

# Collect Process Crashdumps on Windows for Sfc Process

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentets Used](#)

[Problem](#)

[Solution](#)

---

## Introduction

This document describes how to collect Process crashdumps on Windows for sfc process.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Endpoint connector
- Command Prompt Windows

### Componentets Used

This document is not restricted to software and hardware versions. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

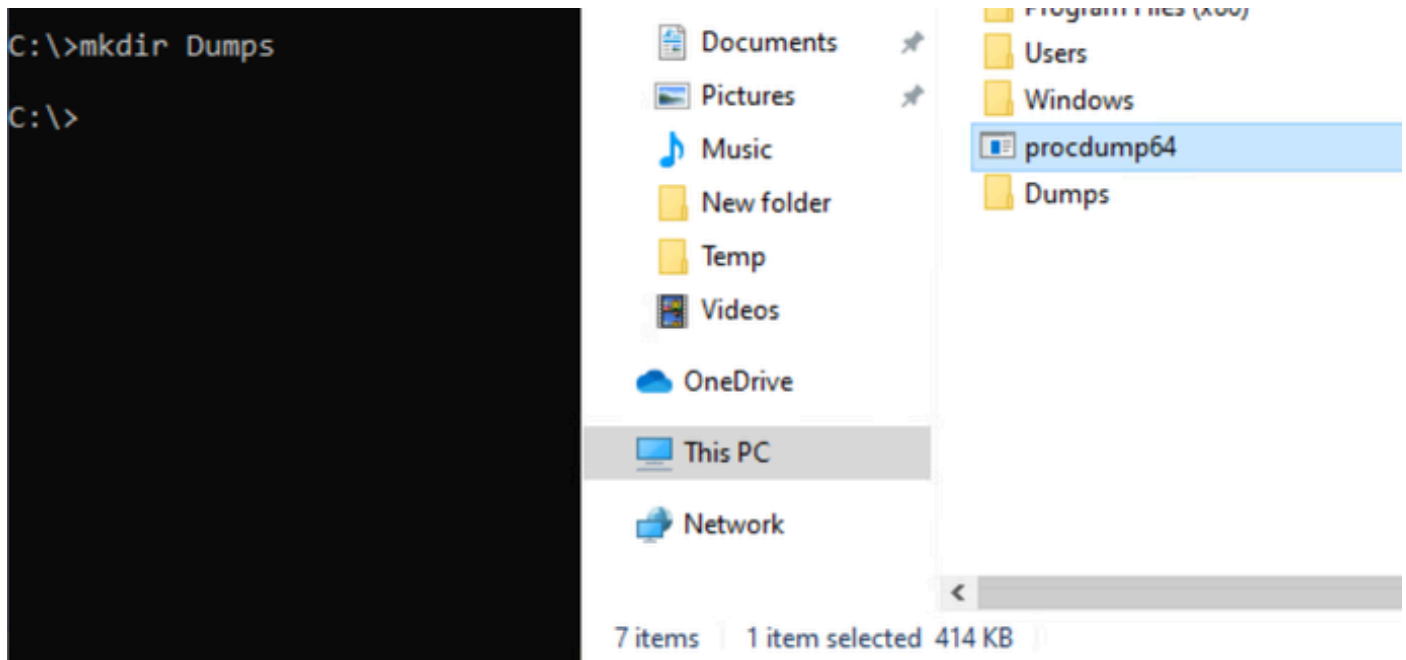
## Problem

- Cisco Secure endpoint application can go to a disabled or disconnected state due to process crash of sfc.exe, which could be related to unexpected windows shutdown or any other activity on windows.
- Windows activates a debugging tool configured in the AeDebug registry values. Any program can be selected in advance as the tool to use in this situation. The chosen program is referred to as the postmortem debugger.

## Solution

Download [Procdump as the \(AeDebug\) postmortem debugger](#) from sysinternals suite.

