# Sfc 프로세스용 Windows에서 프로세스 크래시 덤프 수집

## 목차



## 소개

이 문서에서는 sfc 프로세스를 위해 Windows에서 프로세스 크래쉬덤프를 수집하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Endpoint 커넥터
- 명령 프롬프트 창

### 사용된 구성 요소

이 문서는 소프트웨어 및 하드웨어 버전으로 제한되지 않습니다. 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

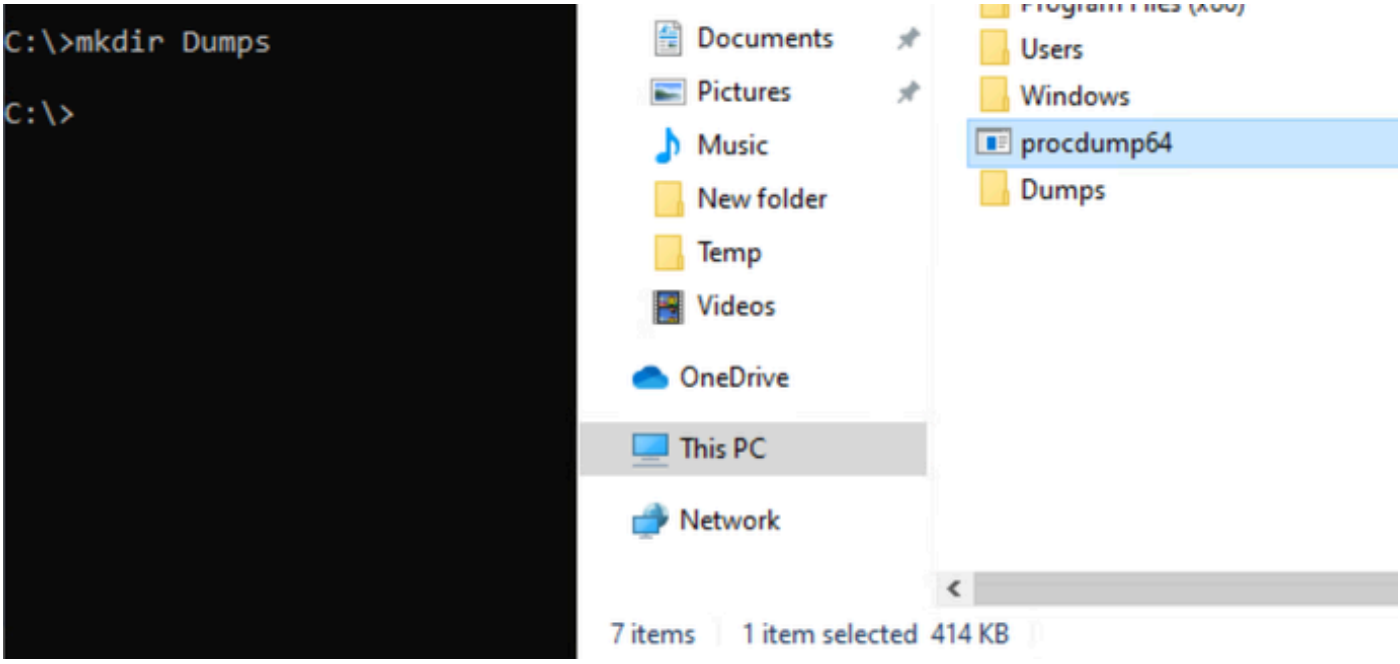
## 문제

- Cisco Secure Endpoint 애플리케이션은 sfc.exe의 프로세스 충돌로 인해 비활성화 또는 연결 끊김 상태로 전환될 수 있으며, 이는 예기치 않은 Windows 종료 또는 Windows에서의 기타 활동과 관련될 수 있습니다.
- Windows에서는 AeDebug 레지스트리 값에 구성된 디버깅 도구를 활성화합니다. 어떤 프로그램도 이러한 상황에서 사용할 도구로 미리 선택할 수 있다. 선택한 프로그램을 사후 디버거라고 합니다.

