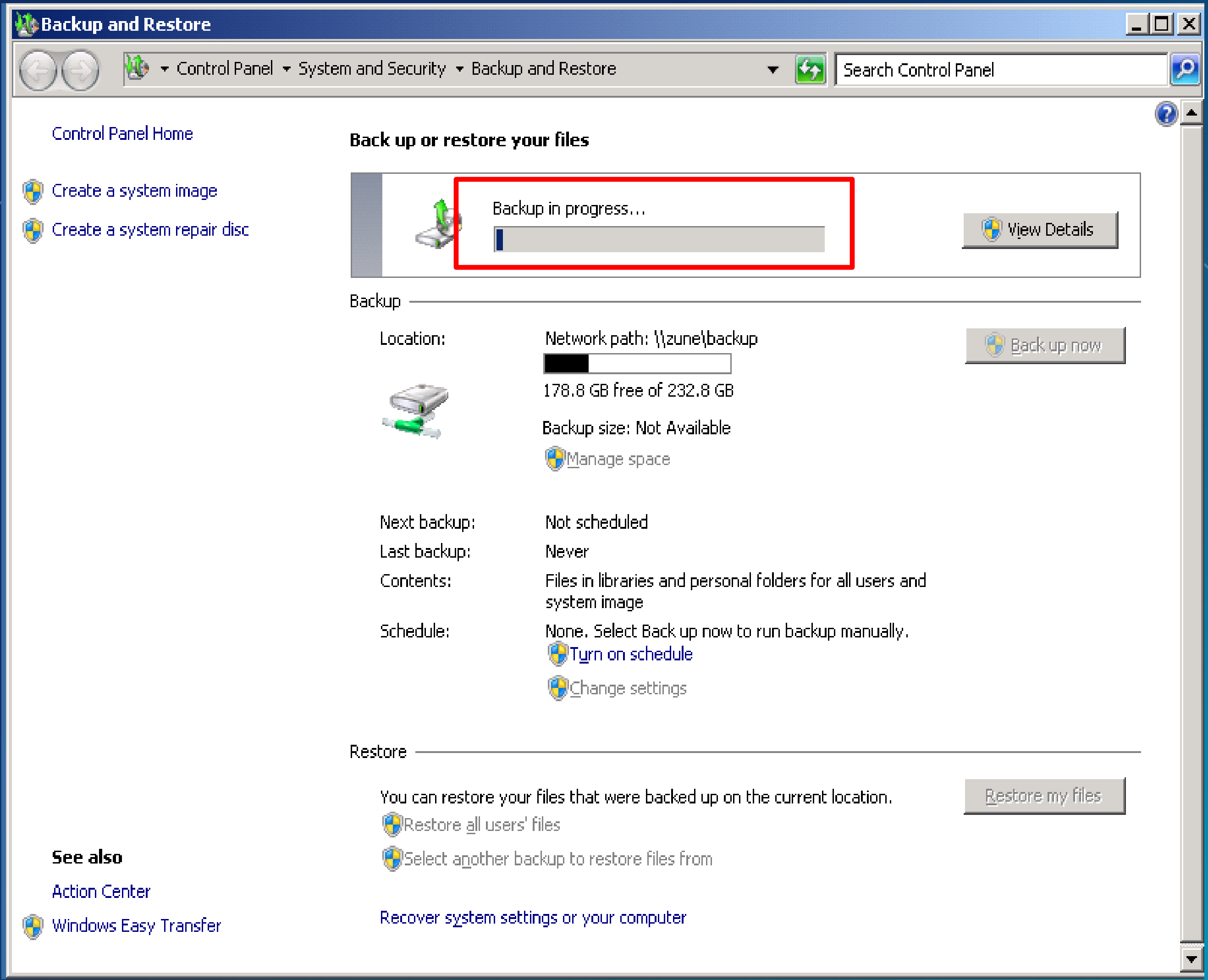
Windows Backup will need the username and password to access the network location when saving your backup. Which credentials should I enter?

Username: dfsqjma

Password: ••••••••••••••

- Specify network location and supply the required credentials.

Data Integrity – System Image Backup



Back up or restore your files

Backup in progress...

Backup

Location: Network path: \\zune\backup

178.8 GB free of 232.8 GB

Backup size: Not Available

Manage space

Next backup: Not scheduled

Last backup: Never

Contents: Files in libraries and personal folders for all users and system image

Schedule: None. Select Back up now to run backup manually.

Turn on schedule

Change settings

Restore

You can restore your files that were backed up on the current location.

Restore all users' files

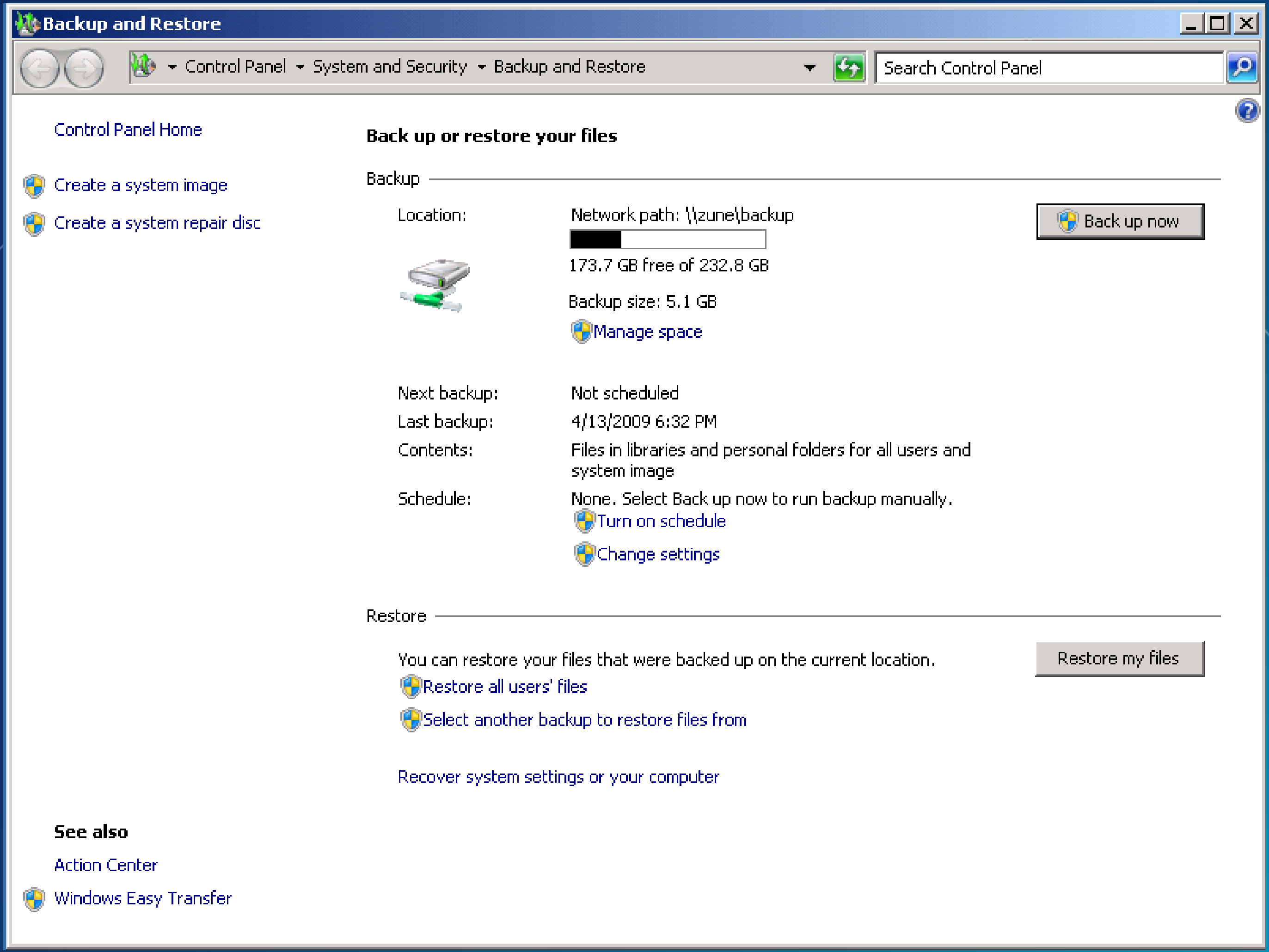
Select another backup to restore files from

Recover system settings or your computer

- Specify network location and supply the required credentials.

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Data Integrity – System Image Backup



Back up or restore your files

Backup

Location: Network path: \\zune\backup

173.7 GB free of 232.8 GB

Backup size: 5.1 GB

Manage space

Back up now

Next backup: Not scheduled

Last backup: 4/13/2009 6:32 PM

Contents: Files in libraries and personal folders for all users and system image

Schedule: None. Select Back up now to run backup manually.

Turn on schedule

Change settings

Restore

You can restore your files that were backed up on the current location.

Restore all users' files

Select another backup to restore files from

Restore my files

Recover system settings or your computer

Once complete backup settings can be viewed or changed

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

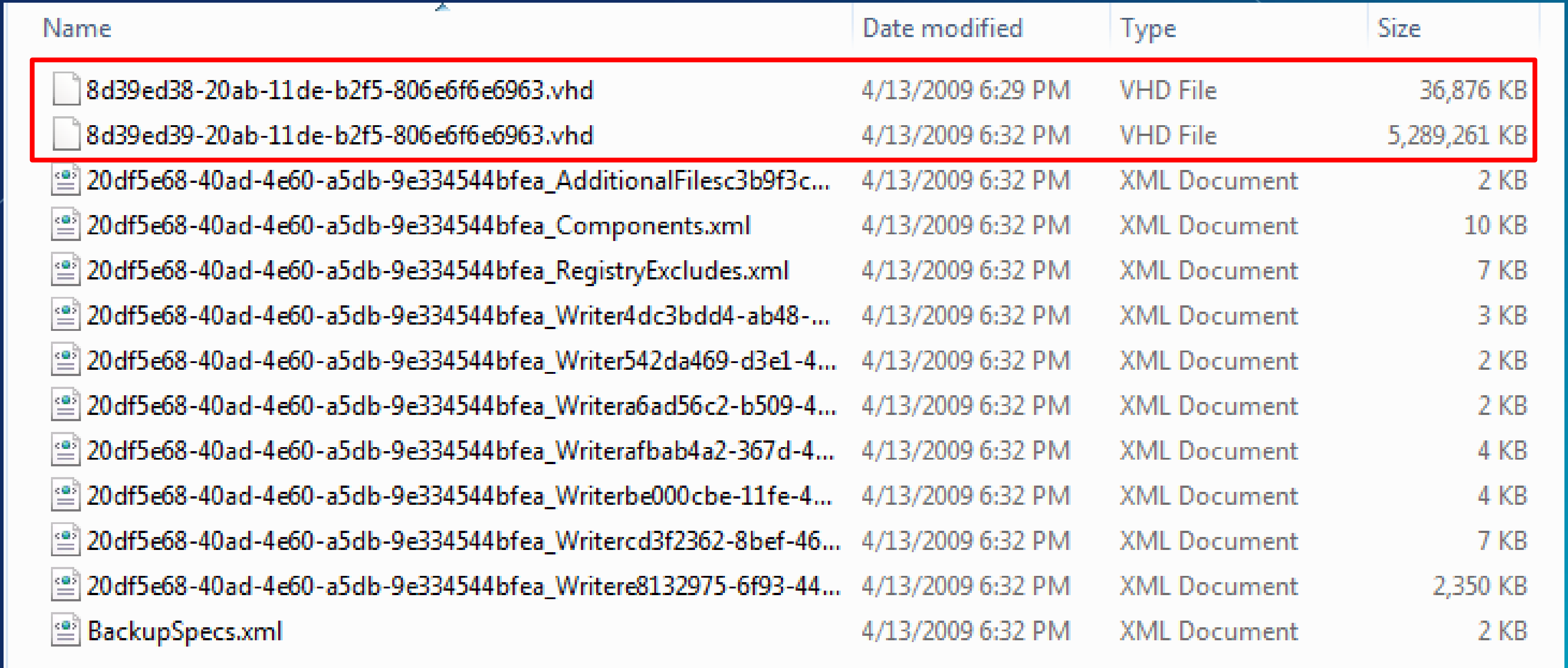
Microsoft | Services

Data Integrity – System Image Backup

- Backup time depends on the size and amount of data within the backup set
- The backup media will have a folder named “WindowsImageBackup”
  - Inside there will be a folder with the computer’s name
    - >Inside this folder is a folder in a similar naming convention as the file backup mechanism

      Backup <year>-<month>-<day>-<hhmmss>

Data Integrity – 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_Writera6ad56c2-b509-4...	4/13/2009 6:32 PM	XML Document	2 KB
20df5e68-40ad-4e60-a5db-9e334544bfea_Writerafbab4a2-367d-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_Writere8132975-6f93-44...	4/13/2009 6:32 PM	XML Document	2,350 KB
BackupSpecs.xml	4/13/2009 6:32 PM	XML Document	2 KB

Data Integrity – System Image Backup

- Within the backup folder there is a series of XML files that house the backup metadata.
- In addition there is an individual file for each volume that has been backed up with the file extension VHD
- The Complete PC Backup format is compatible with Virtual PC, Hyper-V, and the native VHD tools built into Windows 7.

Data Integrity – PC Backup

- This capability has been around for some time…creating Virtual Machines from hard disk backups

  How to create a Virtual PC hard disk image by using a backup disk image file

  http://support.microsoft.com/kb/912826/en-us

Forensic Investigation Topics for Windows 7

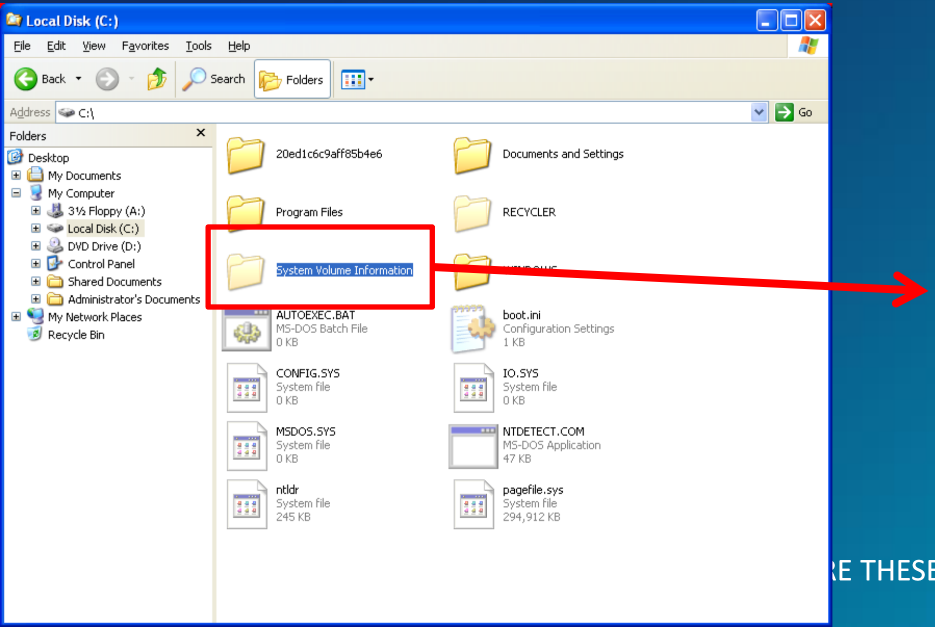
System Restore Using Volume Shadow Copy

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

System Restore Data Available in XP and Vista .. System Configuration

- XP is a simple file directory structure
- Old copies of registry can be easily retrieved