Extract **Procdump** in c drive and create **Dumps folder** for crashdump collection as shown:



Set **Procdump** as AeDebugger:

```
C:\>procdump64.exe -ma -i C:\Dumps

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Set to:
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
    (REG_SZ) Auto      = 1
    (REG_SZ) Debugger = "C:\procdump64.exe" -accepteula -ma -j "C:\Dumps" %ld %ld %p

ProcDump is now set as the Just-in-time (AeDebug) debugger.

C:\>
C:\>_
```

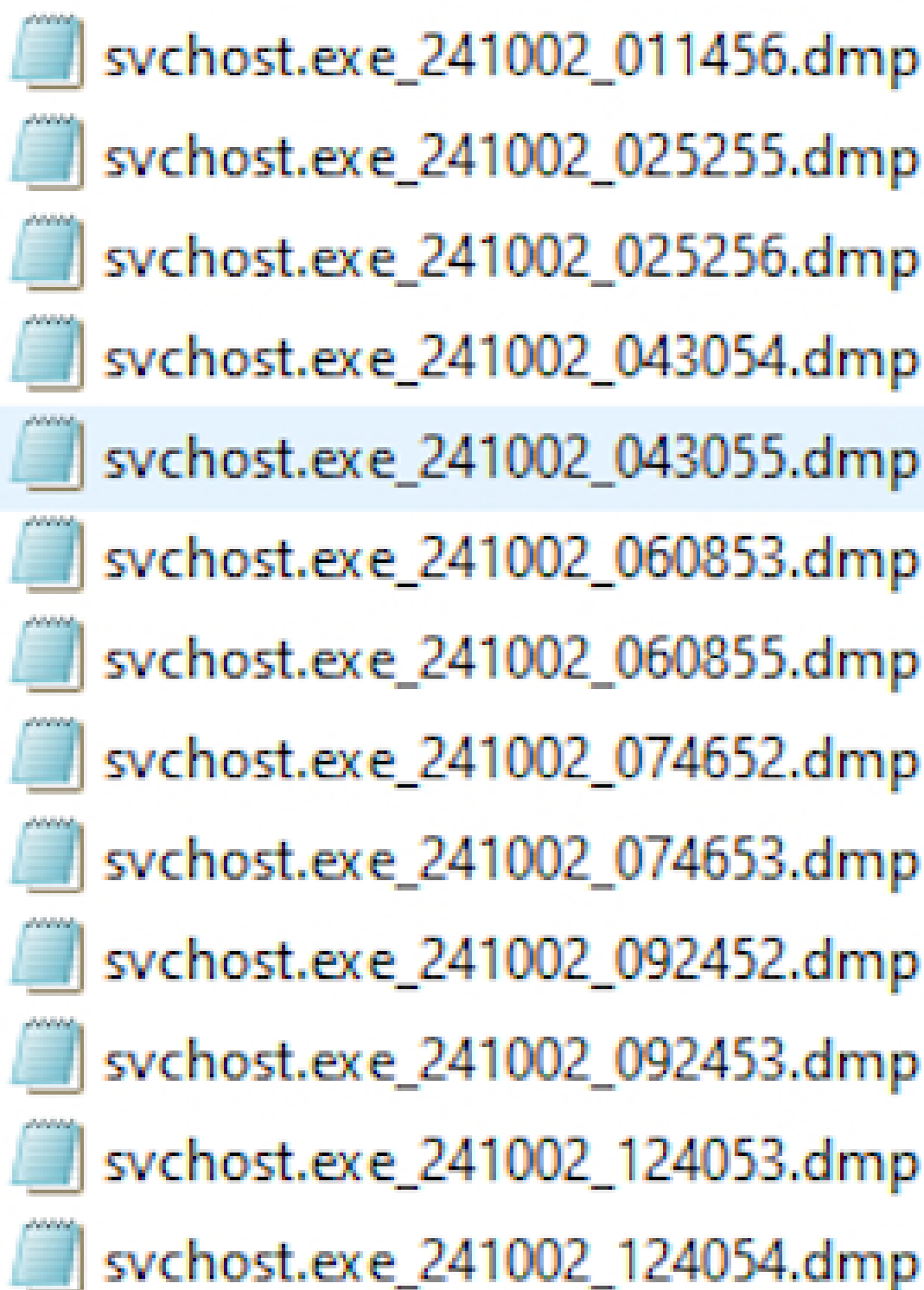
How to Use:

- Launch **CMD** as Administrator.
- Change to the directory where you unpacked procdump tool.
- Command example: **procdump64.exe -ma <PID | Process Name>** or **procdump64.exe -ma -i C:\Dumps**

Example for sfc.exe:

