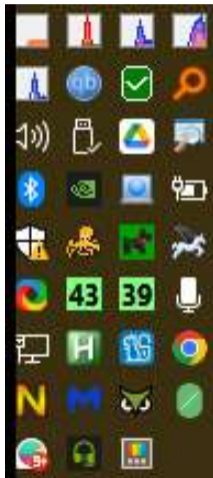


Share

## Process Explorer (sysinternals)

- Shows you what's running – can zoom to detail
- Choose from many columns, move them, sort them
- Check running processes vs Virus Total
- Allows you to see/edit priority, kill processes
- Graphs + numbers –Task Manager on steroids
- 42 minute video: <https://learn.microsoft.com/en-us/shows/defrag-tools/2-process-explorer>
- Taskbar icons show % usage of CPU/GPU/RAM/Network/Disk



System Information

Summary CPU Memory I/O GPU

CPU Usage  
7.06%

System Commit  
24.0 GB

Physical Memory  
18.0 GB

I/O  
47.7 MB

Network  
262.0 MB

Disk  
1.1 MB

**Show  
graphical  
summary**

System Information

Summary CPU Memory I/O GPU

CPU  
13.16%

CPU  
7.73%  
2.54% process\lsass.exe  
10,285.51 PM

Total		CPU		Topology	
Handles	148,792	Context Switch Delta	247,741	Cores	8
Threads	5,320	Interrupt Delta	185,847	Sockets	1
Processes	331	IPC Delta	13,461	Logical Processors	16

Show one graph per CPU

**Or dig  
down  
deeper**

Process Explorer - Sysinternals: www.sysinternals.com [UNKNOWN] (Administrator)

File Options View Process Find Users Help

<Filter by name>

Process	CPU	Priority	VirusTotal	Verified Signer	CPU History	Private B...	Working S...	PID	Description	Company Name
smss.exe		11		(Verified) Microsoft WL...		1,060 K	1,260 K	712	Windows Session Mana...	Microsoft Corpor...
sql.exe	< 0.01	8 4/70		(Verified) Gibson Rese...		5,068 K	18,500 K	23424	SQL: The Internet's se...	Gibson Research
NumLocker.exe		8 2/70		(No signature was pre...		3,828 K	12,480 K	8044	Force key states!	DeadSoul (Myst
WinPatrol.exe	0.33	8 1/70		(Verified) Ruiware, LLC		10,700 K	23,552 K	17108	WinPatrol Monitor	Ruiware
hmpsched.exe	< 0.01	8 1/70		(Verified) SurfRight B.V.		2,064 K	7,824 K	4008	HitmanPro Scheduler	SurfRight B.V.
BraveCrashHandler.exe		4 1/70		(Verified) Brave Softw...		2,188 K	1,096 K	13744	BraveSoftware Update	BraveSoftware I
AsusAppService.exe	< 0.01	8 1/70		(Verified) ASUSTeK C...		5,376 K	20,680 K	6236	ASUS App Service	ASUSTeK COMPI
popfileb.exe	< 0.01	8 1/74		(No signature was pre...		65,200 K	71,288 K	20684	POPFile	The POPFile Proj
net.downloadhelper.coop...		8 1/74		(Verified) ACLAP		21,020 K	34,828 K	5132	Node.js: Server-side Jav...	Node.js
LM_...bdsv.exe		8 1/73		(No signature was pre...		5,324 K	9,912 K	8940	Printer Communication ...	
ROGLiveService.exe	< 0.01	8 0/77		(Verified) ASUSTeK C...		7,380 K	20,672 K	7240	ROG Live Service	ASUSTeK COMPL
WUDFHost.exe		8 0/76		(Verified) Microsoft WL...		2,272 K	7,256 K	1772	Windows Driver Founda...	Microsoft Corpor...
WUDFHost.exe		8 0/76		(Verified) Microsoft WL...		55,836 K	64,908 K	1856	Windows Driver Founda...	Microsoft Corpor...
WUDFHost.exe										

CPU Usage: 15.63% Own CPU Usage: 0.59% Commit Charge: 25.28% Own Commit Charge: 0.22% - Processes: 329 - Own Processes: 4 - .NET Processes: 1 - Own .NET Processes: 0 - Threads: 5267 - Own Threads: 34

