VSS Does Not Protect User Data

2.1 Introduction

VSS, an abbreviation for Volume Shadow Copy Service, is a backup-related function found in Windows XP / Windows Server 2003 and later versions of Windows.

VSS can create snapshots, enabling you to save the state of a volume at a given point in time. Users can access data on a volume from the time a snapshot was created by referencing the snapshot. This includes deleted files and files with data that has been modified. Snapshot data is not updated because it is read-only. Also, files that are locked in a volume are not locked in a snapshot. It is possible to perform a complete backup by taking advantage of such characteristics.

Snapshots are also used for the files that can be restored from the "Previous Versions" tab displayed in the file and folder properties in Windows 7/10 (Figure 1). Many may recall that restoring files from a snapshot was a workaround discussed when Ransomware became prevalent.

Because snapshots can be used to recover attack tools used by attackers in addition to temporary and altered files, they are recognized by analysts as one of the most important pieces of data in digital forensics. However, while performing technical analysis of digital forensic data, we confirmed an issue in Windows 8.1/10 where user data is not saved correctly to snapshots even when VSS is enabled. We investigated the cause of this and the scope of its impact. We also discuss methods for handling this issue here.

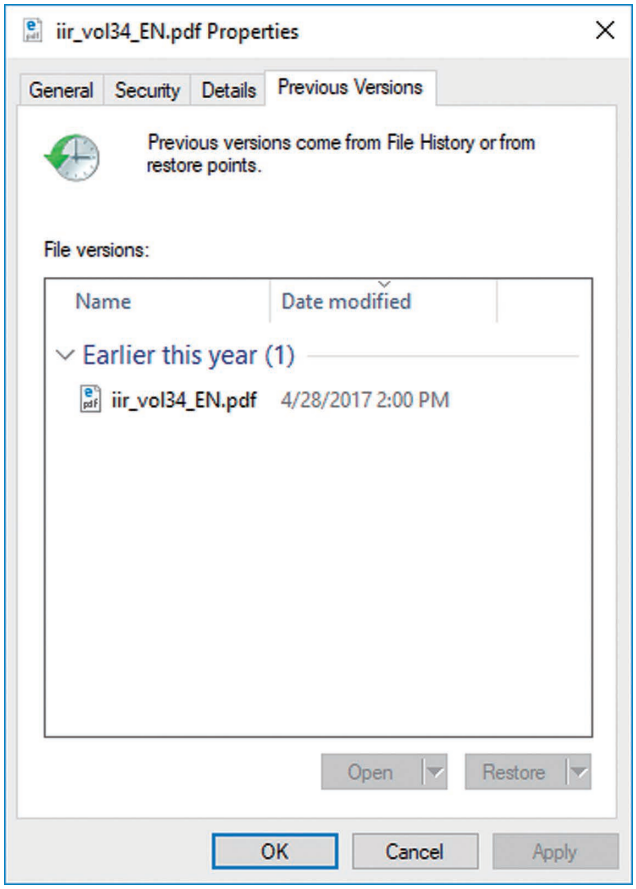

Figure 1: "Previous Versions" Tab

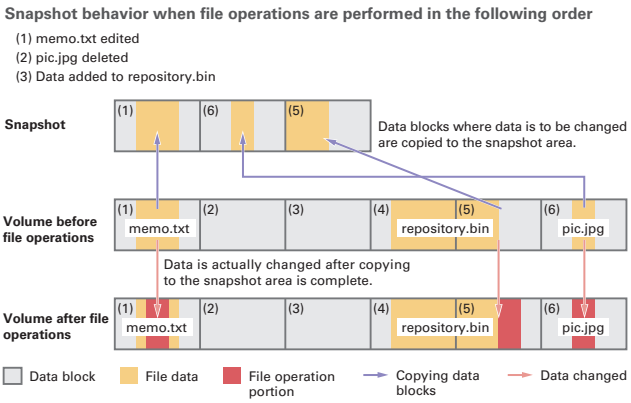

Figure 2: Saving Difference Data

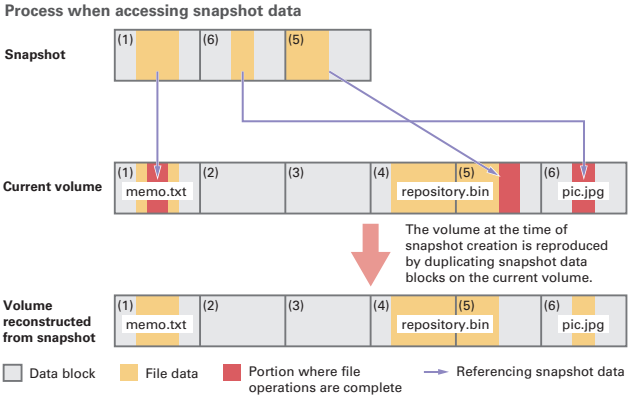

Figure 3: Accessing a Snapshot

2.2 VSS Snapshot Mechanism

As mentioned above, a snapshot saves the state of a volume at any given point in time, but it does not save the data at an individual file level. For example, saving an entire set of files when only 1 MB of a 1 GB total has changed leads to poor utilization of a volume, lowering overall OS performance.

Thus, only difference data is saved to the snapshot. To obtain difference data, the entire volume is split into data blocks of 16 KB each, and data for blocks that were changed after snapshot creation is saved along with the offset (Figure 2). When accessing files in a snapshot, the difference data is transparently integrated with the current volume data, reconstructing the data from when the snapshot was created (Figure 3).

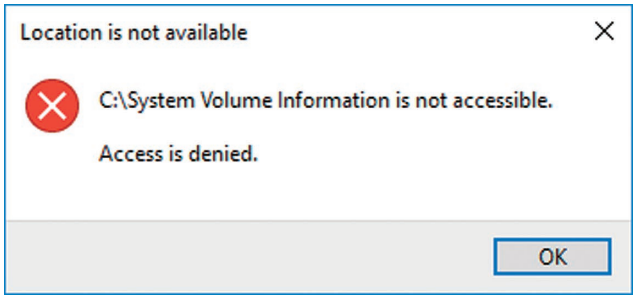

Figure 4: Snapshots Protected from User Access

2.3 VSS Snapshot File Organization

Files related to snapshots are saved to the "System Volume Information" folder directly under the root folder of a volume, but they cannot be accessed using Explorer (Figure 4). In Figure 5, these files are displayed using FTK Imager*1.

