Coletar Despejos de Memória de Processo no Windows para Processo Sfc

Contents

Introdução

Este documento descreve como coletar processos de crashdumps no Windows para o processo sfc.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector Cisco Secure Endpoint
- Janelas de Prompt de Comando

Componentes usados

Este documento não está restrito às versões de software e hardware. As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

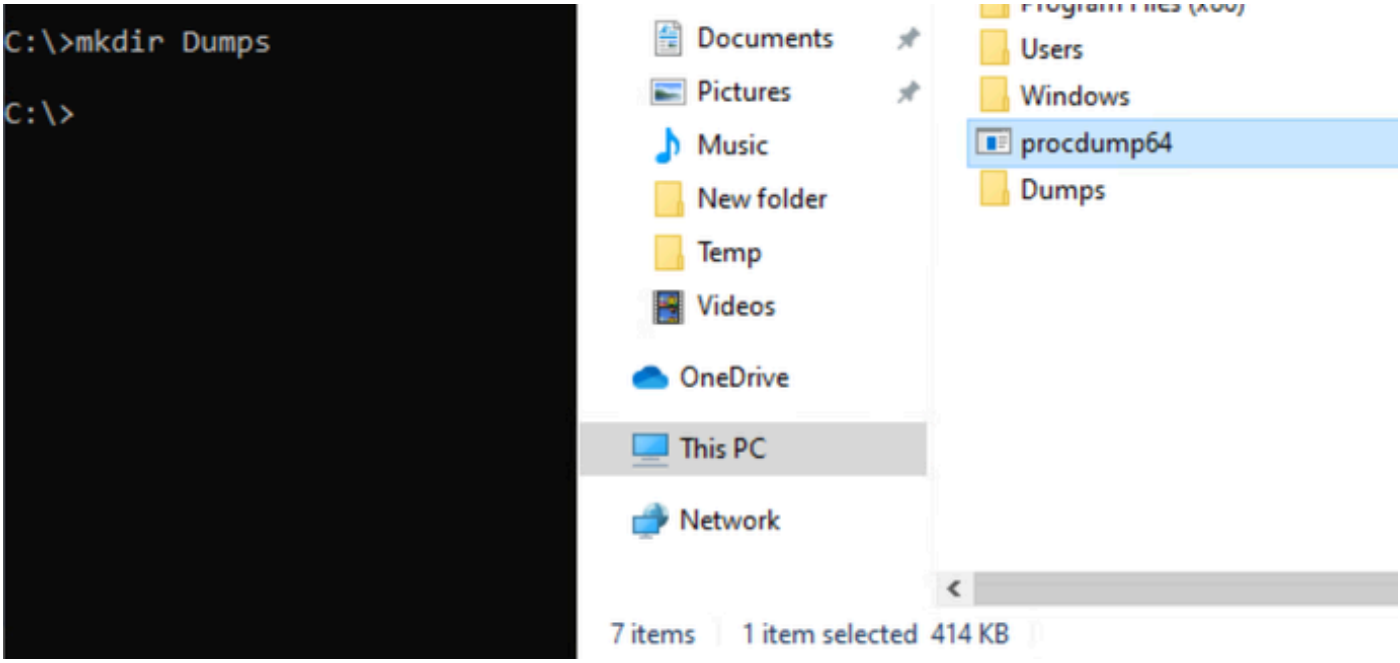
- O aplicativo de ponto de extremidade do Cisco Secure pode entrar em um estado desabilitado ou desconectado devido à falha de processo do sfc.exe, que pode estar relacionado ao desligamento inesperado do Windows ou a qualquer outra atividade no Windows.
- O Windows ativa uma ferramenta de depuração configurada nos valores do Registro AeDebug. Qualquer programa pode ser selecionado antecipadamente como a ferramenta a

ser usada nessa situação. O programa escolhido é conhecido como depurador post-mortem.

