Proposal of unified data management and recovery tool using shadow copy

Naoki Matsutaka and Masato Eguchi, Takuya Okazaki,
Takashi Matsumoto, Tetsutaro Uehara*, Ryoichi Sasaki
Tokyo Denki University
Senjuasahicho 5, Adachi-ku, Tokyo-to, 120-8551 JAPAN
*Ritsumeikan University
Tojiinkitamachi 56-1, kita-ku, Kyoto-fu, 603-8577 JAPAN
matsutaka@isl.im.dendai.ac.jp

ABSTRACT

In recent years, solid state drives (SSD) have started to replace hard disk drives. An SSD is a high-speed storage device with a TRIM function. However, an SSD cannot restore deleted files. Therefore, the user is required to back up data for protection. The Microsoft Volume Shadow Copy Service (VSS) is often recommended for backups. However, although it has tools for backup, they are complicated to use. In addition, VSS does not have enough implemented functions. Therefore, we propose a unified tool named ShadowBox, which easily helps typical users to create a shadow copy and to restore data from it. In addition, we discuss the protection of shadow copy data from attacks due to malicious persons and ransomware.

KEYWORDS

Backup, Shadow Copy, SSD, Ransomware, Data Protection

1 INTRODUCTION

In recent years, solid state drives (SSDs) have begun to replace hard disk drives (HDDs). An SSD, which is a solid-state semiconductor storage device, can read data at high speed, because it does not move a head on the medium. This feature is different from the data reading of a HDD. The usage percentage of SSDs will continue to increase as their data capacity is expanded and their performance is improved.

On the other hand, SSDs have problems such their inability to recover data for digital forensics, and erroneously erased data. An SSD has a function named TRIM, which automatically detects deleted data and creates an empty block. The TRIM function can increase the data writing speed. On the other hand, TRIM has the disadvantage that a deleted file cannot be recovered. The data on an HDD or USB flash memory can be restored just after deleting a file, because such devices do not have a TRIM function. If TRIM is enabled, the SSD recognizes the deleted data as unnecessary. Moreover, the TRIM function completely deletes the actual data. This makes digital forensics difficult with an SSD. For the same reason, when important files are deleted by mistake, they cannot be recovered. As an example, Yamamae et al. (2015) conducted an experiment on restoring the erased files of a SSD [1]. The results showed that the deleted files could not be recovered even immediately after deletion when TRIM was enabled. In addition, most deleted data was lost after only one day even if TRIM was not enabled. Therefore, using an SSD requires backing up data for protection, because recovery of data is impossible.

The Microsoft Volume Shadow Copy Service (VSS) has tools for creating shadow copies and restoring files from these copies. However, using these tools is not easy and they lack some required functions. In addition, no tools capable of protecting shadow copy data from attacks of ransomware or the malicious behavior of internal persons have been proposed.

Therefore, we propose a unified tool named ShadowBox that easily helps the typical user to create shadow copies and to restore data from them. In addition, this tool can protect shadow copy data from attacks of ransomware or malicious internal persons. ShadowBox is made up of three applications: VSSManager, VSSaver and VSSLogger. VSSManager is a tool for easily backing up and restoring shadow copy files. VSSaver and VSSLogger are used cooperatively to protect the shadow copy area and to log attacks against it. Among the three application programs, only VSSManager has actually been developed. The developed program was evaluated by test users from the viewpoint of usability. In this paper, Section 2 describes the backup process using VSS. We deal with related studies and existing tools in Section 3. We describe an overview of ShadowBox in Section 4, and present the details of the developed VSSManager in Section 5. The result of the evaluation of VSSManager is shown in Section 6, and future work is described in Section 7. Section 8 concludes the paper.

2 BACKUP USING SHADOW COPY

VSS is a Windows function for creating snapshots, i.e., shadow copies. It can duplicate stored files in a special area, and these files can be restored even if the original files are deleted. First, VSS takes a snapshot in order to record the state of the storage. It subsequently replicates individual files each time they are deleted or modified. Therefore, the backup time is short compared with that for other methods. Moreover, the data capacity for backup using shadow copies can be decreased, because only the modified or deleted data are stored. Table 1 shows the time and space required for the backup of a normal copy and a shadow copy of a file with a size of 100 GB on a HDD. In addition, though a traditional backup cannot copy files that are either running or are locked, VSS can copy a file in any state.

