Volume Shadow Copy Forensics Report

by

Kyle Heath

Katherine Delude

Patrick Leahy Center for Digital Investigation

Champlain College

30 March 2012

Contents

1 Introduction

1.1 Research Problem

We are trying to determine the forensic viability of Volume Shadow Copy [also known as Volume Shadow Copy Service or Volume Shadow Service]. This program is a default backup service that comes with the Windows operating system. It is a file-system level program that performs backups on a weekly basis in Windows 7. Although shadow copies are used as the basis for System Restore and creating restore points, they have a different structure than restore points. It also creates shadow copies whenever a significant event happens, such as an installation or a system update.

1.2 Field of Research

We are researching the history and forensic viability of Volume Shadow Copy. For the purpose of this project, we are primarily focusing on the forensic viability of shadow copies.

1.3 Research Questions

How can the Volume Shadow Copy service be seen from a forensic standpoint? How can shadow copies be used in a forensic examination or investigation? What information do they contain? How can we access them? In what specific ways (command line v. GUI/program) can a user access shadow copies?

1.4 Contributions

By answering these questions and learning more about the Volume Shadow Copy process, we will be contributing knowledge to the digital forensics community and providing them with a greater understanding of the Volume Shadow Copy process in the context of a forensic investigation.

1.5 Report Overview

We decided to investigate this issue by first conducting research into the Volume Shadow Copy process; specifically, what it does, when it was first originated, and how shadow copies are made. We then constructed a Windows 7 virtual machine in VMWare and added several files to the system—mainly text documents and Microsoft Paint graphics. We then tried several methods to access and examine the data within the shadow copies.

2 Literature Review

In conducting our research into Volume Shadow Copy, we first consulted several digital forensic blogs that had posted on the subject as well as Microsoft's support website. The article "How Volume Shadow Copy Service Works" from Microsoft's TechNet website describes the methods and process of creating a shadow copy. We also read several blog posts from noted digital forensics and incident response blogs on how to access volume shadow copies. Some of these posts detailed how to access and view shadow copies using forensic tools such as EnCase. To tailor our research to our experiment, we found some information on Volume Shadow Copy in Windows 7. A whitepaper from QCCIS entitled "Reliably recovering evidential data from Volume Shadow Copies in Windows Vista and Windows 7" provided a good bulk of information about Volume Shadow Copy service. The whitepaper introduces a new technique for reliably recovering the original files stored in the volume shadow copies which contain these artifacts. This technique maintains the original date & time stamps and is flexible enough to extract everything in a VSS file or down to one specific file/user account. We also did a bit of research on

Volume Shadow Copy in the Windows Registry to learn more about how it functions. As the project progressed further along, We found that there were different methods to reliably recover data from the volume shadow copies in addition to those we had come across in my preliminary research.