**procdump64.exe -accepteula -ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe**

It saves the crashdumps in the Dumps folder as shown. Collect and share it for analysis:



svchost.exe\_241002\_011456.dmp  
svchost.exe\_241002\_025255.dmp  
svchost.exe\_241002\_025256.dmp  
svchost.exe\_241002\_043054.dmp  
svchost.exe\_241002\_043055.dmp  
svchost.exe\_241002\_060853.dmp  
svchost.exe\_241002\_060855.dmp  
svchost.exe\_241002\_074652.dmp  
svchost.exe\_241002\_074653.dmp  
svchost.exe\_241002\_092452.dmp  
svchost.exe\_241002\_092453.dmp  
svchost.exe\_241002\_124053.dmp  
svchost.exe\_241002\_124054.dmp

To uninstall **procdump** use: **procdump64.exe -u**

```
C:\>
C:\>procdump64.exe -u

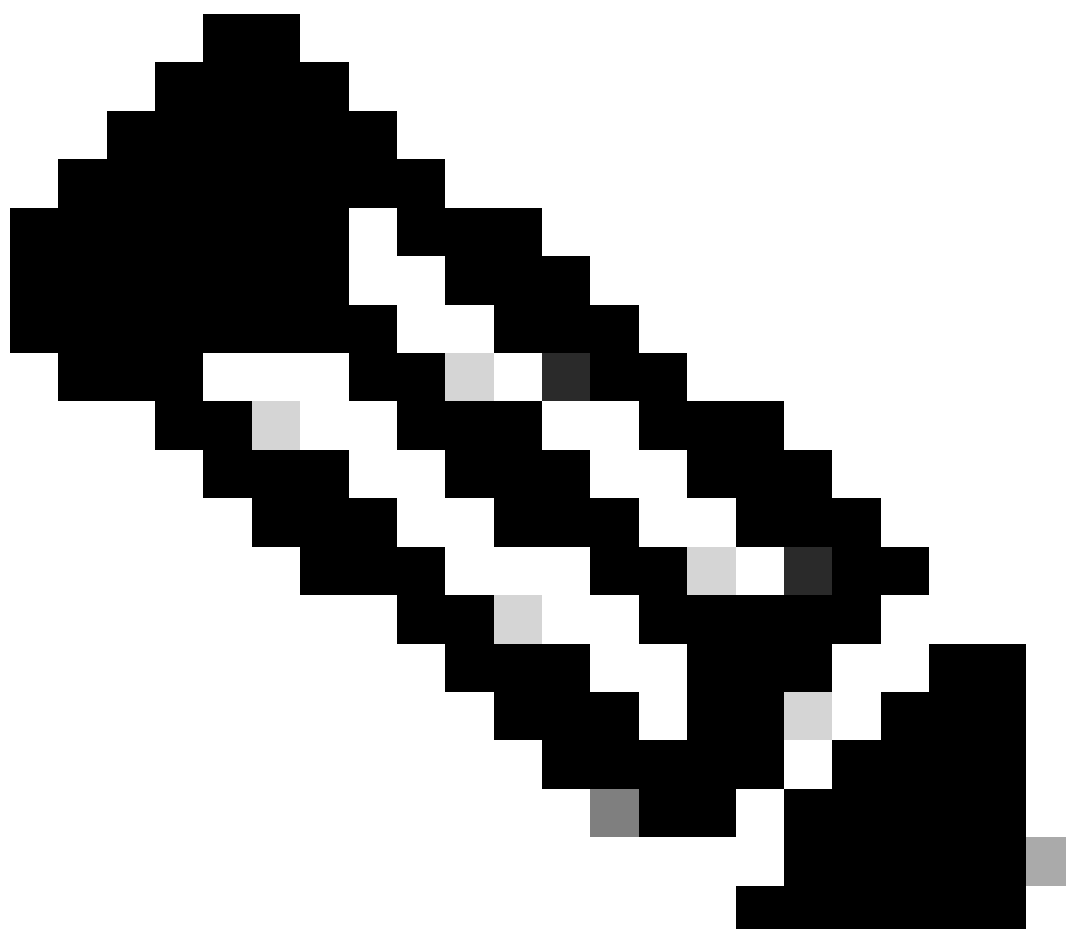
ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

Reset to:
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug
    (REG_SZ) Auto      = <deleted>
    (REG_SZ) Debugger  = <deleted>

ProcDump is no longer the Just-in-time (AeDebug) debugger.

C:\>
```