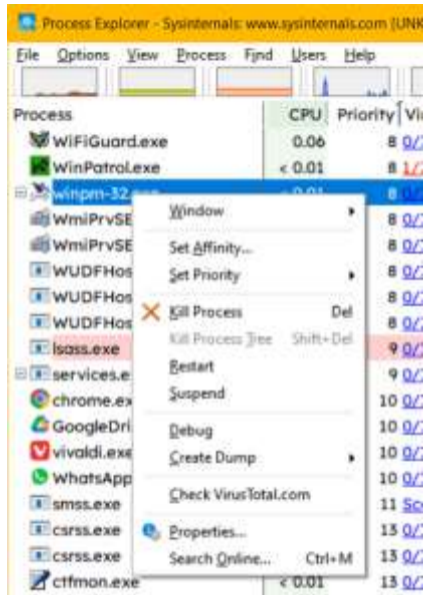
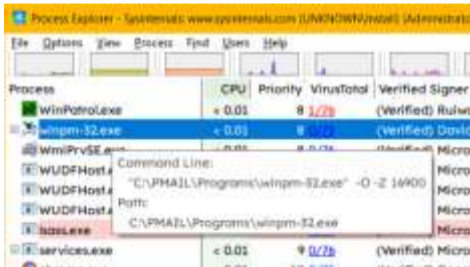
- Columns
  - Choose which to display – many to choose from
  - Sort up or down
- Minigraphs
  - CPU/System commits/RAM/I-O/Network/Disk/GPU

# View/control programs

Right-Click to:

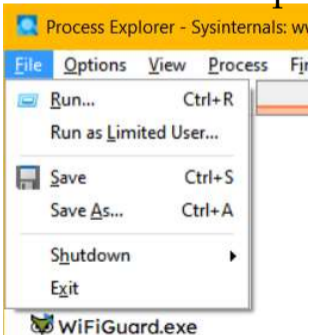
- Set priority
- Kill process
- Suspend
- Check VirusTotal
- See properties
- Search program online

Cursor over to see source



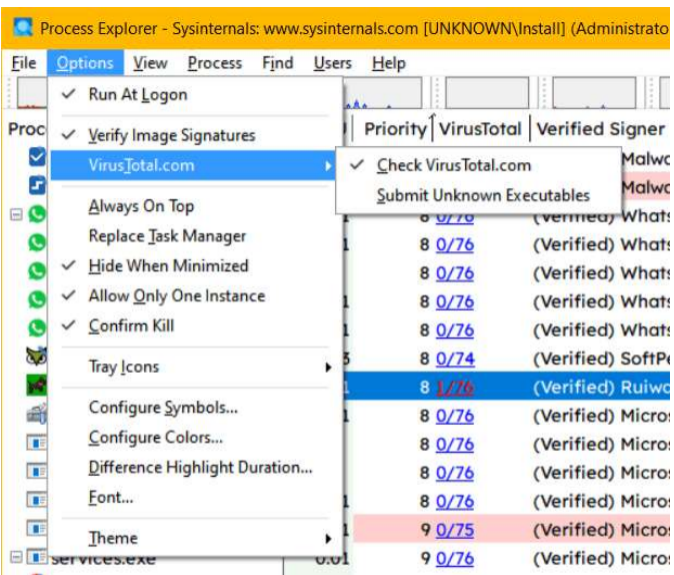
## File:

- Save state
- Run a program
- Shutdown computer



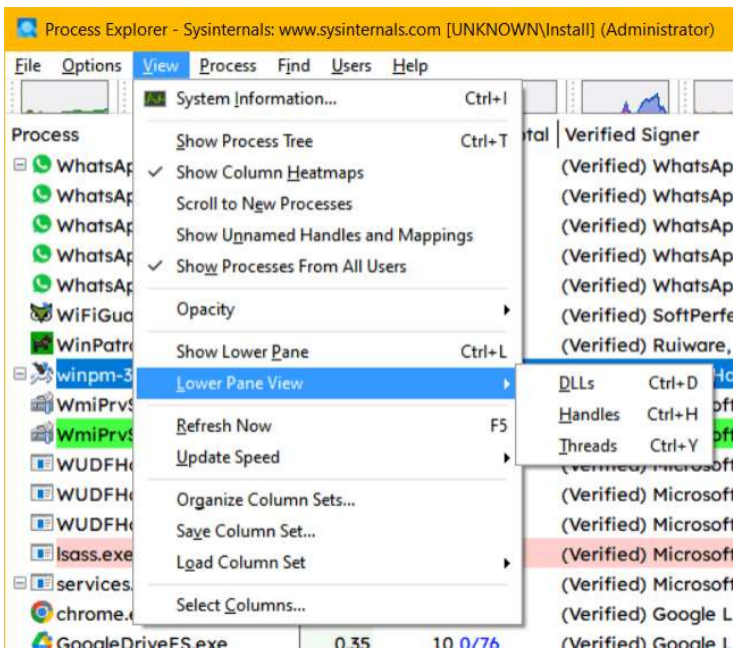
## Options:

- Chose tray icons
- Chose colours
- Virus Total (on & off checks everything)