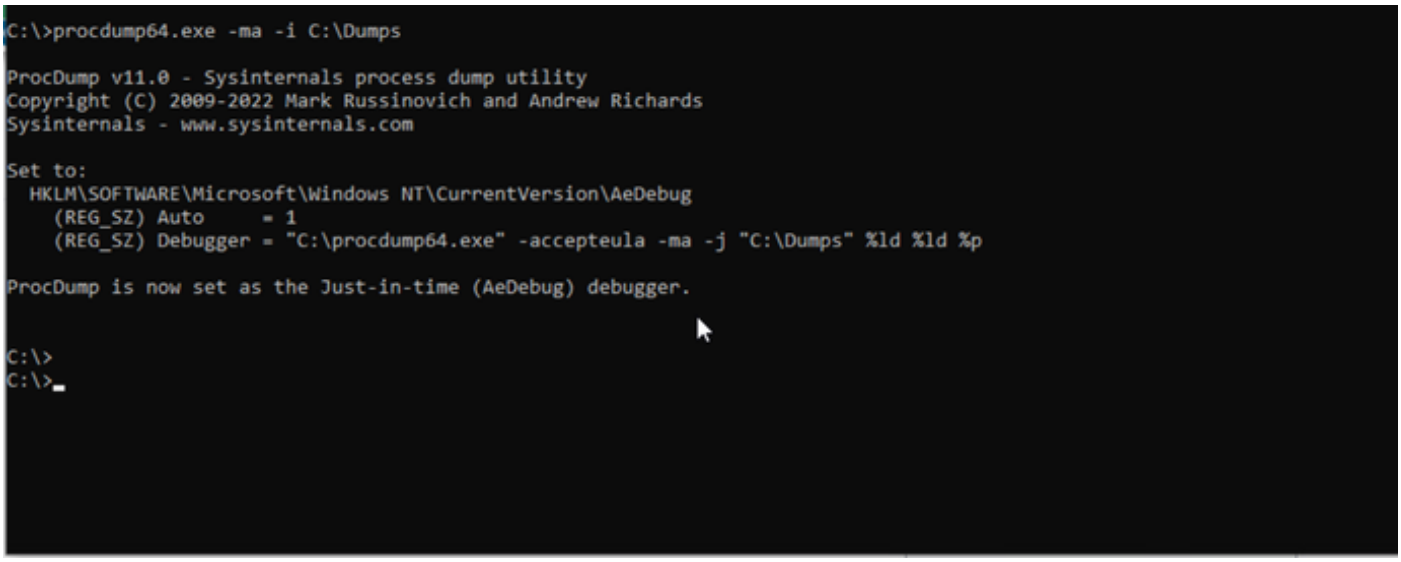
# 솔루션

sysinternals suite에서 (AeDebug) 사후 디버거로 Procdump를 다운로드합니다.

c 드라이브에서 Procdump를 추출하고 다음과 같이 crashdump 컬렉션을 위한 Dumps 폴더를 생성합니다.




Procdump를 AeDebugger로 설정:




사용 방법:

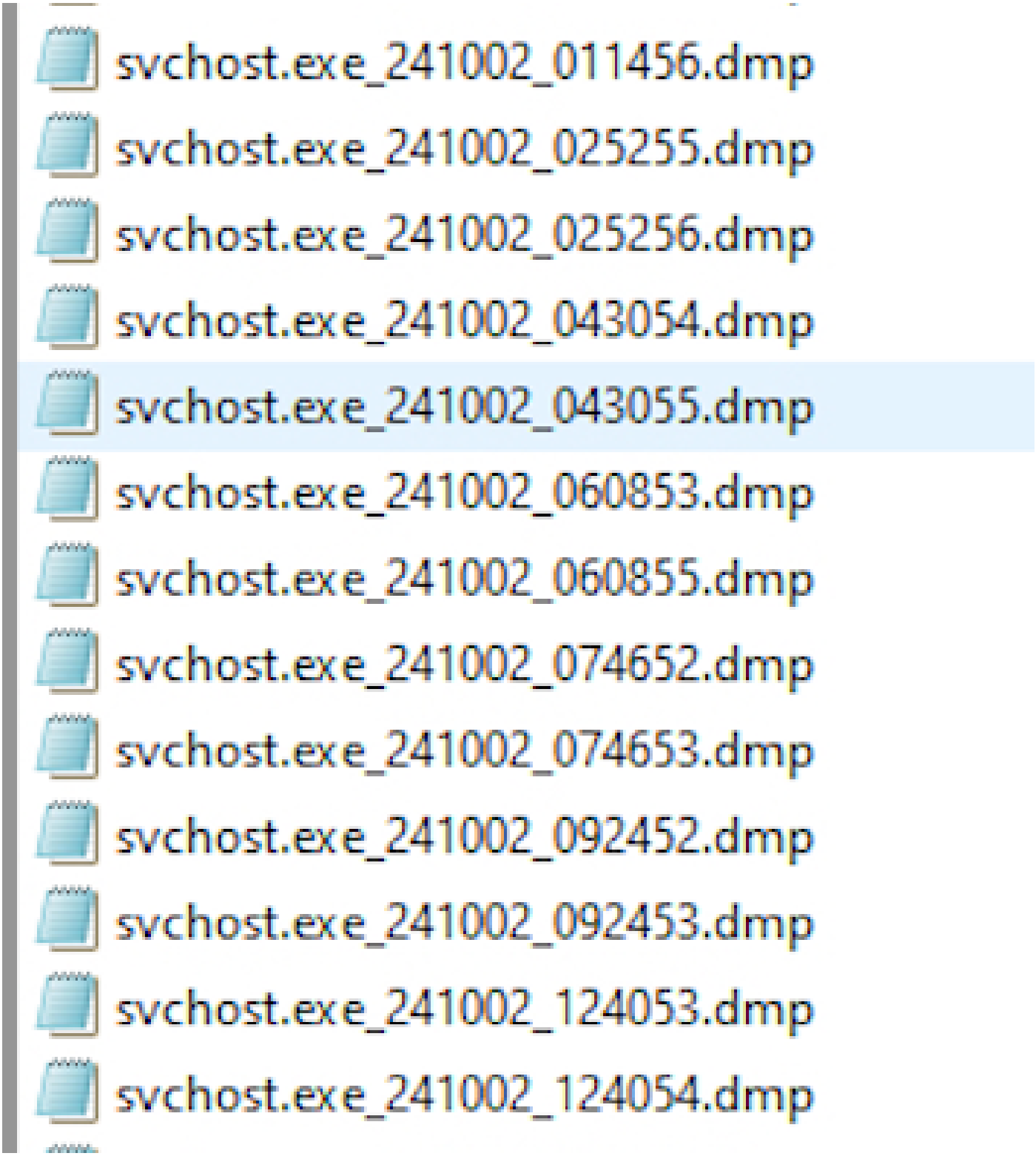
- 관리자로 CMD를 시작합니다.
- Procdump 툴의 압축을 푼 디렉토리로 변경합니다.

- 명령 예: procdump64.exe -ma <PID | 프로세스 이름> 또는 procdump64.exe -ma -i C:\Dumps

sfc.exe 예:

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

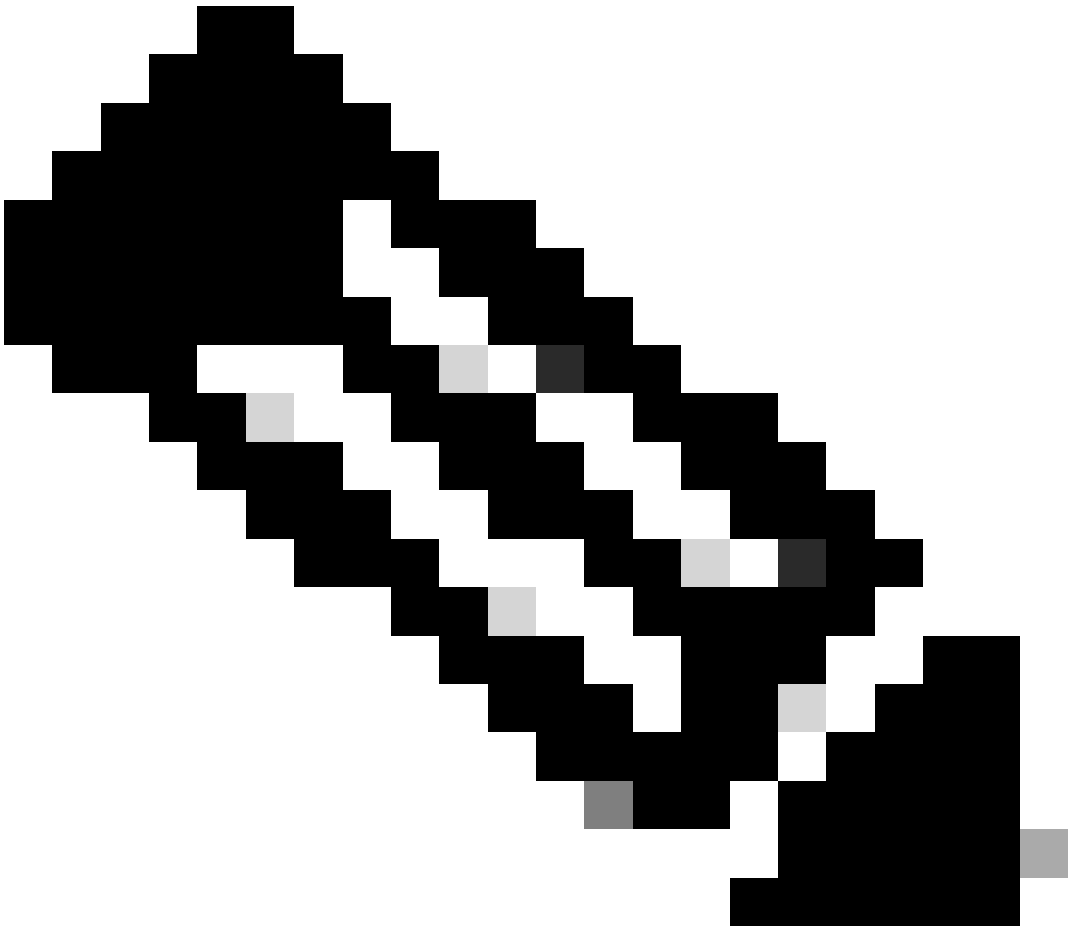
그림과 같이 크래시 덤프를 Dumps 폴더에 저장합니다. 분석을 위해 수집 및 공유:



procdump 사용을 제거하려면 다음을 수행합니다. 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:\>
```

---

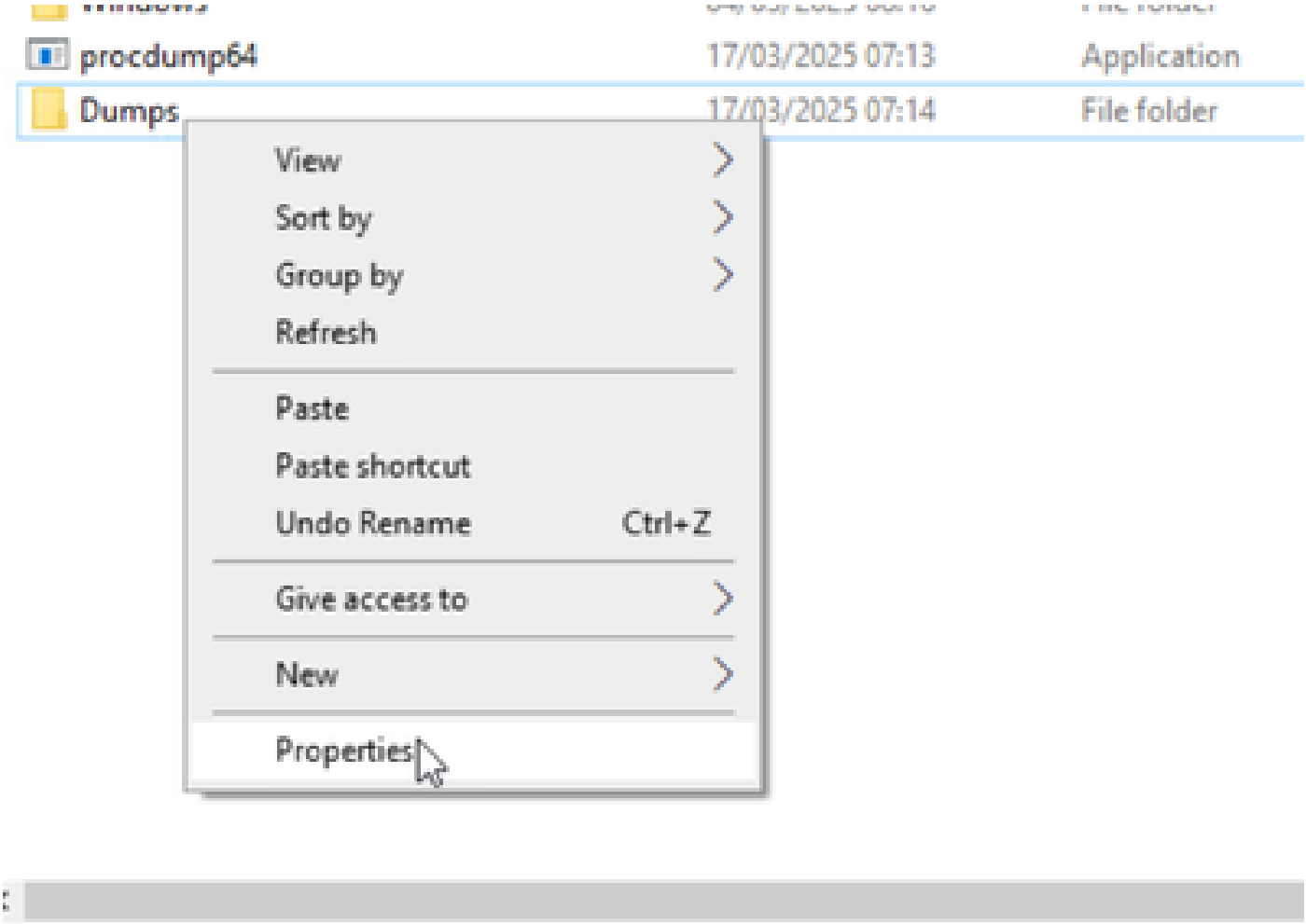


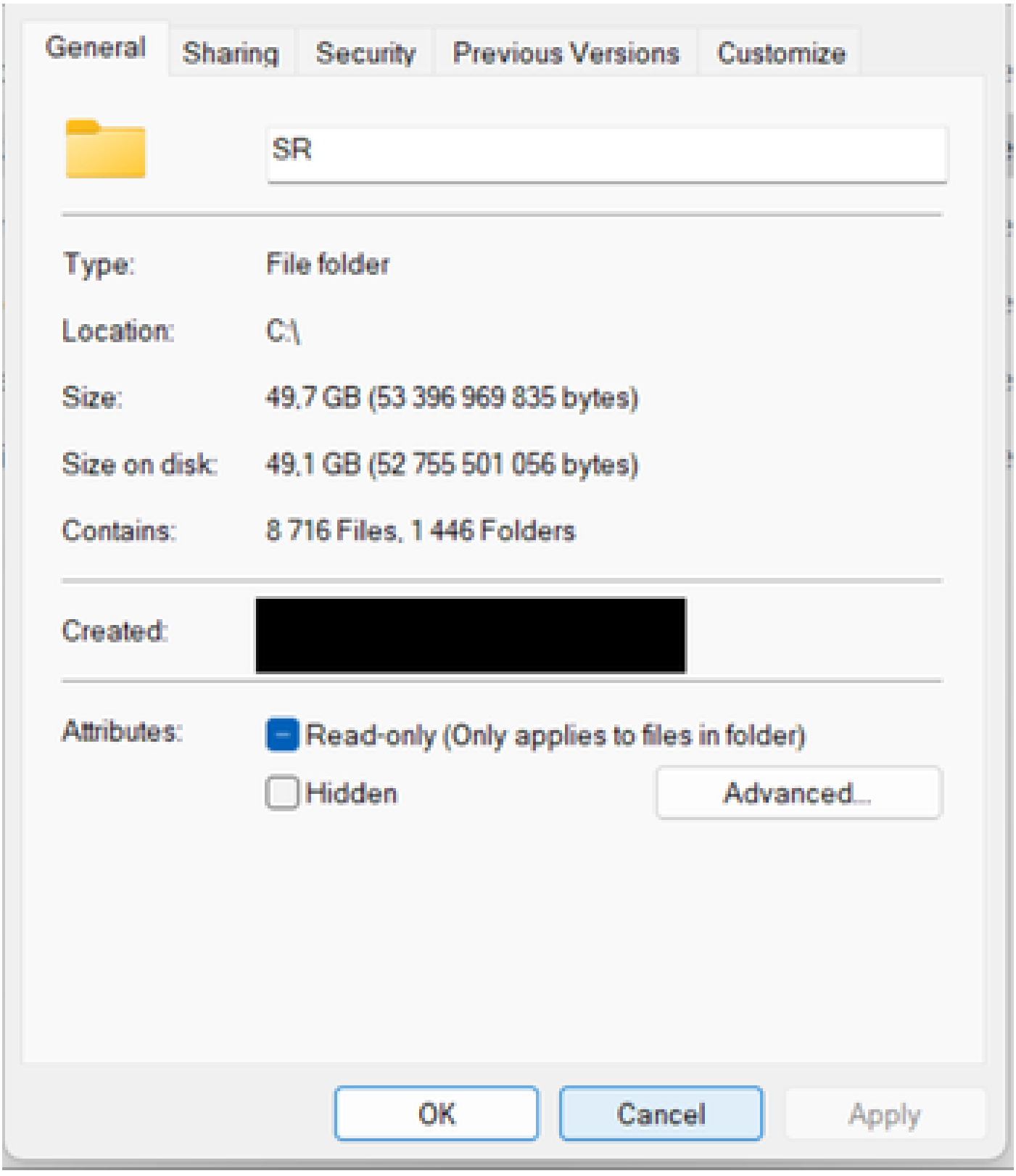
