# Forensic Analysis of Windows 10 Volume Shadow Copy Service

**Ahmad Ghafarian, Ph.D.**
**Dept. of Computer Science & Information Systems**
**Mike Cottrell College of Business**
**University of North Georgia**
**Dahlonega, GA 30597, USA**

**Ethan D. Hills**
**Dept. of Computer Science & Information Systems**
**Mike Cottrell College of Business**
**University of North Georgia**
**Dahlonega, GA 30597, USA**

**Abstract**

The Windows Operating System features a service called Volume Shadow Copy Service (VSS) that may provide evidential information to computer forensic investigators. Since Windows XP, the VSS has been utilized to take a snapshot of the active hard drive to be used in necessary recovery procedures. Originally designed to backup only operating system files, the VSS has become a popular OS software for third party recovery and backup programs for all file types. The volume shadow copy is a service actively running on Windows 10 by default that is triggered by either a Windows update or installation of new software. The forensic value of VSS becomes apparent when investigators are looking for suspicious activities such as deleting files. Comparing shadow copies is crucial for forensic investigators, as old shadows may prove valuable towards an investigation. In this paper, we develop a framework for the forensic analysis of Windows 10 VSS. We then use the framework to extract, analyze and demonstrate the forensic value of volume shadow copy in any forensic investigation.

**Keywords:** Computer forensics, Windows 10, volume shadow copy, volume shadow copy service, and VSS.

## 1. INTRODUCTION

Starting with Windows XP Service Pack 2 and Windows Server 2003, Microsoft has added a feature into the Windows operating systems called volume shadow Service (VSS.) This service allows Windows to take automatic or manual backups, or snapshots, of the current state of the files on a hard drive. Computer forensics investigators can use this feature to access the history of a computer's data as well as deleted or modified files [1].

There are two types of shadow copies, *clones*, and *copy-on-write*. *Clone* duplicates the original data for system restore purposes. In the *Copy-on-write* shadow, as changes are being made to a live system, the information being changed is saved. These changes are collected on a regular basis or when new software or system updates are added. They are stored locally, in the System Volume Information folder [2].

Volume shadow copies are created in two ways, automatically or manually. In the automatic process, shadows are snapped after an installation of a new program has been initialized or when there is a Windows Update. The VSS is activated by the OS and then catches an image of the drive of only files that have changed since the last snapshot. These images are then stored in the Systems information folder where they are protected until they are needed for Windows Recovery. However, some users prefer to create a shadow copy manually. This situation arises when the user makes changes in their files and want to make sure the systems preserve their files at specific points during the process.

From the forensics standpoint, there are also two methods to restore files from a shadow volume copy. The first method uses the built-in Windows feature called Previous Versions. The second method is to use a software tool such as Libvshadow [3] or Forensics Explorer [9]. In this research, we first develop a framework for evidence creation, evidence extraction, and evidence analysis. Subsequently, we use the framework to experimentally demonstrate the forensic value of Windows 10 volume shadow copies.

The rest of this paper is organized as follows. Section 2 discusses the background and previous research. The tools and technologies used in this research are described in section 3. Section 4 details the research method. The conclusion and analysis of the results appear in section 5.

## 2. LITERATURE REVIEW

To the best of our knowledge, there are limited research results on the forensics value Windows 10 Volume Shadow Copy. In Windows XP and Windows Server 2003 R2, volume shadow copy allows users to restore the Windows System back to a point in time. That was done because the Windows would generate a restore point after the installation of new updates or patches. This service was designed to restore only the operating system, not user files [5]. On Windows 10, the Volume Shadow Copy service performs a snapshot of the system at a given point in time. The snapshot also includes user-created files and folders. As a result, the volume shadow copy will allow a user as well as a forensics investigator to revert to a previous version of a file or folder, or restore deleted files or folders.

Heath and Delude [6] formulated a methodology to utilize the VSS in Windows 7 to investigate the forensic value of VSS. Their experiment utilized Encase forensics software, but they found difficulties with trying to view and open shadow files. This is because analysis of VSS requires specific tools. They conducted their experiment in a controlled environment over a brief period. Therefore, the authors suggest that more research is necessary to generate concrete results.

Balan [7] proposes a technique to obtain valuable evidence from Volume shadow copy on windows 7 operating system image. Their method is based on the utilization of the Master File Table (MFT) properties. Based on the Windows MFT properties, a file is represented as a chain of clusters on the hard drive which holds

the file entries. The MFT file entries hold the information about a single file. This includes the information about deleted files as well as modified files. In fact, when a file is deleted, the content of the file is still available. It is just no longer accessible in a normal fashion. They demonstrated that analysis of MFT on volume shadow copies produce valuable forensics artifacts.