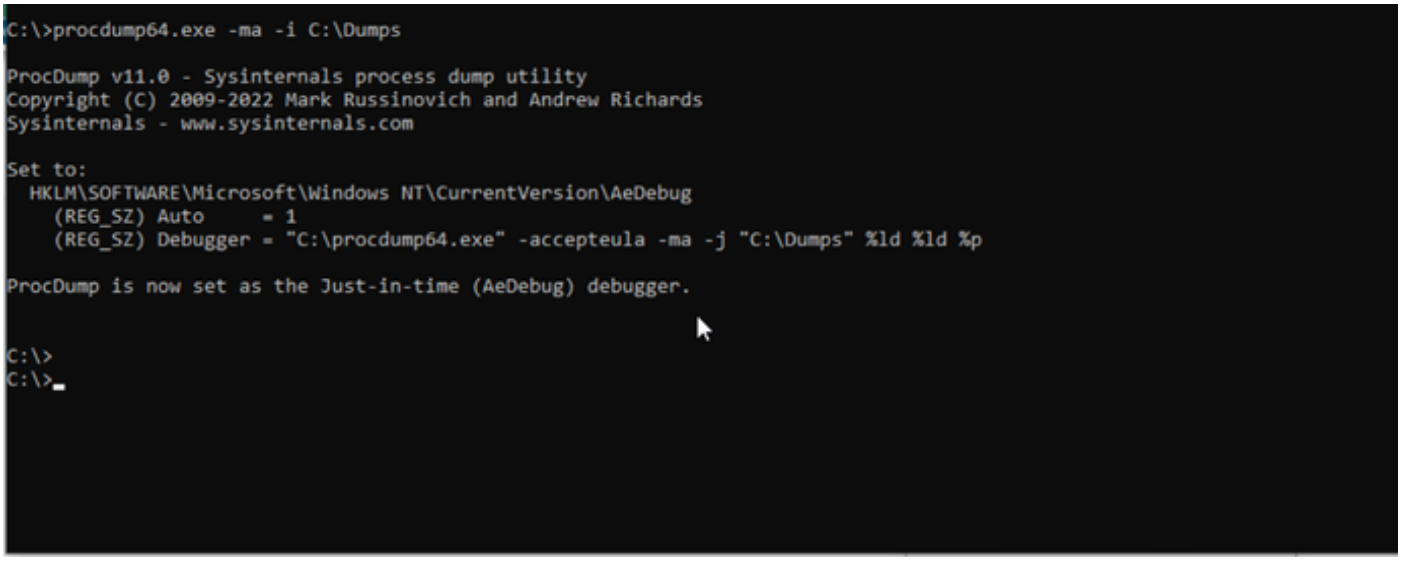
Solução

Baixe Procdump como o depurador post-mortem (AeDebug) do conjunto sysinternals.

Extraia Procdump na unidade c e crie a pasta Dumps para a coleção crashdump como mostrado:



Defina Procdump como AeDebugger:



