**WEEK 5**

**MAINTAIN EFFICIENT PROCESS UTILIZATION ON WINDOWS**

**PROCESS MANAGEMENT**

**PROGRAM :**

Programs are the applications that we can run like the Chrome Browser.

PROCESS:

Programs that are running.

**How Processes Starts :**

1.When we open an application like a for example Word Processor, that process get in something called **Process ID.**

**(PHOTO of PROCESS ID)**

2. Our computer then checks for the requirements of hardware resources that the process will require to run.

3.So, the kernel makes decision to figure out what resources to give it. (the process).

**Background Processes Or Daemon Processes**

1. Background processes are the ones that runs behind.
2. We don’t interact or see them but they are very essential for our system to work properly.
3. Example: Scheduling resources, logging, managing network etc.

**Process Creation and Termination**

Process creation and termination’s working differ from OS to OS. Here we have discussed about two popular working Windows and Linux.

**Windows**

1.When Windows boots up/starts , the first non-kernel user mode that starts is **the Session Manager Subsystem** or **smss.exe**.

2. The smss.exe process is in-charge of setting some stuff up for the OS to work.

3.It kicks off the login process called **winlogon.exe**.

4.Also starts the Client/Server Runtime Subsystem called

**csrss.exe** which handles running windows GUI and command line council.

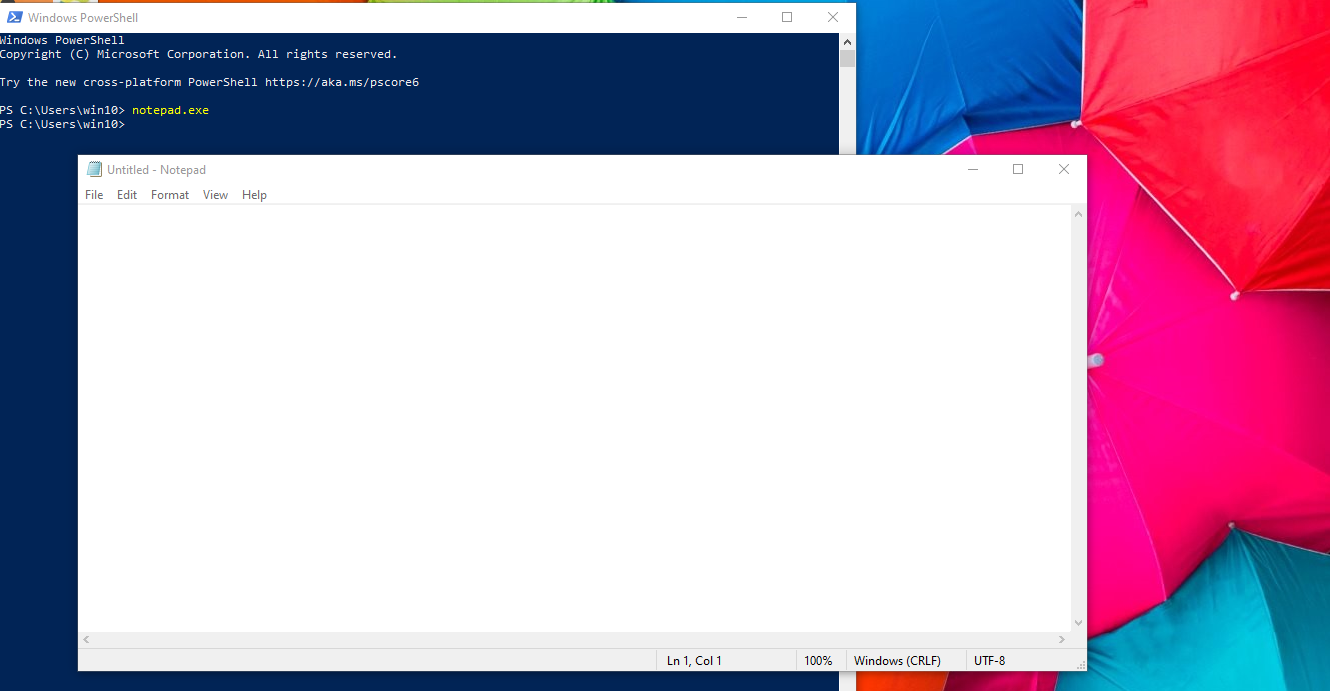
5.In Windows, each new process that’s created needs a parent to tell OS that a new process needs to be made.