Volume shadow copies have been a valuable resource for forensic investigators when examining a Windows machine. Technically, Volume shadow copy runs as a service (volume shadow service) that allow the backup of all files on the volume, including user files. This provides a wealth of historical information on files and data that might have previously been deleted or lost [5]. Handling volume shadow copies is a challenge for computer forensics investigators. This is because the backed-up files are not accurate snapshots that could be exported and viewed with traditional forensic tools such as EnCase or FTK Imager. The volume shadow service is a block level service it requires to restore or examine any volume shadow copy that was stored on the volume. To do that, the investigators are required to mount the volume in their desired forensic tool and then use the volume shadow service to manage the needed backup. A detailed discussion of this service can be found in [5, 8]. These added steps are often time-consuming for an investigator. Alternatively, forensic investigators can use tools such as Internet Evidence Finder (IEF) [5] or Forensics Explorer [9]. In the next few subsections, we will describe different techniques for creating volume shadow copies.

### 2.1 Create Shadow Copies Manually

Shadow Copies are produced two ways: automatically or manually. In the automatic process, shadows are snapped after an installation of a new program has been initialized or when there is a Windows Update. The VSS is activated by the OS and then catches an image of the drive of only files that have changed since the last snapshot. These images are then stored in the Systems Information folder where they are protected until they are needed for Windows Recovery. In Windows 10, the steps are as follows:

a. Open Windows Task Manager at view the VSS activity.
b. Locate the VSS in the services tab of the Task Manager. This section should state that the VSS is not running. This is because the VSS has not been triggered yet.
c. Access the Control Panel and follow this path System => Advanced System Settings => System Protection**.**
d. Create a snapshot of the desired volume
e. Look at the Task Manager and notice that the VSS is now running
f. Wait until the VSS is complete. This process usually takes no more than five minutes to complete

The above steps will allow users to manually backup the current setup of the computer that can be later used in system recovery methods. Note, in our experiment volume shadows are manually created through the restore point feature. This feature allows the system to call for the VSS.

### 2.2 Using Command Prompt to Locate the Shadows

Locating the shadows and viewing them can be done two ways: command prompt and third-party software. To find the shadows via command prompt requires the investigator to utilize both the *vssadmin* and *mslink* commands. The *vssadmin* command comes from the vssadmin.exe system application that enables the command prompt to locate the stored shadows. In earlier versions of Windows, this function allowed for the creation of shadows to be triggered by a single line command. On Windows 10, this feature is no longer available. After locating the shadows in the system, an additional command of *mslink* will allow the administrator to link the shadows to the specified volume to see the files of the shadow in a directory. This, however, does not allow the user to view or open the contents of the data. The purpose of showing this method, despite the ability to open the files, is to further understand how to use shadow files in forensic investigations when it is difficult to access the content of the files. The steps for viewing the shadows via command prompt is listed below

a. Access the command prompt with administrative privilege
b. Use the Command *vssadmin* list shadows. This command will return the list of the current shadows
c. Select the shadow that will be linked and record the Snapshot Name that looks like \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy 1. The number at the end will correlate with the shadow that is needed to link.
d. After the shadow has been identified, input the command *mklink* /dc:\shadowcopy\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1 the return result will place a shortcut folder in the C:\ volume called shadowcopy
e. Locate the shadowcopy file that has been linked and view the contents. This feature of linking to the hidden folder will allow the investigator to view the contents of the shadows and see what files have been added or removed from each new copy. However, this does not let to open and view the individual files; this can only be done through a forensic tool such as Forensic Explorer after mounting the drive.

### 2.3 Using ShadowCopyView

Another way to visualize the shadow file structure is through the ShadowCopyView application. As soon as the application is opened, the GUI will list the existing shadows on the system, but again this does not allow any viewing of the content of individual files. The application will record the shadows in rows with different columns such as Snapshot Name, Explorer Path, Volume Path, Volume Name, Operating Machine and Service Machine, Creation Time, Attributes, and other elements provided by the VSS. By default, the application will sort the shadows from oldest to newest. After selecting the shadow to be viewed, the bottom of the GUI displays the directory where the investigator can navigate through the folder structure of the shadow. Using this application can help determine where files are in the shadows before moving them to the Forensic Explorer tool, for example. There is a feature that allows the user to move a file to the active directory, however doing this will not result in a complete file. Viewing the file structure of the shadow allows the investigator to see where files are in the system.

