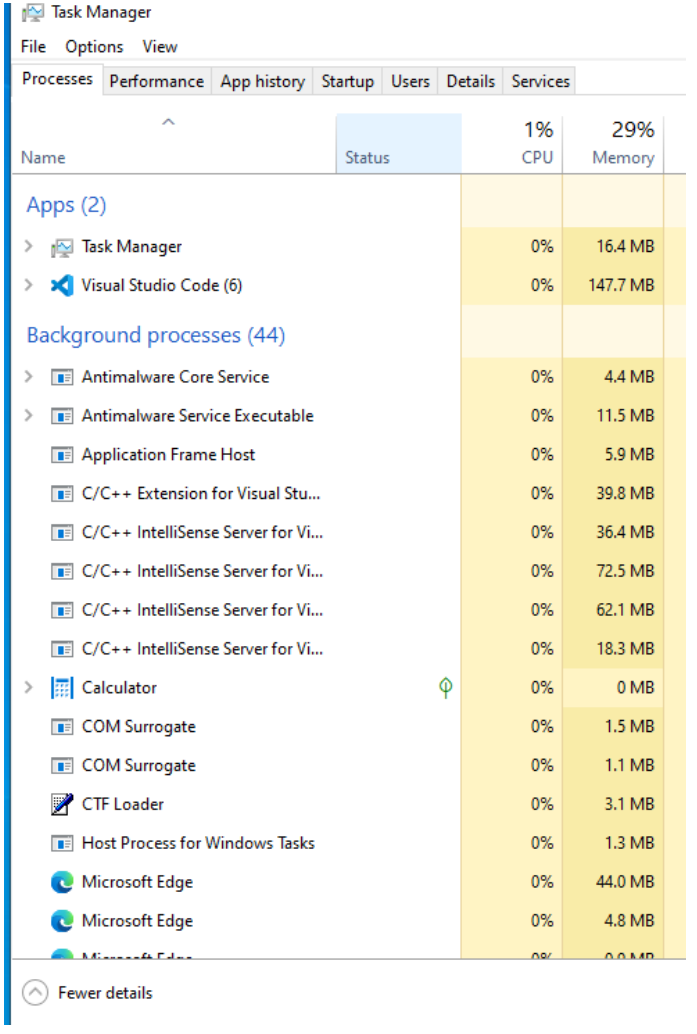
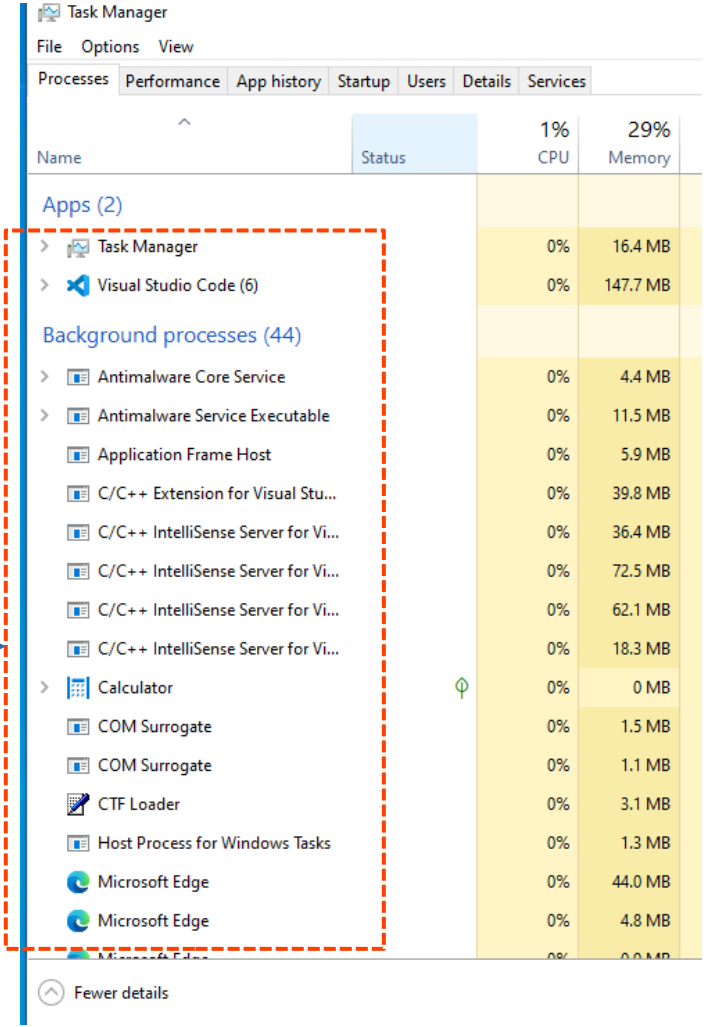
Getting process id of lsass.exe