> 참고: 크래시 덤프는 디스크의 큰 공간을 소비할 수 있으며 수집이 완료되면 procdump를 중지할 수 있습니다.

---

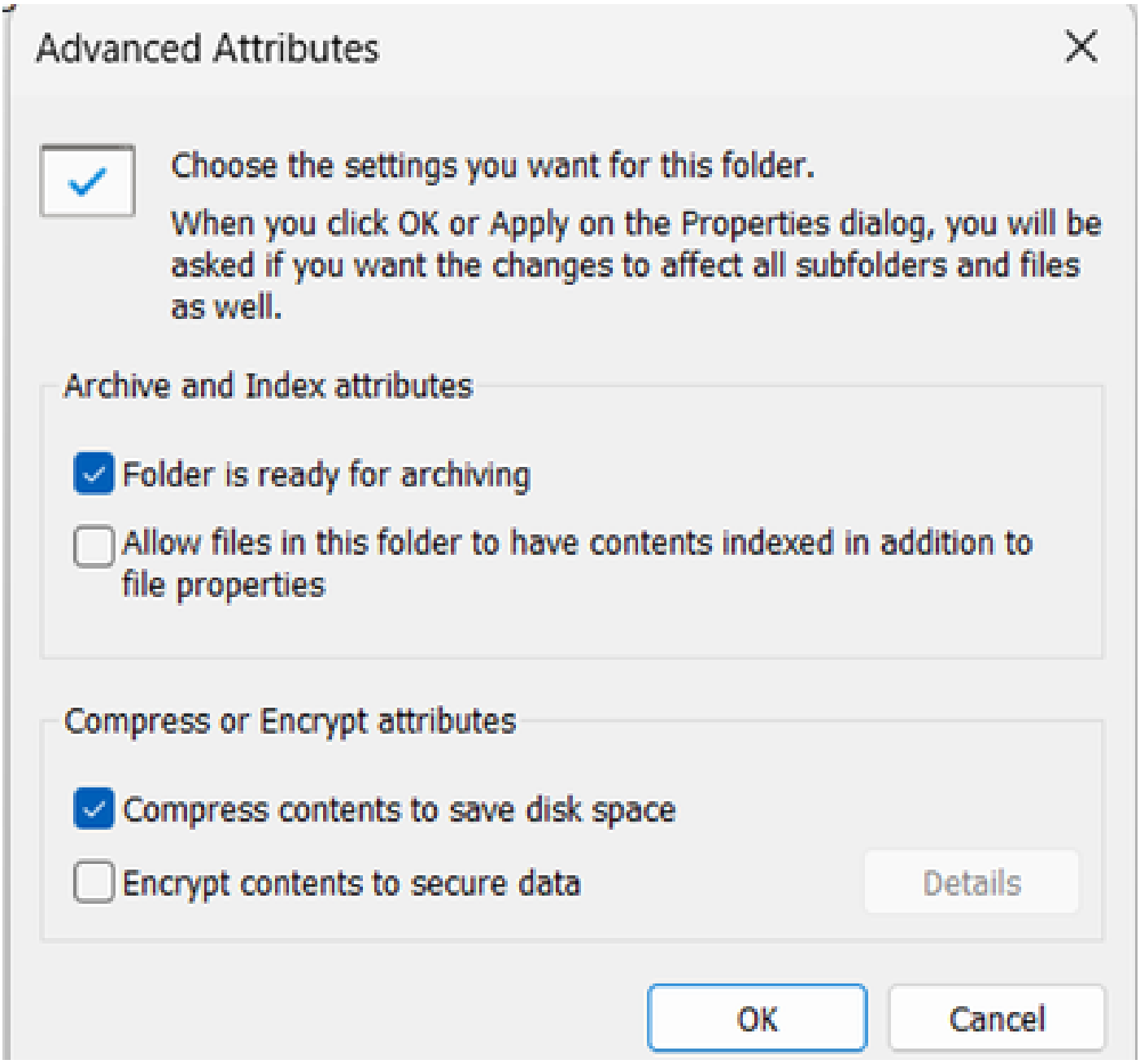
그러나 이 해결 방법을 사용하여 폴더 크기를 압축할 수도 있습니다.