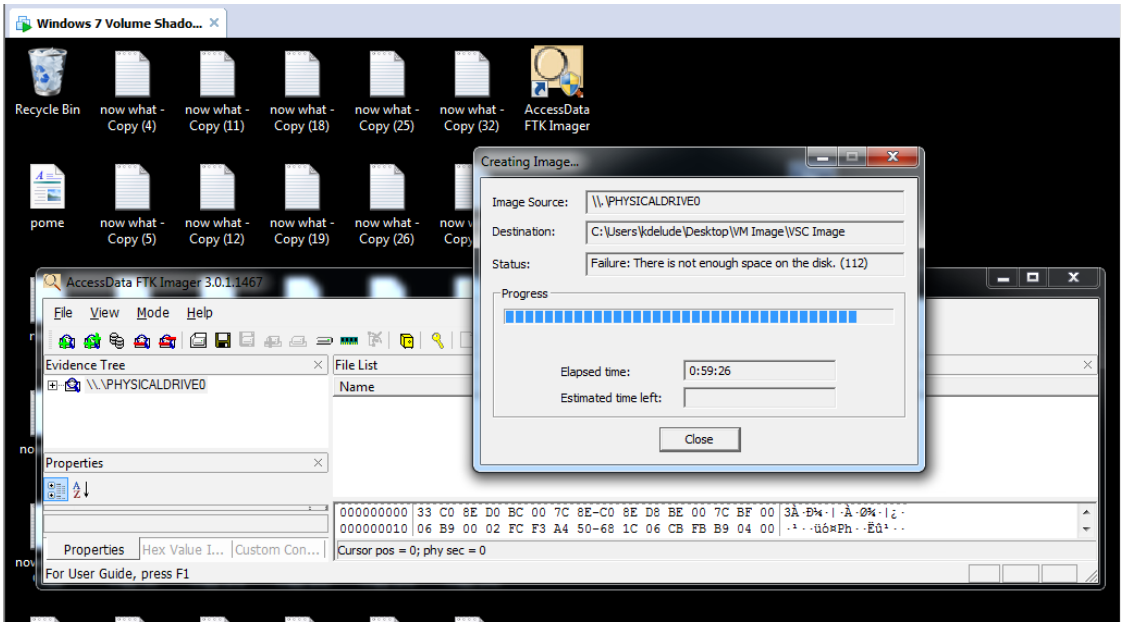
3 Methodology and Methods

We conducted our experiment by constructing a virtual machine using VMWare software of the Windows 7 operating system. We then created and added several files such as text and paint files. We then ran the command 'vssadmin list shadows /for=C:; which listed the shadow copies on the C drive in the virtual machine. This also listed shadow copy metadata, including date and time of creation, attributes, and the Shadow Copy ID, which identifies the shadow copy file and can be verified in EnCase. We then tried to make link for the shadow copies so that we could access them. We ran the command 'mklink /d C:\Volume\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1' which created a symbolic link for Volume Shadow Copy 1. We had some trouble creating a link for the second shadow copy. When we tried to symbolically link the second shadow copy after we had already linked the first one, we received an error message that said "Cannot create a file when the file already exists". We later found out that in this method you can only link shadow copies one at a time. We then moved on to several different methods based on what we had found in our preliminary research and our own skills and expertise.

3.1 Overarching methodology

First we created a Windows 7 virtual machine. We added some text and paint files and took snapshots of the virtual machine at various points to keep track of our progress. We tried to view VM in EnCase v. 6.19, but did not have much luck –specifically, we could not see the files we had created. We thought that we had acquired the wrong virtual machine disk file (VMDK) or that we had botched the acquisition.

With some help from Kyle and Ben Rogers, we installed FTK Imager in the virtual machine to view the virtual machine locally; this created a new shadow copy (01/13/2012 2:37 PM). We forensically imaged the virtual machine using FTK Imager and had to create another, larger hard drive (100 GB) to contain the image because the first hard drive (40 GB) was not large enough.



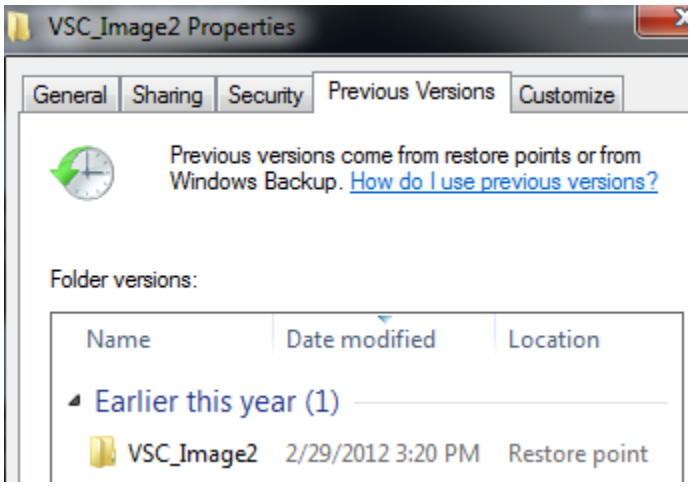
At this point we was able to see files we had put into the VM in FTK and in EnCase. We also saw the shadow copy ID's in EnCase under System Volume Information\SPP\OnlineMetadataCache. Although we knew that the shadow copies were there, we was unable to access them. We tried several different methods to do so. We first tried Log Parser, which was outlined in a post on the SANS' computer forensics blog: http://computer-forensics.sans.org/blog/2011/06/09/vscs-logparser. This method entailed creating a symbolic link for each shadow copy and then using Log Parser to extract data from the mounted shadow copies. It took some time to understand the syntax & how to construct the commands in the program. From there, we was able to access the symbolic link we had created for the first shadow copy and attempted to parse the information. The command said that it had run successfully, but that there had been numerous parse errors. When we attempted to discern what the errors were, it said that there were too many parse errors. We also tried Corey Harrell's method of parsing Volume Shadow Copies that he had delineated on his blog and in his recent DFIR Online post. His method was more approachable from a novice's standpoint and his automation of some of the examination processes was helpful, but, again, we did not have much luck. From there, we began to wonder if it was possible to parse or examine shadow copies that related to system updates or installations versus those that relate to file changes. We was then directed to more GUI-based tools that showed how the file structure looked (e.g, folders on the drive that was specified in the *vssadmin* command) at the time of the shadow copy's creation.

3.2 Data Collection

In the course of our project, there was a total of four shadow copies that the test VM created.

The screenshot above shows the shadow copies in the virtual machine on 23 March 2012. It was here that we had notice that there was a new shadow copy with the creation time of 2/29/2012 at 4:20:25 PM, which likely indicates a time offset.

