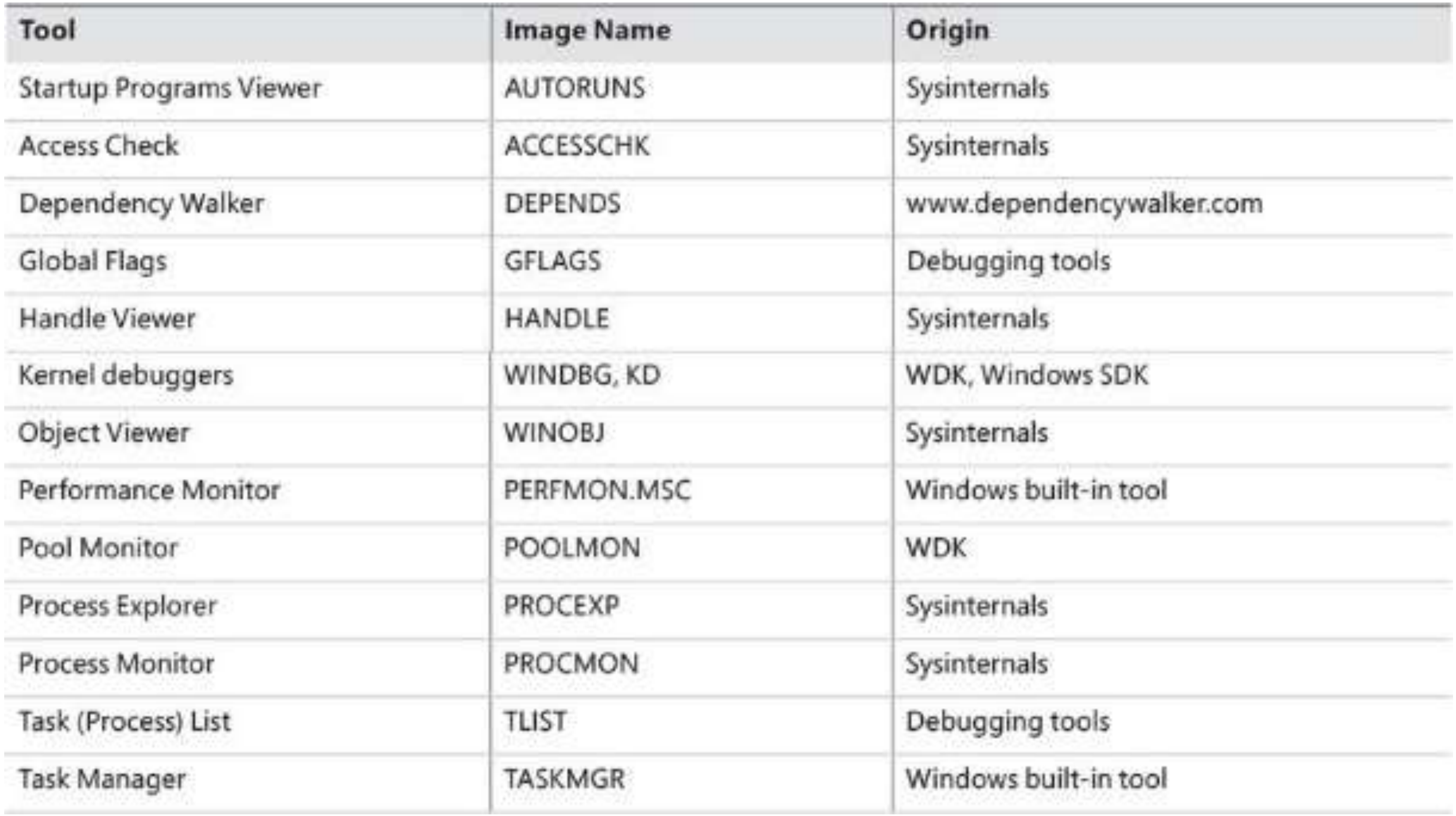
A list of the principal tools



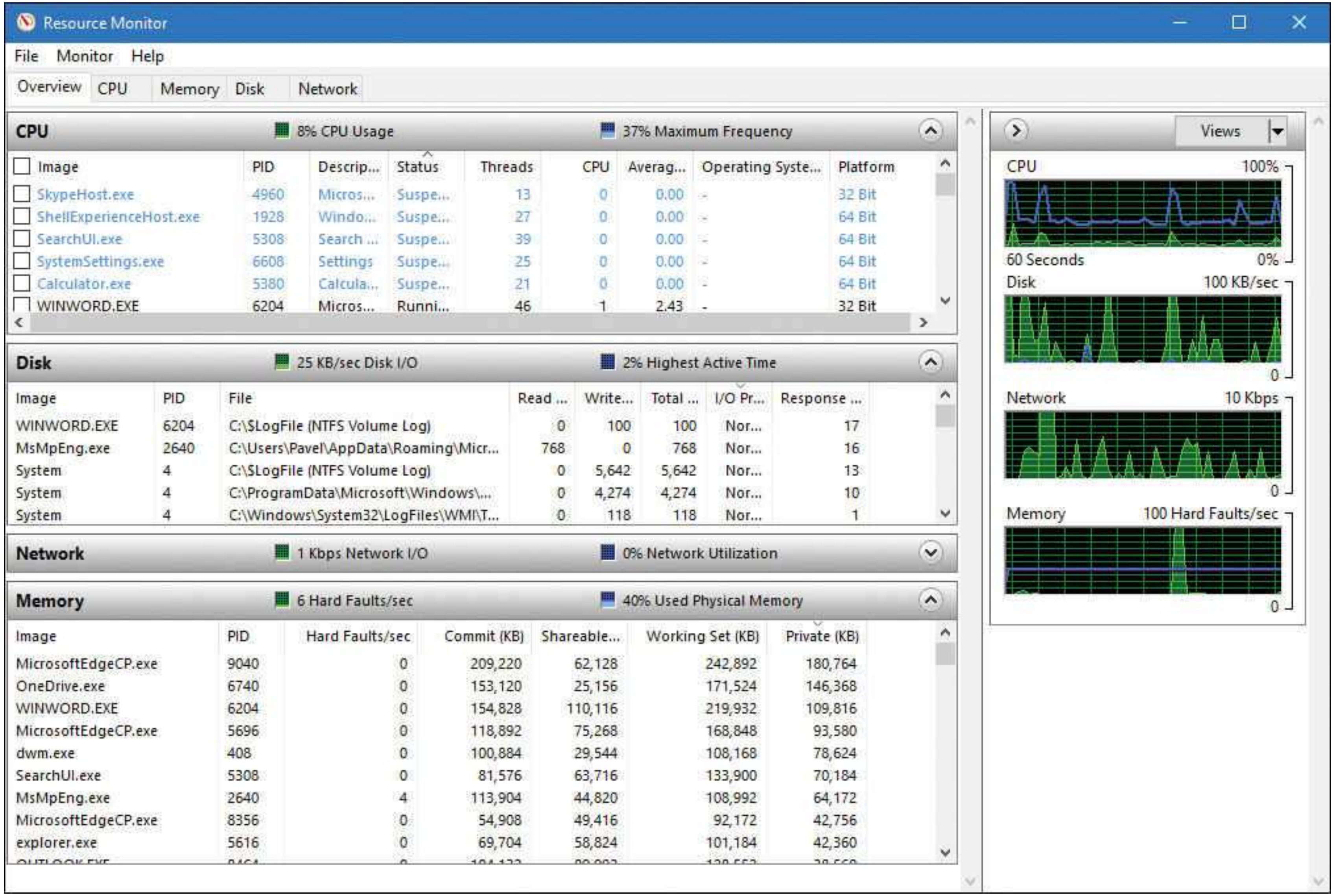
Tool	Image Name	Origin
Startup Programs Viewer	AUTORUNS	Sysinternals
Access Check	ACCESSCHK	Sysinternals
Dependency Walker	DEPENDS	www.dependencywalker.com
Global Flags	GFLAGS	Debugging tools
Handle Viewer	HANDLE	Sysinternals
Kernel debuggers	WINDBG, KD	WDK, Windows SDK
Object Viewer	WINOBJ	Sysinternals
Performance Monitor	PERFMON.MSC	Windows built-in tool
Pool Monitor	POOLMON	WDK
Process Explorer	PROCEXP	Sysinternals
Process Monitor	PROCMON	Sysinternals
Task (Process) List	TLIST	Debugging tools
Task Manager	TASKMGR	Windows built-in tool