### 2.4 Using Forensic Explorer to Open Old Files

The detail steps for this process are listed below.

a. At the welcome screen click New Case
b. Name the Case and Investigator
c. Click OK**.** After selecting OK, the case should be visible in the right panel.
d. Click Add Device. If the result is a blank window, restart the program as sometimes there is an issue with the program displaying active drives correctly.
e. Select the C:/ drive or the volume that has the shadows stored

f. Press add device
g. Press start in the next window. The program will now register the drive itself and will construct the file system. This process will be shown in the Processes tab in the bottom right corner of the application.
h. After the Processes finished and the device is constructed in the program, move to the File Systems tab
i. Now select Shadow Copy
j. A Windows should open up and display the current shadows on the drive just like the command prompt, and ShadowCopyView did. On the Shadow Copy Options screen, the user can select the shadow they wish to observe and then mount the shadow to the system. There are additional methods that can be altered such as the mounting method where only the changed files can be mounted or all the files from the shadow.
k. Select the shadow you want to use
l. Select the option to mount all files. This was later found to be a crucial part of experimentation.
m. The program will then run and organize the shadow files. By selecting all files instead of changed files, the user can see the entire file structure of that shadow. Again, the progress of reading the shadow volumes can be seen in the processes section of the Forensics Explorer.
n. After the program has finished reading the shadows, Select the Shadow Copies directory in the left panel.
o. The result will show the file structure of the shadow. Here the user can navigate to the root directory and see file changes. The question of investigation should be of where to look in the file system. A good start is to follow the Root => Users path to find the specific directory of the suspect.

## 3. TOOLS and TECHNOLOGY

We have employed several hardware and software tools to implement this project. This section outlines those tools and technologies.

### 3.1 Target Machine

For the target machine, we used a Windows 10 machine with the following specification: i7 Intel processor, 16GB RAM, 1TB Hard disk.

### 3.2. VMware Workstation Player

Due to volatility nature of the target machine's memory, we created a VMware Workstation Pro (v14.0) software [10] on the target machine. Then, we installed Windows 10 as a guest operating system on the virtual machine. All the volume shadow snapshots were taken from the guest operating systems.

### 3.3. Forensics Explorer

Forensic Explorer (v3.9.8.6626 released 31 Jul 2017) is a digital forensic software tool designed for the preservation, analysis, and presentation of electronic evidence including volume shadow copies. Primary users of this software are researchers, law enforcement, government, military, and corporate investigation agencies [9]. There is also a feature within Forensic Explorer that allows the user to mount the shadows onto the drive making them readily available to access. Also, Forensic Explorer sees the shadow copy as "a differential backup of the contents of an NTFS formatted drive" and lists the timeline of the files for accurate identification.

### 3.4. ShadowCopyView

ShadowCopyView (v1.0.3) is a simple tool for Windows 10 and earlier that lists the snapshots of the hard drive created by the VSS. Every snapshot contains an older version of your files and folders from the date that the snapshot was created [12].

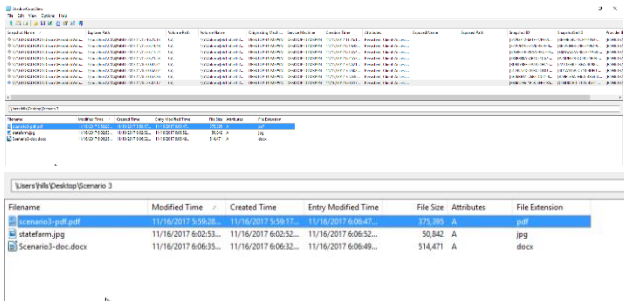


*Figure 1 – ShadowCopyView is able to list all the files within a shadow directory. Though an investigator cannot open the files, this tool allows an investigator to navigate through the directory before using Forensic Explorer.*

## 4. RESEARCH METHOD

As we discussed previously, a Shadow Copy is essentially a differential backup of the contents of an NTFS formatted drive. The Volume Shadow Copy Service (VSS) automatically creates volume shadow copies at regular intervals, but they can also be created by the installation of third-party software, or manually by the user. By examining a Shadow Copy, it is possible to view previous versions of a file, a directory, or a volume.