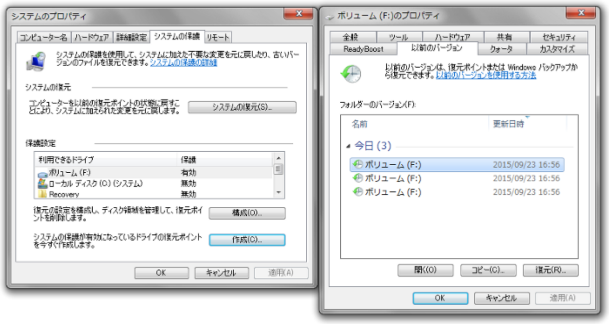
Table 1. 100 GB file backup (HDD)

	Normal Copy	**VSS**
Processing time	777.4 sec	**3.7 sec**
Data capacity	100 GB	**55.5 MB**

3 EXISTING TOOLS AND RELATED STUDIES

3.1 Previous Versions and ShadowExplorer

Some of the backup tools used for VSS include “Previous Versions” and ShadowExplorer. Windows has a Previous Versions that creates a shadow copy, sets a storage area, and then restores the file [2]. Figure 1 shows the dialog boxes of Previous Versions. ShadowExplorer lists the backup files and restores any files from the shadow copy [3]. Figure 2 shows a screenshot of ShadowExplorer.



システムの保護を使用して、システムに加えた不要な変更を元に戻したり、古いバージョンのファイルを復元できます。システムの保護の詳細

コンピューターを以前の復元ポイントの状態に戻すことにより、システムに加えられた変更を元に戻します。

利用できるドライブ	保護
ボリューム (F:)	有効
ローカル ディスク (C:) (システム)	無効
Recovery	無効

復元の設定を構成し、ディスク領域を管理して、復元ポイントを削除します。

システムの保護が有効になっているドライブの復元ポイントを今すぐ作成します。

以前のバージョンは、復元ポイントまたは Windows バックアップから復元できます。以前のバージョンを使用する方法

名前	更新日時
今日 (3)	
ボリューム (F:)	2015/09/23 16:56
ボリューム (F:)	2015/09/23 16:56
ボリューム (F:)	2015/09/23 16:56

Figure 1. Previous Versions (Left: system properties, Right: volume properties)

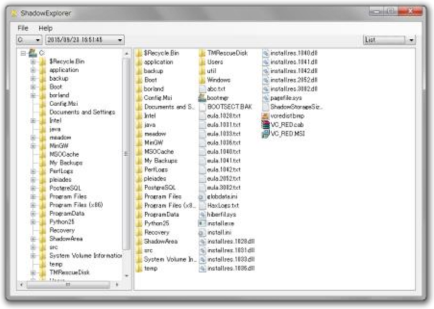


Figure 2. ShadowExplorer

3.2 Problems with existing tools

As described in Section 3.1, Previous Versions creates a shadow copy, sets the storage area, and then restores the file. However, these functions are executed in separate dialog boxes. For example, the System Properties dialog box is used to set the storage area and create the shadow copy. The Volume Properties dialog box is then used to restore a file from the shadow copy. In other words, Previous Versions does not have unified functions for handling the shadow copy. Protecting the data is inconvenient for the user because the backup and restore functions are separate. As a result, measures against an attack cannot be carried out. Opinions such as “much time and effort is required before starting the operation” and “operation is difficult to understand” were given by users. Therefore, Previous Versions has a problem with its operation.

ShadowExplorer was developed for restoring files. It is impossible to use it for creating a shadow copy and setting the parameters for restoring. In addition, the operation of ShadowExplorer is difficult to understand. For example, ShadowExplorer makes it impossible to return to folders in an upper hierarchy in order to open a folder. Moreover, information about the file cannot be shown in the file table for ShadowExplorer. These issues make it difficult to search for a file. Table 2 shows the functions of the existing tools. The circles indicate implemented features. From Table 2, we can see that the functions of these tools are disjointed and therefore difficult to use collectively.