- Vista data in same location
- Data blobs that have to be mounted as a file system



20ed1c6c9aff85b4e6

Documents and Settings

Program Files

RECYCLER

System Volume Information

WINDOWS

AUTOEXEC.BAT
MS-DOS Batch File
0 KB

boot.ini
Configuration Settings
1 KB

CONFIG.SYS
System file
0 KB

IO.SYS
System file
0 KB

MSDOS.SYS
System file
0 KB

NTDETECT.COM
MS-DOS Application
47 KB

ntldr
System file
245 KB

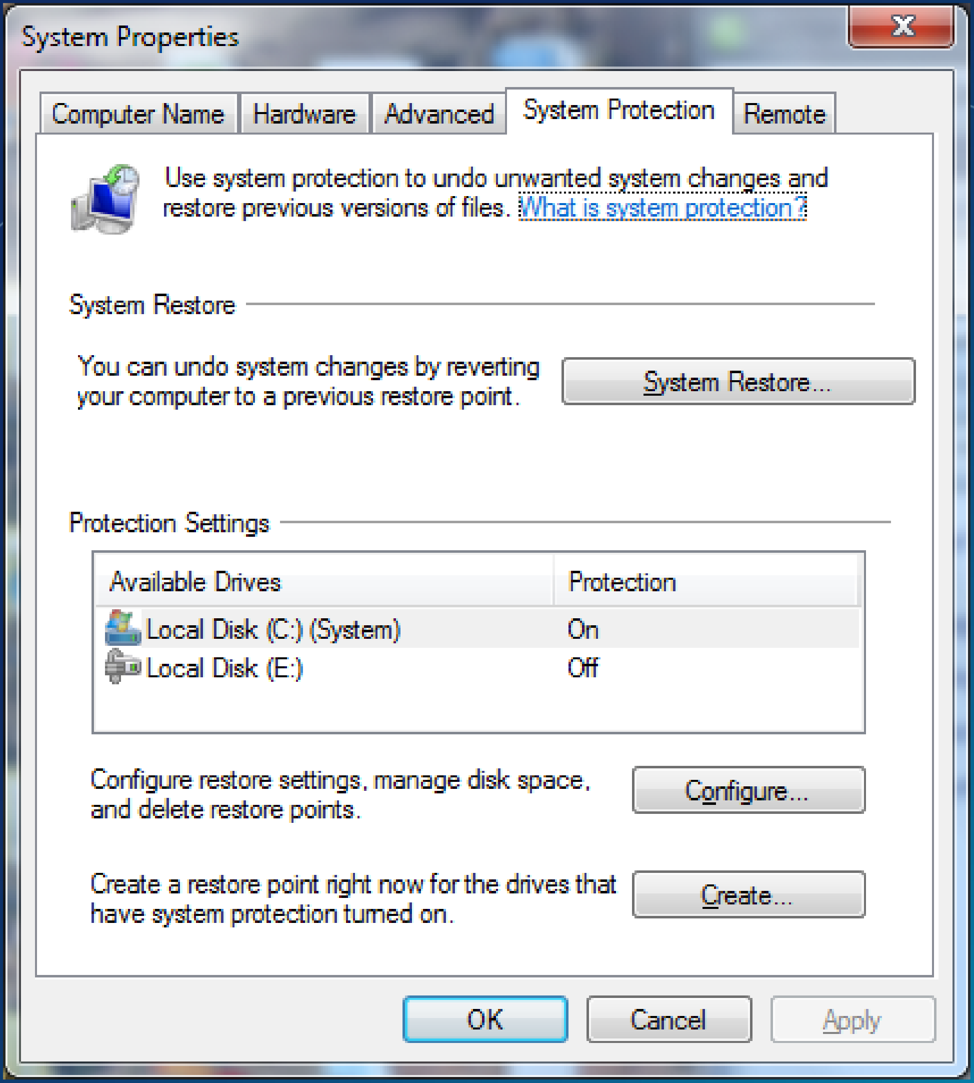
pagefile.sys
System file
294,912 KB

System Restore Data located in System Volume Information

Protection – System Restore

- The System Restore feature in Vista also uses the Volume Shadow Copy Service
- If VSS is recording all changes to the system it should collect changes that affect system stability
- System Restore is only concerned with certain system specific settings

Protection – System Restore



Use system protection to undo unwanted system changes and restore previous versions of files. What is system protection?

System Restore

You can undo system changes by reverting your computer to a previous restore point.

Protection Settings

Available Drives	Protection
Local Disk (C:) (System)	On
Local Disk (E:)	Off

Configure restore settings, manage disk space, and delete restore points.

Create a restore point right now for the drives that have system protection turned on.

- System Protection
  - Create Restore Points
  - Restore from a Restore Point
  - Available in all versions of Win 7

Protection – System Restore

- Move away from the file system filter approach in XP to the Shared Protection Point component that uses the Volume Shadow Copy Service (VSS)

- Gone is the list of files and location for monitoring by the System Restore process
- Remember VSS monitors all files!!!

Protection – System Restore

- Filtering is restore operation specific:
  - System Restore: Only files specific to the System Restore process are used
  - Previous Versions: Only the file(s) and/or folder(s) specific to the Previous Versions process are used
- The term System Restore Point only refers to SR operations and we pull the data from our Volume Snapshot

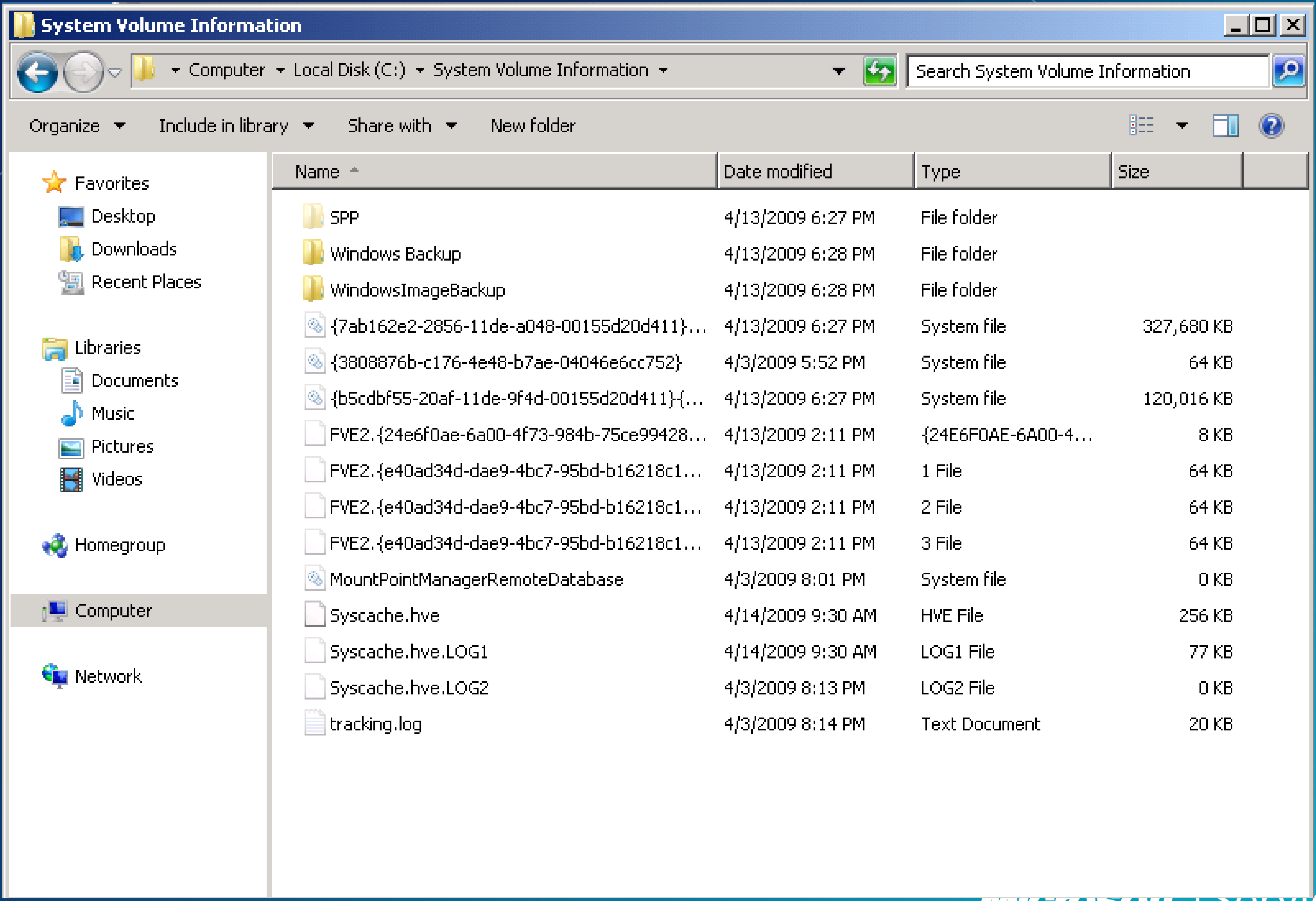
Protection – System Restore

- System Restore has the same functionality as it did with Windows XP we just use a new mechanism
- The mechanism has the capability to monitor system wide changes and System Restore can pull the information it needs from that data set (Volume Snapshot)

Protection – System Restore

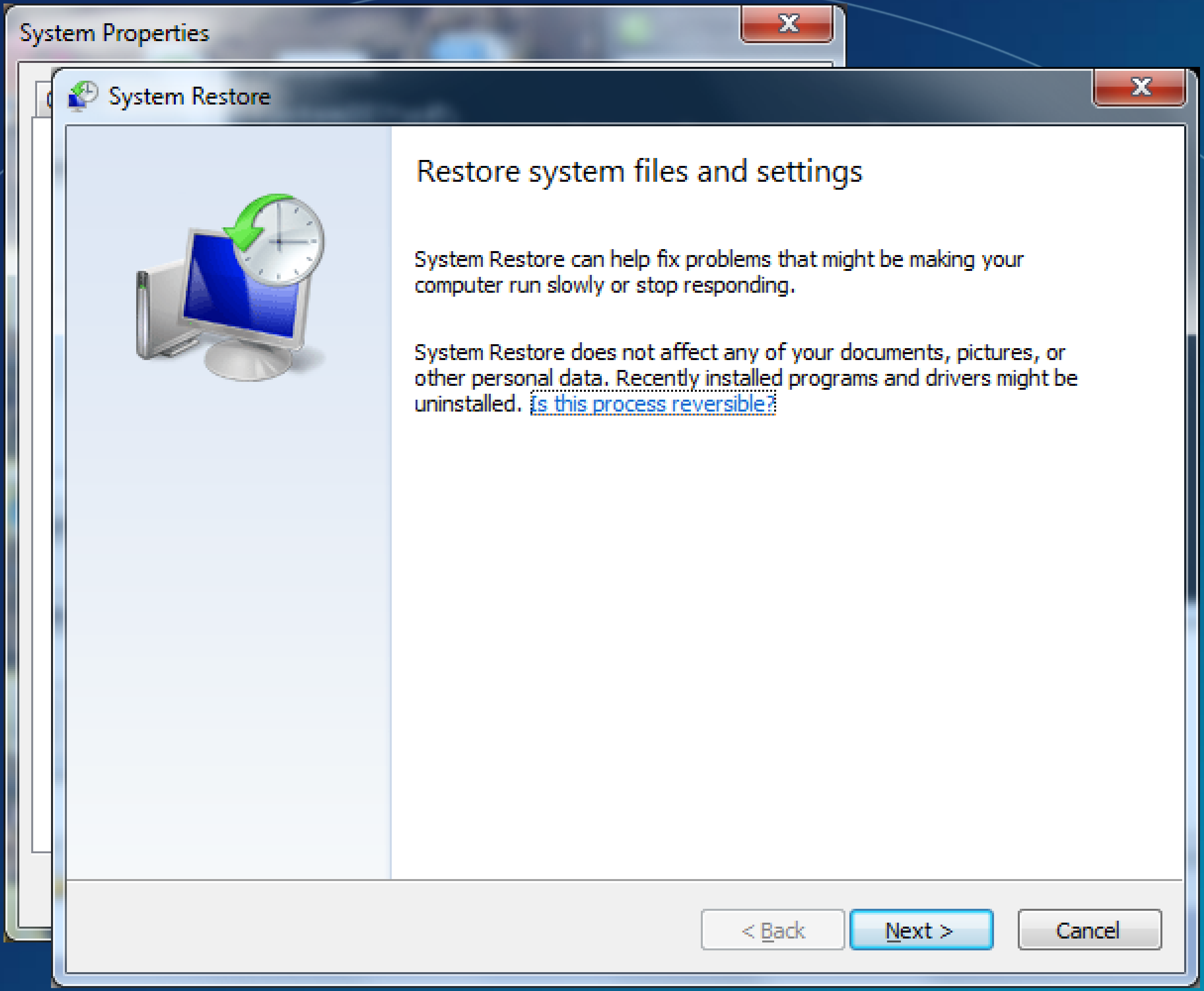
- The volume snapshot data is housed in the same location as System Restore Points in Windows XP and Vista
- The System Volume Information folder is secured to not allow even administrators access to all resources

Protection – System Restore



Name	Date modified	Type	Size
SPP	4/13/2009 6:27 PM	File folder	
Windows Backup	4/13/2009 6:28 PM	File folder	
WindowsImageBackup	4/13/2009 6:28 PM	File folder	
{7ab162e2-2856-11de-a048-00155d20d411}…	4/13/2009 6:27 PM	System file	327,680 KB
{3808876b-c176-4e48-b7ae-04046e6cc752}	4/3/2009 5:52 PM	System file	64 KB
{b5cdbf55-20af-11de-9f4d-00155d20d411}{…	4/13/2009 6:27 PM	System file	120,016 KB
FVE2.{24e6f0ae-6a00-4f73-984b-75ce99428…	4/13/2009 2:11 PM	{24E6F0AE-6A00-4…	8 KB
FVE2.{e40ad34d-dae9-4bc7-95bd-b16218c1…	4/13/2009 2:11 PM	1 File	64 KB
FVE2.{e40ad34d-dae9-4bc7-95bd-b16218c1…	4/13/2009 2:11 PM	2 File	64 KB
FVE2.{e40ad34d-dae9-4bc7-95bd-b16218c1…	4/13/2009 2:11 PM	3 File	64 KB
MountPointManagerRemoteDatabase	4/3/2009 8:01 PM	System file	0 KB
Syscache.hve	4/14/2009 9:30 AM	HVE File	256 KB
Syscache.hve.LOG1	4/14/2009 9:30 AM	LOG1 File	77 KB
Syscache.hve.LOG2	4/3/2009 8:13 PM	LOG2 File	0 KB
tracking.log	4/3/2009 8:14 PM	Text Document	20 KB

