

Verzamel proces crashdumps op Windows voor SFC-proces

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

Inleiding

Dit document beschrijft hoe te om Proces crashdumps op Windows te verzamelen voor SFC-proces.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Endpoint-connector
- Opdrachtprompt Windows

Gebruikte componenten

Dit document is niet beperkt tot software- en hardwareversies. De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

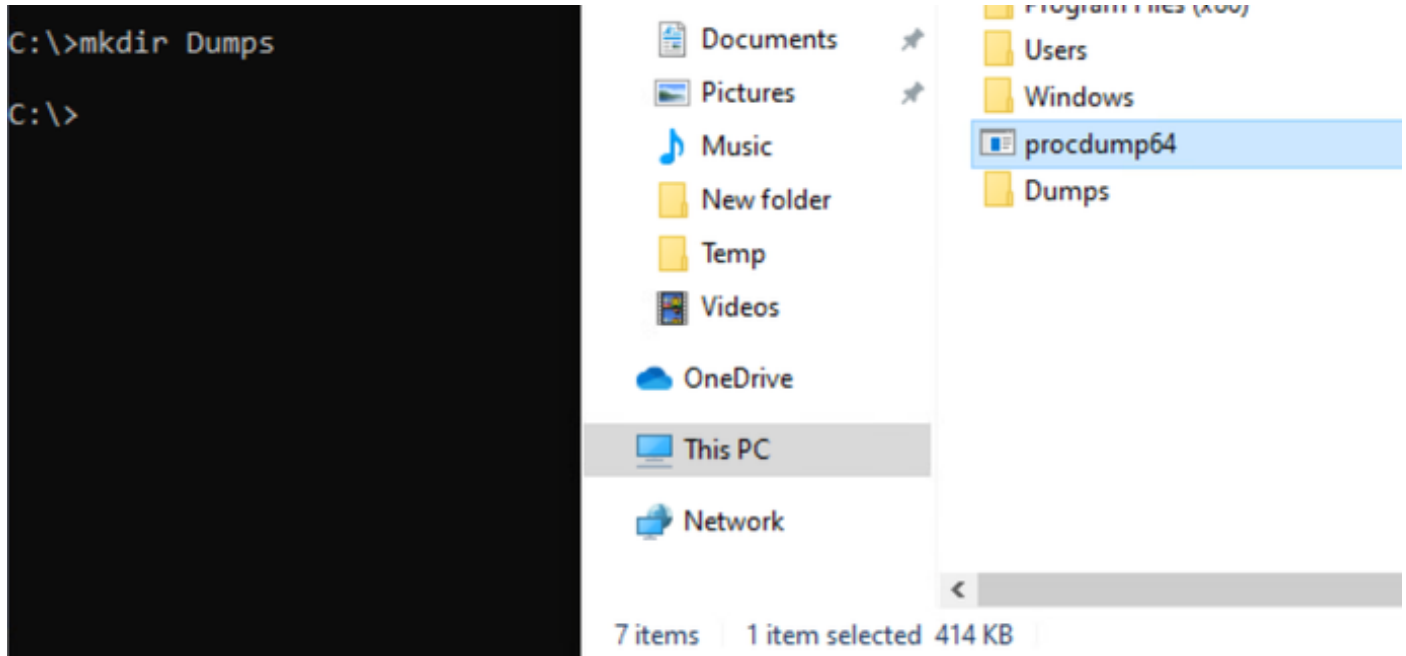
Probleem

- Cisco Secure-endpointtoepassing kan naar een uitgeschakeld of niet-verbonden status gaan als gevolg van een procescrash van sfc.exe, die gerelateerd kan zijn aan een onverwachte blokkering van vensters of enige andere activiteit op vensters.
- Windows activeert een debugging tool geconfigureerd in de AeDebug registerwaarden. Elk programma kan vooraf worden geselecteerd als het te gebruiken gereedschap in deze situatie. Het gekozen programma wordt de postmortem debugger genoemd.

