

VISTA and Windows 7 Shadow Volume Forensics

Rob Lee

Shadow Copy Volume forensics will enable an investigator to examine data at many different time snapshots during a forensic examination. While XP Restore Point snapshots only gather key files including the registry, the shadow copy volume will allow access to them all. Investigating shadow copy volumes in organizations might become a key investigative tool for both e-Discovery and traditional forensics. First off, a hats off to Troy Larson, Senior Forensic Investigator from Microsoft, who just put this information out into the forensic community. In addition to his own research, Troy was able to query the Microsoft development team of the Volume Shadow Copy for additional capabilities. As a result, I have been a happy forensic investigator all day long playing with the capability.

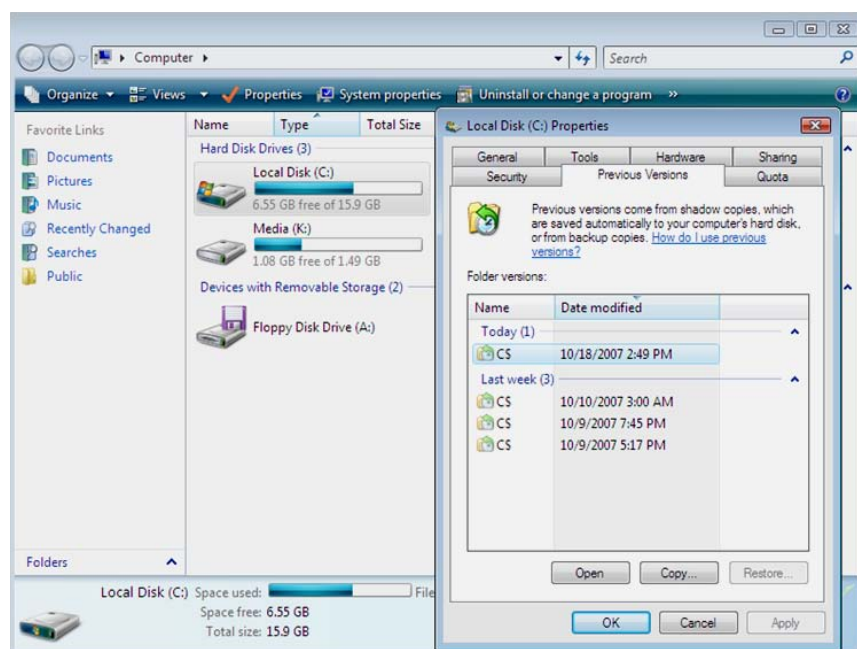
Shadow Copy Volume Background

Shadow copy is an exciting new possibility for forensic investigators looking for an additional edge in computer forensics. Restore point data, similar to what is found in Windows XP, does not exist in the same format in Windows 2003, VISTA, or Server 2008. 2003, VISTA, and Server 2008 now log changes to the entire volume and keep track of the specific clusters that are changed between each snapshot in the new Volume Shadow Copy Service or VSS.

Volume Shadow Copy Service (or Shadow Copy) is very similar to the "Time Machine" service for Macs. It performs a cluster by cluster diffing/backup and stores that information. In a nutshell, you can rewind a file, a directory, or even an entire volume to a previous state. This is wonderful for incident response and forensic investigators.

All versions of VISTA have Shadow Copy enabled by default, however, only Business, Enterprise, and Ultimate have a way to access it easily. In a way, it is very similar in concept to VMware snapshot where it backs up differential changes in the volume into a snapshot file. Note: the following techniques have only been tested on VISTA Business version. Further testing would need to be accomplished on other versions of Microsoft products with Shadow Copy enabled.

Shadow copy enables a user to revert an entire volume, a folder, or a file back in time to a previous version. An investigator can also copy out of the Shadow Copy a previous version of the file and examine the differences. VSS typically takes a snapshot once a day, but more might be found. However, it will not log continuous changes every time the user saves a file.