Protection – System Restore



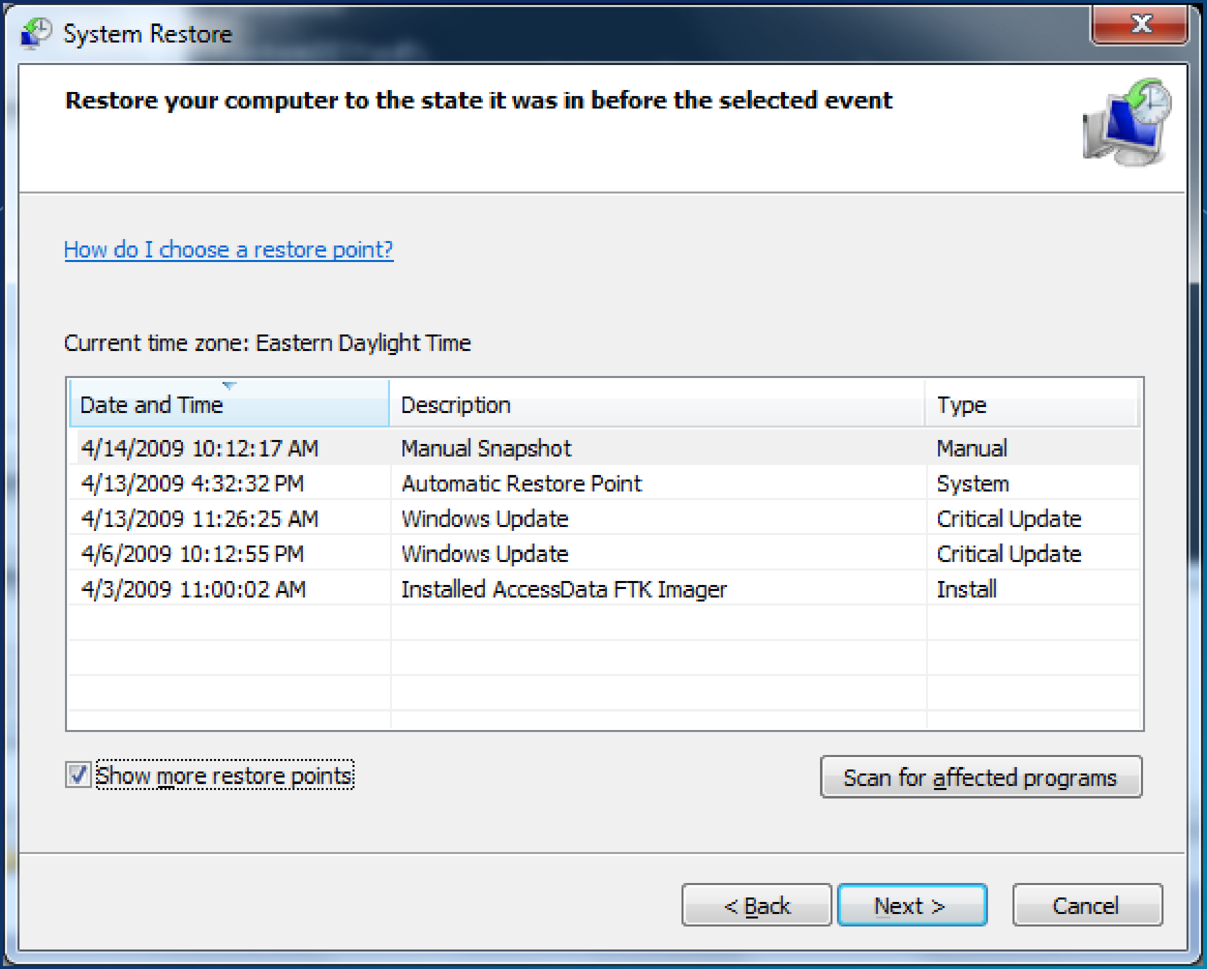
Restore system files and settings

System Restore can help fix problems that might be making your computer run slowly or stop responding.

System Restore does not affect any of your documents, pictures, or other personal data. Recently installed programs and drivers might be uninstalled. Is this process reversible?

- Accessing System Restore Points can be done through the System Protection GUI

Protection – System Restore



System Restore

Restore your computer to the state it was in before the selected event

How do I choose a restore point?

Current time zone: Eastern Daylight Time

Date and Time	Description	Type
4/14/2009 10:12:17 AM	Manual Snapshot	Manual
4/13/2009 4:32:32 PM	Automatic Restore Point	System
4/13/2009 11:26:25 AM	Windows Update	Critical Update
4/6/2009 10:12:55 PM	Windows Update	Critical Update
4/3/2009 11:00:02 AM	Installed AccessData FTK Imager	Install

☑ Show more restore points

- An Investigator can see "Date and Time" as well as description information on each VS

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

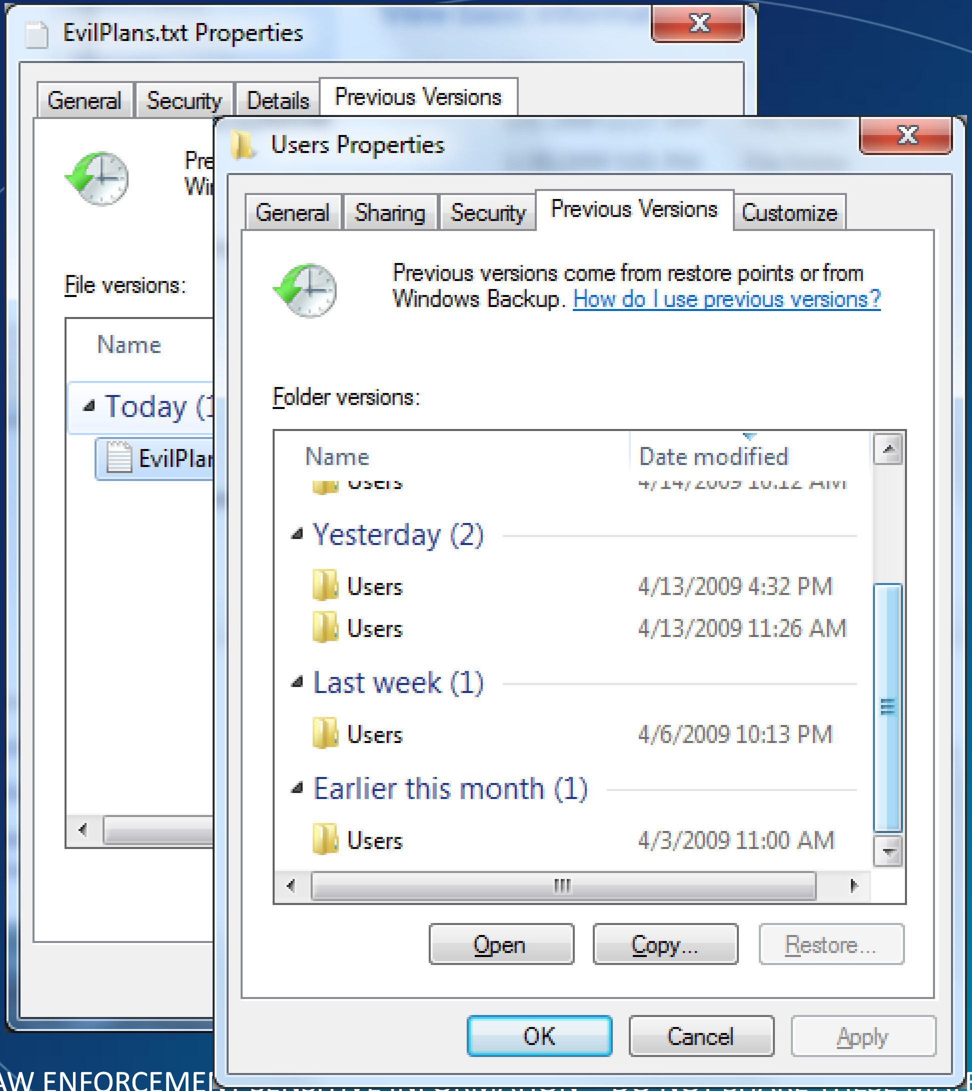
Microsoft | Services

Forensic Investigation Topics for Windows 7

Previous Versions Using Volume Shadow Copy

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Data Integrity - Previous Versions



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Folder versions:

Name	Date modified
Users	4/14/2009 10:12 AM
Yesterday (2)	
Users	4/13/2009 4:32 PM
Users	4/13/2009 11:26 AM
Last week (1)	
Users	4/6/2009 10:13 PM
Earlier this month (1)	
Users	4/3/2009 11:00 AM

- Previous Versions
  - –Restore previous versions of folders and files
  - –Remember only available in: Business, Enterprise and Ultimate

LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

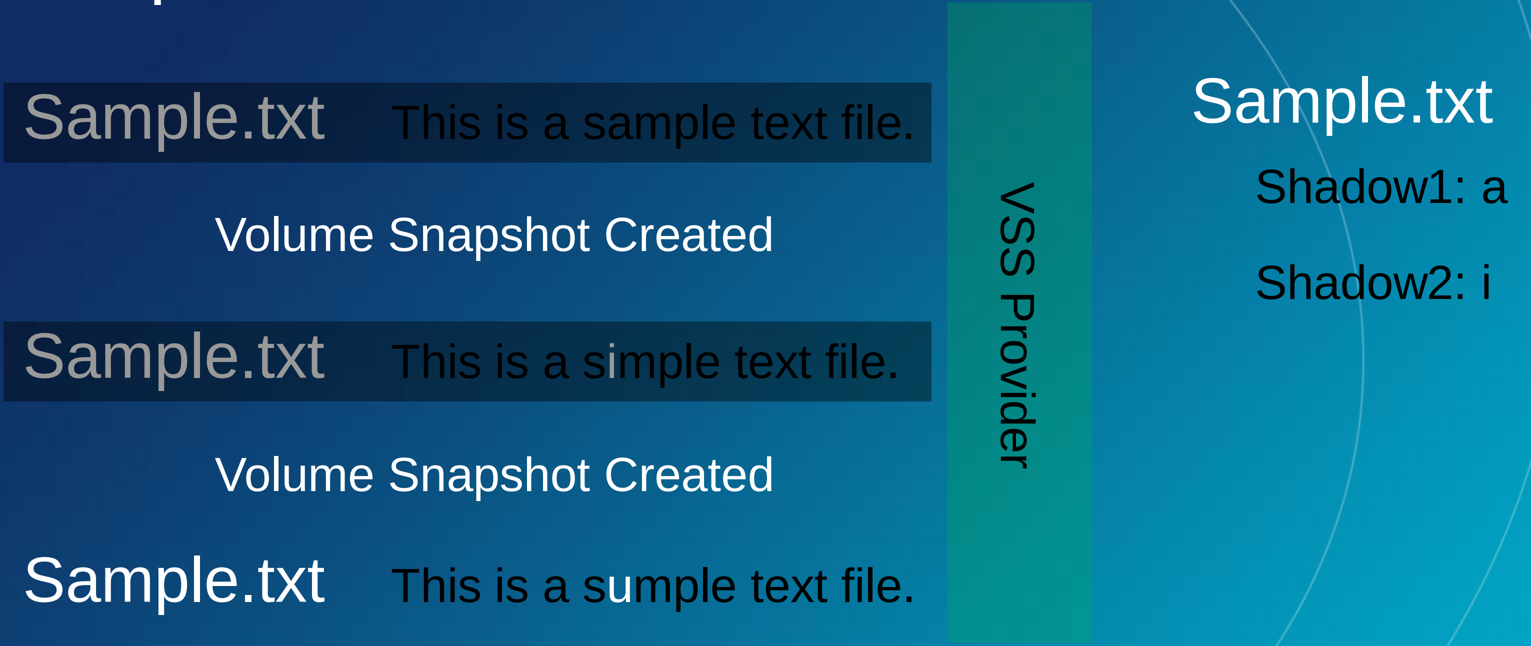
Microsoft | Services

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

- Previous Versions only stores the changes to a particular file in the volume snapshot .
- Example:



Sample.txt This is a sample text file.

Volume Snapshot Created

Sample.txt This is a simple text file.

Volume Snapshot Created

Sample.txt This is a sumple text file.

VSS Provider

Sample.txt

Shadow1: a

Shadow2: i

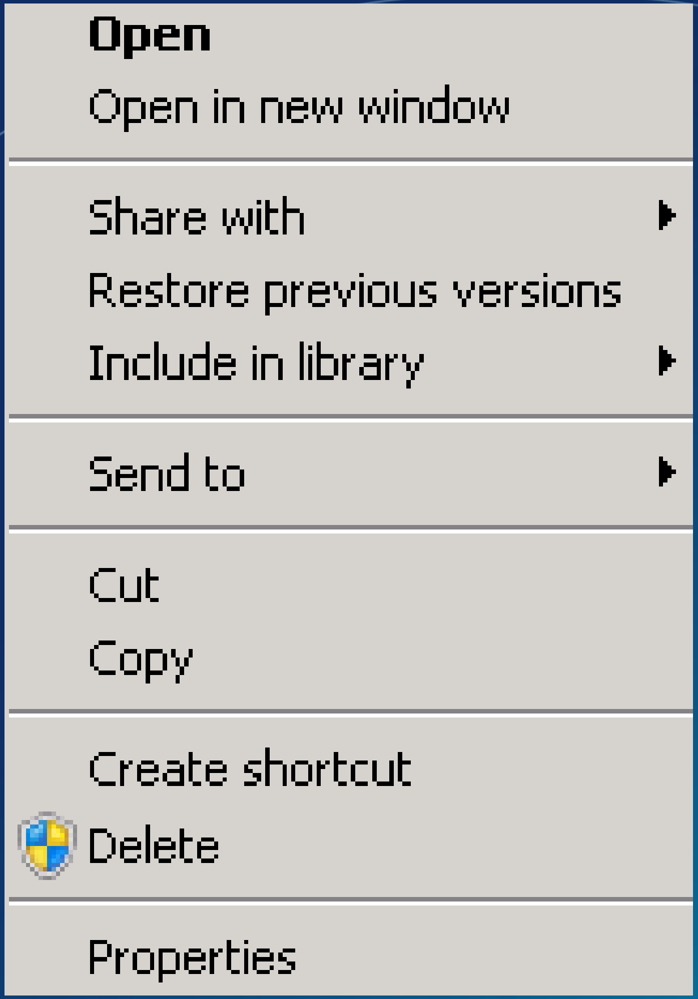
Data Integrity - Previous Versions

- Only one version of a file is saved as a shadow copy. For example, if you modify a file several times in one day, only the version that was current when the volume snapshot was made is saved.
- This is not as granular as a copy of every version of a document…

Data Integrity - Previous Versions

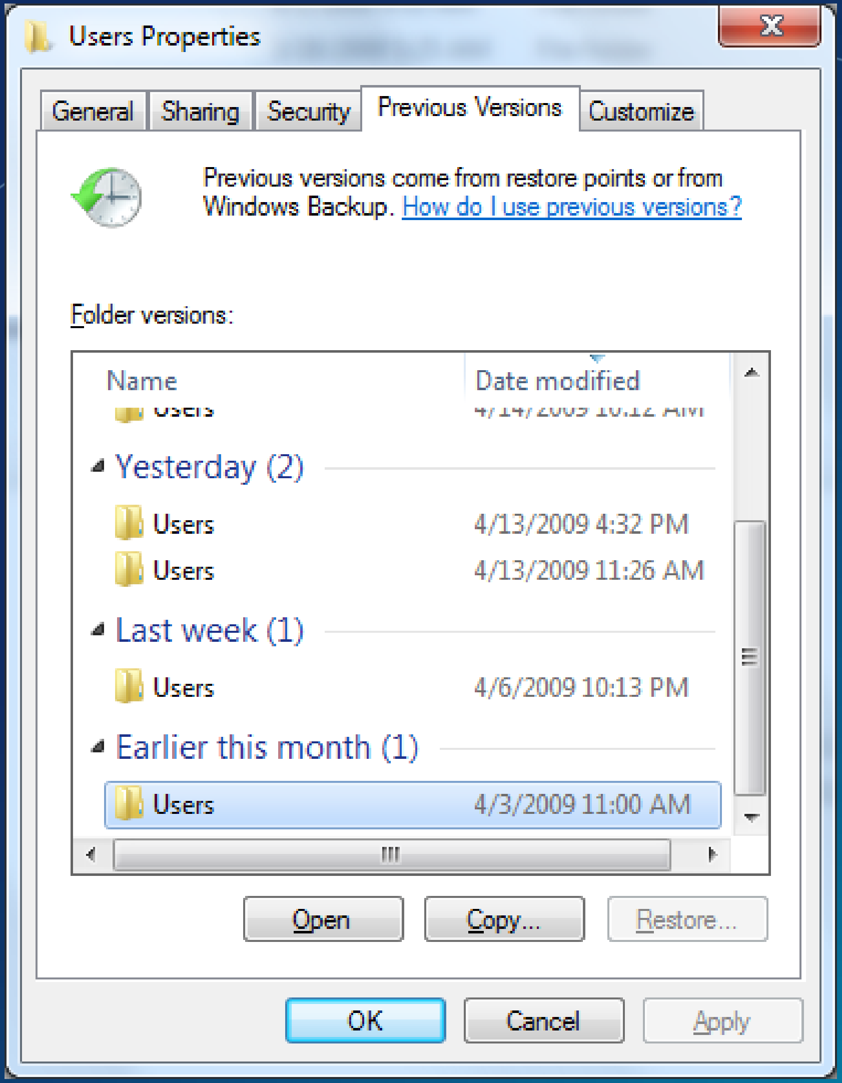
- If you accidentally delete or rename a file or folder, you can restore a shadow copy of that file or folder, but you need to know the location that the file or folder was saved to and its name.
- Works even if the Recycle Bin has been cleared!!
- Depending on the restore…it may even work after several defragmentations