# View:

- Lower pane view
- Update refresh speed from .5 to 10 seconds or Paused

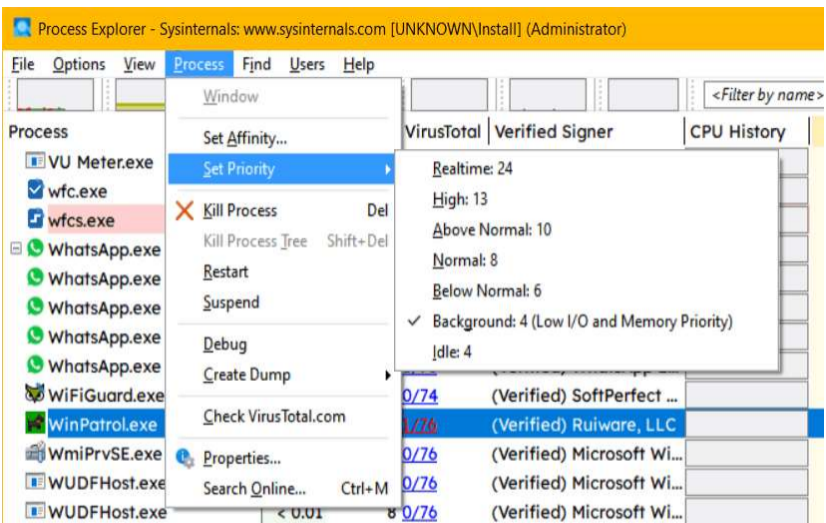


# Process:

- Set priority (can be done with right click, too)
- Kill process (ditto, also Del key)

## Do Not

- Restart process since it changes the user
- Use priorities above 10 for ordinary applications



# Process details

WhatsApp.exe(2016) Properties

Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Storage

Image File

WhatsApp  
Developer: WhatsApp LLC  
Version: 2.20.1.6.4  
Build Time: Mon Nov 02 13:36:40 2021  
Path:  
C:\Users\user\AppData\Local\WhatsApp\app-2.20.1.6.4  
Command line:  
C:\Users\user\AppData\Local\WhatsApp\app-2.20.1.6.4  
Current directory:  
C:\Users\user\AppData\Local\WhatsApp\app-2.20.1.6.4  
Autorun location:  
nil

Parent: WhatsApp.exe(2016)  
Icon: 188800Wam  
Started: 5/11/2021 11:13 Image: 64-bit  
Comment:  
Help link: 5.5

Data Execution Prevention (DEP)  
Address Space Layout Randomization  
Control Flow Guard  
Integrity Checksum  
Stack Protection

CPU  
Priority  
Name: System  
User Time: 00  
Load Time: 00  
Cycles: 114,620

WhatsApp Memory  
Private Bytes: 388.1 MB  
Peak Private Bytes: 388.1 MB  
Private Set: 1.25%  
Page Faults  
Page Faults Delta

Physical Memory  
Memory Priority: 0  
Working Set: 228,720 K  
Private: 388,044 K  
Shared: 66,852 K  
Shared: 29,400 K  
Peak Working Set: 241,736 K

Peak Handles: 228 Handles  
User Handles: 228 Handles

WhatsApp.exe(2016) Properties

Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Storage

CPU Usage: 0.00%

Private Bytes: 388.1 MB

Private Set: 1.25%

WhatsApp.exe(2016) Properties

Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Storage

User: 188800Wam  
SID: S-1-5-31-289571200-289571  
Session: 1 Logon Session: L3-C  
Whitelisted (N): Prohibited: No

Group

- BUILTIN\Performance Log Users
- BUILTIN\Users
- CONSOLE LOGON
- Everyone
- LOCAL
- Mandatory Label\Medium Mandatory Level
- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\INTERACTIVE
- NT AUTHORITY\Local account

Group ID: nil

Privilege: SeChangeNotifyPrivilege  
Flag: Default Enabled

WhatsApp.exe(2016) Properties

Image Performance Performance Graph Disk and Network GPU Graph Threads TCP/IP Security Environment Storage

Threads: 21

TID	CPU	Cycles	Suspend Co.	Start Address
20720				WhatsApp.exe!C:\ProgramData\WhatsApp\History\pe+0x00710
21336				QPatchLoader\X64.dll!onloadAgent+0x0
21400				WhatsApp.exe!v_sleep+0x74080
21342				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
21348				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
21344				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
21364				WhatsApp.exe!v_Isolate:ReleaseCleanupGroupMembers+0x450
21252				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
21240				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
19504				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
19508				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0
19496				WhatsApp.exe!v_Isolate:GetDataFromSnapshotOnce+0x387c0

Thread ID: 20720  
Start Time: 5/11/2021 11:13  
State: Wait (Idle/Request) Stack Priority: 4  
Kernel Time: 3:50:51.700 Dynamic Priority: 4  
User Time: 0:00:00.208 I/O Priority: Normal  
Context Switches: 3,634 Memory Priority: 5  
Cycles: 58,118,811,976 Ideal Processor: 2

OK Cancel



# Sysinternals Process Explorer

- Task Manager on steroids
- I use to:
  - Edit priority
  - Kill processes
  - See resource usage / bottlenecks by process, or in task tray
  - Check for viruses or hanging processes
    - Can report to developers which subprocess got stuck
  - Invaluable for developers