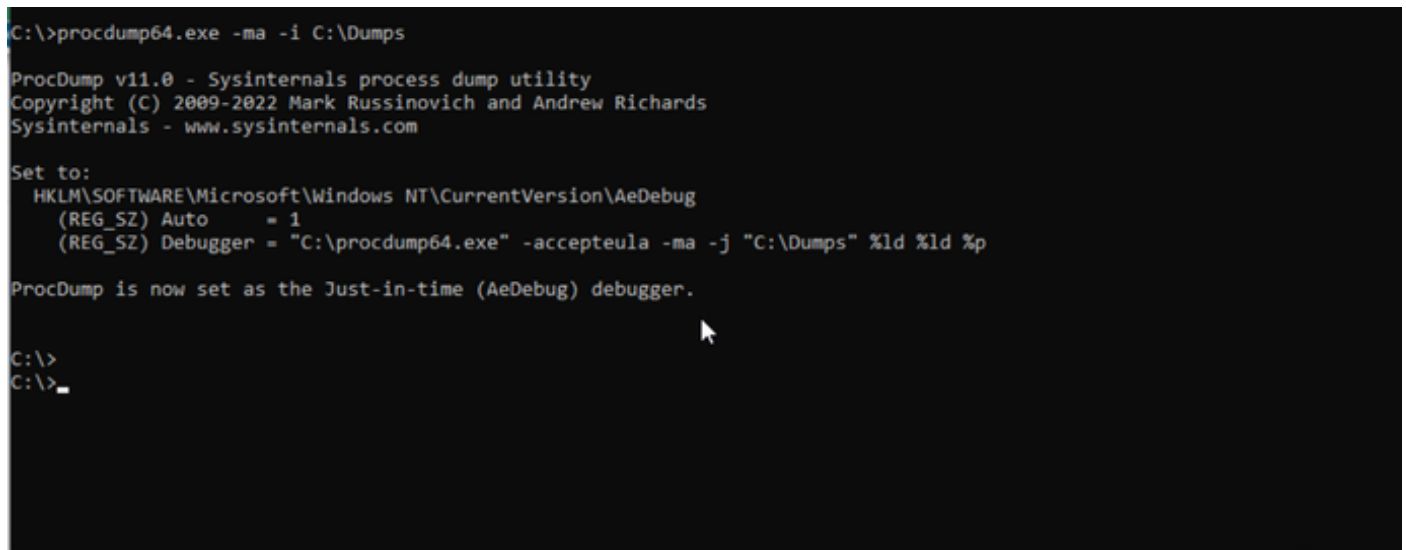
Oplossing

Download [Procdump als de \(AeDebug\) postmortem debugger](#) van sysinternals suite.

Extraheer Procdump in c-station en maak Dumps map voor crashdump collectie zoals getoond:



Procdump instellen als AeDebugger:



Hoe te gebruiken:

- Start CMD als beheerder.
- Verander naar de map waarin u procdump tool uitpakt.
- Opdrachtvoorbeeld: procdump64.exe -ma <PID | Procesnaam> of procdump64.exe -ma -i

C:\Dumps

Voorbeeld van sfc.exe:

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

Het slaat de crashdumps op in de map Dumps zoals getoond. Verzamel en deel het voor analyse:

 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

Zo verwijdert u het gebruik van de projector: procdump64.exe -u

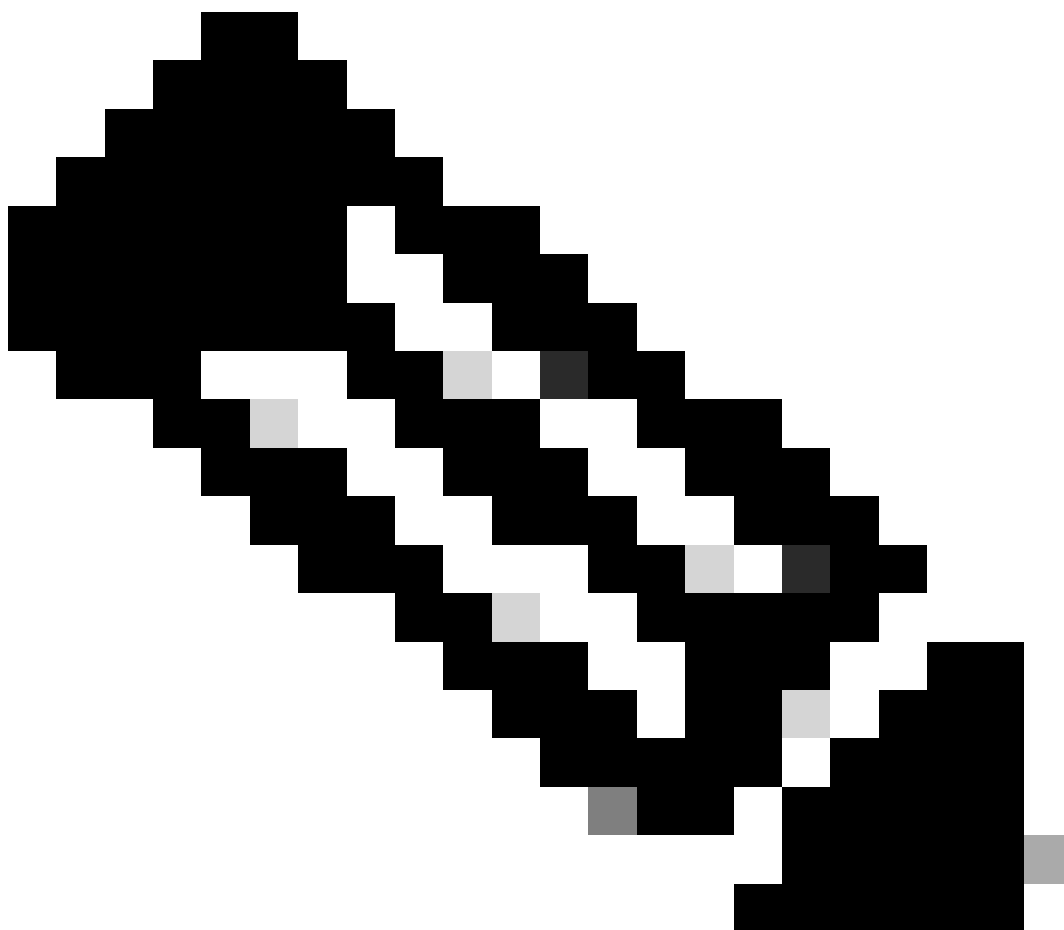