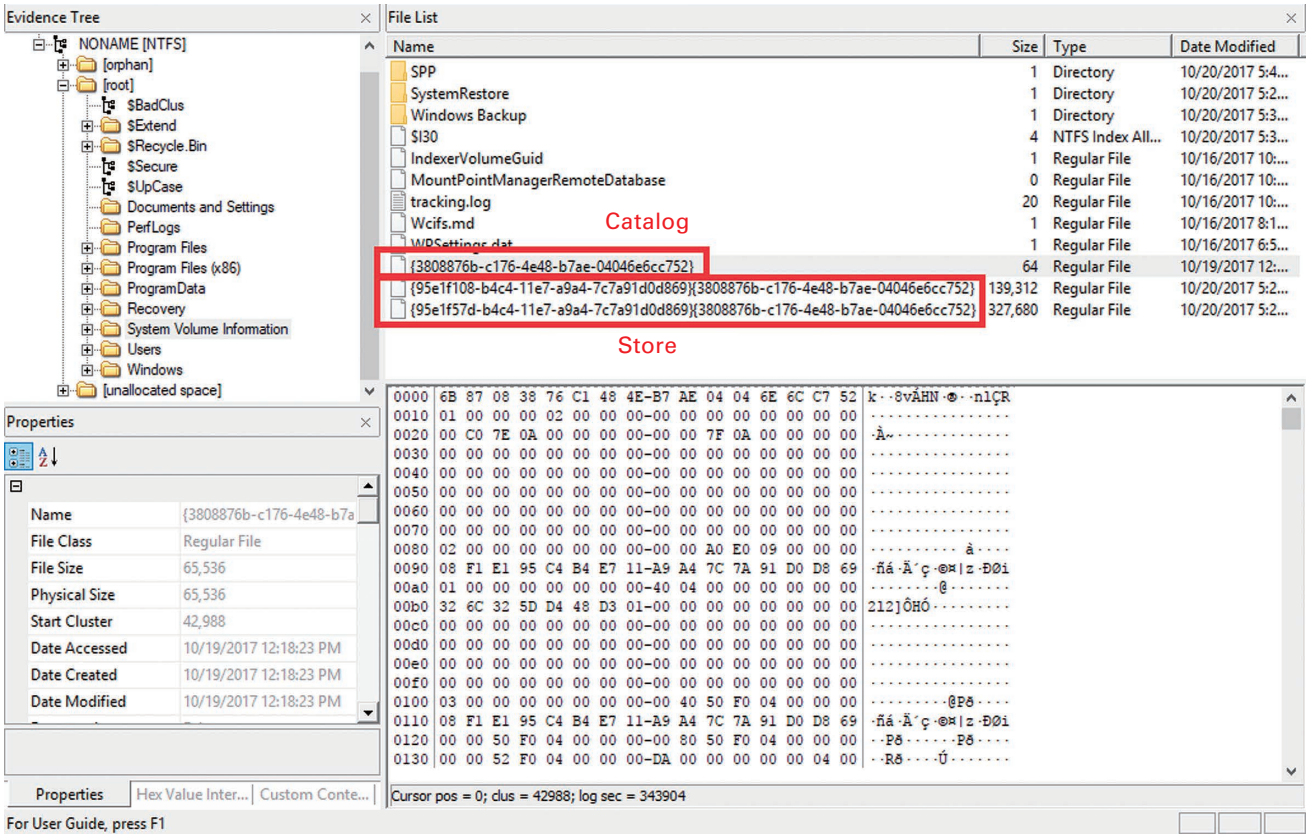

Figure 5: File Organization in the "System Volume Information" Folder

*1 FTK Imager (https://accessdata.com/product-download).

Snapshots consist of two file types: “catalog” and “store” files. Catalog files have “{Catalog GUID}” as their file name, and contain metadata such as the day the snapshot was created and the store GUID. Store files contain the actual data, and have the file name “{Store GUID}{Catalog GUID}*2.”

2.4 Enabling VSS and Snapshot Operations

You can check whether VSS is enabled in “System Properties” (Figure 6). If it is disabled, click the “Configure” button to display the “System Protection for Local Disk” dialog box. Select “Turn on system protection,” set the “Disk Space Usage,” and then click the “OK” button (Figure 7). To create a snapshot manually, click the “Create” button in Figure 6.

It is possible to create multiple snapshots within the same volume, but the oldest snapshot will be deleted when the “Disk Space Usage” configured in Figure 7 is exceeded.

You can view a list of created snapshots and delete them using vssadmin.exe. Open the Command Prompt as an administrator and execute “vssadmin.exe list shadows” to obtain a list of snapshots (Figure 8). It is also possible to perform snapshot operations from WMI and PowerShell.

2.5 File Recovery Tests

We tested the recovery of files saved to a snapshot to verify whether files created by a user are saved correctly to the snapshot. As test user data, we saved the ten PDF files for IIR Vol.26 to Vol.35, which are available on our website, in a folder named “PDF” on the desktop, and then created a snapshot.