Table 2. Functions of existing tools

Function	Previous Versions		Shadow Explorer
	System	Volume	
Create SC*	○	-	-
Delete SC	○	-	-
Set storage	○	-	-
List SC	-	-	○
Restore file	-	○	○
Search file	-	○	-

*Shadow Copy

3.3 Related studies

No backup tools against ransomware or unauthorized deletion are currently supported by SSDs. This includes VSS, and a new backup tool based on VSS has not yet been proposed. However, many backup tools have been proposed for cloud computing and peer-to-peer networks. Arthur et al. (2011) proposed a secure cloud backup system [4]. This system manages backup data and ensures the safety of the data by encryption. However, the backup time depends on the online baud rate, so these systems are not suitable for replicating a large number of files. Yoshida et al. (2016) built a backup system for disaster or failure using a peer-to-peer network [5]. This system builds a network of trusted users. As a result, it achieves the needed redundancy, dispersion and security. These systems can protect data from ransomware and release data from a local device. However, if one of the users is a malicious person, these systems cannot protect the data.

4 PROPOSAL OF SHADOWBOX

4.1 Overview of the proposed tool

The purpose of this study is safe management of data by the development of ShadowBox, which has a function to protect shadow copy files from attacks by malicious persons or ransomware. The main features of the implementation are described below in steps 1-3.

1. Create a shadow copy and restore a file.
2. Protect the shadow copy from an unauthorized deletion command.
3. Provide the information gathered in step 2 to the administrator.

Step 1 is a basic function found in traditional backup tools. ShadowBox makes it possible to use the function easily and efficiently by solving the problems of the existing tools.

Moreover, it prevents incorrect deletions and manages data by implementing the functions in steps 2 and 3. ShadowBox also provides a unified function for safely protecting data in a PC.

4.2 Proposed method

ShadowBox is made up of three applications: VSSManager, VSSaver, and VSSLogger. VSSManager is a tool for easily backing up and restoring files using VSS. VSSaver and VSSLogger are used cooperatively to protect the shadow copy area and to keep a log of attacks to this area. ShadowBox starts VSSaver as a resident application and monitors the Delete command given to the shadow copy area. If a process attempts to delete the shadow copy area, it detects the attempt and stops the process. At the same time, ShadowBox starts VSSLogger. VSSLogger identifies the parent process that issued the Delete command. This information and a dump file are then provided to the administrator. If the file is encrypted by ransomware, VSSManager restores the file from the data in the shadow copy. Figure 3 shows the structure of ShadowBox. We developed VSSManager first, and it is the only currently developed application. VSSManager is further described in the next section.

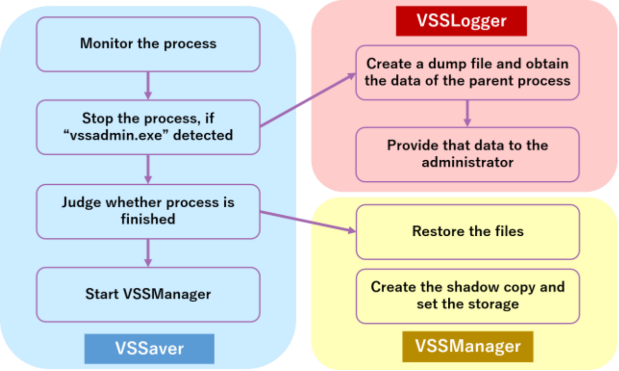

Monitor the process
Stop the process, if "vssadmin.exe" detected
Judge whether process is finished
Start VSSManager
VSSaver
VSSLogger
Create a dump file and obtain the data of the parent process
Provide that data to the administrator
Restore the files
Create the shadow copy and set the storage
VSSManager

Figure 3. Overview of ShadowBox

5 DEVELOPMENT of VSSManager

5.1 Development environment

VSSManager is written in C# and runs in Windows 7. The total number of lines in the developed program is approximately 4617. Table 4 shows the development environment of VSSManager. ShadowBox uses the AlphaVSS library to create the shadow copy and to list the backup files. [6]

Table 3. Development environment

OS	Windows 7
Language	C#
Library	.NET Framework4.0 AlphaVSS.1.2.4000.3
Lines	4617

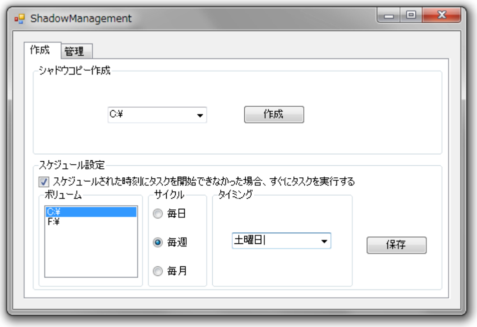
5.2 Overview of VSSManager

VSSManager, which was developed to solve the problems described in Section 3.2, implements the functionality required by the user at the time of backup and restore. We developed a GUI by assuming the operation of typical users. As mentioned earlier, VSSManager has the ability to create and manage the shadow copy, and restore a file. VSSManager can efficiently back up data and restore files by unifying the basic functions. Table 4 shows the problems of existing tools and the improvement by VSSManager.