---





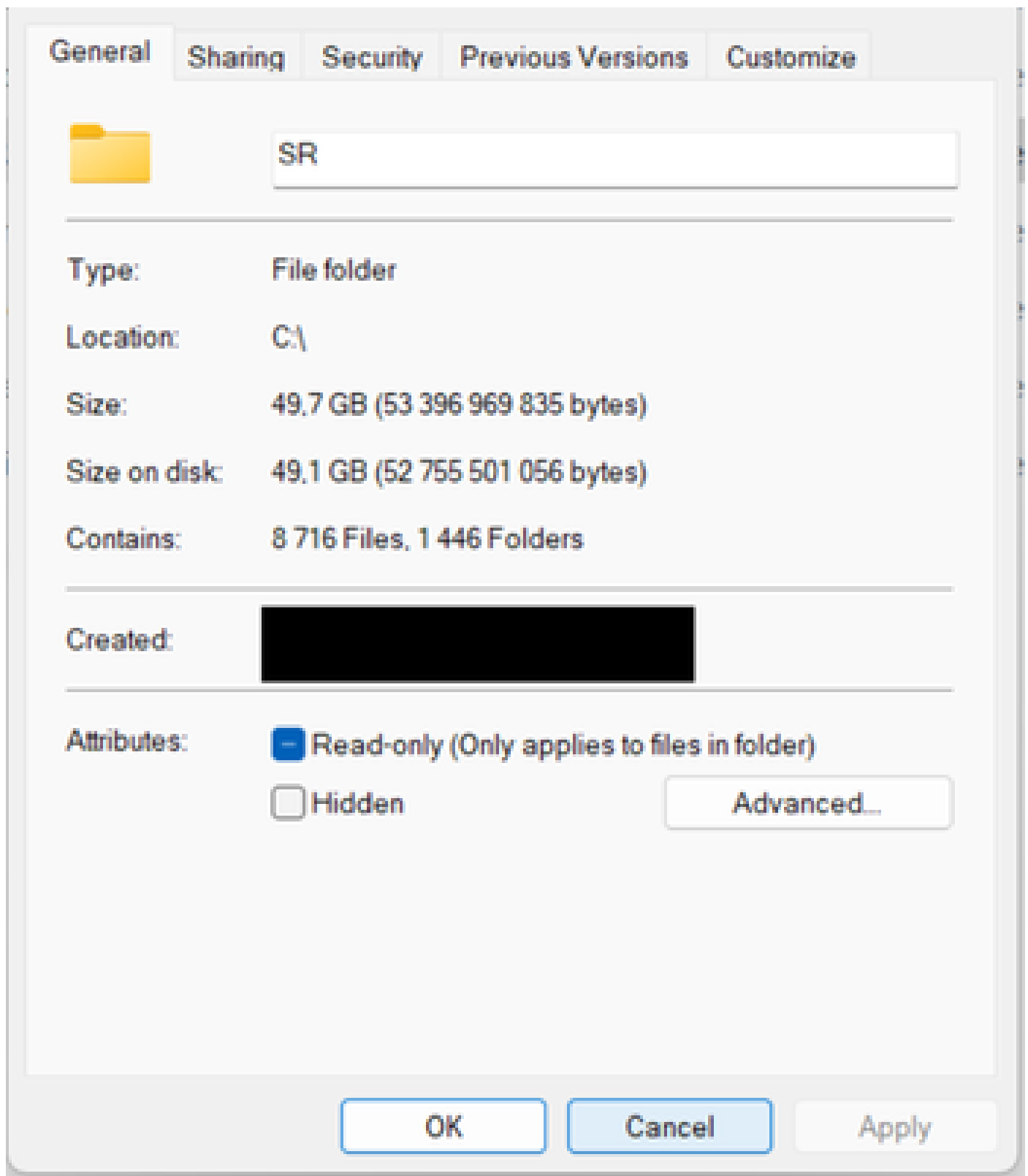
**Note:** Crash Dumps can consume large space on the disk and procdump can be stopped once collection is done.