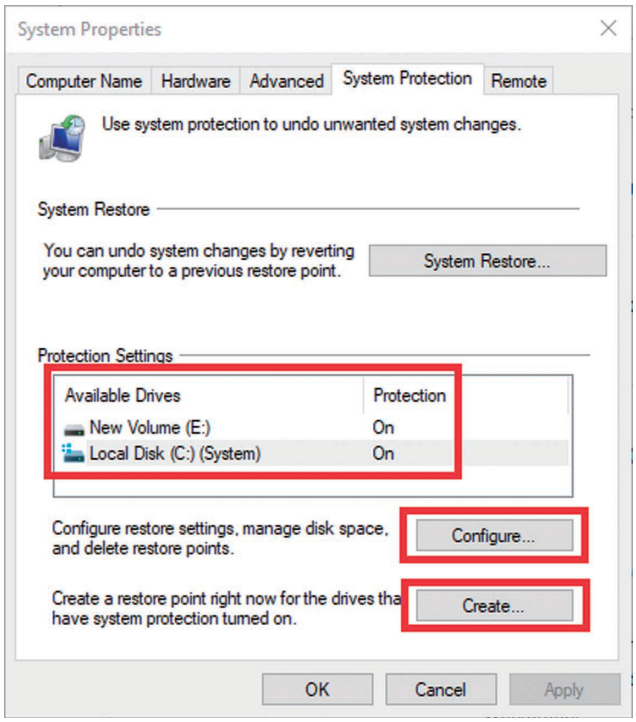

Figure 6: “System Properties” Dialog Box

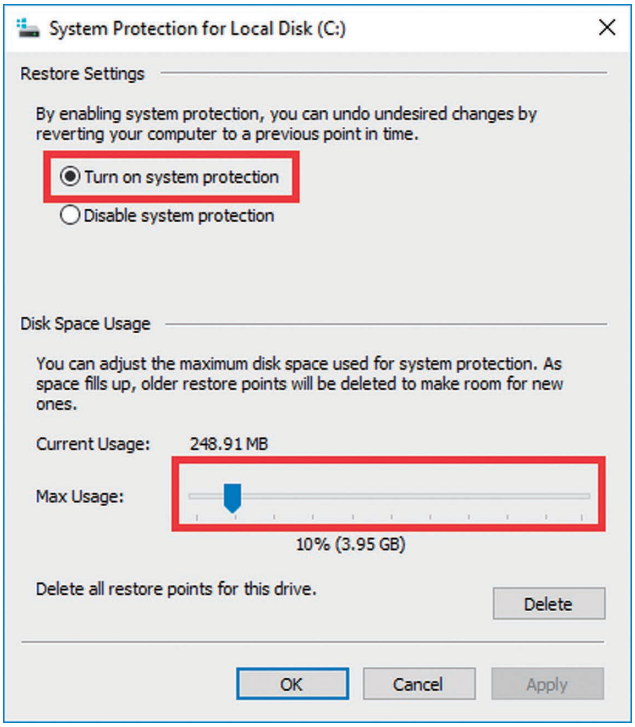

Figure 7: “System Protection for Local Disk” Dialog Box

*2 We do not address the file or data structure of snapshots here. For more information, Volume Shadow Snapshot (VSS) (https://github.com/libyal/libvshadow/blob/master/documentation/Volume%20Shadow%20Snapshot%20(VSS)%20format.asciidoc) is a very useful reference document.

We used the SDelete*3 file deletion tool to delete the files in the "PDF" folder, and then recovered the data from the snapshot using ShadowExplorer*4.

We performed these tasks in Windows 7 SP1 and Windows 10 1703 environments, and listed the MD5 hash values*5 of each PDF file recovered from the snapshot in Table 1. Although we were able to successfully recover all files in Windows 7, all files were corrupted in Windows 10.