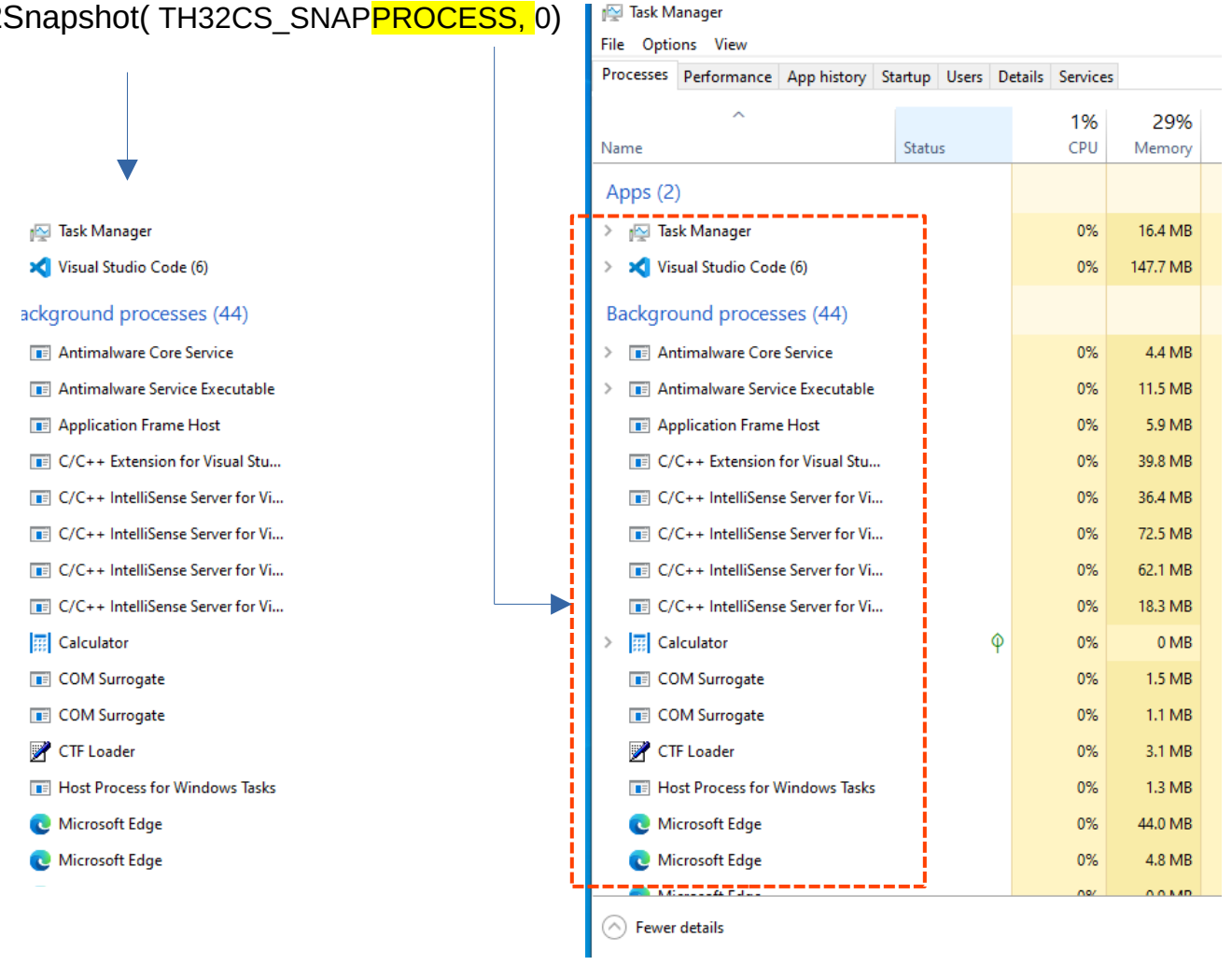


CreateToolhelp32Snapshot(FLAG, pid)

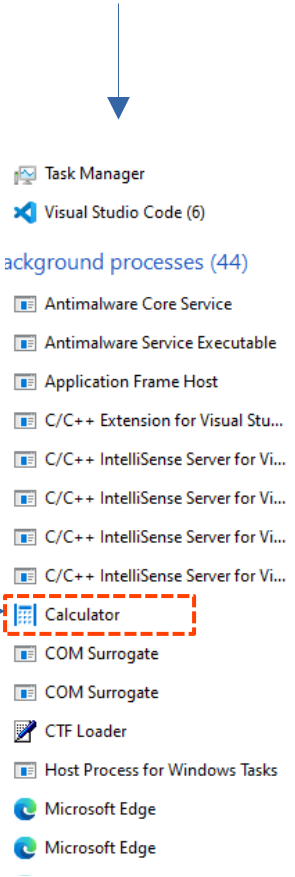
TH32CS_SNAPHEAPLIST
TH32CS_SNAPPROCESS
TH32CS_SNAPTHREAD
TH32CS_SNAPMODULE