Data Integrity - Previous Versions



- To access Previous Versions of a resource simply right mouse click and choose the option to “Restore previous versions”

Data Integrity - Previous Versions



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Folder versions:

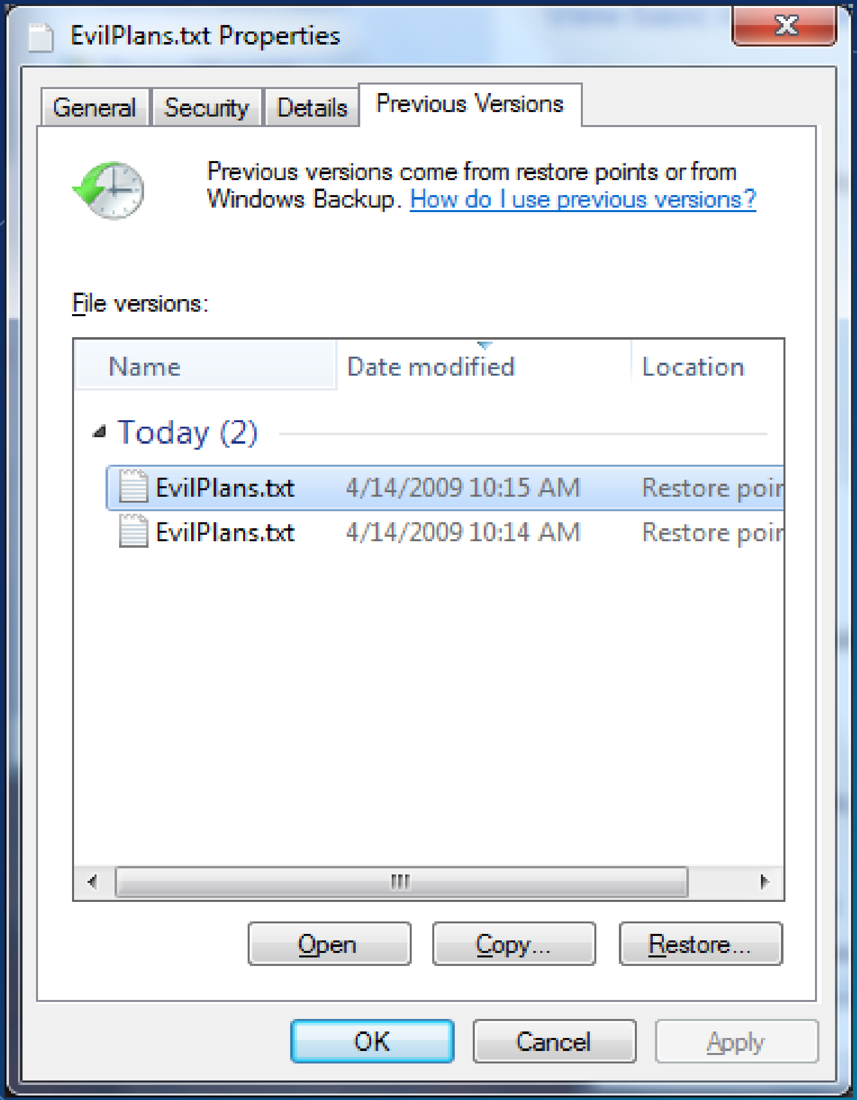
Name	Date modified
Users	4/14/2009 10:12 AM
Yesterday (2)	
Users	4/13/2009 4:32 PM
Users	4/13/2009 11:26 AM
Last week (1)	
Users	4/6/2009 10:13 PM
Earlier this month (1)	
Users	4/3/2009 11:00 AM

- 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 it 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



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

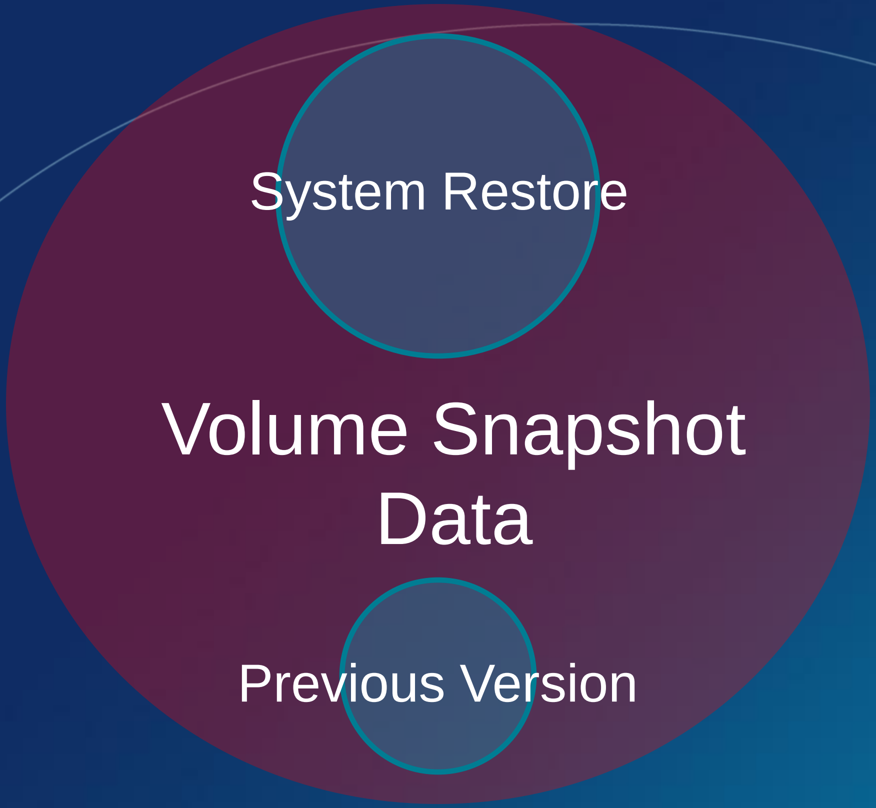
File versions:

Name	Date modified	Location
Today (2)		
EvilPlans.txt	4/14/2009 10:15 AM	Restore poir
EvilPlans.txt	4/14/2009 10:14 AM	Restore poir

- The data needed to successfully restore a file is:
  - The original file

    +
  - The change data
- Defragmentation may affect recoverability

Volume Snapshots



System Restore

Volume Snapshot Data

Previous Version

- Restore Points and Previous Versions are both pulled from the same snapshot data

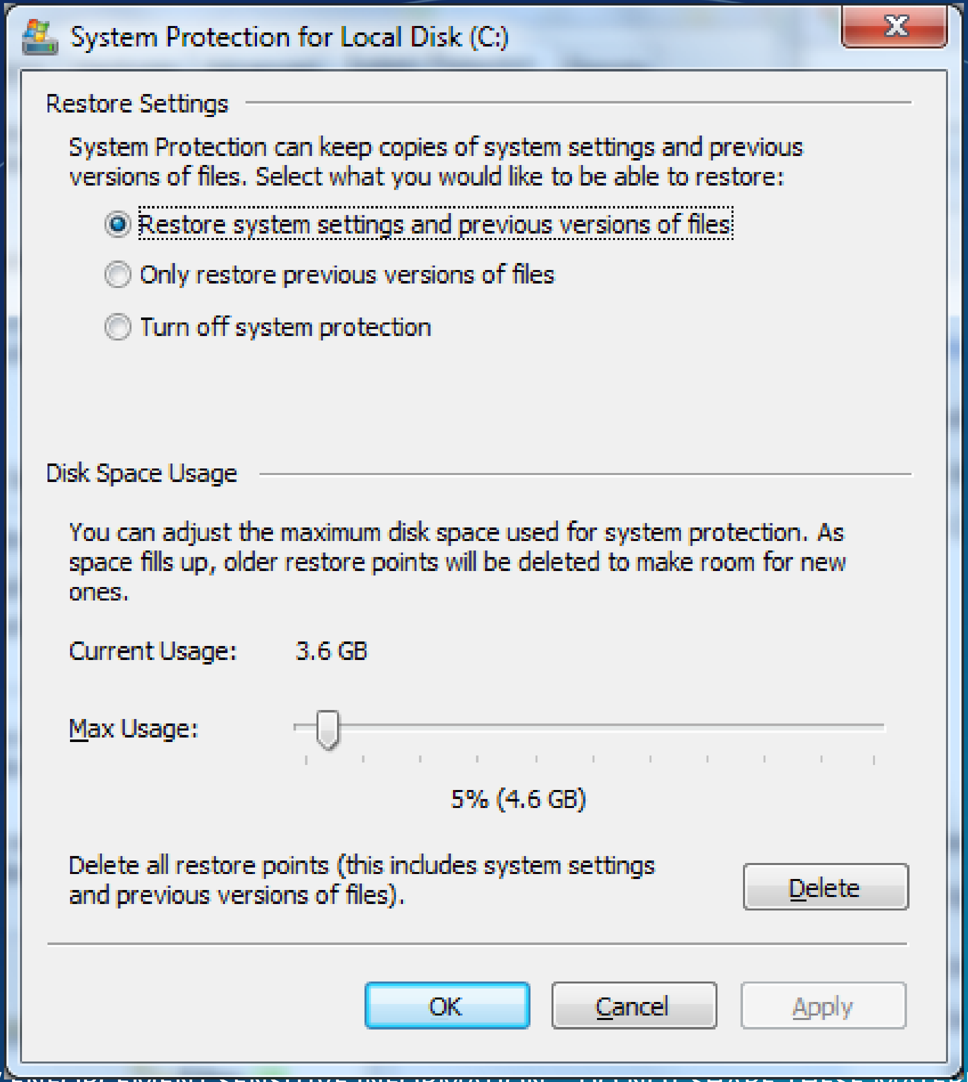
Forensic Investigation Topics for Windows 7

Mounting and Accessing Volume Shadow Copy Data from Evidence Drives

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



System Protection for Local Disk (C:)

Restore Settings

System Protection can keep copies of system settings and previous versions of files. Select what you would like to be able to restore:

● Restore system settings and previous versions of files

○ Only restore previous versions of files

○ Turn off system protection

Disk Space Usage

You can adjust the maximum disk space used for system protection. As space fills up, older restore points will be deleted to make room for new ones.

Current Usage: 3.6 GB

Max Usage:

5% (4.6 GB)

Delete all restore points (this includes system settings and previous versions of files).

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

Accessing and Mounting Volume Shadow Copy Stores

- Three basic methods of accessing store
  - Mount drive in **Vista Enterprise or Ultimate forensic workstation** and use the GUI
  - Mount drive in Vista Enterprise or Ultimate forensic workstation and mount the data blobs via command line
  - Use third party tool to access the Volume Shadow Copy data store

Mount Drive in Forensic Workstation and Use Workstation GUI to Recover Files

- Pluses
  - Works every time
  - Easy
- Minuses
  - Only gets previous versions of EXISTING files
  - You can recover files if you know the exact file name

How?

- Connect write blocked suspect drive to forensic workstation
- Forensic workstation must be running Vista Enterprise or Ultimate

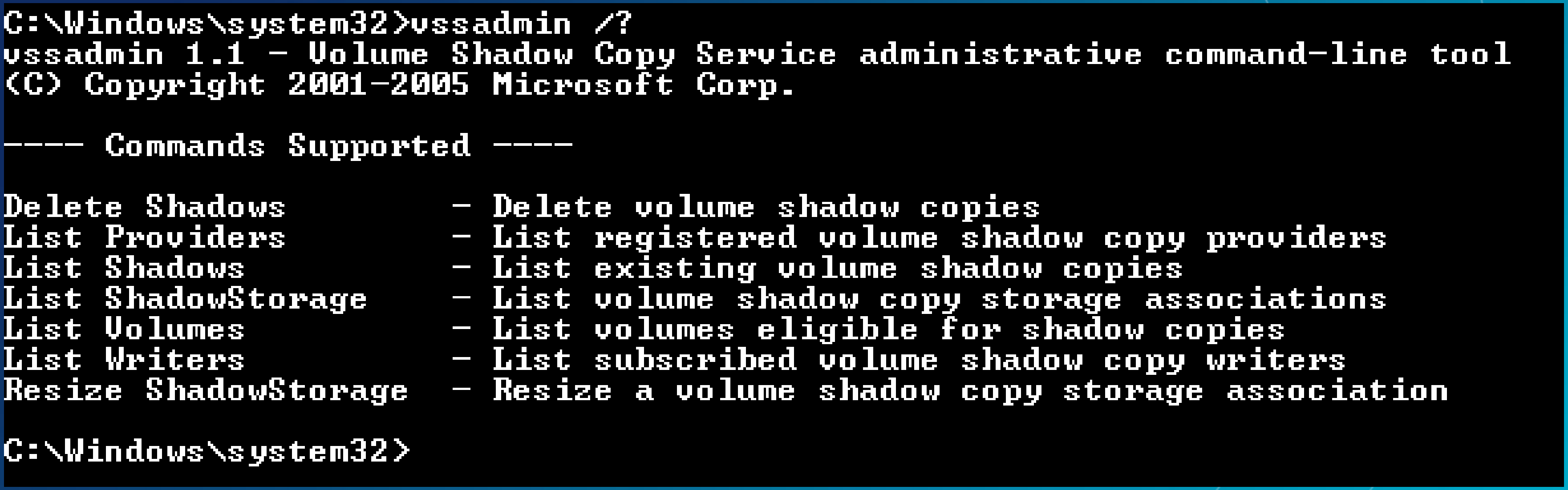
Microsoft | Services

Forensic Investigation Topics for Windows Vista

Tools for Dealing with Volume Shadow Copy Data

VSS Tools

- The main tool that ships with all versions of Win 7 is called VSSAdmin
- From this tool an administrator can perform a number of operations



```
C:\Windows\system32>vssadmin /?
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

---- Commands Supported ----

Delete Shadows        - Delete volume shadow copies
List Providers        - List registered volume shadow copy providers
List Shadows          - List existing volume shadow copies
List ShadowStorage    - List volume shadow copy storage associations
List Volumes          - List volumes eligible for shadow copies
List Writers          - List subscribed volume shadow copy writers
Resize ShadowStorage  - Resize a volume shadow copy storage association

C:\Windows\system32>
```