Table 4. Problems and improvements of existing tools

Problems with existing tools	VSSManager
Cannot collectively use the functions	Has centralized functions (described in Section 5.1)
Cannot create a shadow copy on a per-volume basis	Selects volumes when creating the shadow copy
Searches files that target a single shadow copy	Allows searches for multiple shadow copies
Difficult to set storage	Has an intuitive user interface
Not enough displayed file information	Displays files with icons or thumbnails
Troublesome to move between folders	Implements "back" and "forward" buttons and displays current folder path

We developed the user interface to help the typical user to conduct backups easily. In Previous Versions, the shadow copy is created automatically and controlled by the Windows OS. However, because a complex procedure is required to create the shadow copy, it is difficult for users to execute the application in a timely manner. Therefore, we developed the function to set the timing freely when creating the shadow copy using Previous Versions. VSSManager has the functions "Create shadow copy", "Manage storage", "Restore a file", and "Search for a file". Figures 4-7 show the dialog boxes of VSSManager.



C:¥

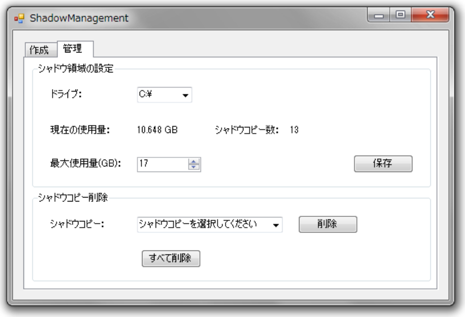
☑ スケジュールされた時刻にタスクを開始できなかった場合、すぐにタスクを実行する

ボリューム: C:¥ (selected), F:¥

サイクル: ○ 毎日 ● 毎週 ○ 毎月

タイミング: 土曜日

Figure 4. Dialog for creating a shadow copy



ドライブ: C:¥

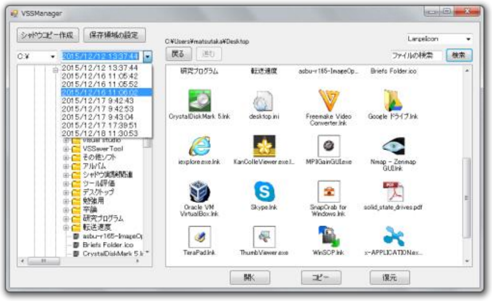
現在の使用量: 10.648 GB

シャドウコピー数: 13

最大使用量(GB): 17

シャドウコピー: シャドウコピーを選択してください

Figure 5. Dialog for setting storage



C:¥

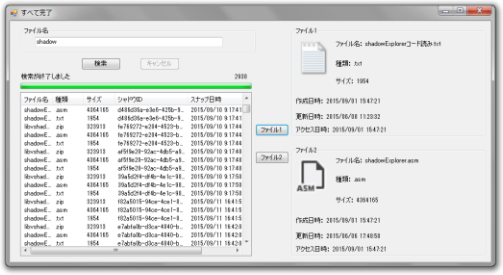
2015/12/12 13:37:44

2015/12/12 13:37:44
2015/12/16 11:05:42
2015/12/16 11:05:52
2015/12/16 11:06:02
2015/12/17 9:42:43
2015/12/17 9:42:53
2015/12/17 9:43:04
2015/12/17 17:39:51
2015/12/18 11:30:53