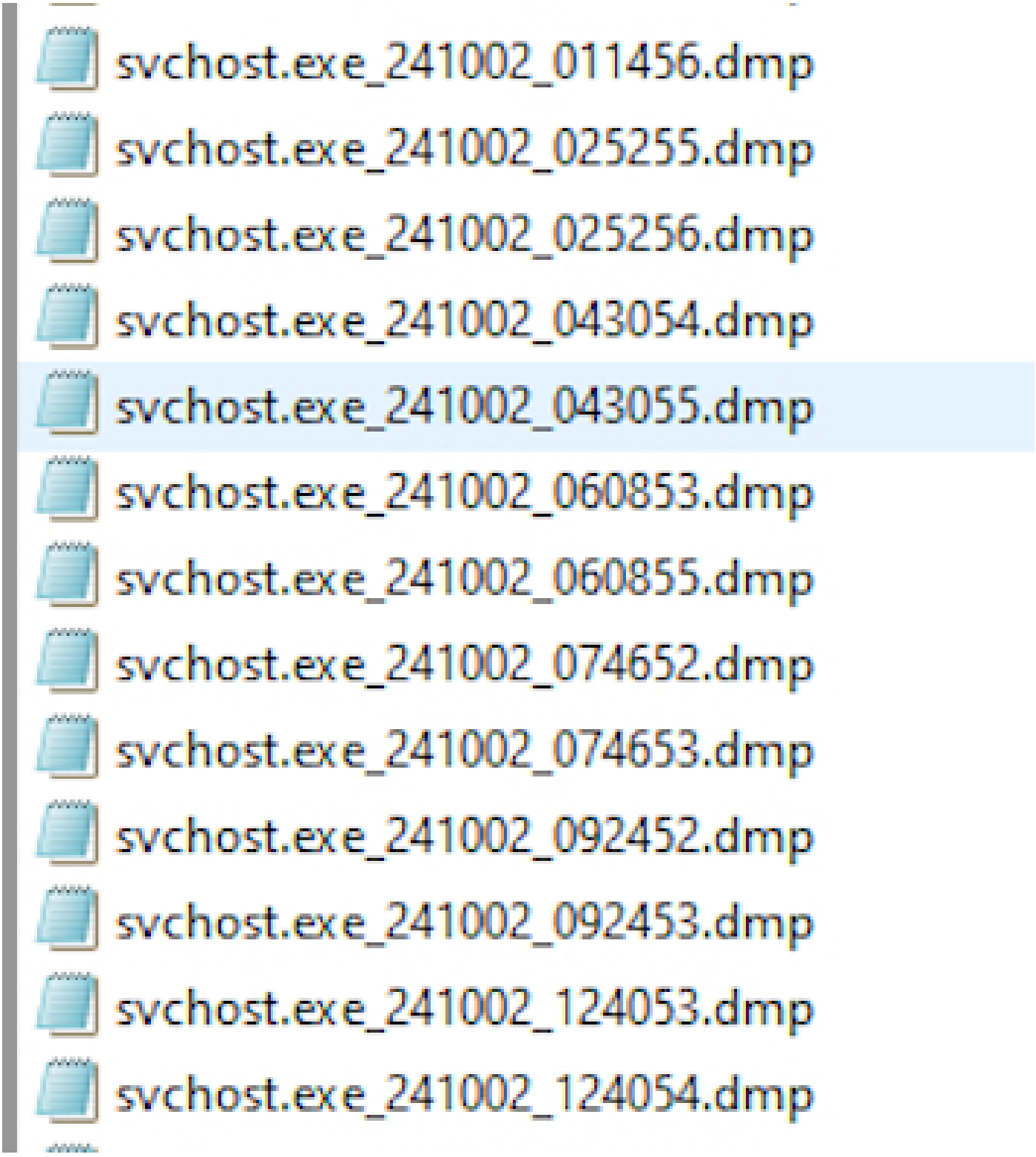
How to Use:

- Inicie o CMD como administrador.
- Altere para o diretório onde você desempacotou a ferramenta procdump.
- Exemplo de comando: procdump64.exe -ma <PID | Process Name> ou procdump64.exe -ma -i C:\Dumps

Exemplo para sfc.exe:

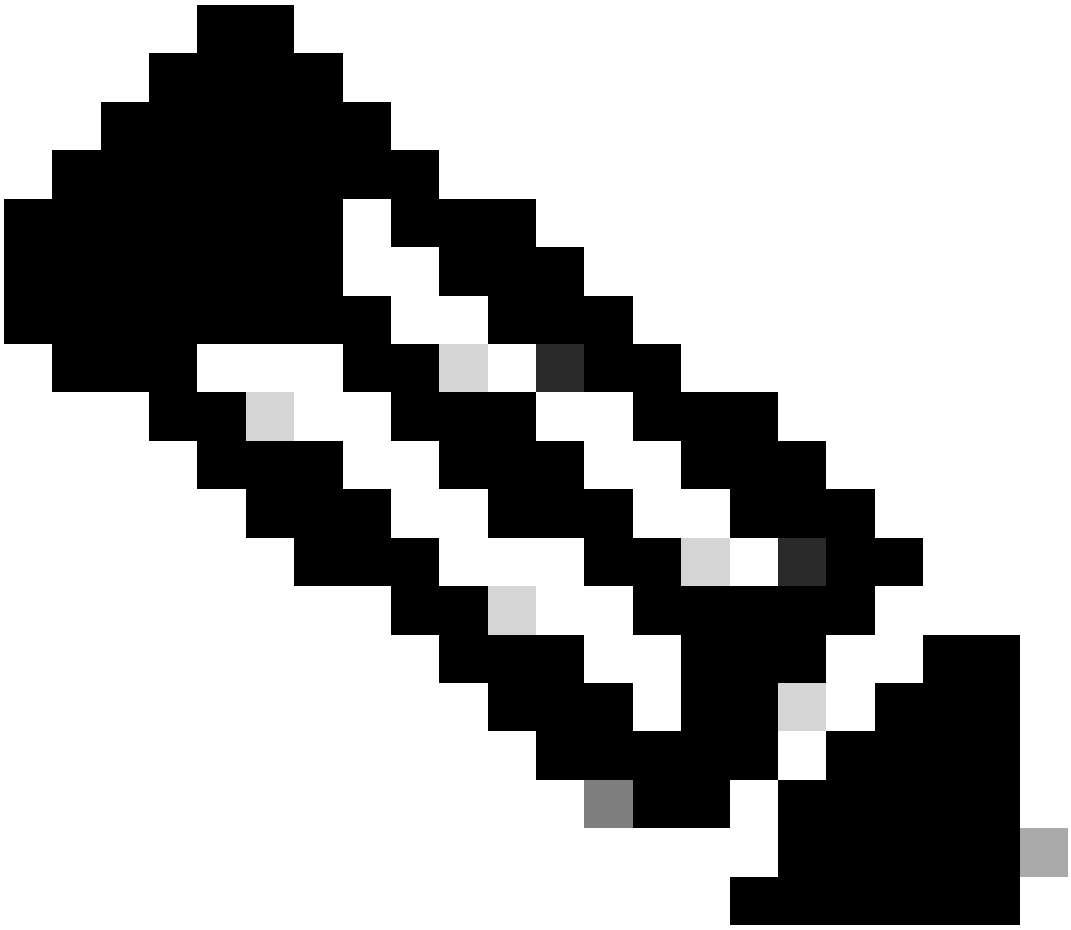
procdump64.exe -accept -ma -e -x c:\install %ProgramFiles%\Cisco\AMP\8.2.3.30119\sfc.exe

Salva os despejos de memória na pasta Despejos, como mostrado. Colete e compartilhe para análise:



Para desinstalar o procdump, use: procdump64.exe -u

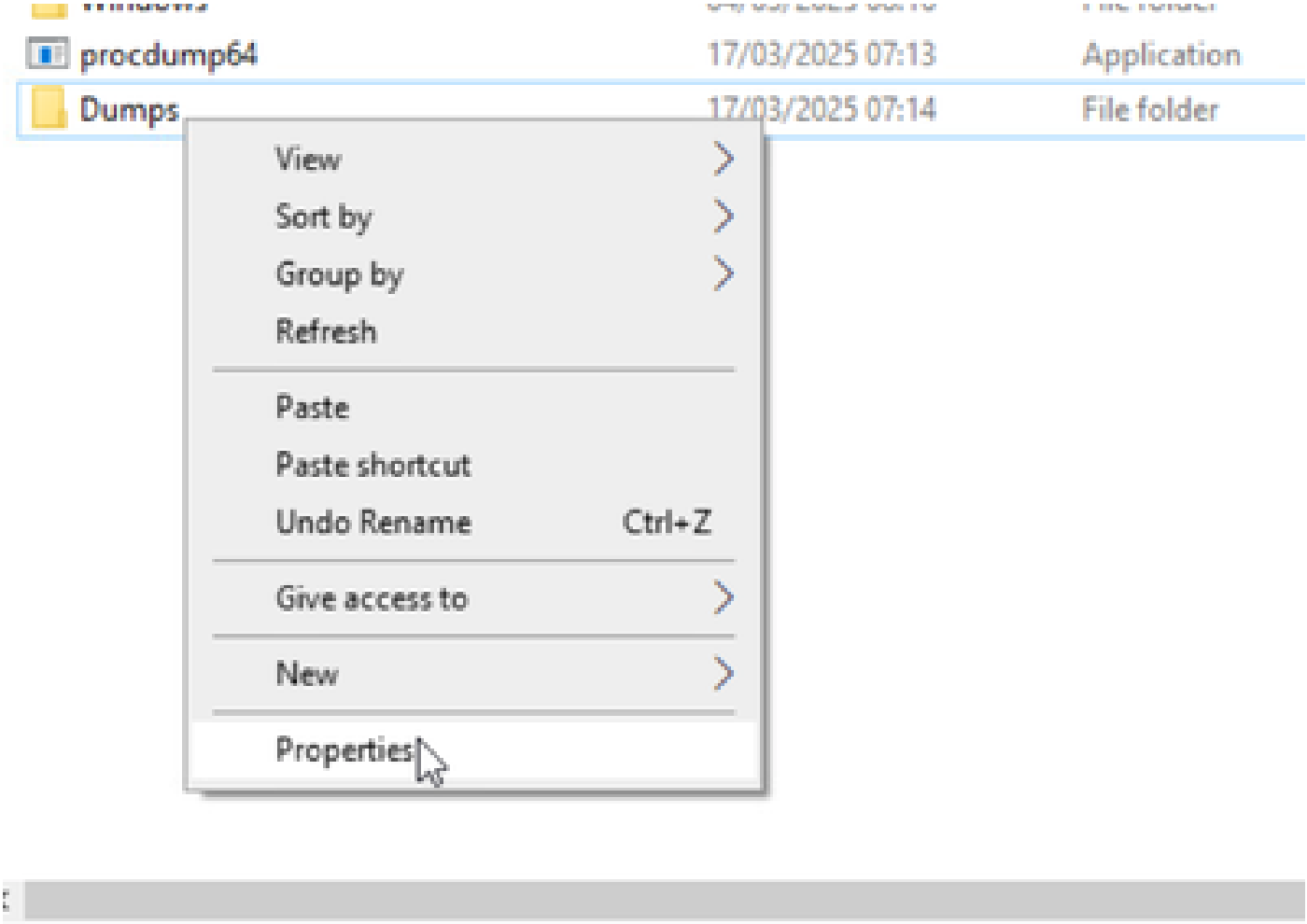
```
C:\>
C:\>procdump64.exe -u

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:\>_
```