VSS Tools

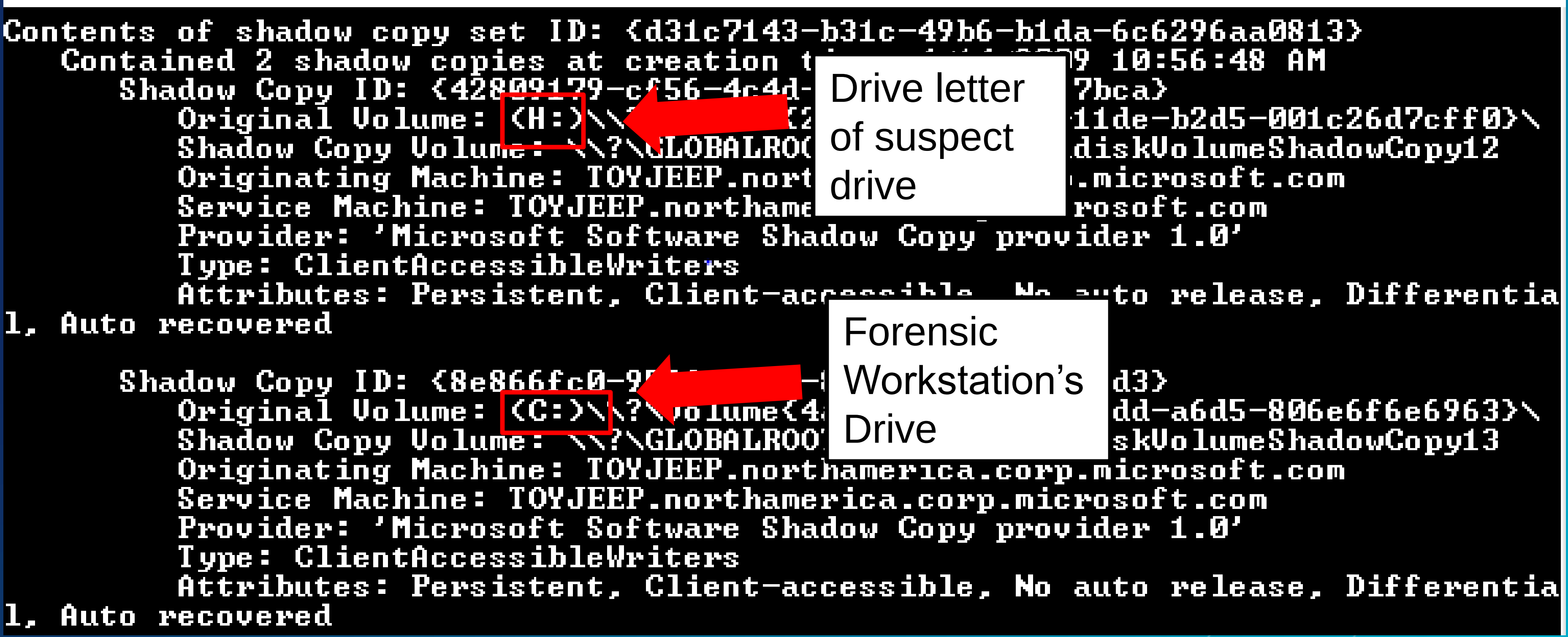
- The most interesting for investigators is the command to show all Volume snapshots on the system

```
vssadmin list shadows
```

- With this output we can determine how far back a suspect snapshot data goes

VSS Tools

- Highly dependent on system activity and available disk space



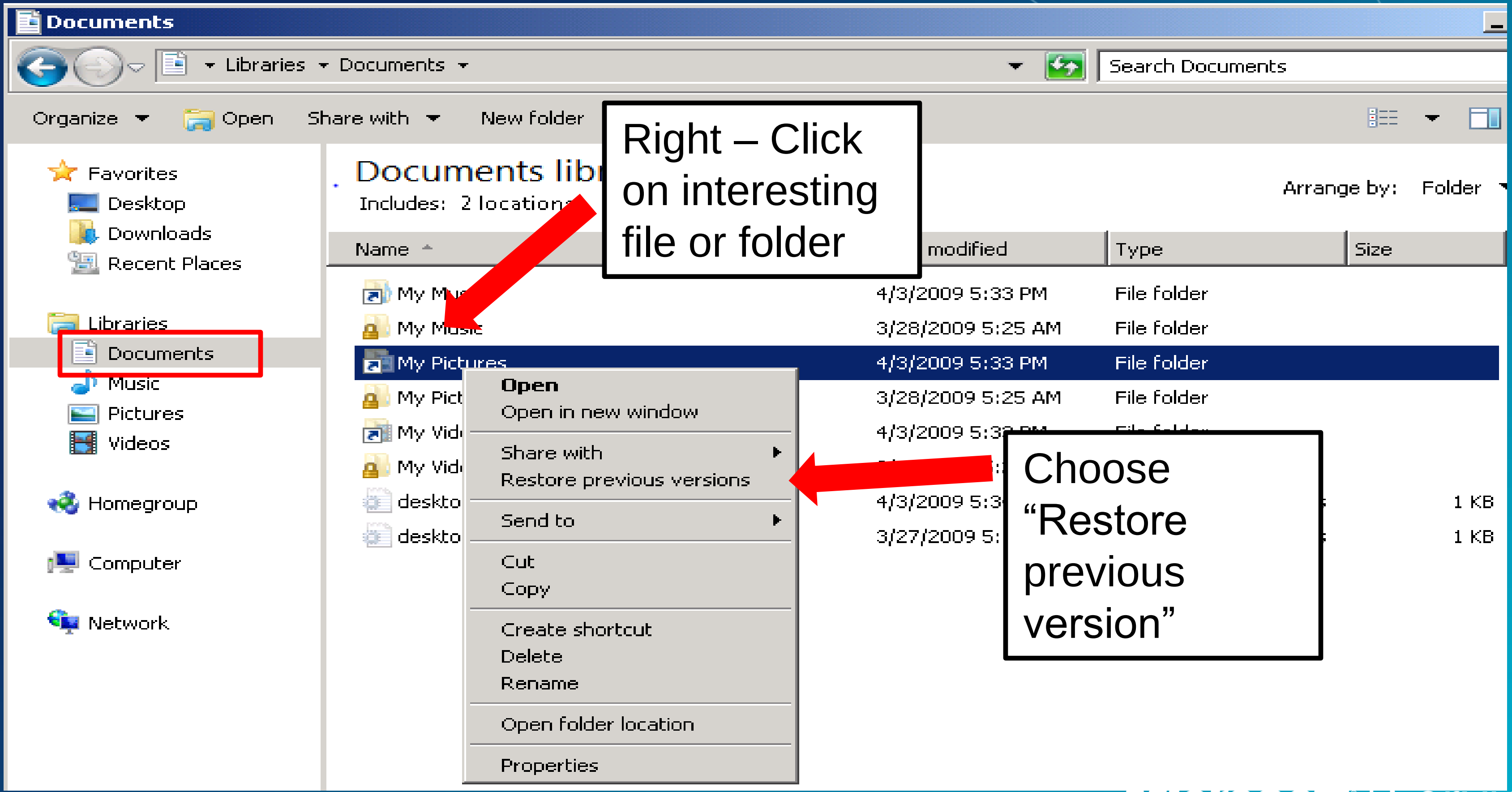
```
Contents of shadow copy set ID: {d31c7143-b31c-49b6-b1da-6c6296aa0813}
   Contained 2 shadow copies at creation t                9 10:56:48 AM
      Shadow Copy ID: {42809179-cf56-4c4d-             7bca}
         Original Volume: (H:)\\                   11de-b2d5-001c26d7cff0}\
         Shadow Copy Volume: \\?\GLOBALROO          diskVolumeShadowCopy12
         Originating Machine: TOYJEEP.nort          .microsoft.com
         Service Machine: TOYJEEP.northame          rosoft.com
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-acc          uto release, Differentia
l, Auto recovered

      Shadow Copy ID: {8e866fc0-9         -          d3}
         Original Volume: (C:)\\?\Volume{4           dd-a6d5-806e6f6e6963}\
         Shadow Copy Volume: \\?\GLOBALROOT          skVolumeShadowCopy13
         Originating Machine: TOYJEEP.northamerica.corp.microsoft.com
         Service Machine: TOYJEEP.northamerica.corp.microsoft.com
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differentia
l, Auto recovered
```

Drive letter of suspect drive

Forensic Workstation's Drive

Previous Versions - Evidence

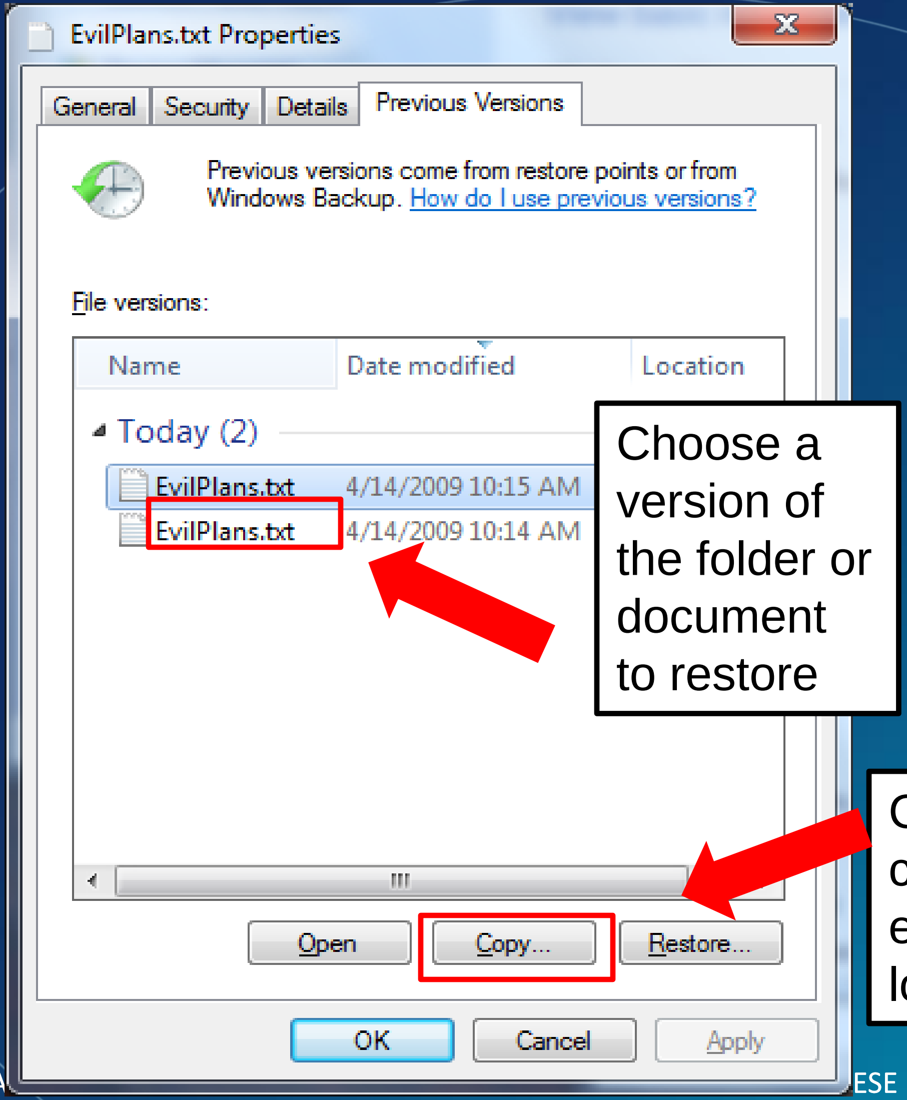
- In Windows Explorer browse to suspect drive and folders/files you are interested in



Right – Click on interesting file or folder

Choose "Restore previous version"

Previous Versions - Evidence



Previous versions come from restore points or from Windows Backup. How do I use previous versions?

Name	Date modified	Location
Today (2)		
EvilPlans.txt	4/14/2009 10:15 AM	
EvilPlans.txt	4/14/2009 10:14 AM	

Choose a version of the folder or document to restore

Choose to copy it to a evidence location

- If previous versions are available for a resource they will be populated in the window

Interesting Places to Look

- Users\%user%\
  - User profile
    - >User.dat portion of the registry
    - >Documents
    - >Desktop
    - >Thumbcache files
    - >Temporary Internet files
    - >Internet history files
    - >Internet bookmarks

Interesting Places to Look

- Windows\system32\config
  - –Restore point type information
    - >System portion of the registry
    - >SAM
    - >System logs
- Any other folders or individual files you see

Mount Drive in Forensic Workstation and Mount Data Blobs Via Command Line

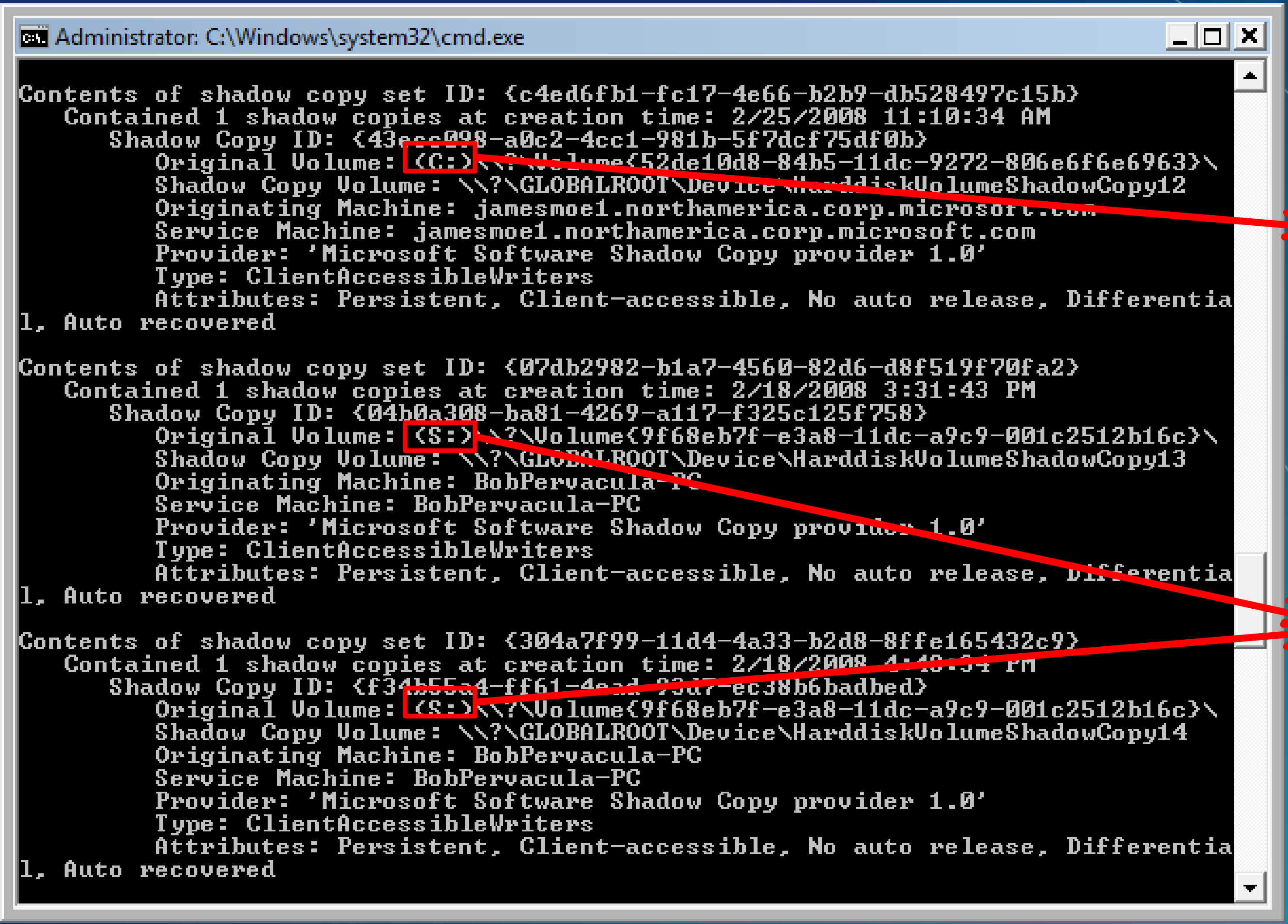
- Pluses
  - Get consolidated access to files stored
- Minuses
  - Complicated command line syntax
  - Difficult to navigate data at times