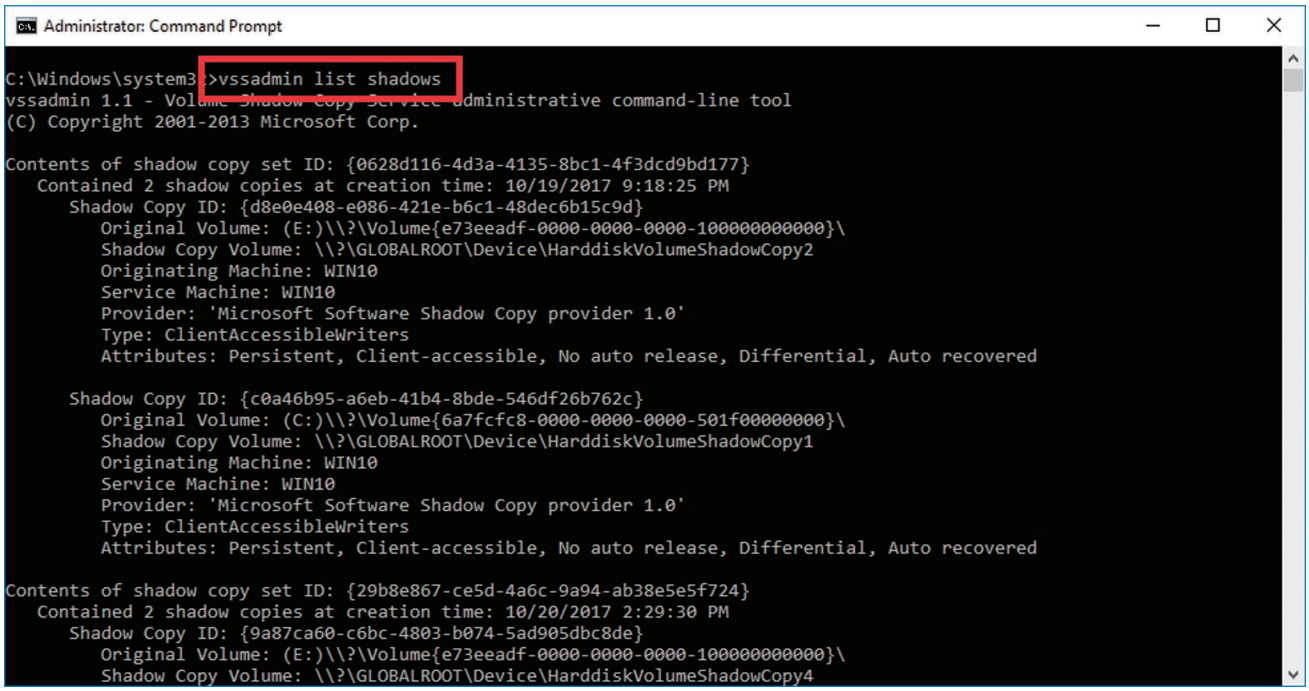

Figure 8: Snapshot List

File name	MD5 of original file	Windows 7 SP1		Windows 10 1703	
		MD5 of recovered file	Match	MD5 of recovered file	Match
iir_vol26_EN.pdf	a3002c631ca894034b594ec4e1a7c285	a3002c631ca894034b594ec4e1a7c285	Yes	42b4ac3f7e2f349ed8a0d3e240db35a6	No
iir_vol27_EN.pdf	09339fc3375988f8f769ccfa7ac75d4f	09339fc3375988f8f769ccfa7ac75d4f	Yes	e4986e8866435b7273f16a7f8fe60a14	No
iir_vol28_EN.pdf	89fee5ffccfb5be9749639e7e65a218e	89fee5ffccfb5be9749639e7e65a218e	Yes	86ff8c095a5b116e1ff34e12d6999053	No
iir_vol29_EN.pdf	42edeccedd51eecc20d0d9c123329b9a	42edeccedd51eecc20d0d9c123329b9a	Yes	5a8a530c084e5ee8ec129c62afa5ab0e	No
iir_vol30_EN.pdf	25df11281a2b1fb72a3f6d48d697c6b4	25df11281a2b1fb72a3f6d48d697c6b4	Yes	a4a68b122007b80a24ca2457e69b0902	No
iir_vol31_EN.pdf	79eac7926477141397f179654d307473	79eac7926477141397f179654d307473	Yes	b8cac677d7cf6bf15594a477c4b1b104	No
iir_vol32_EN.pdf	a99869ea8ea3cbda032d36ba000cdd26	a99869ea8ea3cbda032d36ba000cdd26	Yes	1bd79719c9c91c52e1de214a16572f90	No
iir_vol33_EN.pdf	a246c3f7ef836a141eb9c181899003f3	a246c3f7ef836a141eb9c181899003f3	Yes	17b820ab7f61a6de25cfcc89a1f49e62	No
iir_vol34_EN.pdf	093f3757b7a9269655d9fa6816b6dc72	093f3757b7a9269655d9fa6816b6dc72	Yes	b3c354a635ec62d747ae20aa71f46ab0	No
iir_vol35_EN.pdf	256dd74e71e1080170ddf59d0757e230	256dd74e71e1080170ddf59d0757e230	Yes	6220ce0b3df16961123438bd524568ce	No

Table 1: Comparison of Recovered Files

*3 SDelete (https://docs.microsoft.com/en-us/sysinternals/downloads/sdelete).
*4 ShadowExplorer.com (http://www.shadowexplorer.com/)
*5 MD5 hashes are known to be prone to collisions, but they were used here to compare the identity of specific files, as well as due to space limitations.

2.6 Cause of File Corruption and Countermeasures

Comparing a corrupted file and normal file using a binary editor, we can see that part of the file has been overwritten with null bytes (0x00) (Figure 9). The original file is shown on the left, while a file recovered using Windows 10 is on the right. The red part is where the data does not match. The part overwritten with null bytes differs for each file.