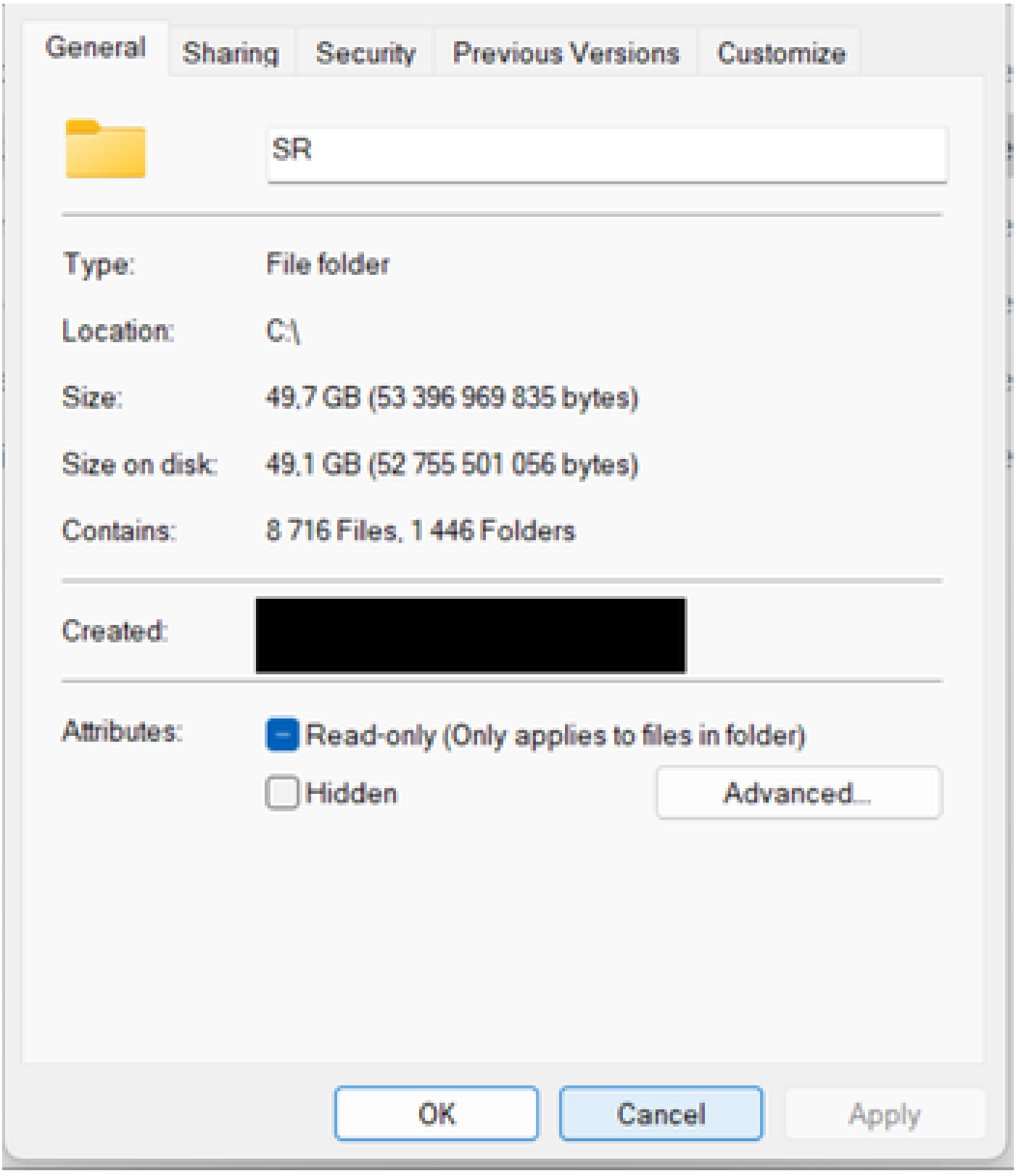


> Note: Os despejos de travamento podem consumir muito espaço no disco e o procdump pode ser interrompido após a coleta.