TH32CS_SNAPMODULE32
TH32CS_SNAPALL
TH32CS_INHERIT



CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)



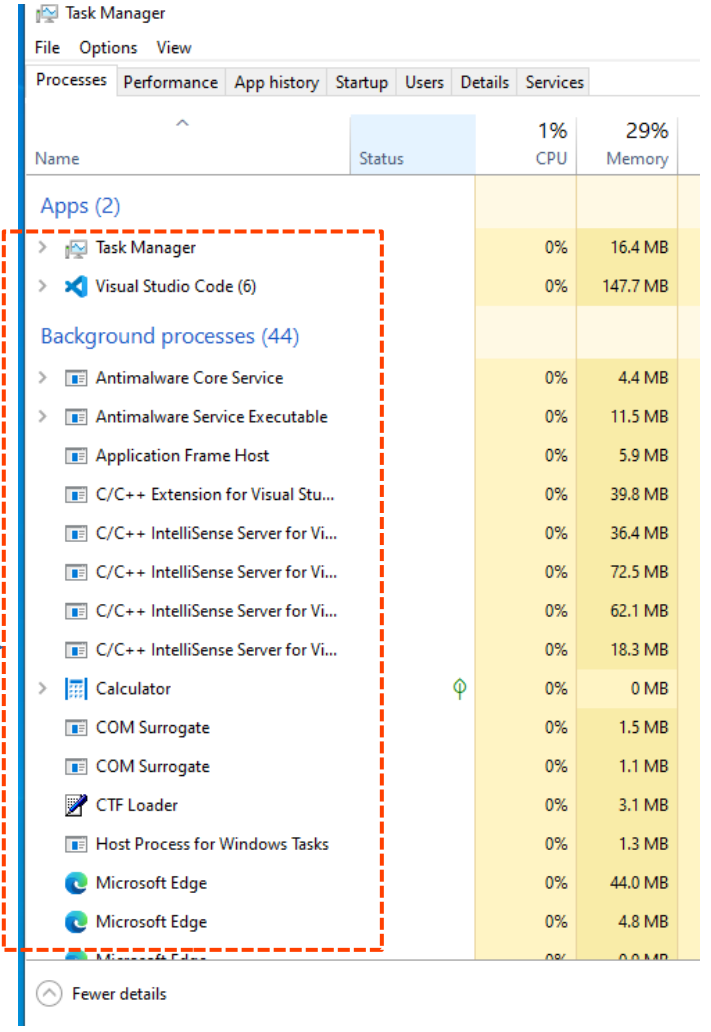
CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)