We conducted our experiment on the virtual machine using VMWare software. Before experimentation began, a Windows Update was received on the workstation. This opportunity allowed for the monitoring of the VSS when the update is installing. During this update, the service was running as seen within the services section of the task manager. A Shadow was created within the time during the windows update. To illustrate the VSS's capability of being triggered by the installation of new software, or third-party software, the VSS service was "stopped. Then we installed new software, application, i.e., Notepad++, and noticed that VSS started "running" and created a shadow of the active drive.

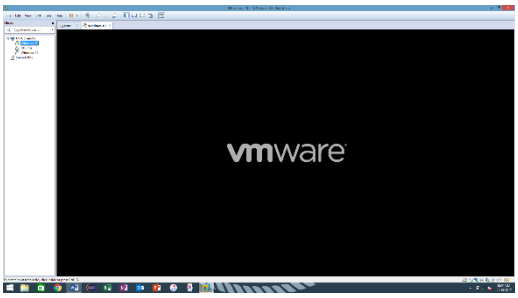


*Figure 2- We used VMWare in our experiment. It is important to not use a live system in any forensic investigation.*

The experiment consists of three stages namely, evidence creation, evidence extraction, and evidence analysis. During the evidence creation stage, the evidence will be generated and created. After files have been created and altered to reflect normal use, the shadows will be located via the command shell during the evidence extraction. After the evidence extraction

stage is complete, we will then analyze the documents to represent the evidence analysis stage and what potential damage the files would or were used for. We used three different scenarios are in the area of health information, financial information, and personal information. Each scenario will feature different types of files such as .docx, .txt, .xls, .pdf, and other files

**Scenarios**

**Scenario 1**: An investigator is looking for traces of stolen financial information. In this scenario, files will be created, moved around the directory, and then deleted to show three different shadow copies moving files. This scenario will utilize three file types: .docx, .pdf, and .txt.

**Scenario 2**: Investigator is looking for traces of identity theft. In this scenario, files will be created, modified, and written over, and deleted to prevent traces. There will be three different shadow copies utilized. This scenario will utilize three file types: .png, .xls, and .docx.

**Scenario 3:** Investigator is looking for traces of stolen health information. In this scenario files will be created, modified, moved, deleted, and written over to prevent traces. There will be four different shadow copies utilized. This scenario will use three file types: .pdf, .docx, and .jpeg

The experiment went through eight phases as described below:

Phase 1: Understand how the VSS works with manual activation with Command Prompt and System protection. This phase also features using mklink to link the shadows to the active drive.
Phase 2: Use ShadowCopyView to view the shadows like that of using Command Prompt.
Phase 3: Utilize the VSS's ability to activate automatically with the installation of new software and a Windows Update
Phase 4: Creating files and experimenting with them for Scenario 1
Phase 5: Creating files and experimenting with them for Scenario 2
Phase 6: Creating files and experimenting with them for Scenario 3
Phase 7: Observe and record how Forensic Explorer interacts with this data
Phase 8: Additional experimentation

### 4.1 Scenario 1

In this example, the investigator is locating three specific files that they were informed about. The first file is a .txt file that has credit card information on it. The second file is a .pdf of a W2 form. The third example is a document of a check. The information was stored initially on the desktop of the account being used for the experimentation. A shadow was taken of the volume with the three files on the desktop directory. After the shadow is made, the files are then dispersed around the file directories. After the second shadow is created, the files are then deleted from where they were placed. A final shadow is made to show the current makeup of the system. Using ShadowCopyView, we could locate the three shadows that were made. They were listed with the Snapshot Name of HarddiskVolumeShadowCopy7-9. The shadows were then mounted using Forensic Explorer to consider the shadows themselves. When examining the first shadow, all three files were on the desktop and were accessible. The text file opened on command, the pdf found success opening with a browser and .docx file was opened with MS Word. When examining the second shadow, all three files were accurately displayed in their dispersed location. The files could be recovered. When examining the third shadow, all three files were located within the $Recycle.Bin. Here we could locate the correct files and open them as normal with no problem.

