

Getting process id of lsass.exe

Task Manager

File Options View

Processes Performance App history Startup Users Details Services

Name	Status	1% CPU	29% Memory
Apps (2)			
> Task Manager		0%	16.4 MB
> Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
> Antimalware Core Service		0%	4.4 MB
> Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
> Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB
Microsoft Edge		0%	0.0 MB

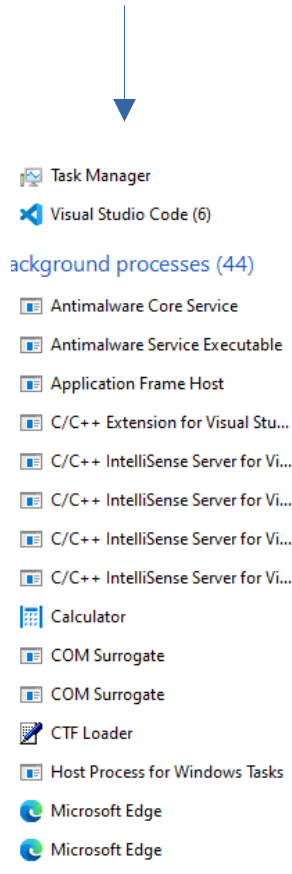
^ Fewer details

CreateToolhelp32Snapshot(FLAG, pid)

TH32CS_SNAPHEAPLIST
TH32CS_SNAPPROCESS
TH32CS_SNAPTHREAD
TH32CS_SNAPMODULE
TH32CS_SNAPMODULE32
TH32CS_SNAPALL
TH32CS_INHERIT

Name	Status	1% CPU	29% Memory
Apps (2)			
Task Manager		0%	16.4 MB
Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
Antimalware Core Service		0%	4.4 MB
Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB
Microsoft Edge		0%	0.0 MB

CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)



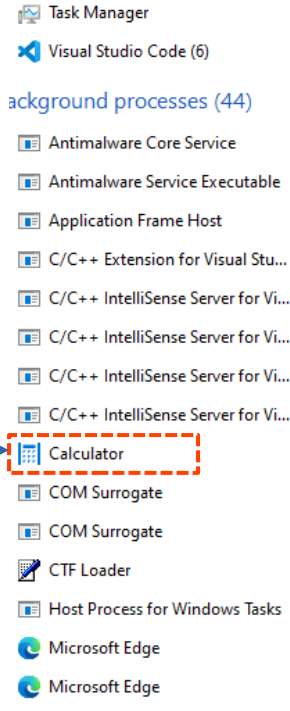
Name	Status	1% CPU	29% Memory
Apps (2)			
Task Manager		0%	16.4 MB
Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
Antimalware Core Service		0%	4.4 MB
Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB
Microsoft Edge		0%	0.0 MB

CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)

PROCESSENTRY32

It is a structure defined in the Windows API that holds detailed information about a module (like a DLL or EXE) loaded into the address space of a process.

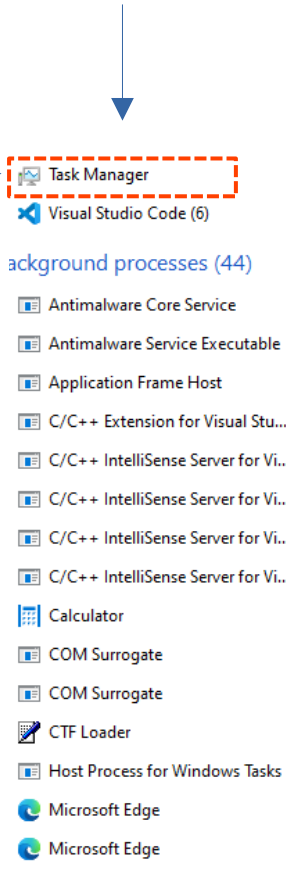
(Module ID, Process ID, Base Addr, Base Size, Module name, module path)



Name	Status	1% CPU	29% Memory
Apps (2)			
Task Manager		0%	16.4 MB
Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
Antimalware Core Service		0%	4.4 MB
Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB
Microsoft Edge		0%	0.0 MB

CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)

Process32First(hSnapshot,&ProcessEntry)
Info about the first process



Name	Status	1% CPU	29% Memory
Apps (2)			
Task Manager		0%	16.4 MB
Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
Antimalware Core Service		0%	4.4 MB
Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB
Microsoft Edge		0%	0.0 MB

CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)

Process32First(hSnapshot,&ProcessEntry)
Info about the first process

Process32Next(hSnapshot,&ProcessEntry)
Info about the next process

- Task Manager
- Visual Studio Code (6)
- background processes (44)
 - Antimalware Core Service
 - Antimalware Service Executable
 - Application Frame Host
 - C/C++ Extension for Visual Stu...
 - C/C++ IntelliSense Server for Vi...
 - C/C++ IntelliSense Server for Vi...
 - C/C++ IntelliSense Server for Vi...
 - C/C++ IntelliSense Server for Vi...
 - Calculator
 - COM Surrogate
 - COM Surrogate
 - CTF Loader
 - Host Process for Windows Tasks
 - Microsoft Edge
 - Microsoft Edge

Name	Status	1% CPU	29% Memory
Apps (2)			
Task Manager		0%	16.4 MB
Visual Studio Code (6)		0%	147.7 MB
Background processes (44)			
Antimalware Core Service		0%	4.4 MB
Antimalware Service Executable		0%	11.5 MB
Application Frame Host		0%	5.9 MB
C/C++ Extension for Visual Stu...		0%	39.8 MB
C/C++ IntelliSense Server for Vi...		0%	36.4 MB
C/C++ IntelliSense Server for Vi...		0%	72.5 MB
C/C++ IntelliSense Server for Vi...		0%	62.1 MB
C/C++ IntelliSense Server for Vi...		0%	18.3 MB
Calculator		0%	0 MB
COM Surrogate		0%	1.5 MB
COM Surrogate		0%	1.1 MB
CTF Loader		0%	3.1 MB
Host Process for Windows Tasks		0%	1.3 MB
Microsoft Edge		0%	44.0 MB
Microsoft Edge		0%	4.8 MB