Upon investigation, we found that the corruption of snapshot user data was caused by a function called “ScopeSnapshots*6,” which was first introduced in Windows 8*7. When this function is enabled, the data to be saved in a snapshot is limited to Windows system-related files, meaning user data will not be saved*8. This function is only applied to the system volume (C drive), but in recent years, many PCs have a drive configuration with just a C drive, so it will have a significant impact.

Details of the functional specifications have not been disclosed, so in part, this is a guess based on the test results, but it appears that the operation limiting the files is not perfectly controlled, and in some cases only part of the user data is saved in the snapshot. It is possible that missing data is overwritten with 0x00 when trying to restore this incomplete user data. Also, resident*9 files were saved to the snapshot when they were user data.

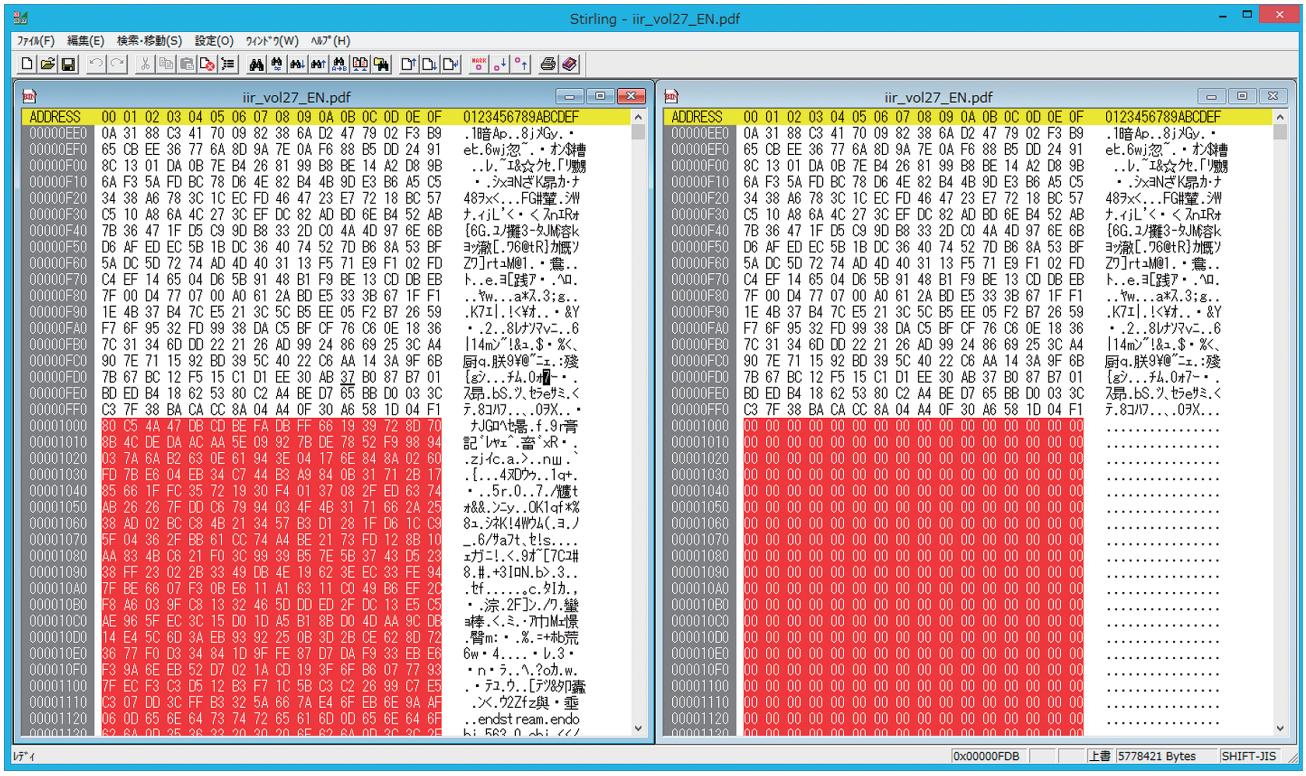

Figure 9: Comparison of Normal and Corrupted Data

*6 Calling SRSetRestorePoint (https://msdn.microsoft.com/en-us/library/windows/desktop/aa378727(v=vs.85).aspx).