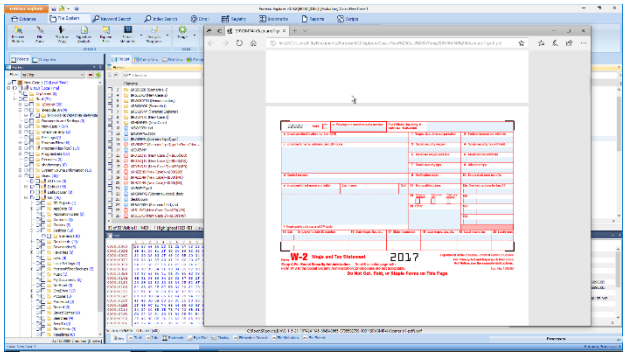

*Figure 3 - Each shadow file was able to be opened properly with Forensic Explorer.*

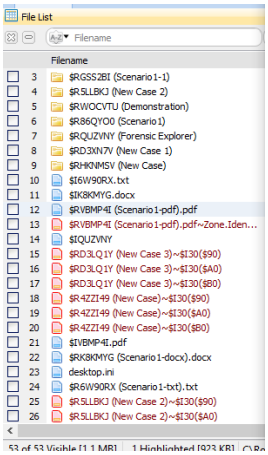


*Figure 4 - All files within the $RecycleBin can easily be located and displayed with their appropriate name in parentheses.*

### 4.2 Scenario 2:

In this example, the investigator is locating three files that they were informed about being on the volume. The first file is .png of a social security card. The second file is .xls of mailing address information. The third file is .docx of a birth certificate. The information was stored initially on the desktop. Three shadows were taken of the files as they were moved, modified, and written over. During this scenario, only the files that were different from the shadow and the current system were mounted.

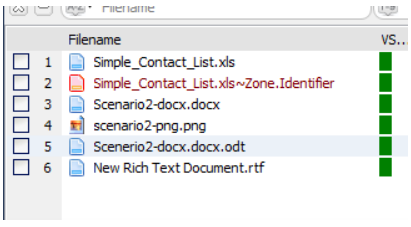


*Figure 5 - All three files in Scenario 2 are able to be recovered.*

Some problems were experienced with setting up this scenario, as files were not responding properly. We decided to delete all

the shadows on the current system to see if there was a correlation. During this experimentation, there were 13 shadows in the system. After doing this and creating new shadows, the files could be fully recovered.

Since this scenario originally changed the shadow mounting to only mount the files that changed, it was found that only two files were present, but neither one of them could be viewed properly. After rerunning the shadow copy with the setting returned to mounting all files, the three files were visible and could be opened properly. It was then decided to mount all files for the remainder of the experimentation.

After mounting the entire file structure for the rest of the scenario, it was found that the second shadow was successful in showing that the files were modified. It is assumed that the files will be placed on a secured account owned by the suspect and has been solely edited by that suspect. The time stamp provides a crucial timeline on when the suspect changes the evidence. This experiment is showing how Forensic Explorer can be used to handle and view shadow files on a Windows 10 system. Normal metadata on files can be shown on who created the file, when it was last modified, and who last modified it. This would be great evidence to see if the suspect attempted to alter or modify the incriminating information.

In the last shadow, the files were written over. This meant that a brand-new document replaced the name location of the file. In this situation, all the files reflected the written change of the files. This is evidence that the suspect wrote over the location of the file in memory with a blank file.

### 4.3 Scenario 3

In Scenario 3, there were three file types, i.e. .pdf, .jpeg, .docx to demonstrate the health information scenario. The pdf was an example of a Medicare insurance card. The jpeg was a picture of an insurance card. The docx file was a health application. Each file was used to represent common files that may be discovered during a criminal investigation involving medical fraud.

The first shadow was taken with all three files on the desktop of the workstation. The second shadow was taken when the files were modified and moved within the directory. The third shadow was taken with the files deleted, and the disk was cleaned of any traces. The cleaning of traces involved a disk defragmentation and a standard cleanup of the recycling bin and other locations. During the analysis of the first shadow, it was discovered that the pdf and the jpeg were both recovered. However, the word document had trouble being recovered. This may be because the shadow was taken while the program was still open in word.

Another trial was conducted to find whether the above findings were true regarding the ongoing edit of the word document. After closing Word and saving the file, the shadow file was opened without any difficulty.