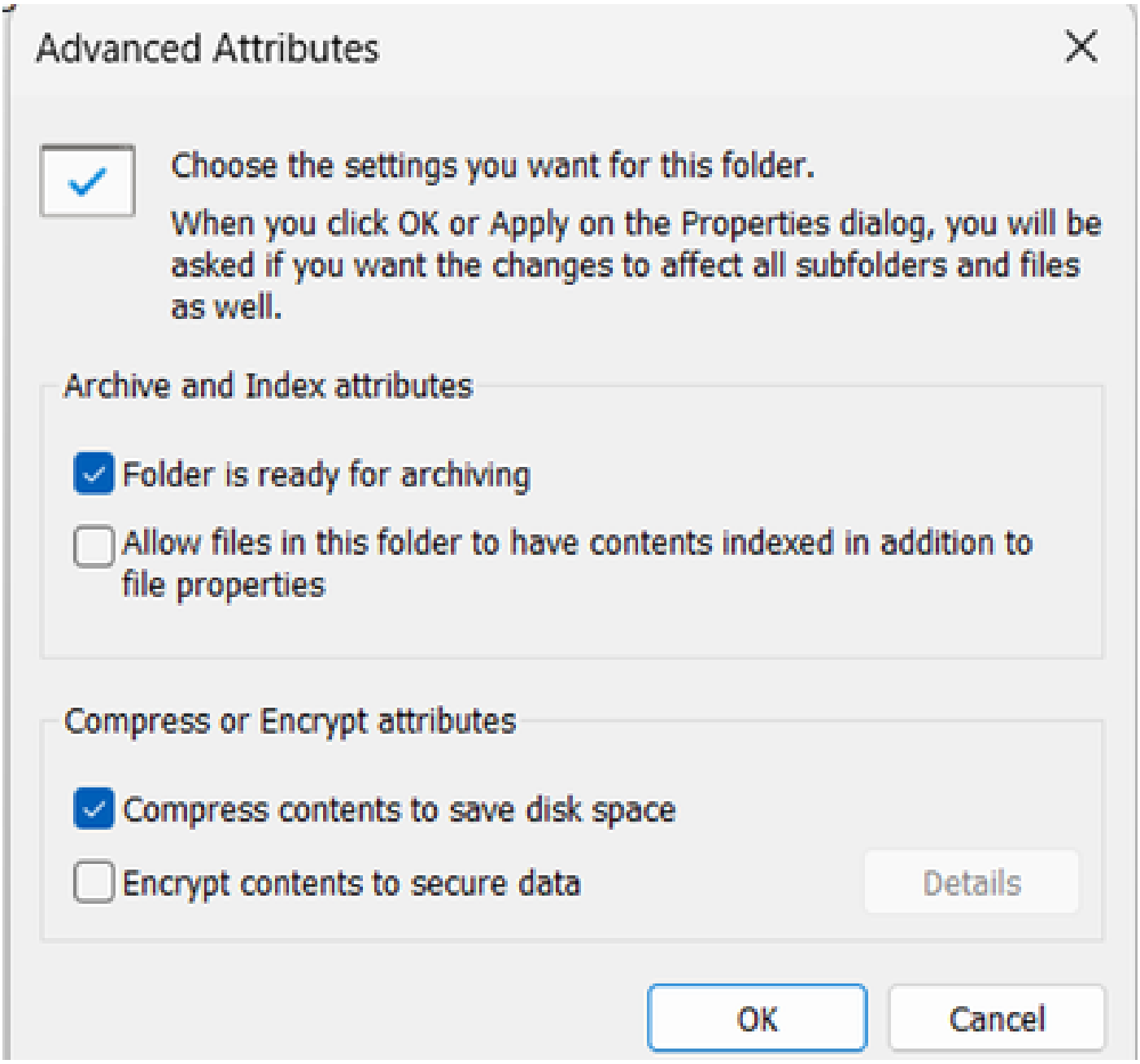
Embora, você também possa usar a solução alternativa para compactar o tamanho da pasta:

1- Navegue até as propriedades da pasta Dumps e verifique o tamanho original da pasta no disco como mostrado:

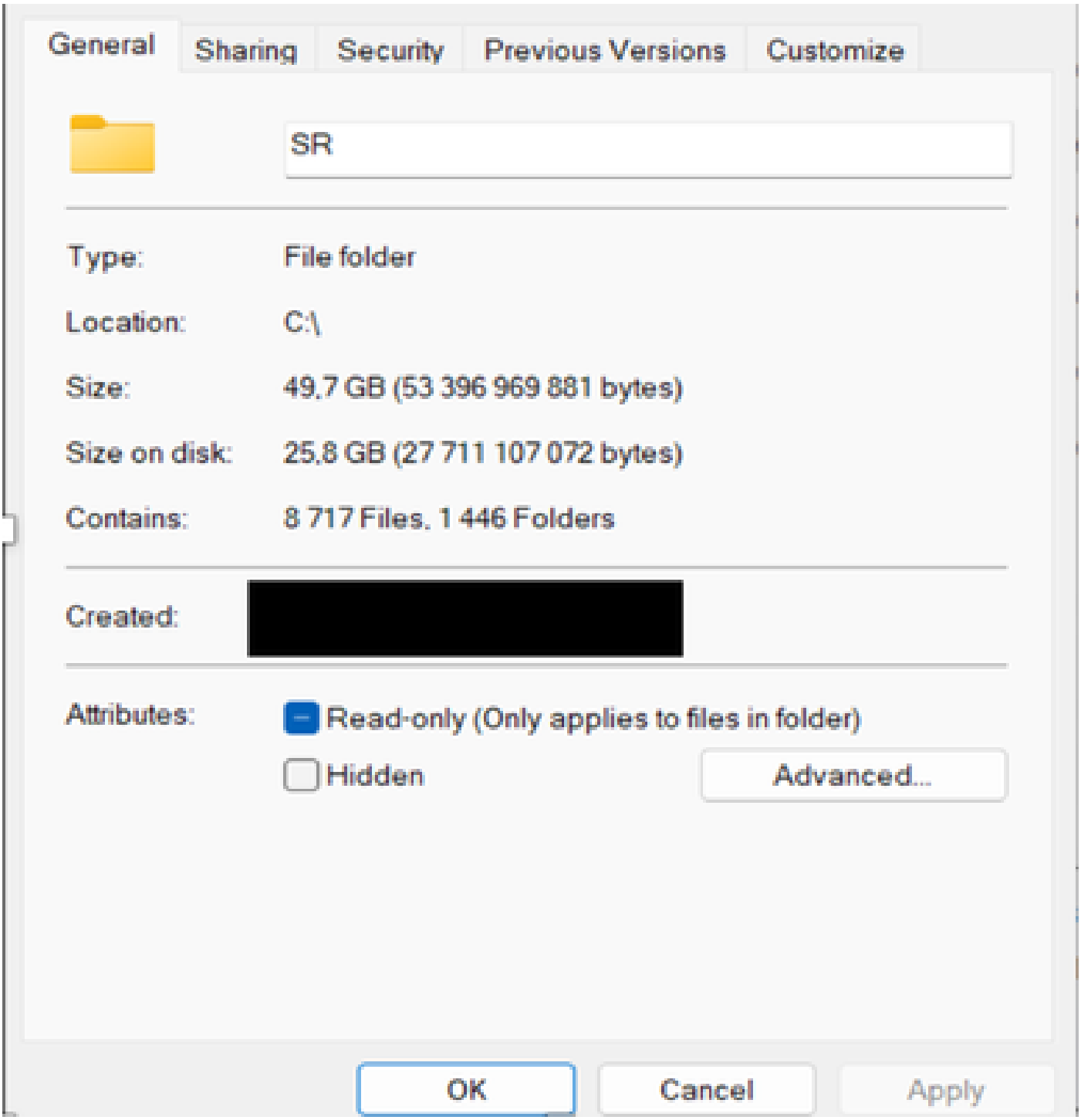

procdump64
17/03/2025 07:13
Application
Dumps
17/03/2025 07:14
File folder
View
Sort by
Group by
Refresh
Paste
Paste shortcut
Undo Rename
Ctrl+Z
Give access to
New
Properties



2- Navegue para a opção Advanced e habilite compressão e aplique que que leva vários minutos:



3- No final, você pode ver que o tamanho da pasta se reduz a quase metade do tamanho original, como mostrado:



4- Você também pode usar esse comando no prompt de comando para obter o mesmo:

compact /c /s:c:\instalar

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.