VISTA and Windows 7 Shadow Volume Forensics

Rob Lee

Vista Previous Versions

This is a snapshot of the of the restoration points created by VSS. If you notice the entire volume of C can be backed up to earlier dates. This would mean that if a user wiped a file today it could be recoverable at an earlier point in time that was where a shadow copy snapshot took place. If an investigator examined the shadow volume created from the previous day's snapshot, the file is recoverable from that volume. The shadow volume that can be examined is an exact duplicate backup of the entire volume including unallocated space.

How many shadow volumes will an investigator have access to? It depends on disk size. Generally 15% of disk space is allocated for the volume shadow, however, upwards of 30% of disk space could be utilized.

Which versions of VISTA are VSS enabled? For all versions, system restore will utilize the VSS in order to back the computer up to a previous snapshot. For Business, Enterprise, and Ultimate versions, "Previous Versions" is enabled that will allow a user to "rewind" a file, a directory, or an entire volume. However, the VSS service is up and running on the basic and home versions of VISTA, but the previous versions option is not displayed.

Important: Currently, you can only examine shadow copy volumes if you have the original device the shadow copy volumes are on. You cannot examine or recover shadow copy volumes from a disk image file mounted on your workstation via ntfs-3g, Encase, vdk, or mount image pro. However, you can examine a volume image duplicated from the Shadow Copy Volume. More on this shortly...

You have to mount, in read-only mode, your original hard drive that contains the shadow copy volumes on an VISTA machine. This might change as more capability is developed, but it is important to note that the best way to analyze/examine shadow copy volumes is by having access to the original drive or machine where they were created from.

List the Shadow Copy Volumes

How many Volumes are stored on the system you are examining? You can obtain a list of existing shadow volumes in the Volume Shadow copy Service by executing the tool, vssadmin.

To obtain a list of the shadows execute: `C:\> vssadmin list shadows /for=C:`

Things to notice:

1. The Shadow Copy Volume is the name of the volume that we will use to examine the contents of that specific volume. You might want to write the exact name down.
2. The originating machine would be noteworthy if you have plugged in an NTFS drive from another shadow copy enabled machine.
3. The system time at the moment the volume was created. This time is important as it may indicate which shadow copy volume may contain your data.

From the output of vssadmin, note the total number of shadow copy volumes from the machine. In this example, it only shows three. But there were 15 total shadow copy volumes that were listed as a result of running the "vssadmin list shadows" command. This particular machine had a 700 GB partition volume allocated for the C drive. If you decide to image the shadow copy volumes, you could theoretically have over 16 separate 700 GB logical images created from this one machine, each one from a different point in time.

VISTA and Windows 7 Shadow Volume Forensics

Rob Lee

```
ca: D:\IR\vista\cmd.exe
C:\>vssadmin list shadows /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Contents of shadow copy set ID: {2aaba183-7800-440f-a7ae-dcda1ac569e6}
  Contained 1 shadow copies at creation time: 10/21/2007 12:00:32 AM
  Shadow Copy ID: {92283529-31f5-4fe3-9e07-5199ec865d88}
  Original Volume: (C:)\?\Volume{83c56c2b-afcf-11db-8b03-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2
  Originating Machine: vista-test
  Service Machine: vista-test
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1, Auto recovered

Contents of shadow copy set ID: {87eac5e5-8ed6-4581-a82d-8c92e7d899a8}
  Contained 1 shadow copies at creation time: 9/24/2008 11:52:15 PM
  Shadow Copy ID: {7dc9f35f-df50-465b-be68-11fffe70ad90}
  Original Volume: (C:)\?\Volume{83c56c2b-afcf-11db-8b03-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
  Originating Machine: vista-test
  Service Machine: vista-test
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
1, Auto recovered

Contents of shadow copy set ID: {d156c210-4c8a-4f8b-b048-7f5b48bfa0bf}
  Contained 1 shadow copies at creation time: 9/25/2008 12:30:50 AM
  Shadow Copy ID: {8a41221f-2b97-45a0-9db8-8237d94d46a7}
  Original Volume: (C:)\?\Volume{83c56c2b-afcf-11db-8b03-806e6f6e6963}\
  Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
  Originating Machine: vista-test
  Service Machine: vista-test
  Provider: 'Microsoft Software Shadow Copy provider 1.0'
  Type: ClientAccessibleWriters
  Attributes: Persistent, Client-accessible, No auto release, Differential
```