---

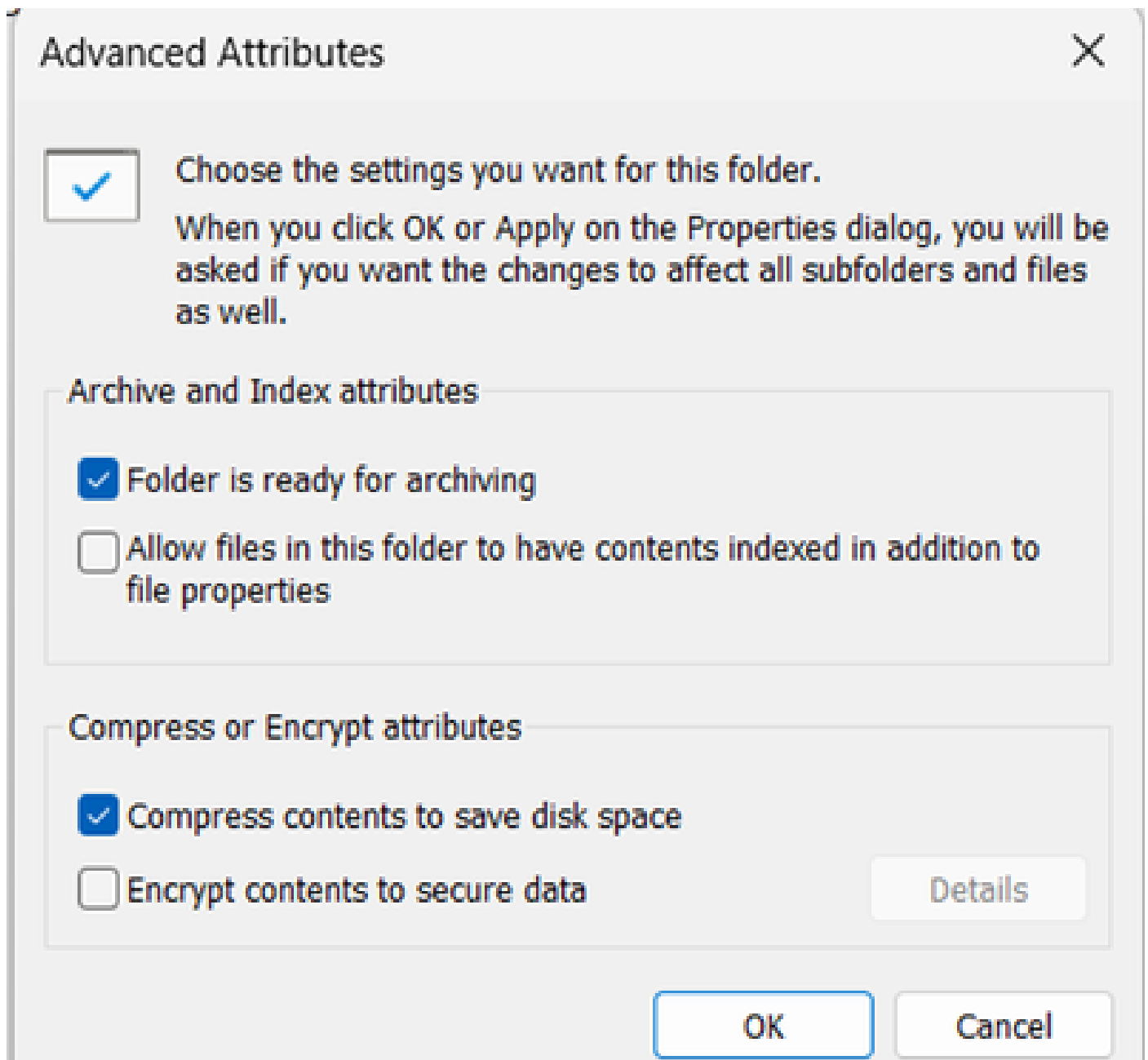
Although, you can also use the workaround to compress the size of the folder:

1- Navigate to **properties** of the **Dumps** folder and check **original size** of the folder on the disk as shown :