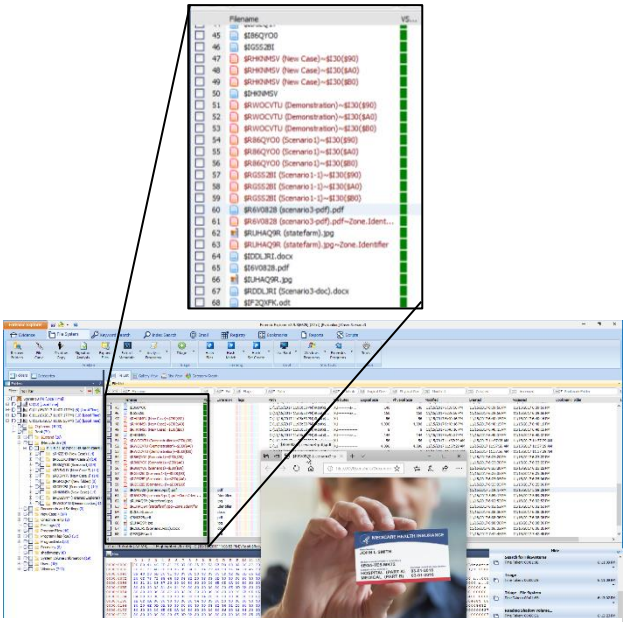

*Figure 6 - Forensic Explorer can list file extension information and original names of each file in the $RecycleBin folder, making it easier to locate a specific shadow file.*

The second shadow was more responsive than the first on showing changes to the files. All files were read and corresponded with their appropriate changes. The third shadow showed no traces of the files anywhere. Some files were found, but all names were destroyed corresponding to the file. This shows how utilizing the VSS as a source of gathering evidence is valuable if current files were wiped from the system.

## 5. CONCLUSION

In this paper, we developed a framework for the forensic analysis of Windows 10 volume shadow copies. Then, we used the framework to extract, analyze and demonstrate the forensic value of volume shadow copy in any forensic investigation. We defined three scenarios to show the different capabilities of VSS in data recovery. Using software tools such as Forensic Explorer allowed the files to be located and recovered to investigate what information was modified or destroyed by the suspect. In the first scenario, through VSS we were able to access the history of the files that were deleted from the target machine. This ability gives the investigator a way to see a timeline of when the suspect deleted evidence from the workstation. Each shadow that was taken illustrates how the computer's backup recovery software can be used in a forensic setting. The second scenario revealed how the VSS could be used in response to situations where the file has been written over or modified to the point where the current evidence is unusable. The VSS gives the ability for the investigator to go back in the time of the volume being used to see how the drive has changed over time. Timelining the files on a volume will allow investigators the ability to pinpoint where in time the suspect attempted to modify or delete a file. We showed that the VSS could capture time, file types, file identifiers, and the history of the files as they change over time. With the assistance of software tools, investigators can access the contents of shadows for evidential information.

**REFERENCES**


[1] L. Abrams. How to Recover Files and Folders Using Shadow Volume Copies. **Bleepingcomputer,** 2016. Retrieved from https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/

[2] B. Matt. Windows Wednesday: Volume Shadow Copies. **Medium**, 2016. Retrieved from https://medium.com/@mbromileyDFIR/windows-wednesday-volume-shadow-copies-d20b60997c22

[3] Libvshadow. Library and tools to access the Volume Shadow Snapshot (VSS) format. GiHub, 2017. Retrieved from https://github.com/libyal/libvshadow

[4] Blackbag Training Team. An Overvie: Windows Volume Shadow Copies, 2017, **Blackbag**, retrieved from https://www.blackbagtech.com/blog/2017/02/03/an-overview-windows-volume-shadow-copies/

[5] Magnet Forensics. Volume shadow copy forensics", 2014. **Magnet Forensic**, retrieved from https://www.magnetforensics.com/computer-forensics/volume-shadow-copy-forensics/

[6] Heath, K. and Delude K, "*Volume Shadow Copy Forensics Report*", 2012. **Patrick Leahy Center for Digital Investigation Champlain College**

[7] Balan, S.S.C.C. "*Forensic Analysis of Volume Shadow Copy in Windows 7*". 2016 **International Conference on Emerging Technological Trends [ICETT]**.

[8] Cravey, H. Accessing Volume Shadow Copies", 2011, **Windows Incident Response.** Retrieved from http://windowsir.blogspot.ca/2011/01/accessing-volume-shadow-copies.html

[9] GetData, *Forensics Explorer*. **Advanced Foresnics Software.** Retrieved from http://www.forensicexplorer.com/shadow-copy.php

[10] VMware Workstation Player. Retrieved from https://www.vmware.com/products/workstation-player.html

[11] Technet Library, 2003. *What is volume shadow copy service?* Retrieved from https://technet.microsoft.com/enus/library/cc757854(v=ws.10).aspx

[12] Nirsoft, 2016. *ShadowCopyView*. **Nirsoft.** Retrieved from http://www.nirsoft.net/utils/shadow_copy_view.html