Performance Monitor and Resource Monitor

- Provides more information about how your system is operating than any other single utility

- Low-level system monitoring

Performance Monitor and Resource Monitor



CPU 🟩 8% CPU Usage 🟦 37% Maximum Frequency

	Image	PID	Descrip...	Status	Threads	CPU	Averag...	Operating Syste...	Platform
□	SkypeHost.exe	4960	Micros...	Suspe...	13	0	0.00	-	32 Bit
□	ShellExperienceHost.exe	1928	Windo...	Suspe...	27	0	0.00	-	64 Bit
□	SearchUI.exe	5308	Search ...	Suspe...	39	0	0.00	-	64 Bit
□	SystemSettings.exe	6608	Settings	Suspe...	25	0	0.00	-	64 Bit
□	Calculator.exe	5380	Calcula...	Suspe...	21	0	0.00	-	64 Bit
□	WINWORD.EXE	6204	Micros...	Runni...	46	1	2.43	-	32 Bit

Disk 🟩 25 KB/sec Disk I/O 🟦 2% Highest Active Time

Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Response ...
WINWORD.EXE	6204	C:\$LogFile (NTFS Volume Log)	0	100	100	Nor...	17
MsMpEng.exe	2640	C:\Users\Pavel\AppData\Roaming\Micr...	768	0	768	Nor...	16
System	4	C:\$LogFile (NTFS Volume Log)	0	5,642	5,642	Nor...	13
System	4	C:\ProgramData\Microsoft\Windows\...	0	4,274	4,274	Nor...	10
System	4	C:\Windows\System32\LogFiles\WMI\T...	0	118	118	Nor...	1

Network 🟩 1 Kbps Network I/O 🟦 0% Network Utilization

Memory 🟩 6 Hard Faults/sec 🟦 40% Used Physical Memory

Image	PID	Hard Faults/sec	Commit (KB)	Shareable...	Working Set (KB)	Private (KB)
MicrosoftEdgeCP.exe	9040	0	209,220	62,128	242,892	180,764
OneDrive.exe	6740	0	153,120	25,156	171,524	146,368
WINWORD.EXE	6204	0	154,828	110,116	219,932	109,816
MicrosoftEdgeCP.exe	5696	0	118,892	75,268	168,848	93,580
dwm.exe	408	0	100,884	29,544	108,168	78,624
SearchUI.exe	5308	0	81,576	63,716	133,900	70,184
MsMpEng.exe	2640	4	113,904	44,820	108,992	64,172
MicrosoftEdgeCP.exe	8356	0	54,908	49,416	92,172	42,756
explorer.exe	5616	0	69,704	58,824	101,184	42,360

Kernel debugging

- Examining internal kernel data structures
- Stepping through functions in the kernel
- Necessary files and tools:
  - Symbols for kernel debugging
  - Debugging Tools for Windows

Kernel debugging

- Symbols for kernel debugging:
  - Contain the names of functions and variables and the layout and format of data structures
  - Generated by the linker and used by debuggers
  - To use any of the kernel-debugging tools to examine internal Windows kernel data structures you must have the correct symbol files for at least the kernel image, Ntoskrnl.exe

Kernel debugging

- Debugging Tools for Windows:
  - Used in to explore Windows internals.
  - There are four debuggers included in the tools: cdb, ntsd, kd, and WinDbg.
  - All are based on a single debugging engine implemented in DbgEng.dll

Windows Software Development Kit

- Contains the C header files and the libraries necessary to compile and link Windows applications
- From a Windows internals perspective, items of interest in the Windows SDK include the Windows API header files
- Path: C:\Program Files (x86)\Windows Kits\10\Include
- Visual Studio also provides the option of installing the SDK

Windows Driver Kit

- Is aimed at developers of device
- Is an abundant source of Windows internals information

Sysinternals tools

- The most popular tools include Process Explorer and Process Monitor
- Mark Russinovich, coauthor of this book, wrote most of these tools.
- Most of these tools need the installation and execution of kernel-mode device drivers and thus require administrator.
- See *Windows Sysinternals Administrator's Reference by Mark Russinovich and Aaron Margosis* (Microsoft Press, 2011).