```
C:\>
C:\>procdump64.exe -u

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.

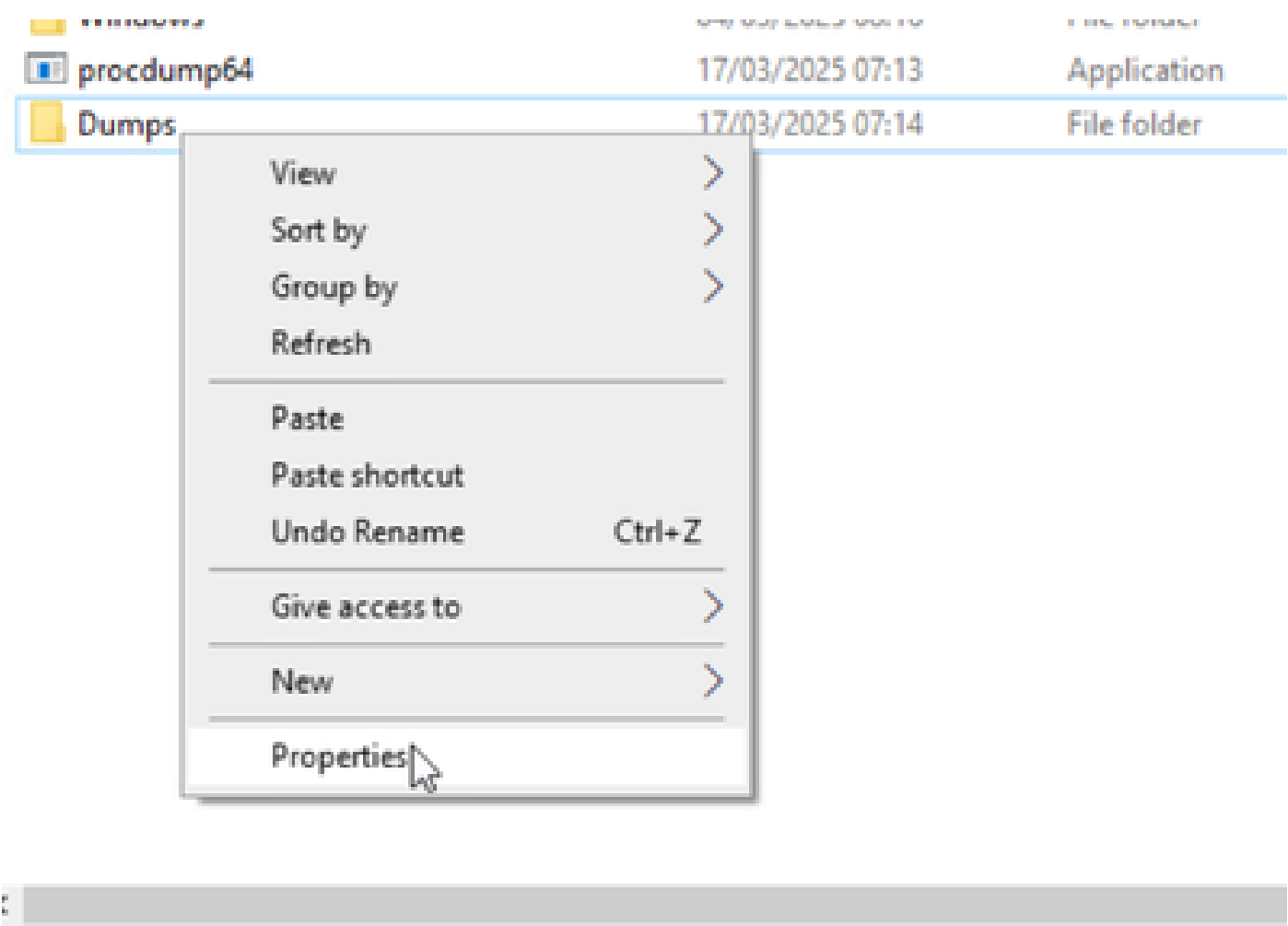
C:\>
```