Directly Mounting Volume Shadows

- Create a symbolic link to shadows
  - Symbolic link similar to mechanism for directing “My Documents” to the new “Users” directory
  - NOT A SHORTCUT
  - Deeper in the file system
  - Command to create a symbolic link is MKLINK

Directly Mounting Volume Shadows

- Step 1
  - Verify you can see the suspect drive shadows
  - In this example write-blocked drive was assigned a drive letter of s:
  - Opened a command box on forensic examination machine
  - Typed: vssadmin list shadows



```
Contents of shadow copy set ID: {c4ed6fb1-fc17-4e66-b2b9-db528497c15b}
   Contained 1 shadow copies at creation time: 2/25/2008 11:10:34 AM
      Shadow Copy ID: {43ecc098-a0c2-4cc1-981b-5f7dcf75df0b}
         Original Volume: (C:)\\?\Volume{52de10d8-84b5-11dc-9272-806e6f6e6963}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy12
         Originating Machine: jamesmoe1.northamerica.corp.microsoft.com
         Service Machine: jamesmoe1.northamerica.corp.microsoft.com
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differentia
l, Auto recovered

Contents of shadow copy set ID: {07db2982-b1a7-4560-82d6-d8f519f70fa2}
   Contained 1 shadow copies at creation time: 2/18/2008 3:31:43 PM
      Shadow Copy ID: {04b0a308-ba81-4269-a117-f325c125f758}
         Original Volume: (S:)\\?\Volume{9f68eb7f-e3a8-11dc-a9c9-001c2512b16c}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy13
         Originating Machine: BobPervacula-PC
         Service Machine: BobPervacula-PC
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differentia
l, Auto recovered

Contents of shadow copy set ID: {304a7f99-11d4-4a33-b2d8-8ffe165432c9}
   Contained 1 shadow copies at creation time: 2/18/2008 4:40:54 PM
      Shadow Copy ID: {f34b55a4-ff61-4ead-93d7-ec38b6badbed}
         Original Volume: (S:)\\?\Volume{9f68eb7f-e3a8-11dc-a9c9-001c2512b16c}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy14
         Originating Machine: BobPervacula-PC
         Service Machine: BobPervacula-PC
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differentia
l, Auto recovered
```

Forensic Workstation's Volume Shadow Blob(s)

Suspect's drive Volume Shadow Blob(s)

Mount Suspect’s Data Blob

```
C:\>mklink /d C:\snapshot649 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy649\
```

(be sure to include the trailing backslash)

Name and location of the symbolic link you want to create

Full snapshot name as listed in the VSSAdmin output

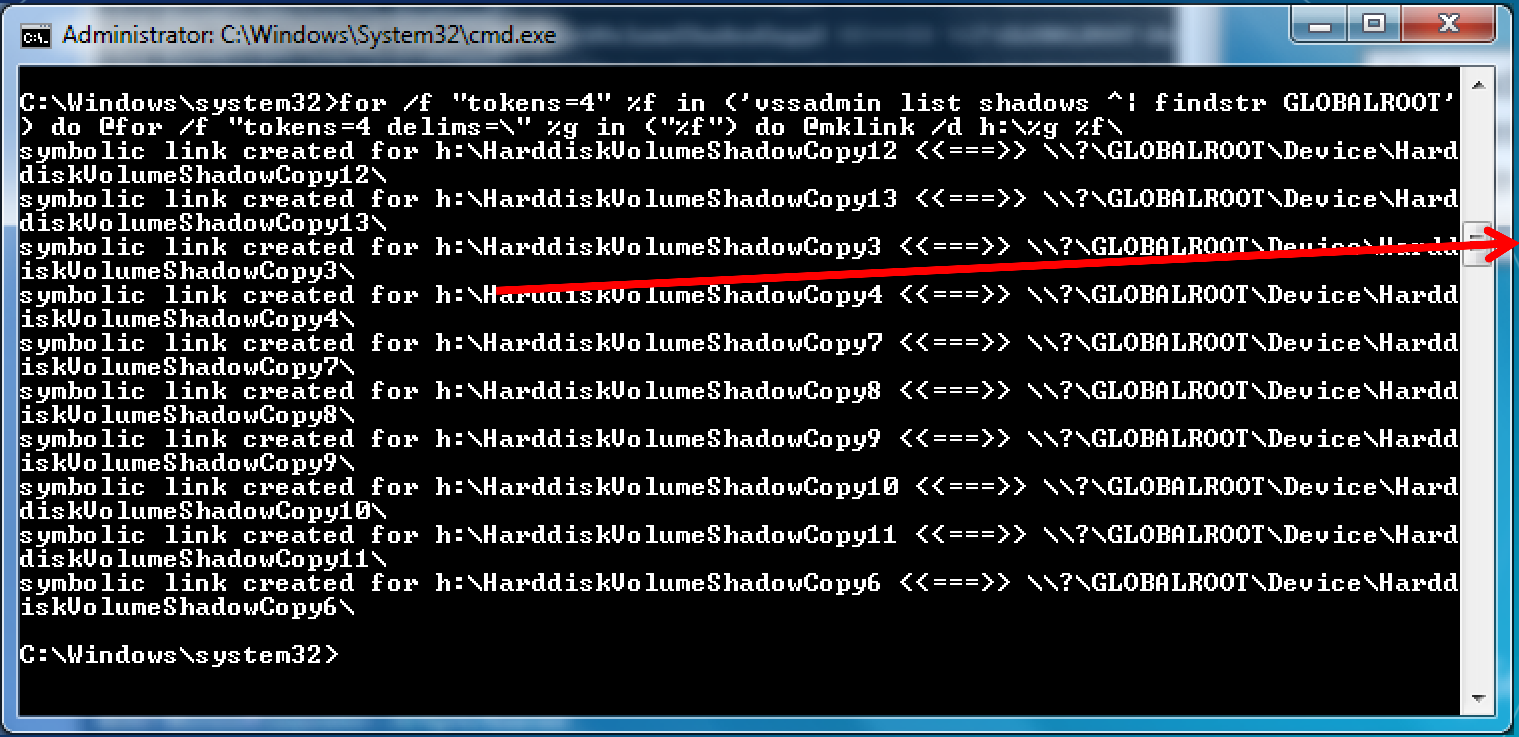
LAW ENFORCEMENT SENSITIVE INFORMATION – DO NOT SHARE THESE MATERIALS

Mount Suspect’s Data Blob

- Mount all volume shadow data blobs on the suspect drive

-
  ```
  for /f "tokens=4" %f in ('vssadmin list shadows ^| findstr GLOBALROOT') do @for /f "tokens=4 delims=\" %g in ("%f") do @mklink /d %SYSTEMDRIVE%\%g %f\
  ```
- %SYSTEMDRIVE% is the drive letter of the suspect hard drive

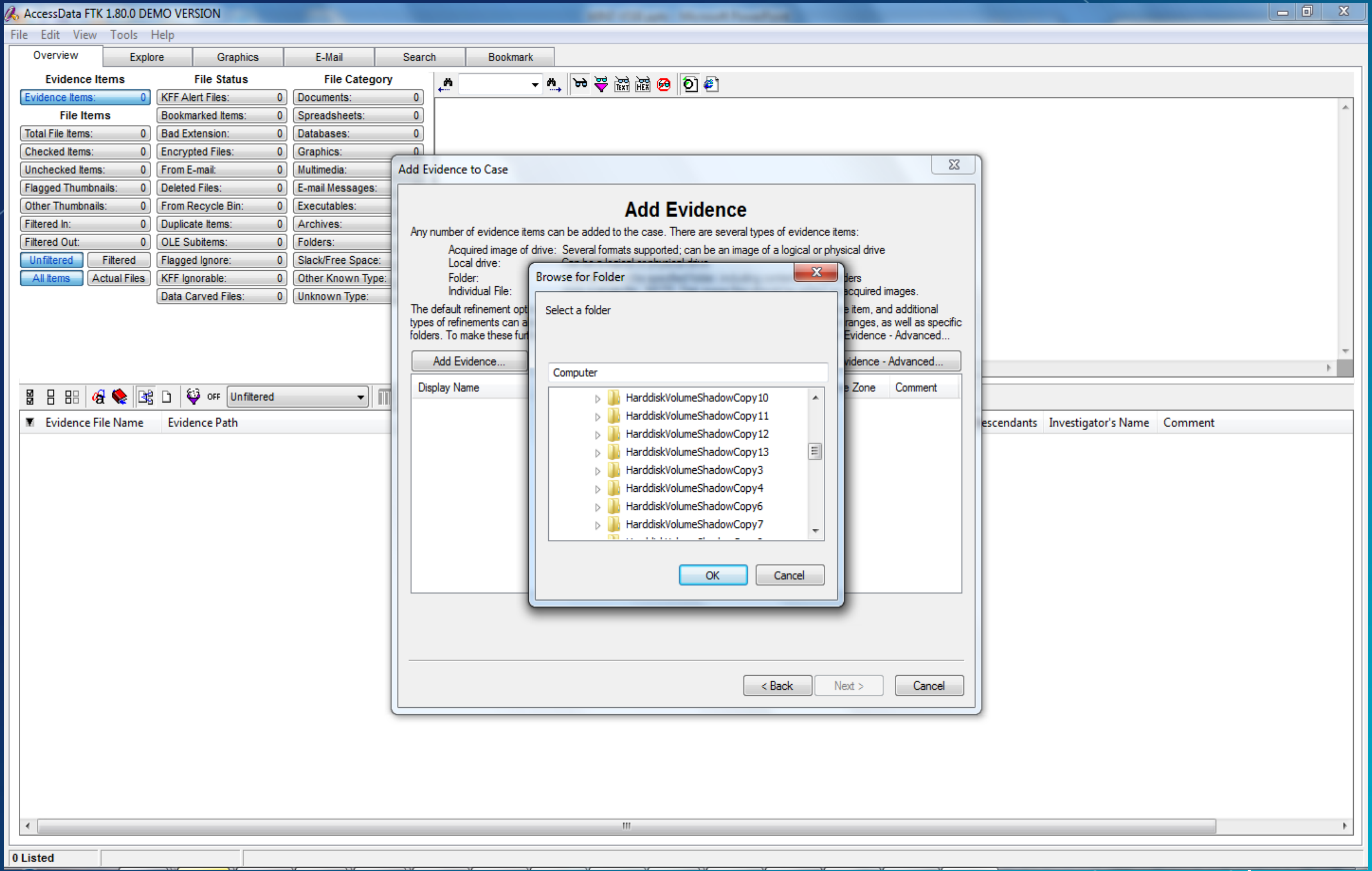
Mount Suspect’s Data Blob



```
C:\Windows\system32>for /f "tokens=4" %f in ('vssadmin list shadows ^| findstr GLOBALROOT'
) do @for /f "tokens=4 delims=\" %g in ("%f") do @mklink /d h:\%g %f\
symbolic link created for h:\HarddiskVolumeShadowCopy12 <<===>> \\?\GLOBALROOT\Device\Hard
diskVolumeShadowCopy12\
symbolic link created for h:\HarddiskVolumeShadowCopy13 <<===>> \\?\GLOBALROOT\Device\Hard
diskVolumeShadowCopy13\
symbolic link created for h:\HarddiskVolumeShadowCopy3 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy3\
symbolic link created for h:\HarddiskVolumeShadowCopy4 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy4\
symbolic link created for h:\HarddiskVolumeShadowCopy7 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy7\
symbolic link created for h:\HarddiskVolumeShadowCopy8 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy8\
symbolic link created for h:\HarddiskVolumeShadowCopy9 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy9\
symbolic link created for h:\HarddiskVolumeShadowCopy10 <<===>> \\?\GLOBALROOT\Device\Hard
diskVolumeShadowCopy10\
symbolic link created for h:\HarddiskVolumeShadowCopy11 <<===>> \\?\GLOBALROOT\Device\Hard
diskVolumeShadowCopy11\
symbolic link created for h:\HarddiskVolumeShadowCopy6 <<===>> \\?\GLOBALROOT\Device\Hardd
iskVolumeShadowCopy6\

C:\Windows\system32>
```

All shadow volumes mounted for suspect drive

Image Symbolic Links



Add Evidence to Case

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
Local drive:
Folder:
Individual File:

...ders
...cquired images.

The default refinement opt... types of refinements can a... folders. To make these fur...

...item, and additional ...ranges, as well as specific ...Evidence - Advanced...

Browse for Folder

Select a folder

Computer

- HarddiskVolumeShadowCopy10
- HarddiskVolumeShadowCopy11
- HarddiskVolumeShadowCopy12
- HarddiskVolumeShadowCopy13
- HarddiskVolumeShadowCopy3
- HarddiskVolumeShadowCopy4
- HarddiskVolumeShadowCopy6
- HarddiskVolumeShadowCopy7

Microsoft Services

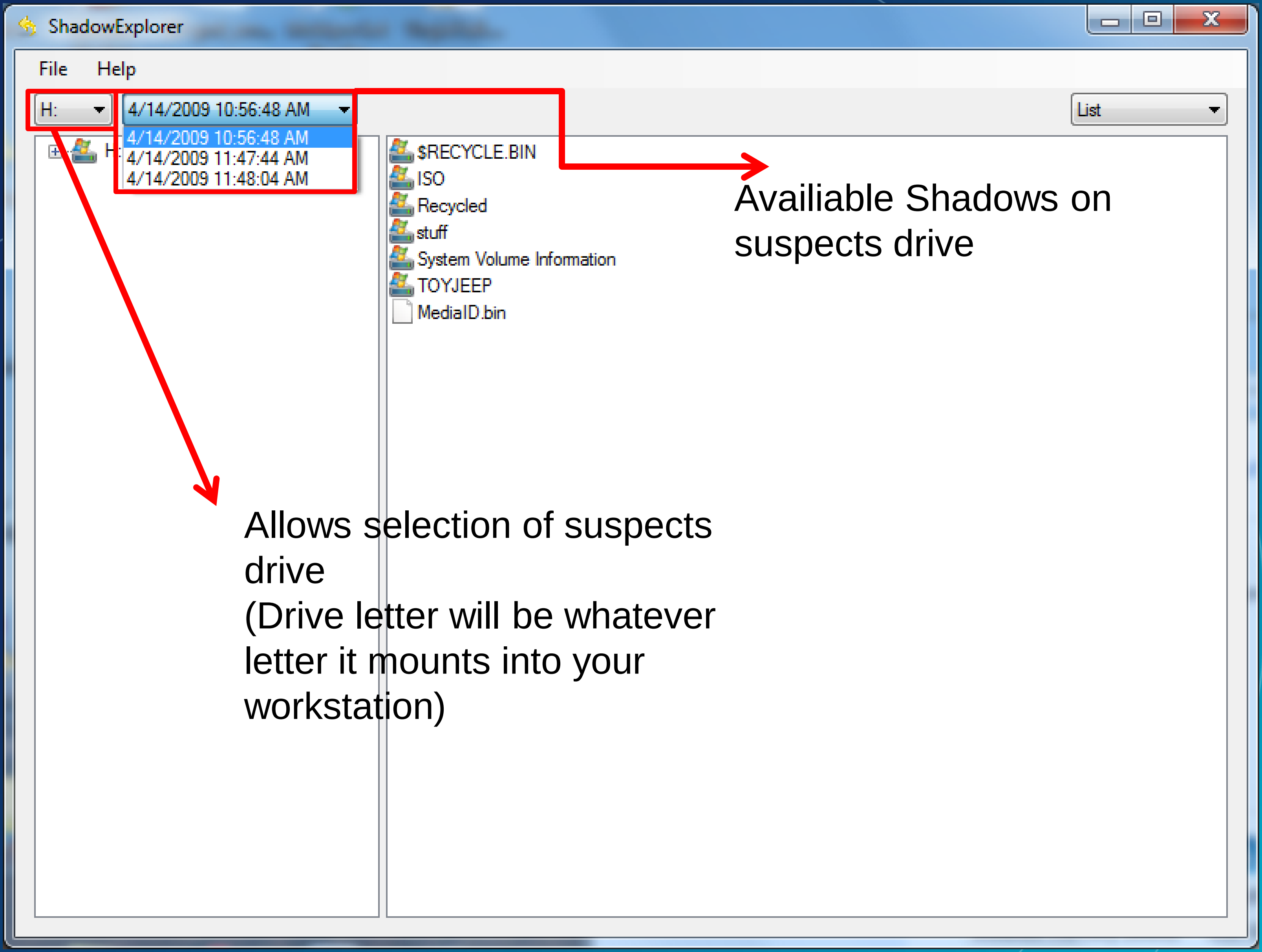
Mount Drive in Forensic Workstation and Use Workstation Third Party Utility to Access Volume Shadow Data

