==========

Chall-Link "VSSDetector" Usage Guide

English Version Ver.1.0.0

Creating 7-Zip Encrypted Archives

Using Restore Point VSS Snapshots

Full Drive Backup Capability

==========

■Software Used in This Usage Guide

1. **7-Zip Enhanced Script Chall-Link "PreFAS Backup"※ (Available from GitHub)**
2. **7-Zip (LGPL License) (Available from https://www.7-zip.org/)**

> ※ Scheduled for release around the same time after VSSDetector publication

---

■Overview: About This Guide

Chall-Link "VSSDetector" unlocks Windows' hidden feature **VSS Snapshots** = drive states saved in an unchangeable form at a specific point in time, making them freely reusable by general users.

This usage guide introduces specific procedures for executing backup software and backup programs using Windows restore points as archive sources, demonstrating the combination of VSSDetector with Chall-Link "PreFAS Backup" or 7-Zip.

■Procedures: Specific Usage Examples

1. Objective: Creating 7-Zip Archives Using Folders in VSS Snapshots as Archive Sources

> Traditional source path specification example: D:\ ※ Work on D: had to be suspended during processing
>
> ↓
>
> VSSDetector "VSS Path" specification example: \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1*
> ※Work can continue during processing

`VSSDetector enables simultaneous 7-Zip backup processing of large folders (drives) while continuing PC work on large folders (drives)!`

2. Preparation: Creating Restore Points

> ⚠️ Creating new restore points should be done with administrator/co-administrator consent
> Approximately 20% or more free space is required on the target drive when creating restore points.
> Insufficient free space may prevent normal processing.

2.1. Step 1: Enabling System Restore Function

(1) Accessing System Restore Settings

Search for "Create a restore point" in the Windows search box and open it
The "System Protection" tab of the "System Properties" window opens

(2) [Required Setting] System Drive (usually C:) Protection Settings

System Restore cannot enable other drives unless the system drive (C:) is enabled first
If "Windows(C:) (System)" protection is disabled, select the system drive (C:)
Select "Configure" → "Turn on system protection" to enable system drive (C:) protection
Disk Space Usage: 5-10% of disk size

(3) [Important Setting] Data Drive (e.g., D:) Protection Settings

Select the data drive to be backed up and click "Configure"
Select "Turn on system protection"
Disk Space Usage: 1-3% (1-2% for small capacity drives)

> 👉 Simply enabling it does not create restore points yet

2.2. Step 2: Creating Restore Points

> 💡 If you want the latest state backup, we recommend not waiting too long between restore point creation and backup creation

(1) Restore Point Creation:

Click the "Create" button in the "System Protection" tab of the "System Properties" window

(2) Enter Identification Description

Enter an easily identifiable name in the restore point description field
Example: "backup-25-06-06-1200"

(3) Execute Restore Point Creation Process

Clicking the "Create" button in the "System Protection" window starts creating snapshots of all currently enabled drives

(4) Confirm Successful Creation

Creation is complete when you see "The restore point was created successfully"

✔ `Static state preservation of drives = Windows VSS Snapshot creation is now complete!`

3. VSS Path Acquisition Using VSSDetector

Use VSSDetector to obtain VSS paths for restore point VSS snapshots

3.1. Step 1: Running VSSDetector

(1) Right-click ChaL-VSSDetector.bat and select "Run as administrator"

(2) VSS snapshot analysis processing is executed

(3) Execution Complete

After confirming the "Script execution completed" message, you can close the screen.
All analysis results have been saved to the output file.

3.2. Step 2: Confirming and Using VSSDetector "VSS Path" Information

(1) Output Result File

Open "ChaL-RESULT-VSSDetector.txt" created in the execution folder
This file is overwritten each time you run the script

(2) VSSDetector "VSS Path" Information Display Example:

```
_____________________________
[1] HarddiskVolumeShadowCopy1 (Drive D:)
    Creation Time: 2024/06/06 14:30:25
    Type: System Restore Point
    Full Drive Path: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\*
    Folder Path: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\(folder name)
_____________________________
```

(3) Selecting and Copying VSSDetector "VSS Path"

Copy the optimal VSS path corresponding to your backup target drive/folder

> ⚠️ Difference between VSSDetector "VSS Path" full drive specification and folder specification
> **Full Drive Specification**: Requires "*" at the end (example: ~Copy1*)
> **Specific Folder Specification**: Replace (folder name) with the actual exact folder name

✔ `VSS path extraction for direct access to VSS snapshots is complete!`

👉 `Next, we'll explain how to create 7-Zip archives using VSS snapshots as sources with the 7-Zip enhanced script Chall-Link "PreFAS Backup" or 7-Zip File Manager`

4. Archive/Backup Execution

4.1. Configuration Conditions and Precautions

■ Configuration Examples

[Case1] Small-scale folders that finish processing quickly as archive sources
Source Folder: `d:\folder1\sub-folder2\`
Output Destination: `e:\7-Zip-output\`
[Case2] Large-scale sources like entire drives requiring long-term processing as archive sources
※ Please note that executing entire drives may take 12+ hours