PROCESSENTRY32

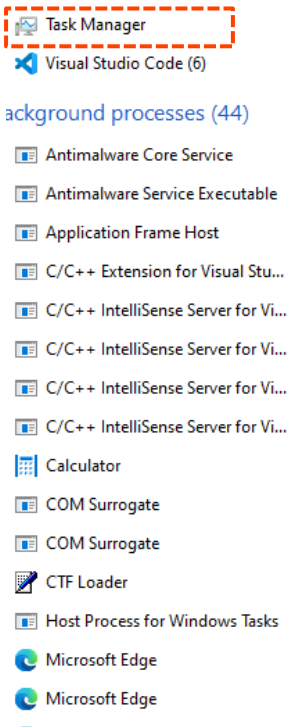
It is a structure defined in the Windows API that holds detailed information about a module (like a DLL or EXE) loaded into the address space of a process.

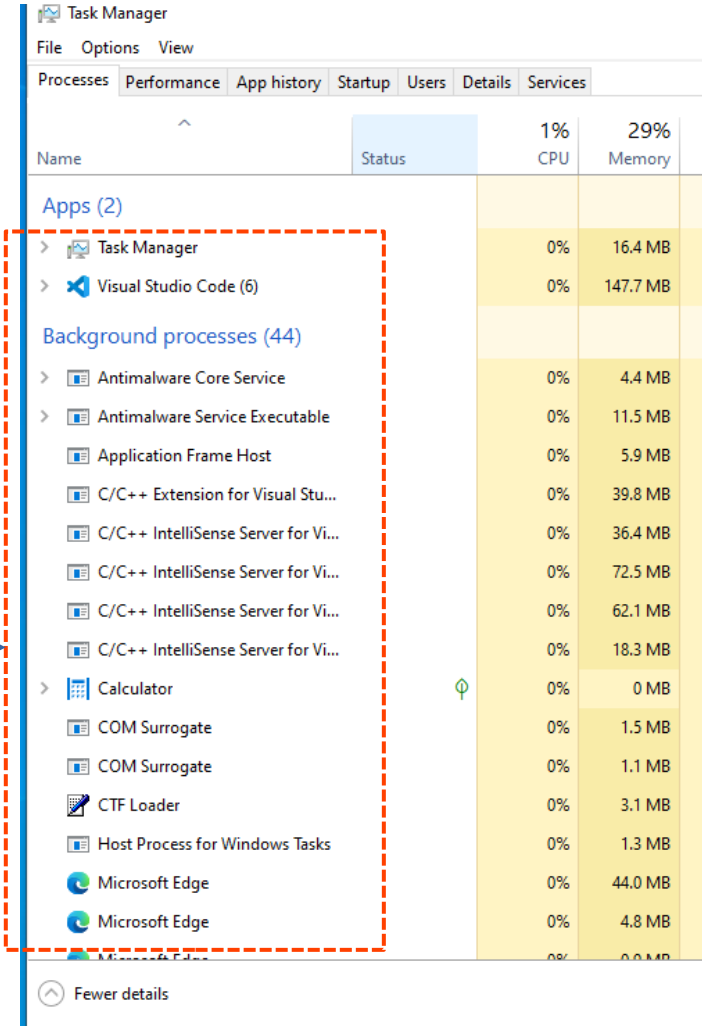
(Module ID, Process ID, Base Addr, Base Size, Module name, module path)



CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)

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





CreateToolhelp32Snapshot(TH32CS_SNAPPROCESS, 0)

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

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