



Process Hacker

[Features](#)

A very incomplete feature list for Process Hacker 2:

Processes

- View processes in a tree view with highlighting
- View detailed process statistics and performance graphs
- Process tooltips are detailed and show context-specific information
- Select multiple processes and terminate, suspend or resume them
- (32-bit only) Bypass almost all forms of process protection
- Restart processes
- Empty the working set of processes
- Set affinity, priority and virtualization
- Create process dumps
- Use over a dozen methods to terminate processes
- Detach processes from debuggers
- View process heaps
- View GDI handles
- Inject DLLs
- View DEP status, and even enable/disable DEP
- View environment variables
- View and edit process security descriptors
- View image properties such as imports and exports

Threads

- View thread start addresses and stacks with symbols
- Threads are highlighted if suspended, or are GUI threads
- Select multiple threads and terminate, suspend or resume them
- Force terminate threads
- View TEB addresses and view TEB contents
- (32-bit only) Find out what a thread is doing, and what objects it is waiting on
- View and edit thread security descriptors

Tokens

- View full token details, including user, owner, primary group, session ID, elevation status, and more
- View token groups
- View privileges and even enable, disable or remove them
- View and edit token security descriptors

Modules

- View modules and mapped files in one list
- Unload DLLs
- View file properties and open them in Windows Explorer

Memory

- View a virtual memory list
- Read and modify memory using a hex editor
- Dump memory to a file
- Free or decommit memory
- Scan for strings

Handles

- View process handles, complete with highlighting for attributes

- Search for handles (and DLLs and mapped files)
- Close handles
- (32-bit only) Set handle attributes - Protected and Inherit
- Granted access of handles can be viewed symbolically instead of plain hex numbers
- View detailed object properties when supported
- View and edit object security descriptors

Services

- View a list of all services
- Create services
- Start, stop, pause, continue or delete services
- Edit service properties
- View service dependencies and dependents
- View and edit service security descriptors

Network

- View a list of network connections
- Close network connections
- Use tools such as whois, traceroute and ping