C:¥Users¥matsutaka¥Desktop

LargeIcon

Figure 6. Dialog for restoring file



ファイル名: shadow

検索が終了しました 2938

ファイル名	種類	サイズ	シャドウID	スナップ日時
shadowE...	.asm	4364165	d486d35a-e3e6-425b-9...	2015/09/10 9:17:41
shadowE...	.txt	1954	d486d35a-e3e6-425b-9...	2015/09/10 9:17:41
libvshad...	.zip	323913	fe769272-e284-4523-b...	2015/09/10 9:17:44
shadowE...	.asm	4364165	fe769272-e284-4523-b...	2015/09/10 9:17:44
shadowE...	.txt	1954	fe769272-e284-4523-b...	2015/09/10 9:17:44
libvshad...	.zip	323913	af5f9e20-92ac-4db5-a9...	2015/09/10 9:17:48
shadowE...	.asm	4364165	af5f9e20-92ac-4db5-a9...	2015/09/10 9:17:48
shadowE...	.txt	1954	af5f9e20-92ac-4db5-a9...	2015/09/10 9:17:48
libvshad...	.zip	323913	39a5d2f4-df4b-4e1c-98...	2015/09/10 9:17:50
shadowE...	.asm	4364165	39a5d2f4-df4b-4e1c-98...	2015/09/10 9:17:50
shadowE...	.txt	1954	39a5d2f4-df4b-4e1c-98...	2015/09/10 9:17:50
libvshad...	.zip	323913	f82a5015-94ce-4ce1-8...	2015/09/11 16:41:5
shadowE...	.asm	4364165	f82a5015-94ce-4ce1-8...	2015/09/11 16:41:5
shadowE...	.txt	1954	f82a5015-94ce-4ce1-8...	2015/09/11 16:41:5
libvshad...	.zip	323913	e7abfa0b-d3ca-4840-b...	2015/09/11 16:42:0
shadowE...	.asm	4364165	e7abfa0b-d3ca-4840-b...	2015/09/11 16:42:0
shadowE...	.txt	1954	e7abfa0b-d3ca-4840-b...	2015/09/11 16:42:0

ファイル1

ファイル名: shadowExplorerコード読み.txt

種類: .txt

サイズ: 1954

作成日時: 2015/09/01 15:47:21

更新日時: 2015/06/08 11:28:32

アクセス日時: 2015/09/01 15:47:21

ファイル2

ファイル名: shadowExplorer.asm

種類: .asm

サイズ: 4364165

作成日時: 2015/09/01 15:47:21

更新日時: 2015/06/06 17:48:58

アクセス日時: 2015/09/01 15:47:21

Figure 7. Dialog for searching for file

6 EVALUATION

6.1 Method of evaluation

An evaluation was conducted to determine whether the developed tool is suitable for operation by a typical user. Ten students in our laboratory participated as users in the experimental evaluation. They used the developed VSSManager as well as existing tools. The users were taught how to use the tools in advance. They evaluated the usefulness with a five-point score. Here, "very hard to use" was 1 and "very easy to use" was 5. Moreover, the users described their impressions of using the tools.

6.2 Results of evaluation

Table 5 shows the evaluation results. As mentioned above, “very hard to use” was 1 and “very easy to use” was 5. The table shows the average values of the evaluations of Previous Versions and ShadowExplorer along with VSSManager.

Table 5. Evaluation of tools (SC=shadow copy)

Function	Previous Versions	Shadow Explorer	**VSS Manager**
Creation of SC	2.6	×	**4.7**
Setting storage	1.5	×	**4.9**
Searching for file	3.4	3.0	**3.6**

From Table 5, VSSManager obtained a higher rating than the existing tools in the creation of a shadow copy and setting the storage area from the viewpoint of “Creation of shadow copy” and “Setting storage area”. From the result, it is considered that VSSManager offers simplified and intuitive operation. In the users’ opinions, VSSManager would obtain better evaluations if given more options to evaluate, such as “fewer steps” and “operation easy to understand”. Therefore, we can verify that we were able to achieve the purpose of this research. On the other hand, the file search function is almost identical for VSSManager and existing tools. Some opinions about the file search included “it was very hard to search for a file”. Therefore, a more effective file search function is required. In addition, one opinion was that it was difficult to become familiar with the user interface of VSSManager. The presumed reason is that the users normally use the Windows OS and manipulate files in Windows Explorer. For this reason, they think it is easier to use Previous Versions, which is similar to Window Explorer. That is, because the look and feel of VSSManager is different from that of Windows Explorer, they might feel a sense of incongruity.