The first shadow copy correlated with a VMWare Tools installation. It was created on 9 November 2011 at 2:25:16 PM. The second shadow copy correlated with a Windows Update and was created a short time later, on 9 November 2011 at 2:41:33 PM. When we tried to examine the virtual machine in EnCase and look for what we found, these were the only two listed but we could not find the files that we had created in the virtual machine. The third shadow copy correlated with the FTK Imager installation and was created on 13 January 2012 at 2:38:17 PM. Finally, the fourth shadow copy correlated with the previous version of the VSC_Image2 folder on the desktop in the Virtual Machine. The folder had a previous version, which listed the Modify time as 29 February 2012 at 3:20 PM, unlike the other files we had created in the virtual machine. We also noticed that the installation of Log Parser 2.2 was very close to the 'previous version' M time of the VSC_Image2 folder. The MAC times of Log Parser 2.2 are 29 February 2012, 3:22:14 PM. Toward the end of our project, the *vssadmin* command did not list the first shadow copy relating to the VMWare Tools Installation.



3.3 Analysis

In regards to a particular folder, shadow copies are stored in the System Volume Information folder. This can be verified in EnCase.

In Shadow Explorer, we was able to see what was affected by the creation of a volume shadow copy. Specifically, the NTUSER.DAT file and the BCD file are affected by the creation of a shadow copy. BCD (Boot Configuration Data) is a registry hive, and BCD.LOG files act as records for the hive and exists for recovery if the need arises. NTUSER.DAT , another registry file, contains information about settings for a particular individual account. Since the primary shadow copies that were on our virtual machine were primarily correlated to installations and updates, it would make some sense that the NTUSER.DAT file would be affected.

Path	File Type	Size	Modify Date	Modify Time	Access Date	Access Time	Create Date	Create Time
C:\Boot\BCD	File	24 KB	29-Feb-12	3:20:24 PM	29-Feb-12	2:52:35 PM	9-Nov-11	5:19:44 PM
C:\Boot\BCD.LOG	Text document	21 KB	29-Feb-12	3:20:24 PM	9-Nov-11	5:19:44 PM	9-Nov-11	5:19:44 PM
C:\Users\kdelude\NTUSER.DAT	DAT file	768 KB	29-Feb-12	3:20:24 PM	29-Feb-12	2:52:29 PM	9-Nov-11	2:23:58 PM
C:\Users\kdelude\ntuser.dat.LOG1	LOG1 file	225 KB	29-Feb-12	3:20:24 PM	9-Nov-11	2:23:58 PM	9-Nov-11	2:23:58 PM

4 Results

We found that there are specific files that change when a shadow copy is created, and that certain tools can show how a system/file structure looked at the time of a shadow copy's creation in a GUI format.

5 Conclusion

5.1 Forensic Standpoint

From a forensic standpoint, volume shadow copies contain information about how a specific file, folder, or even system has changed. This can be used to prove whether a suspect committed a certain crime and tried to hide or delete the evidence.

5.2 Investigation/Examination

Shadow copies can play a pivotal role in a digital forensic investigation because of the information they contain. They contain information about how a file system or folder structure looked at the time of the shadow copy's creation, which programs were installed, and which files were intact or deleted.

5.3 How can one access them?

There are several methods for accessing and extracting data from Volume Shadow Copies in a forensically sound manner.

5.4 What specific methods?

There are command-line and GUI methods for accessing and extracting data from Volume Shadow Copies in a forensically sound manner. Depending on the exigent circumstances and the practitioner's level of comfort with command-line interfaces, either method can work. These programs can allow one to examine how a file system or folder structure looked at the time of a shadow copy's creation without tampering with the original evidence.

6 Further Work

One particular further question we had was: Can one examine shadow copies that relate to system updates/installations? One could (and perhaps should) be able to do so, but it has not exactly been tried yet. From what we came across in my research, it was not discussed in much detail.

2. What are we trying to accomplish in our research?

a. When making recommendations on accessing and viewing shadow copies, certain methods work better than others based on experience/level of comfort with programming or the exigent circumstances.

b. We seek a deep understanding on how it works and what is affected or changed, and need to test these methods to ensure that they are forensically viable in a court of law.

c. We conducted our experiment in a controlled environment over a very short period of time. If the experiment had been conducted with a standard desktop machine or perhaps several servers over a longer period of time—for example, three years—there would be many more shadow copies to examine over a larger volume.

d. Recommendations and guidelines: Again, certain methods have their advantages and disadvantages depending on the situation and practitioner's level of experience and comfort with command-line and GUI tools.

3. The easiest and cheapest option would be to seek open-source tools that accomplish the tasks that one needs. The problem with that option is that not everyone is familiar with open-source tools or programming interfaces. If there is a time constraint, one may use the automation of processes through methods such as batch files to help with analysis.

a. Much of the software that we used was free and open-source, but the forensic software such as EnCase or FTK Imager will need to be licensed and maintained.

4. At a certain point, we can expose law enforcement to methods that would help them analyze shadow copies in an easy and time-efficient way.