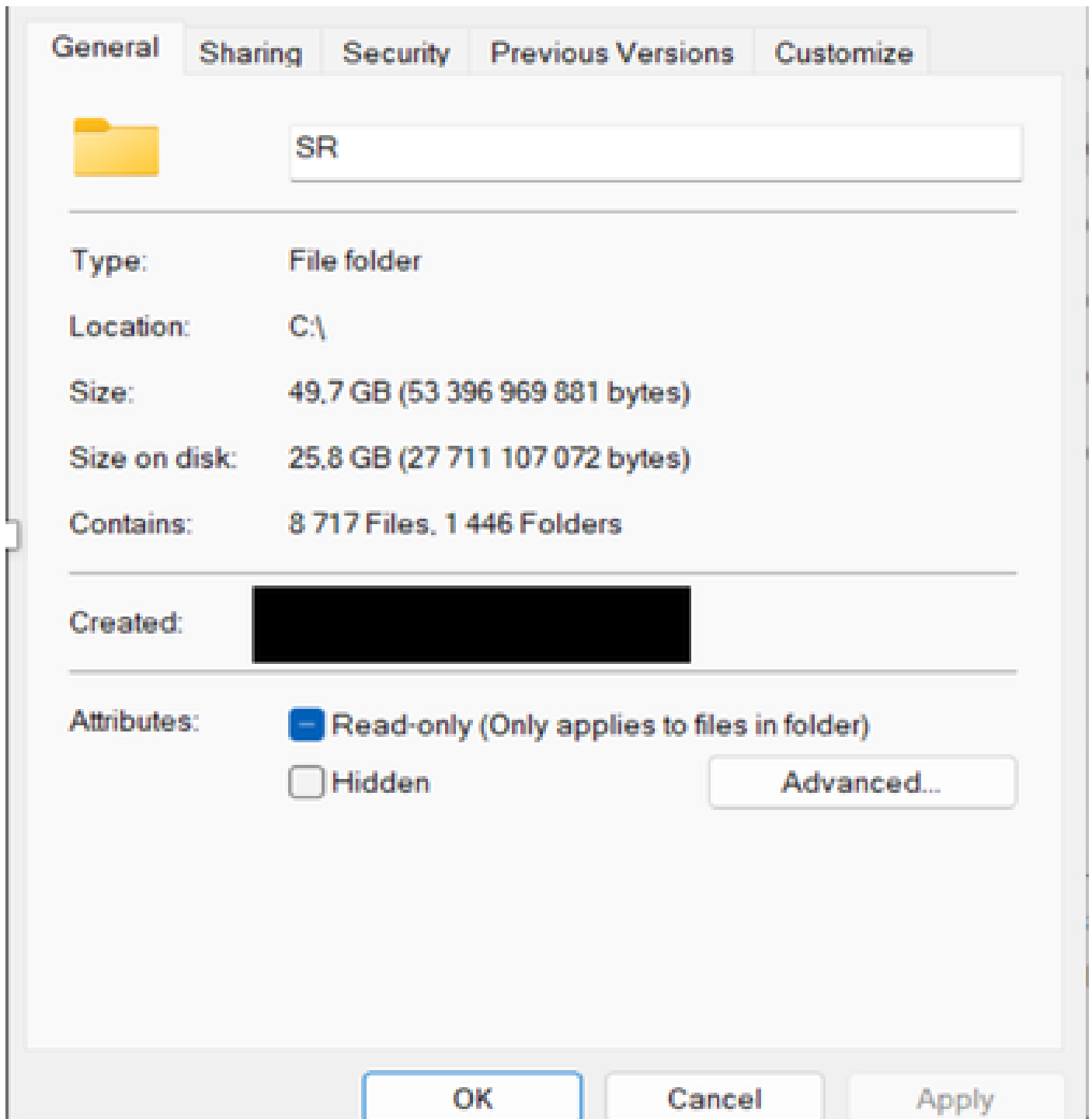
	procDump64	17/03/2025 07:13	Application
	Dumps	17/03/2025 07:14	File folder
<div> <div>View &gt;</div> <div>Sort by &gt;</div> <div>Group by &gt;</div> <div>Refresh</div> <hr/> <div>Paste</div> <div>Paste shortcut</div> <div>Undo Rename Ctrl+Z</div> <hr/> <div>Give access to &gt;</div> <hr/> <div>New &gt;</div> <hr/> <div>Properties</div> </div>			



2- Navigate to **Advanced** option and enable **compression** and apply which takes several minutes:



3- In the end, you can see the folder size reduces to nearly half the original size as shown:



4- You can also use this command on Command prompt to achieve the same:

**compact /c /s:c:\install**