Process Monitor v3.93

Article • 03/09/2023 • 2 minutes to read

By Mark Russinovich

Published: March 9, 2023

 **Download Process Monitor** (3.3 MB)

Download Procmon for Linux (GitHub)

Run now from Sysinternals Live.

Introduction

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Overview of Process Monitor Capabilities

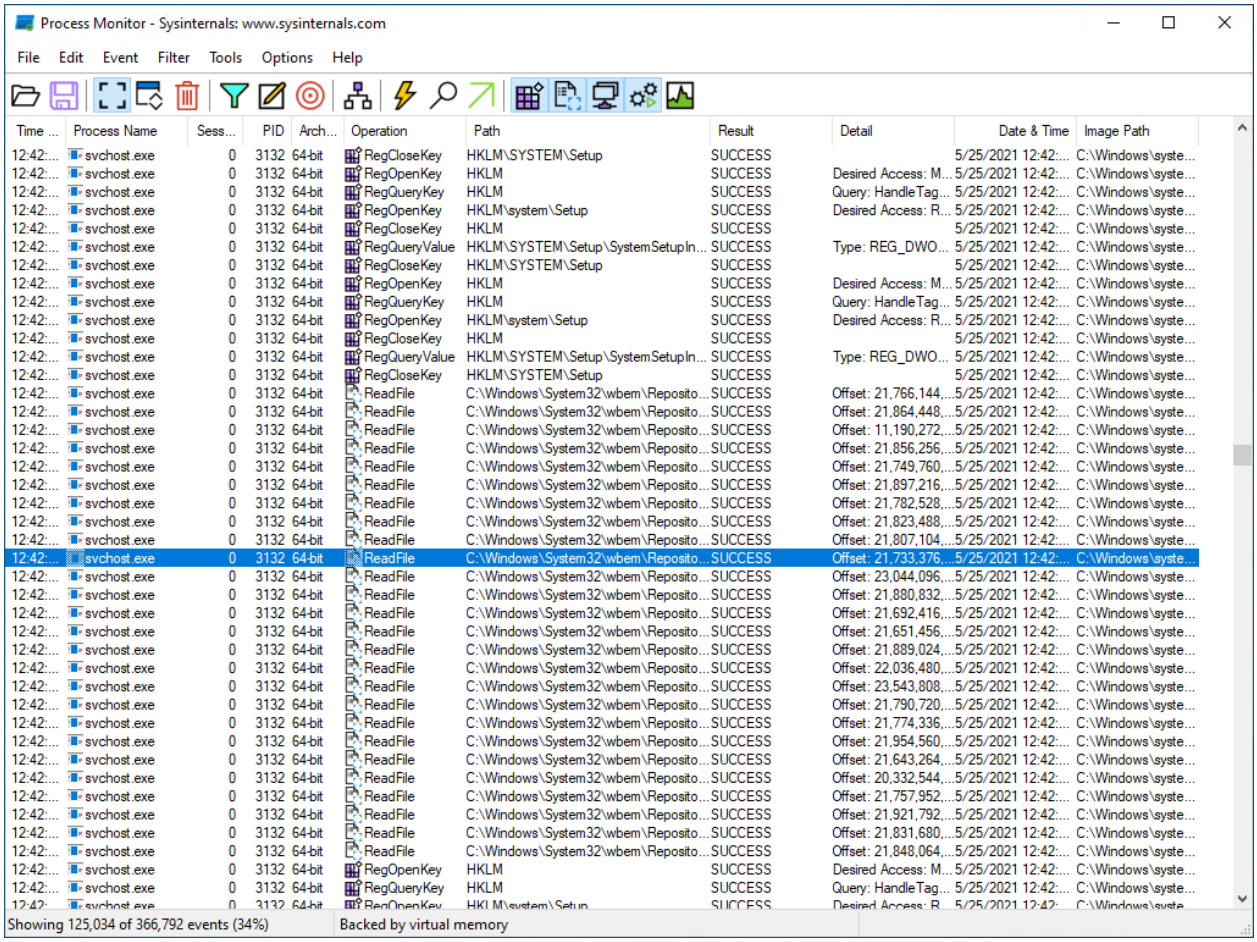
Process Monitor includes powerful monitoring and filtering capabilities, including:

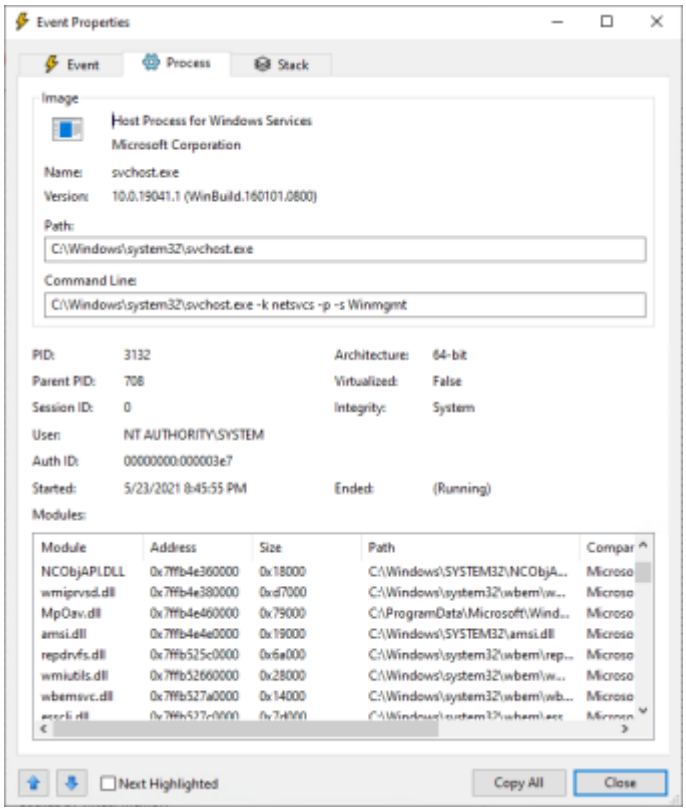
- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
- Process tree tool shows relationship of all processes referenced in a trace

- Native log format preserves all data for loading in a different Process Monitor instance
- Process tooltip for easy viewing of process image information
- Detail tooltip allows convenient access to formatted data that doesn't fit in the column
- Cancellable search
- Boot time logging of all operations

The best way to become familiar with Process Monitor's features is to read through the help file and then visit each of its menu items and options on a live system.

Screenshots





Related Links

- Windows Internals Book
  The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- Windows Sysinternals Administrator's Reference
  The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

Download Process Monitor (3.3 MB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows 8.1 and higher.
- Server: Windows Server 2012 and higher.