> ⚠ **Important Verification:**
> In production, always verify that you can open the file with 7-Zip File Manager after backup creation and properly browse the file tree
> The author assumes no responsibility if password mismatch or backup corruption occurs after deleting the source following backup creation

4.2. [Method 1] Manual Execution with 7-Zip GUI (Recommended for small-scale archives)

[Case1] Small-scale folders that finish processing quickly as archive sources

(1) Launch "7-Zip File Manager" with administrator privileges

(2) Direct Access with VSSDetector "VSS Path"
For 7-Zip File Manager, remove the final * from the full drive path specification
Enter the VSSDetector "VSS Path" in the address bar **(excluding the final *)**
Example: \?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\

(3) Archive Target Selection
Select target folder (example: folder1\sub-folder2) → Select "Add" to open compression window

(4) [Important] Change Output Destination
By default, the compressed file output destination is set to inside the snapshot
\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\
This is inside the snapshot and cannot be written to.
Change the compression destination to an actual output folder that allows writing (e:\7-Zip-output).
If you set the output filename to file-1.7z, it becomes:
e:\7-Zip-output\file-1.7z

[Case2] Large-scale sources like entire drives requiring long-term processing as archive sources

〜〜〜 Omitted 〜〜〜
👉 For large-scale long-term processing like entire drives, we recommend using the 7-Zip enhanced script Chall-Link "PreFAS Backup" rather than the GUI method

---

4.3. [Method 2] Enhanced 7-Zip Processing with PreFAS Backup (For large-capacity backups)

> **■ About Chall-Link "PreFAS Backup"...**
>
> Chall-Link "PreFAS Backup" was developed with the concept of protecting valuable files from disasters by converting large-scale drives and folders into portable archives with 7-Zip AES-256 encryption and storing them on cloud storage or M-Disc (100-year durable optical discs).
>
> **[PreFAS Backup Features]**
>
> - Secure Archives: Strong data protection with AES-256 encryption
> - Load Reduction and Work Continuation: Controls 7-Zip CPU load, suppressing sustained high load while enabling comfortable editing work in source folders
> - Large-scale Support: Fully automated backup of terabyte-class folders/drives
> - Optical Disc Optimization: Efficient split size settings for 25GB, 50GB, 100GB optical discs
> - Professional-grade Reliability: Error handling system comparable to commercial software

(1) PreFAS-Sub.bat Configuration

Open ChaL-PreFAS-Backup-SUB-en.bat in a text editor and edit variable values:

[Case1] Small-scale folders that finish processing quickly as archive sources

```
set SOURCE_FOLDER="\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\folder1\sub-folder2\"
```

[Case2] Large-scale sources like entire drives requiring long-term processing as archive sources

```
set SOURCE_FOLDER="\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\*"
```

> In this case, the final * is required

---

(2) Other Required/Important Variable Settings

Open ChaL-PreFAS-Backup-SUB-en.bat in a text editor and edit variable values

Output Archive Filename Setting

`file-1` (no extension required)

Archive File Output Folder Setting

`e:\7-Zip-output\`

Exclude Files and Folders Specification (Example)

`set EXCLUDE=-xr!"*.tmp" -xr!"*.temp"`

(3) Reliable Execution of ChaL-PreFAS-Backup-MAIN-en.bat

Right-click → "Run as administrator"

(4) Password Setting

Enter a strong password for AES-256 encryption twice (for high confidentiality, 20-30 characters with alphanumeric characters and symbols recommended)

(5) Automatic Processing Start

- Background color displays in cyan, and advanced automatic processing begins
- CPU load is controlled by Chall-Link "PreFAS Backup", enabling normal file editing during archive processing
- "Everything is Ok" is displayed upon completion, indicating successful processing

🎉 `Backup creation using VSSDetector is complete! Excellent work!`

■Important Matters in This Usage Guide

Required Actions

- After archive completion, check password and file list with 7-Zip File Manager

Prohibited Actions

- Deleting "System Restore and Shadow Copies" in Disk Cleanup during processing

Precautions

- If you notice abnormal PC fan rotation during long-term processing, immediately stop PreFAS Backup

Recommendations

- Create the latest restore point before PreFAS Backup
- Store passwords appropriately and safely. Recovery is impossible if lost.

■Deleting Restore Point Snapshots

> ⚠ In shared environments, consult with administrators before implementation

(1) Search for "Create a restore point" in the Windows search box and access
(2) Select the target drive for deletion and click "Configure"
(3) Select the "Delete" button to delete snapshots

■[Disclaimer]

- The author assumes no responsibility for any damage or issues arising from executing these procedures.

- For important data, always create separate backups beforehand.
- Create this backup as one of multiple backup methods, not as a single backup solution.

End