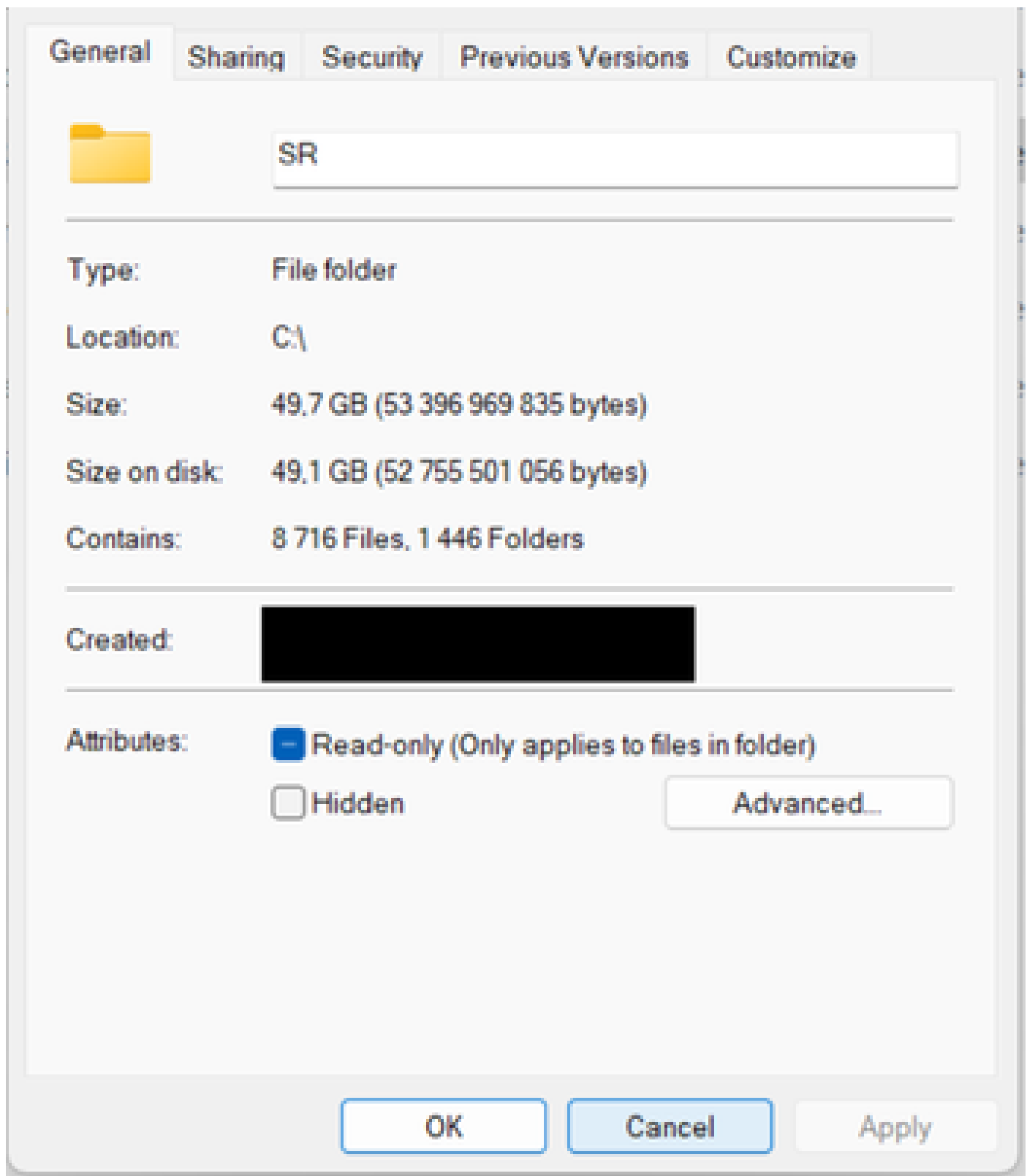


Opmerking: Crash Dumps kan grote ruimte op de schijf verbruiken en procdump kan worden gestopt zodra de collectie is gedaan.