Live Shadow Volume Examination

On a live machine it might be useful to manually browse or scan a directory that contains a shadow copy volume. It is relatively easy to do this from an administrator enabled command prompt using the tool mklink. mklink creates symbolic links, which are new to VISTA, from the command line. You can create a symbolic link from a shadow copy volume to your desktop easily by executing the following command.

From your previous output of vssadmin, select one of the "Shadow Copy Volume" names based off of the date in time you would like to examine. Then create the symbolic link using mklink pointing it at a directory followed by the device name of the shadow copy volume you wish to parse.

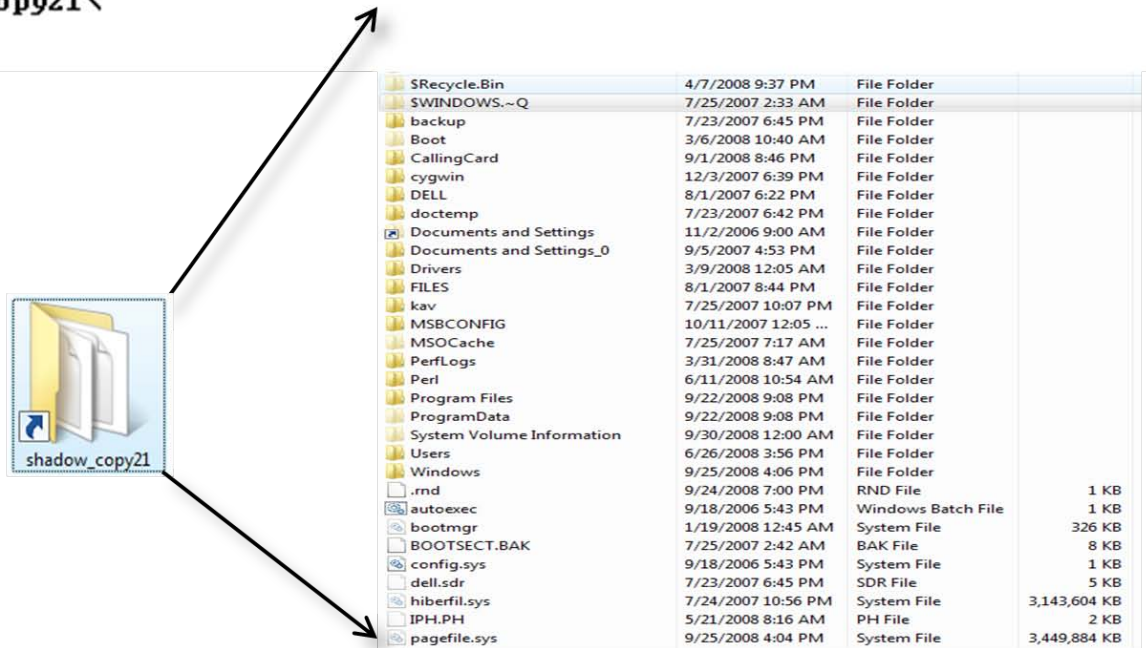
```
C:\> mklink /d C:\shadow_copy21 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy21\
```

Very important! It is important you do NOT forget the trailing slash at the end of the mklink command!!! Without it you will receive a permission error.