- Pluses
  - Better file exploration presentation
  - Easier to use than command line arguments
- Minuses
  - No guarantee of quality from the tool
  - Not a Microsoft supported tool

Shadow Explorer

- www.shadowexplorer.com
- Free utility
- Features
  - Show dates of all snapshots
  - Browse through Shadow Copies
  - Retrieve previous versions of files and folders

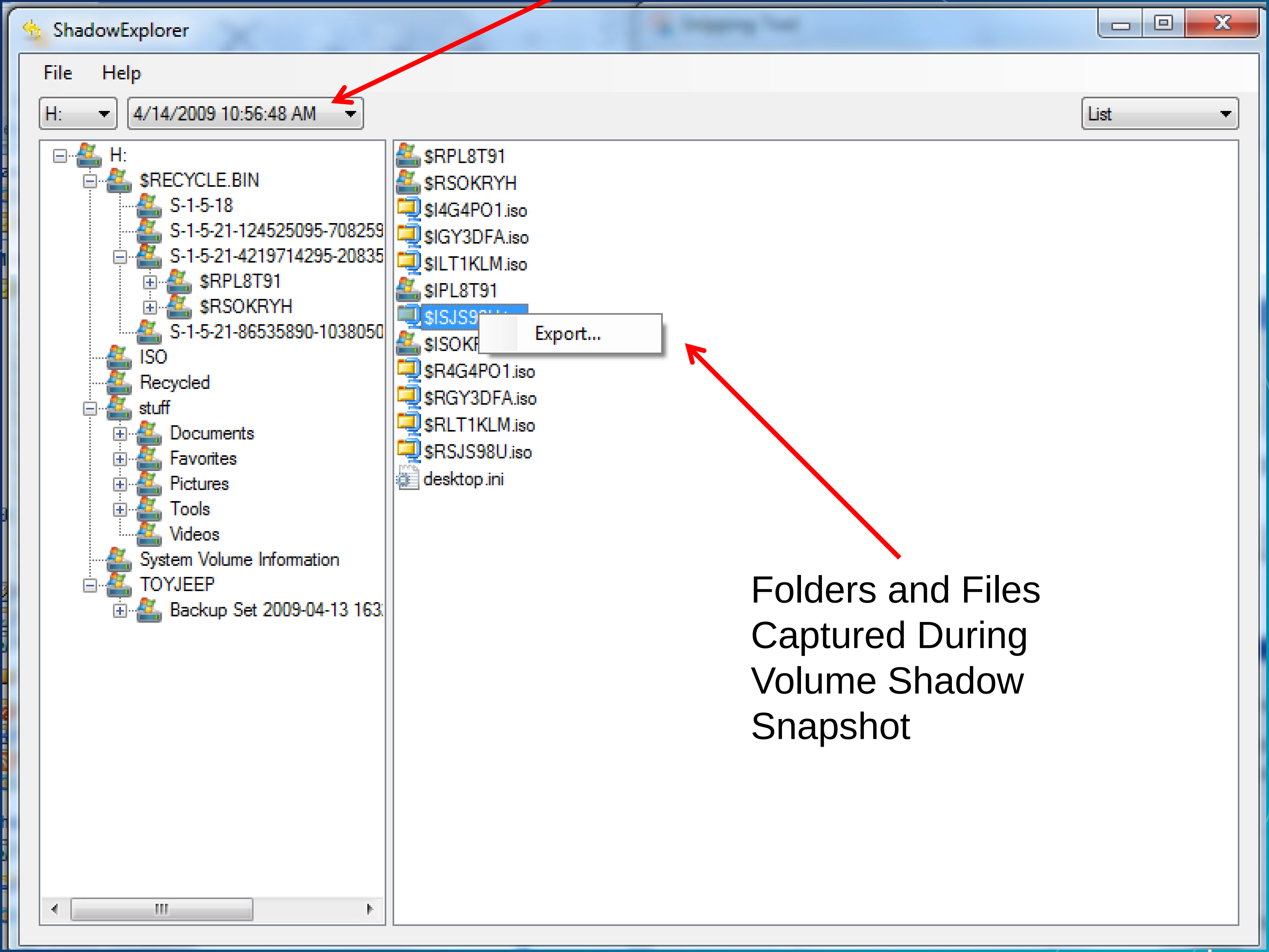
NOTE: This is not a Microsoft product. It is shown as an example of a third party utility leveraging the API to the volume shadow store. No responsibility is taken for this or any other third party utility.



Availiable Shadows on suspects drive

Allows selection of suspects drive
(Drive letter will be whatever letter it mounts into your workstation)

Date and Time of Snapshot



H: | 4/14/2009 10:56:48 AM | List

```
H:
  $RECYCLE.BIN
    S-1-5-18
    S-1-5-21-124525095-708259
    S-1-5-21-4219714295-20835
      $RPL8T91
      $RSOKRYH
    S-1-5-21-86535890-1038050
  ISO
  Recycled
  stuff
    Documents
    Favorites
    Pictures
    Tools
    Videos
  System Volume Information
  TOYJEEP
    Backup Set 2009-04-13 163
```

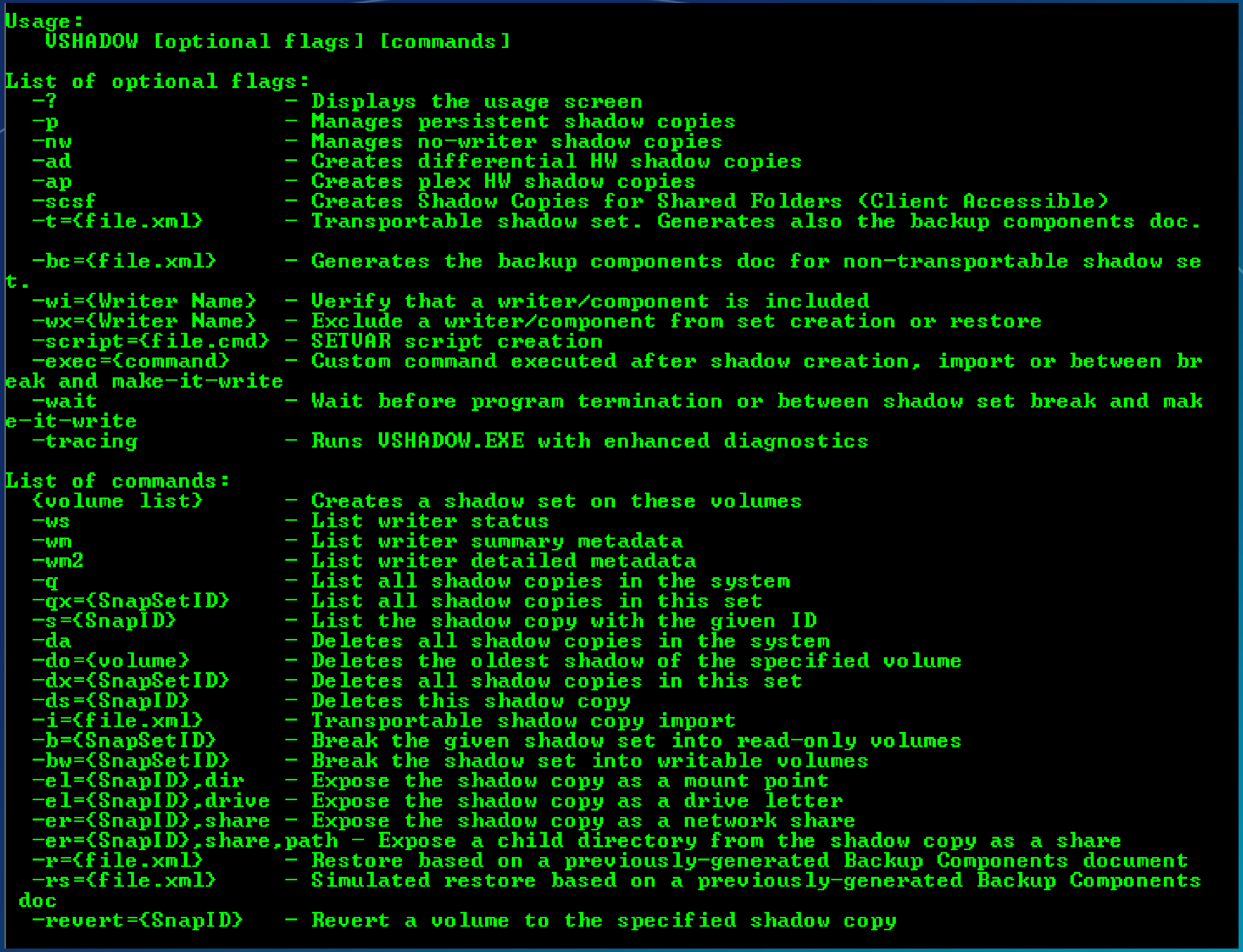
```
$RPL8T91
$RSOKRYH
$I4G4PO1.iso
$IGY3DFA.iso
$ILT1KLM.iso
$IPL8T91
$ISJS9
$ISOKF
$R4G4PO1.iso
$RGY3DFA.iso
$RLT1KLM.iso
$RSJS98U.iso
desktop.ini
```

Folders and Files Captured During Volume Shadow Snapshot

VSS Tools

- Vshadow is a tool included in the Volume Shadow Copy Software Development Kit and it has increased functionality
- With Vshadow and administrator can:
  - List all volume snapshots
  - Mount certain types of snapshots as a drive letter in Windows Explorer
  - **DELETE** all volume snapshot data

VSS Tools

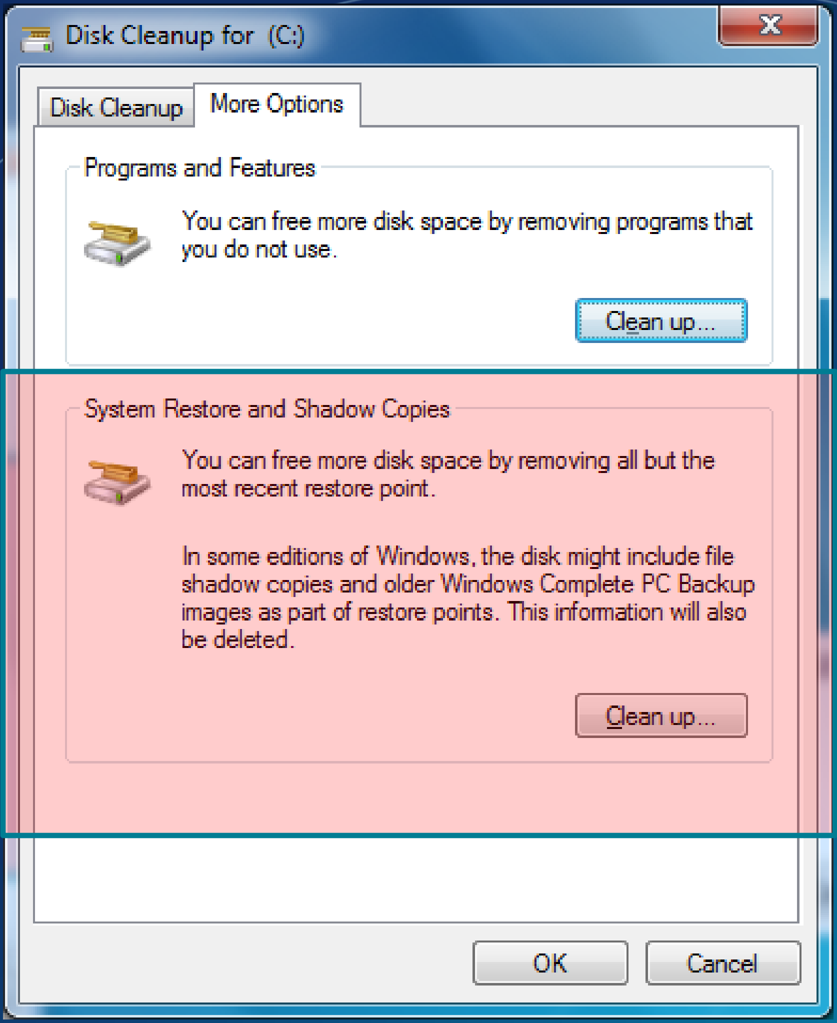


```
Usage:
   VSHADOW [optional flags] [commands]

List of optional flags:
  -?                 - Displays the usage screen
  -p                 - Manages persistent shadow copies
  -nw                - Manages no-writer shadow copies
  -ad                - Creates differential HW shadow copies
  -ap                - Creates plex HW shadow copies
  -scsf              - Creates Shadow Copies for Shared Folders (Client Accessible)
  -t={file.xml}      - Transportable shadow set. Generates also the backup components doc.

  -bc={file.xml}     - Generates the backup components doc for non-transportable shadow se
t.
  -wi={Writer Name}  - Verify that a writer/component is included
  -wx={Writer Name}  - Exclude a writer/component from set creation or restore
  -script={file.cmd} - SETVAR script creation
  -exec={command}    - Custom command executed after shadow creation, import or between br
eak and make-it-write
  -wait              - Wait before program termination or between shadow set break and mak
e-it-write
  -tracing           - Runs VSHADOW.EXE with enhanced diagnostics

List of commands:
  {volume list}      - Creates a shadow set on these volumes
  -ws                - List writer status
  -wm                - List writer summary metadata
  -wm2               - List writer detailed metadata
  -q                 - List all shadow copies in the system
  -qx={SnapSetID}    - List all shadow copies in this set
  -s={SnapID}        - List the shadow copy with the given ID
  -da                - Deletes all shadow copies in the system
  -do={volume}       - Deletes the oldest shadow of the specified volume
  -dx={SnapSetID}    - Deletes all shadow copies in this set
  -ds={SnapID}       - Deletes this shadow copy
  -i={file.xml}      - Transportable shadow copy import
  -b={SnapSetID}     - Break the given shadow set into read-only volumes
  -bw={SnapSetID}    - Break the shadow set into writable volumes
  -el={SnapID},dir   - Expose the shadow copy as a mount point
  -el={SnapID},drive - Expose the shadow copy as a drive letter
  -er={SnapID},share - Expose the shadow copy as a network share
  -er={SnapID},share,path - Expose a child directory from the shadow copy as a share
  -r={file.xml}      - Restore based on a previously-generated Backup Components document
  -rs={file.xml}     - Simulated restore based on a previously-generated Backup Components
 doc
  -revert={SnapID}   - Revert a volume to the specified shadow copy
```

VSS Tools

- There are a number of ways to prevent shadow copies from being created and/or deleting volume snapshot data.
  - Disable the Volume Shadow Copy Service
  - Disk Cleanup option allows for removal of all but the most current snapshot
  - Deselect disks in the System Protection GUI disables VSS from creating new and deletes all existing snapshots
  - Vshadow –da removes all snapshots

VSS Tools



Disk Cleanup for (C:)

Disk Cleanup | More Options

Programs and Features

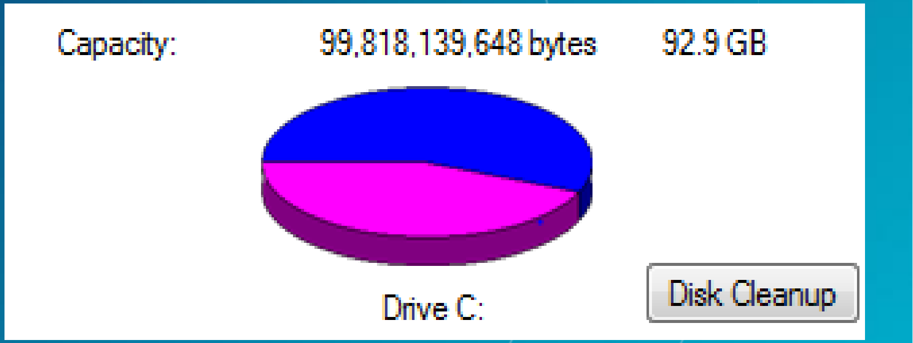
You can free more disk space by removing programs that you do not use.