*7 We have also received a response from Microsoft indicating that it is highly likely this function is the cause of the file corruption.

*8 Although the reasons for this specification change have not been made public, we speculate that it is related to performance issues from saving all data into a snapshot, utilization efficiency issues in the snapshot area, excessive expansion of user data, and the fact that “file history” is now recommended for backing up user data.

*9 NTFS stores small file data directly in the $DATA attribute of the NTFS MFT record instead of allocating space for it. This state is known as “resident.”

You can disable ScopeSnapshots by creating "ScopeSnapshots" with a DWORD value of "0" in the "HKLM\Software\Microsoft\Windows NT\CurrentVersion\SystemRestore" registry key, and then rebooting the OS (Figure 10). We have also confirmed that it is possible to recover user data from a snapshot correctly in Windows 10 with ScopeSnapshots disabled*10.

As far as we can tell, user data can be recovered correctly from snapshots without disabling ScopeSnapshots in Windows Server products. Table 2 shows whether recovered user data was corrupted in each OS under default settings.

2.7 Conclusion

VSS is a function that has been present since the Windows XP era, but here we identified that the specifications have changed along with updates to the OS version. As such, specifications may change for functions that have been used in the past, so it is important to check for specification updates and verify the tools you use when new OS versions are released.

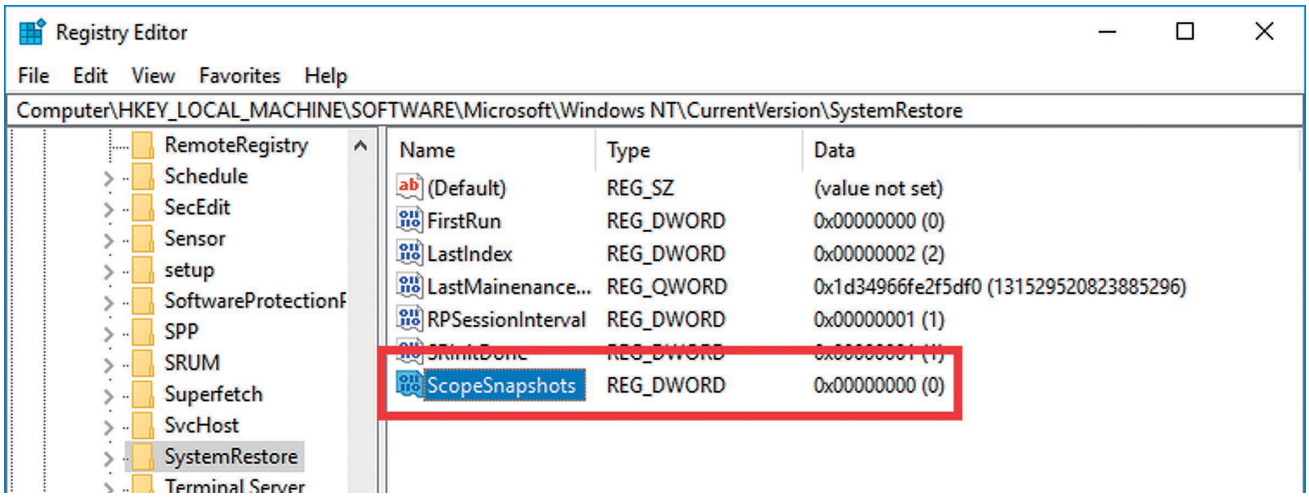

Figure 10: Disabling ScopeSnapshots

Table 2: Corruption of Recovered User Data by OS

	Windows 7 SP1	Windows 8.1	Windows 10	Windows Server 2012/2012 R2	Windows Server 2016
Corruption of Recovered User Data	No	Yes	Yes	No	No

Authors:
Mamoru Saito
Director of the Advanced Security Division, and Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ. After working in security services development for enterprise customers, in 2001 Mr. Saito became the representative of the IIJ Group emergency response team IIJ-SECT, which is a member team of FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member for several industry groups, including ICT-ISAC Japan, Information Security Operation providers Group Japan, and others.

Minoru Kobayashi (VSS Does Not Protect User Data)
Office of Emergency Response and Clearinghouse for Security Information, Advanced Security Division, IIJ

*10 We also performed a series of tests using Windows 8.1, and the results were the same as for Windows 10.