7 FUTURE WORK

7.1 Improvement of VSSManager

From the results of the experimental evaluation, we know that the file search function should be improved. In the case of VSSManager, the function to search for files directly by file name is not effective, because sometimes there are a very large number of matches. Moreover, the user sometimes does not remember the file name. Therefore, an approach different from using the filename is required. We suggest a new feature that lists the deleted files and the updated files to make it easier to find the desired file. The following two approaches can be considered. After implementing the following two approaches in VSSManager, the user could evaluate them.

Approach 1: Compare the current volume and the shadow copy.

This approach compares the file in the current volume and the file in the shadow copy.

Then, deleted files are defined as those that exist only on the shadow copy side. Updated files are defined as having an equivalent and updated timestamp. This approach significantly narrows down the number of target files, and so it would be possible to reduce the effort to look for files. Figure 8 shows a method to compare the current volume and the shadow copy.

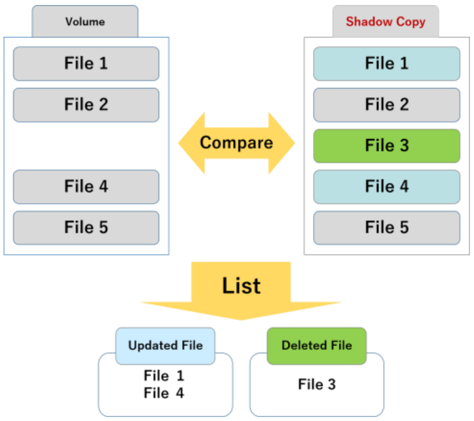


Figure 8. Approach 1: Comparing the current volume and the shadow copy

Approach 2: Detect the deleted files

This method monitors the files in the volume and records the paths of the deleted files. Then, in the shadow copy, it enumerates the files that have been deleted by referring to the file paths. This approach reduces the time to find the desired files. Figure 9 shows the method for detecting the deleted files.

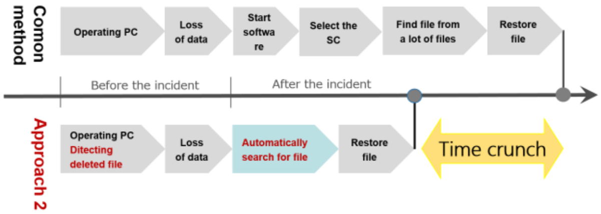


Figure 9. Approach 2: Detect the deleted files

7.2 Development of ShadowBox

VSSManager is one of the existing applications of ShadowBox. The goal of this study is the full development of ShadowBox. Therefore, we are now developing the two remaining applications, VSSaver and VSSLogger. Once developed. VSSaver and VSSLogger will be evaluated for security and usability.

8 CONCLUSION

We proposed the unified tool named ShadowBox, which helps typical users to create a shadow copy and to restore data from it. This tool has a function to protect the data in the shadow copy against the attacks of ransomware or malicious internal persons. ShadowBox consists of three applications, VSSManager, VSSaver, and VSSLogger. VSSManager, which is the only application that we have actually developed, is a tool for easily backing up and restoring files using a shadow copy. The experimental results showed that the usefulness of the program is better than that of existing tools. In the near future, we will improve the searching function of VSSManager and continue to develop and evaluate VSSaver and VSSLogger.

REFERENCES

[1] A.Yamamae, Y.Kobayashi, T.Uehara, R.Sasaki, “Experiment and evaluation of recoverability of removed files in SSD”, IPSJ SIG-DPS, 2015-DPS-162, 39, 1 – 7, 2015-02-26

[2] Volume Shadow Copy Service, https://msdn.microsoft.com/en-us/library/windows/desktop/bb968832(v=vs.85).aspx

[3] How do I configure and use shadow copy in Microsoft Windows?, http://www.techrepublic.com/blog/windows-and-office/how-do-i-configure-and-use-shadow-copy-in-microsoft-windows/

[4] A.Rahumend, H.Chen, Y.Tang, P.Lee, and J.Lui, “A Secure Cloud Backup System with Assured Deletion and Version Control” International Conference on Parallel Processing Workshops, 40, 160-167, 2011.9.

[5] T.Yoshida, T.Odaka, J.Kuroiwa and H.Shirai, “Fault Tolerant Data Backup System Using Peer-to-Peer Network” 64, 57-63, 2016-2.

[6] AlphaVSS, http://alphavss.codeplex.com/