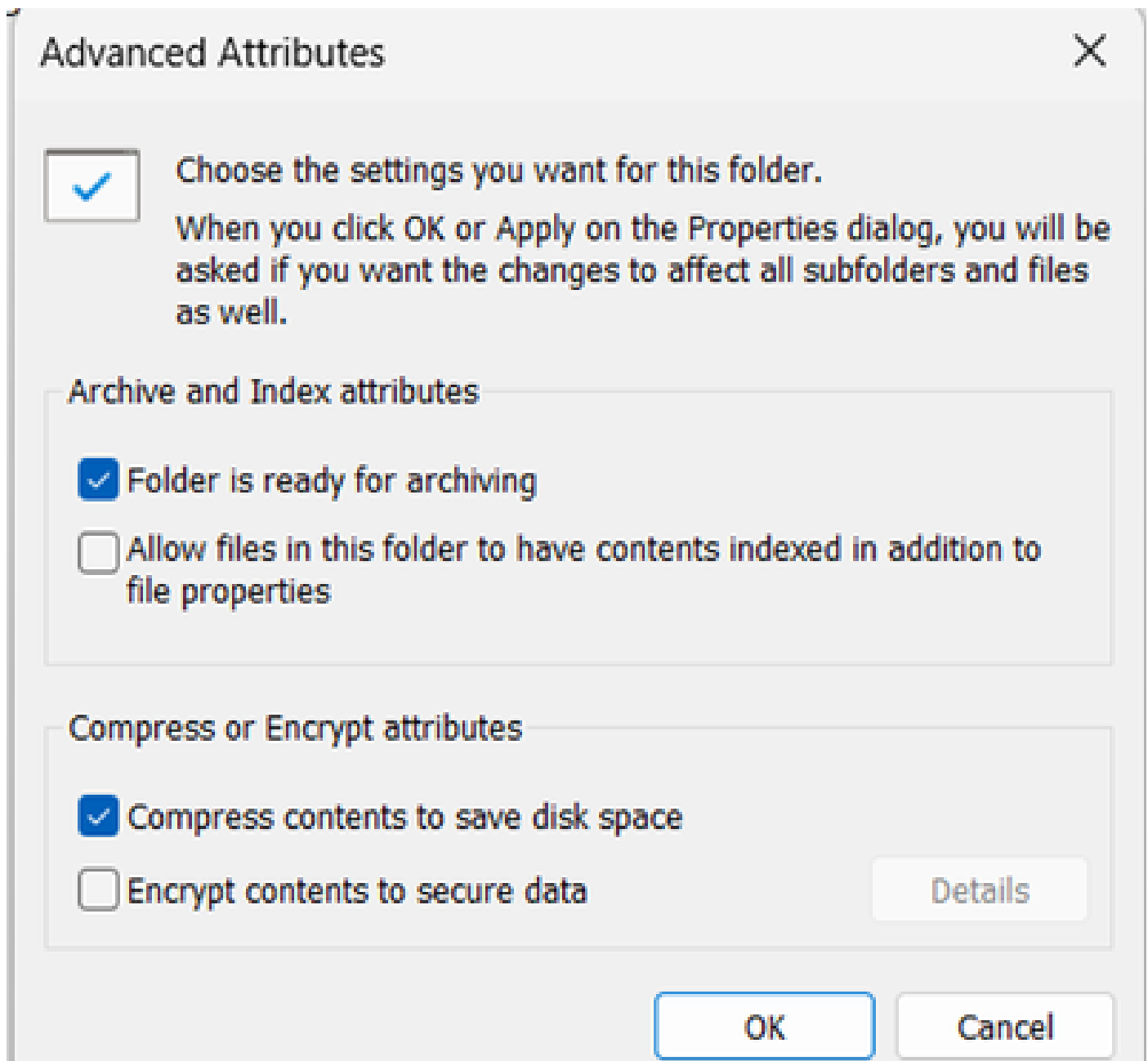
U kunt echter ook de tijdelijke oplossing gebruiken om de grootte van de map te comprimeren:

1- Navigeer naar eigenschappen van de map Dumps en controleer de oorspronkelijke grootte van de map op de schijf zoals aangegeven :