System Restore and Shadow Copies

You can free more disk space by removing all but the most recent restore point.

In some editions of Windows, the disk might include file shadow copies and older Windows Complete PC Backup images as part of restore points. This information will also be deleted.

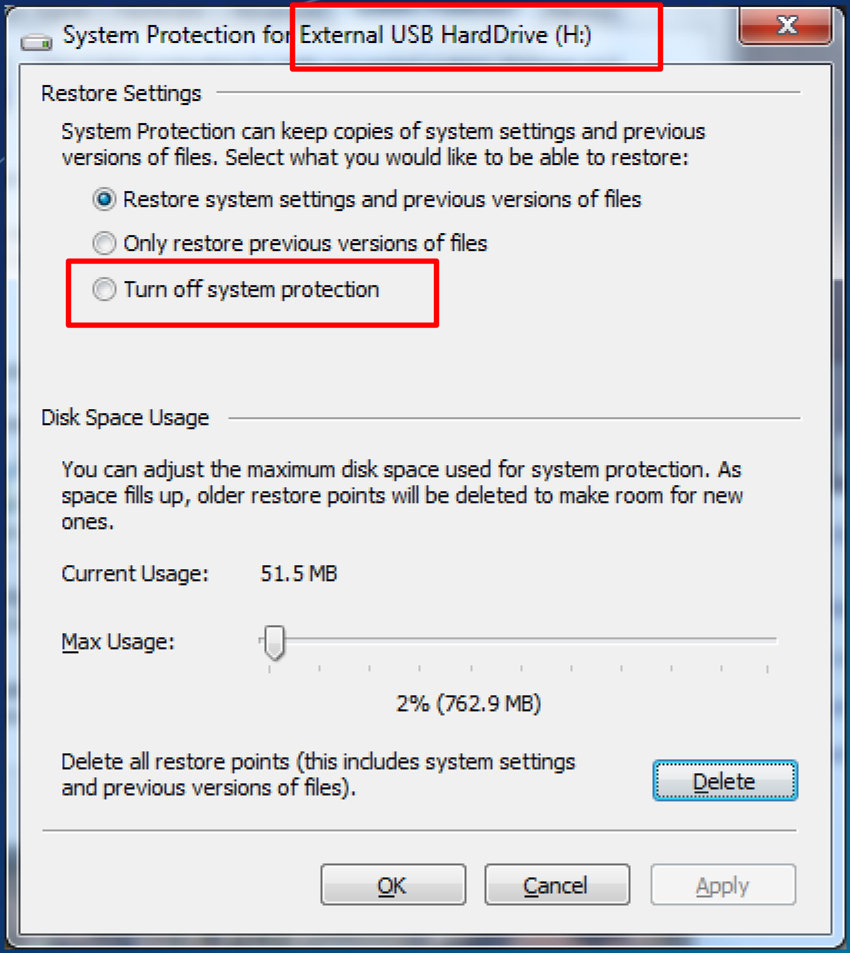
- “You can free more disk space by removing all but the most recent restore point”



Capacity: 99,818,139,648 bytes 92.9 GB

VSS Tools

VSS can be disabled on a drive by drive basis



System Protection for External USB HardDrive (H:)

Restore Settings

System Protection can keep copies of system settings and previous versions of files. Select what you would like to be able to restore:

● Restore system settings and previous versions of files

○ Only restore previous versions of files

○ Turn off system protection

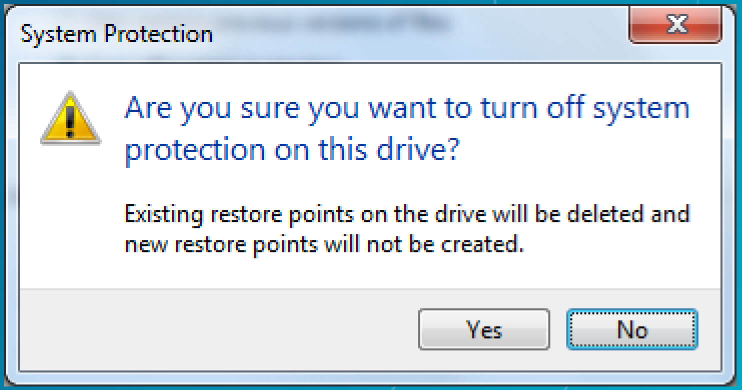
Disk Space Usage

You can adjust the maximum disk space used for system protection. As space fills up, older restore points will be deleted to make room for new ones.

Current Usage: 51.5 MB

Max Usage: 2% (762.9 MB)

Delete all restore points (this includes system settings and previous versions of files).



System Protection

Are you sure you want to turn off system protection on this drive?

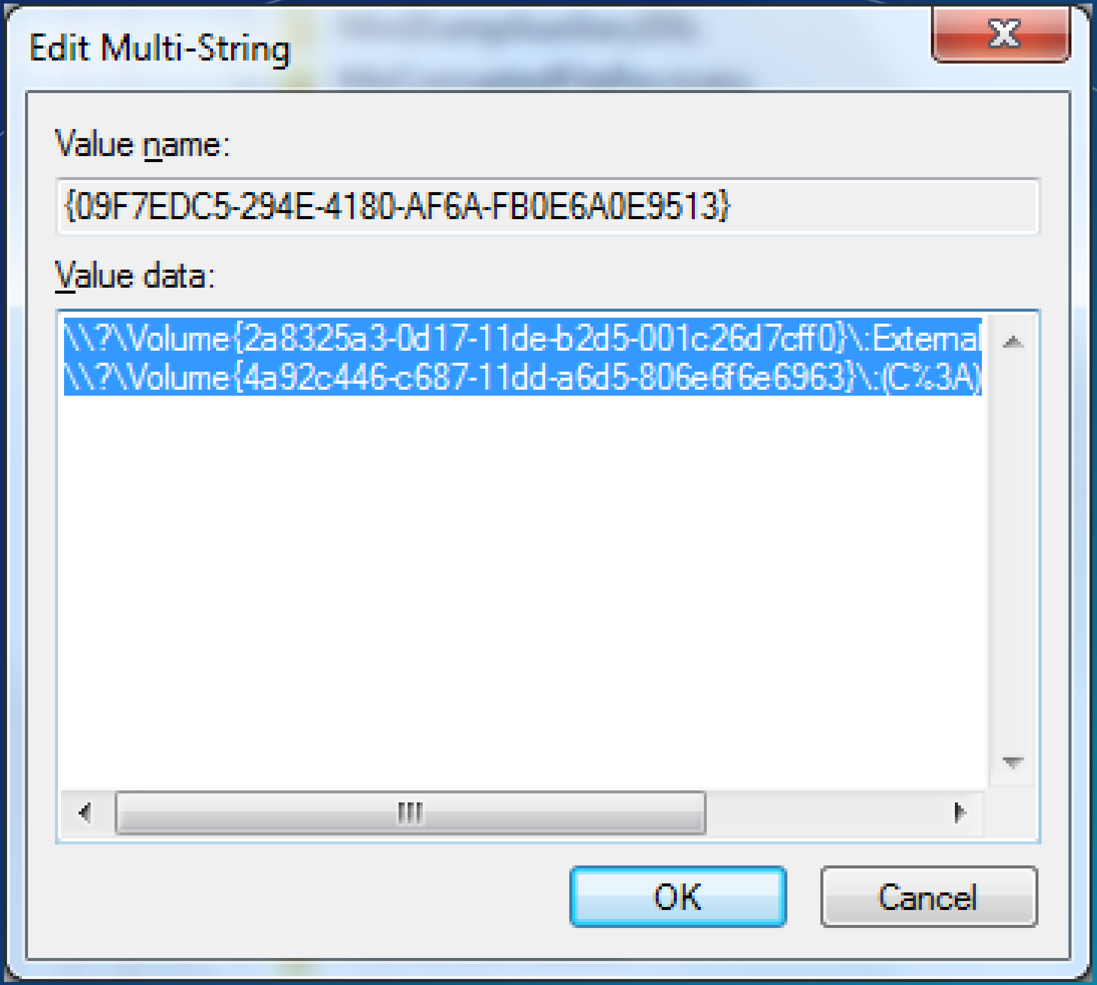
Existing restore points on the drive will be deleted and new restore points will not be created.

VSS Tools

- Settings for which volumes are currently being monitored on the system are located in the following registry key:

  HKLM\SOFTWARE\Microsoft\WINDOWS NT\CURRENTVERSION\SPP\Clients\{09F7EDC5-294E-4180-AF6A-FB0E6A0E9513}

VSS Tools



Value name:

{09F7EDC5-294E-4180-AF6A-FB0E6A0E9513}

Value data:

```
\\?\Volume{2a8325a3-0d17-11de-b2d5-001c26d7cff0}\:Externa
\\?\Volume{4a92c446-c687-11dd-a6d5-806e6f6e6963}\:(C%3A)
```

- All volumes monitored in System Protection are listed in this MULTI_SZ value

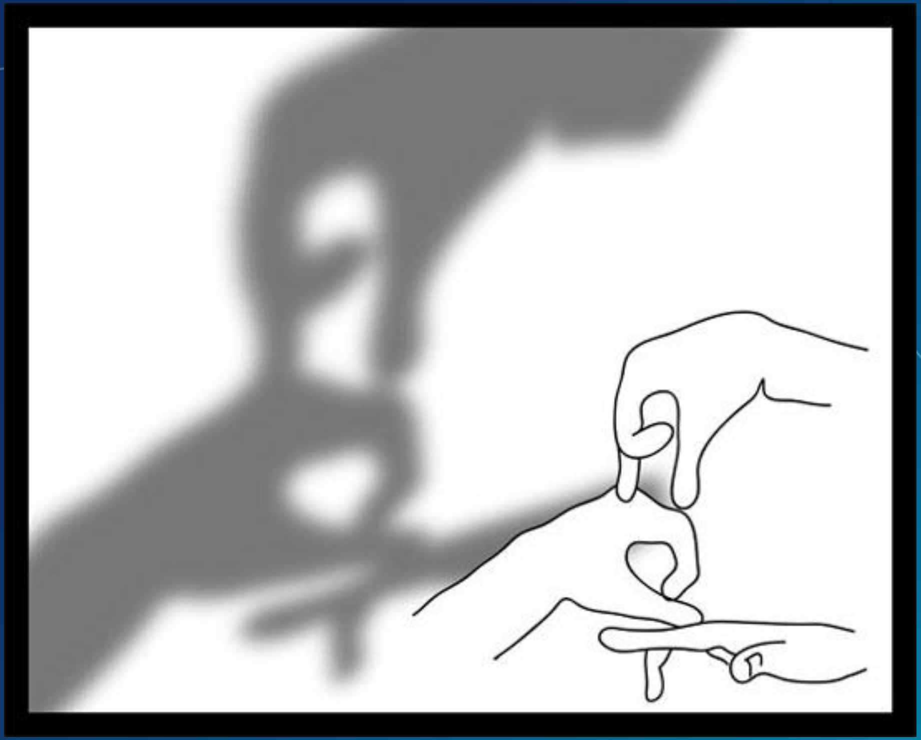
Can Volume Shadow Services be Disabled?

- There are a number of ways to prevent shadow copies from being created and/or deleting volume snapshot data
  - Disable the Volume Shadow Copy Service
  - Disk Cleanup option allows for removal of all but most current snapshot
  - Deselect System Protection via the GUI prevents VSS from creating new and deletes all existing snapshots
  - Vshadow –da removes all snapshots

Questions?

20

Minutes



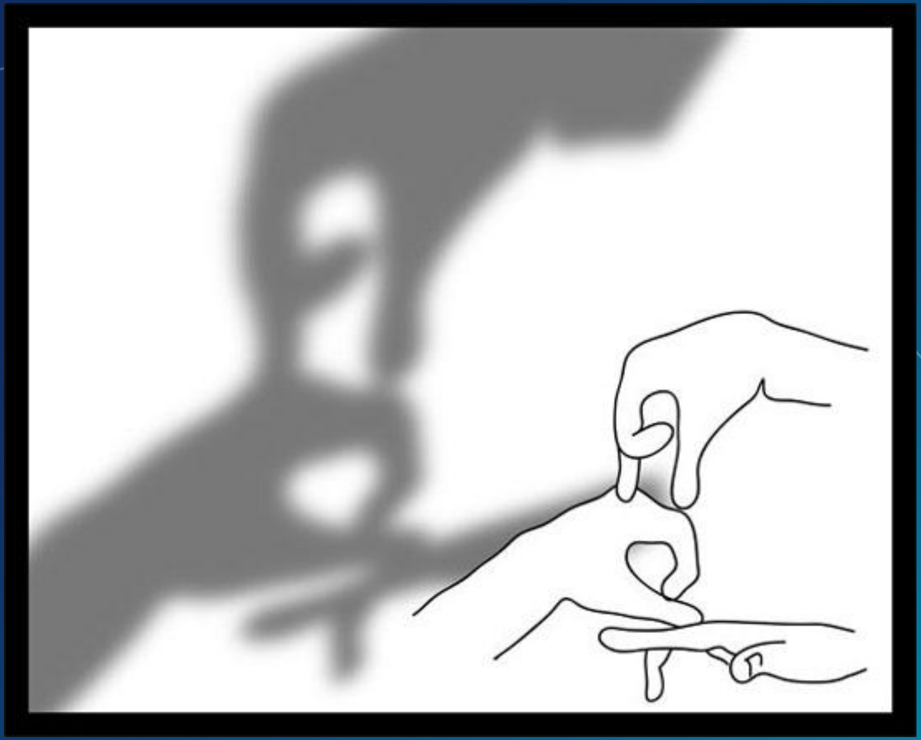
Using the File Backup Feature

Exercise

Microsoft | Services

30

Minutes



Recovering Previous Versions and Deleted Files

Exercise

Microsoft® | Services