1- Dumps 폴더의 속성으로 이동하여 표시된 대로 디스크에 있는 폴더의 원래 크기를 확인합니다.

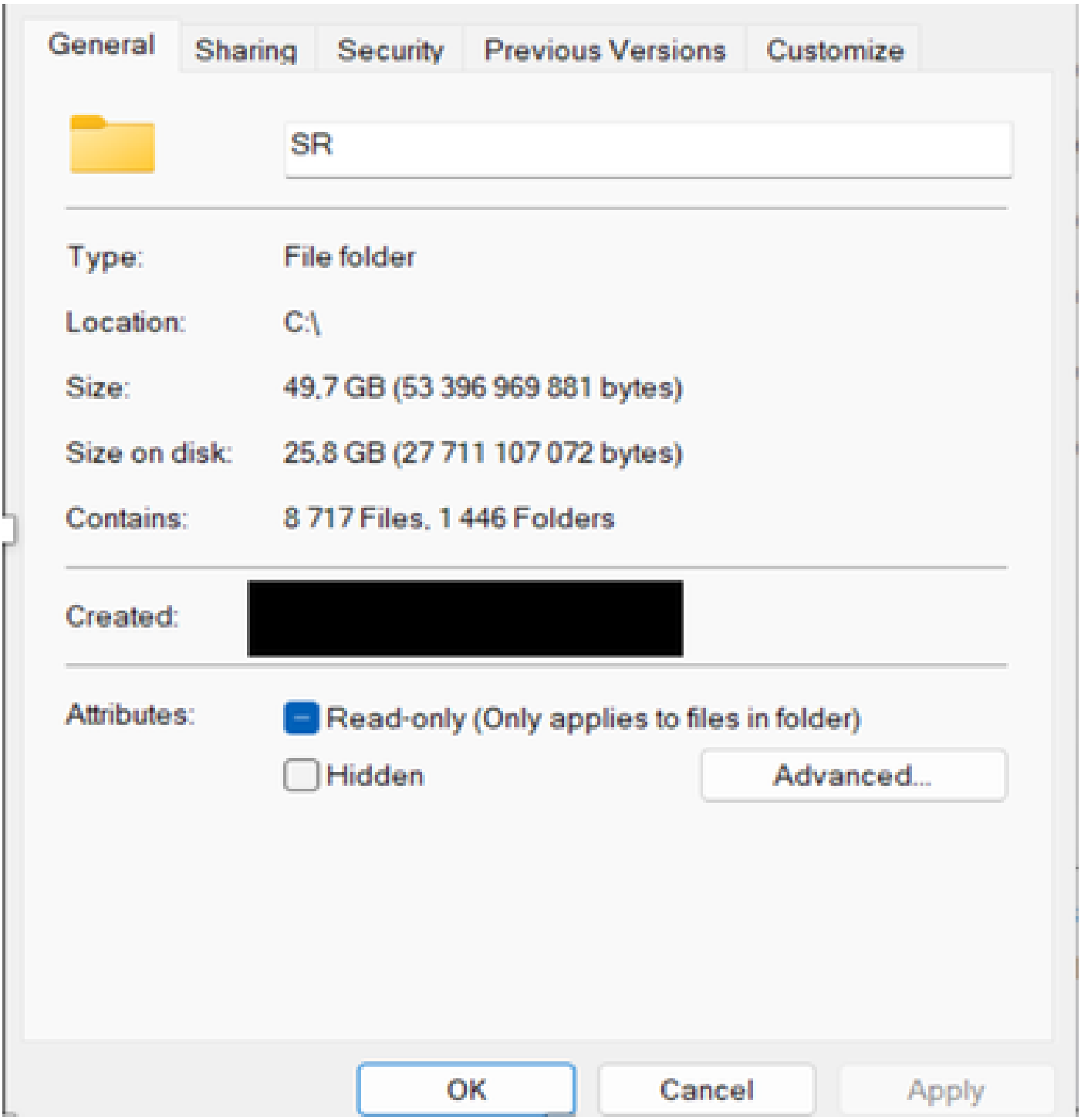





2- Advanced(고급) 옵션으로 이동하여 압축을 활성화하고 몇 분 정도 걸리는 적용:




3- 폴더 크기가 다음과 같이 원래 크기의 거의 절반으로 줄어든 것을 확인할 수 있습니다.




4- 명령 프롬프트에서 이 명령을 사용하여 동일한 작업을 수행할 수도 있습니다.

압축 /c /s:c:\install

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.