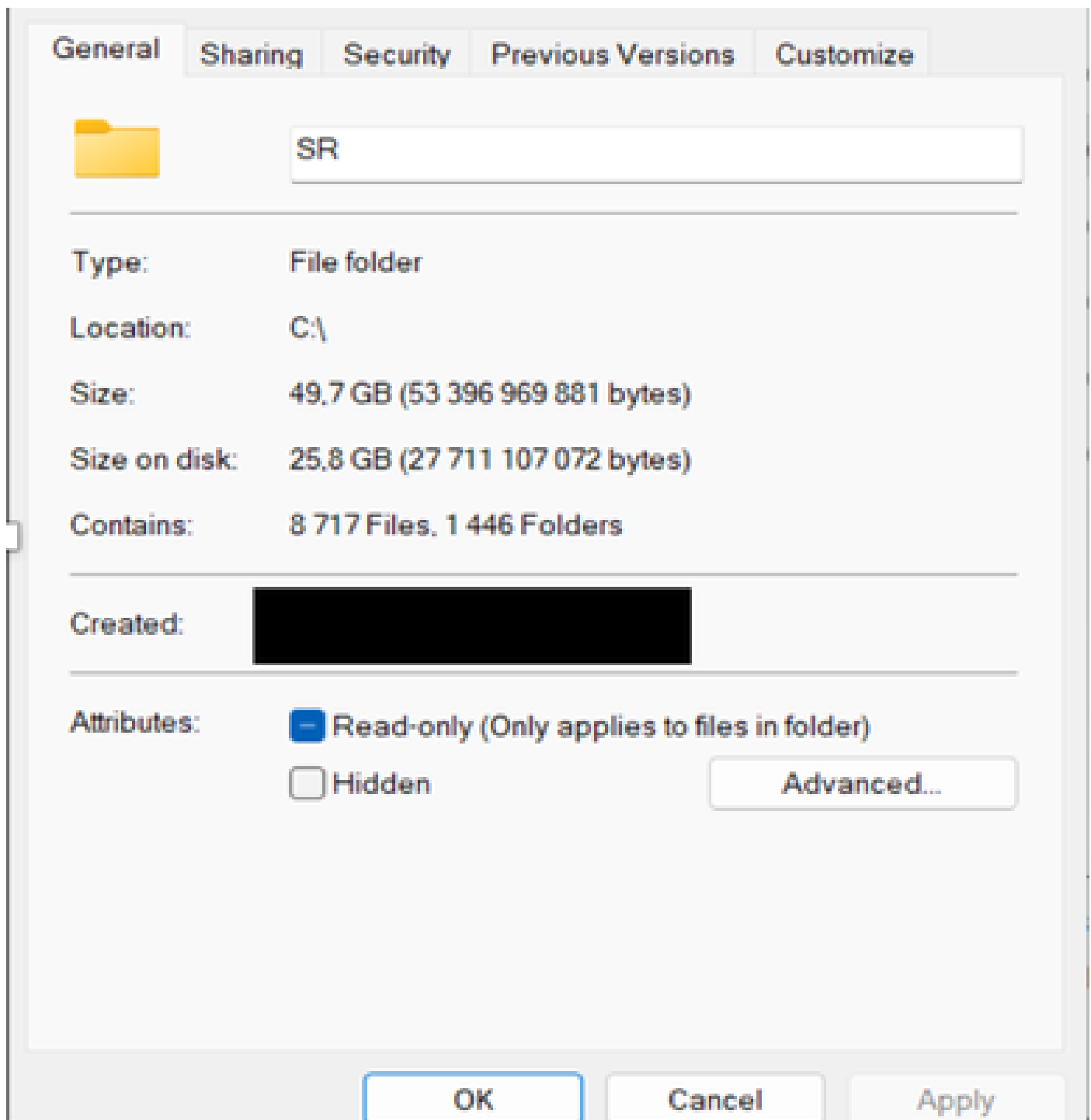




2- Navigeren naar geavanceerde optie en compressie inschakelen en toepassen wat een aantal minuten duurt:



3- Uiteindelijk kunt u zien dat het mapformaat wordt verkleind tot bijna de helft van het oorspronkelijke formaat, zoals wordt aangegeven in de afbeelding:



4- U kunt deze opdracht ook gebruiken in de opdrachtprompt om hetzelfde te bereiken:

```
compact /c /s:c:\install
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.