VISTA and Windows 7 Shadow Volume Forensics

Rob Lee

```
C:\>mklink /d C:\shadow_copy21 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy21\  
symbolic link created for C:\shadow_copy21 <<===>> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy21\  
C:\>
```



Creating A Symbolic Link To A Shadow Copy Volume

This capability would be incredibly useful in situations where a bad guy might have wiped a file. You could recover it by going back a day or two in the shadow copy volume to retrieve the file from allocated space.

Imaging a Shadow Volume

It is also rather simple to image the full volume of a specific shadow by utilizing one of the latest versions of the dd.exe command by George Garner and the output from the vssadmin list shadows command.

Using the “vssadmin list shadows” output, identify the shadow copy volume number you wish to image. In this situation, you would utilize the part of the device name that includes “HarddiskVolumeShadowcopy#” The # (number) is the number of the shadow copy volume you wish to acquire a full disk image from.

All the regular options in dd apply, but to image execute a command similar to the following on your machine that contains the volume shadow copy or the read-only original drive containing the volume shadow copy.

In this command F: is a USB drive plugged into bn.; the machine. The --localwrt option allows the dd.exe tool write to a local mounted drive.

```
dd.exe if=\\.\HarddiskVolumeShadowCopy4 of=F:\snapshot4.img -localwrt
```

```
F:\fau\FAU.x86>dd if=\\.\HarddiskVolumeShadowCopy4 of=F:\snapshot4.img --localwrt  
Copying \\.\HarddiskVolumeShadowCopy4 to F:\snapshot4.img
```

Imaging a Shadow Copy Volume using dd.exe

VISTA and Windows 7 Shadow Volume Forensics

Rob Lee

Shadow Forensics

Mounting your collected shadow copy volume image is easy using the ntfs-3g command from your SIFT workstation.

Commands typed:

```
# ntfs-3g -o ro,loop,show_sys_files snapshot4.img /mnt/hack/snapshot4
```

In addition, you can examine the image utilizing any of the sleuthkit tools, perform unallocated space analysis, and perform file carves as you would a normal image. Remember we had 15 shadow copy volumes and the original volume. We could theoretically examine 16 total images from a single machine. Each one a full disk volume from that moment in time.

```
[root@SIFTWorkstation /]# cd /images/windowsforensics/
[root@SIFTWorkstation windowsforensics]# ls
snapshot4.img
[root@SIFTWorkstation windowsforensics]# mkdir /mnt/hack/snapshot4
[root@SIFTWorkstation windowsforensics]# ntfs-3g -o ro,loop,show_sys_files snapshot4.img /mnt/hack/s
napshot4/
[root@SIFTWorkstation windowsforensics]# cd /mnt/hack/snapshot4/
[root@SIFTWorkstation snapshot4]# ls
$AttrDef      $Boot          $Extend       ProgramData    test
autoexec.bat  bootmgr        hiberfil.sys  Program Files  $UpCase
$BadClus     BOOTSECT.BAK  $LogFile      $Recycle.Bin  Users
$Bitmap      config.sys     $MFTMirr     $Secure        $Volume
Boot         Documents and Settings  pagefile.sys  System Volume Information  Windows
```

ntfs-3g mount of acquired shadow image

With the shadow copy volume mounted, an investigator can browse to the share directory of the SIFT Workstation by clicking from their Windows machine (START->RUN>and type \\SIFTWorkstation). They should see two directories (hack and images). In the hack directory, a subdirectory with the shadow mount (in this case snapshot4) will be seen and an investigator can now parse and examine any file from a windows machine in read-only mode.

More research needs to be accomplished as to how to examine or enable this feature on Windows XP machines. Apparently, the VSS Service is enabled, but when I checked on several versions of it there were no Shadow Copy Volumes created. I have started reading about how to enable a back feature utilizing NTBACKUP, but will continue down that path shortly. In the end, this capability might be incredibly useful to investigators and incident responders in many situations and could help solve many crimes.