6. **Child process** inherits some things from its parents like variables and settings which we collectively call as environment.

7.Just for the creation of the process is we need a parent process. After **that Windows processes can operate independently of their parents**.

**Example of creating a new Process in Windows Using PowerShell**

1. Let’s start a new notepad program.
2. Open PowerShell -> type the command notepad.exe.



3.Here notepad is a child process of parent process,PowerShell.

4.Once notepad starts it exhibits independent properties from PowerShell.

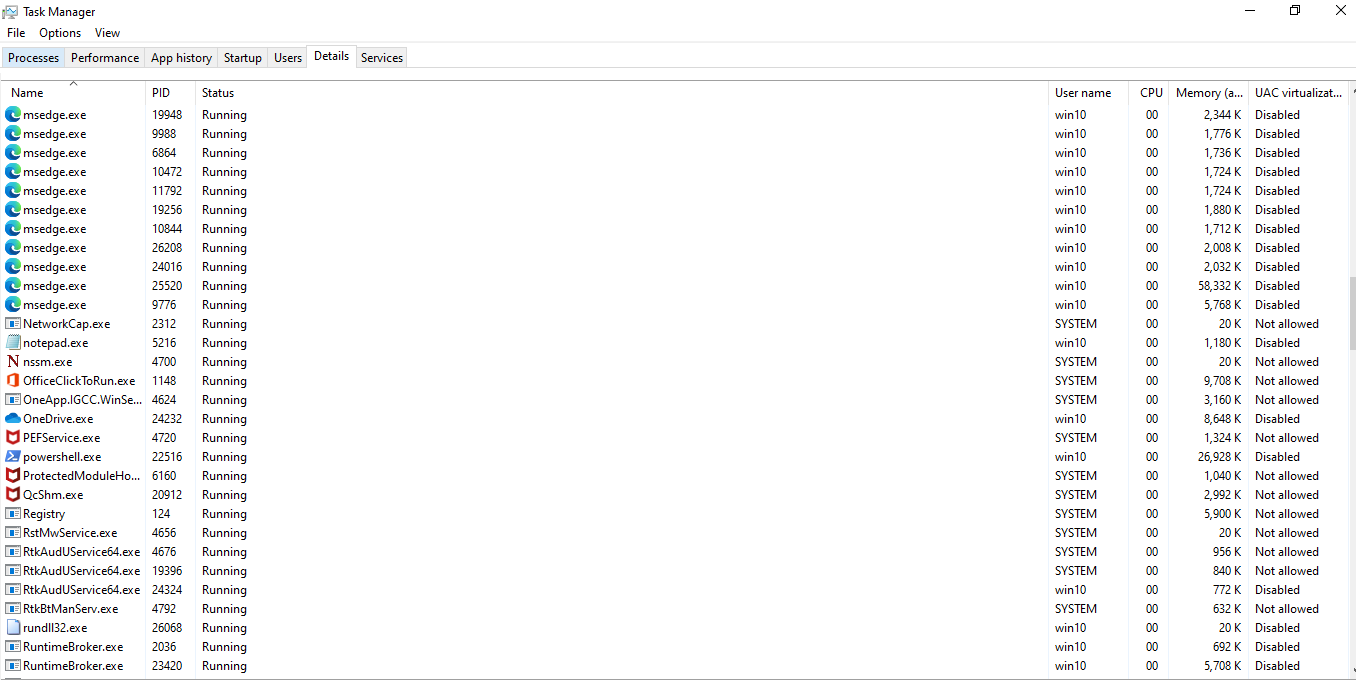
5.Now, even if you terminate the parent program the child process will continue to exist.

**To terminate a process from command prompt**

1. Use command **taskkill** from task kill utility.
2. It will put the process to halts in a number of ways.
3. One of which is using identification number or the Process ID.
4. To open TaskManger:

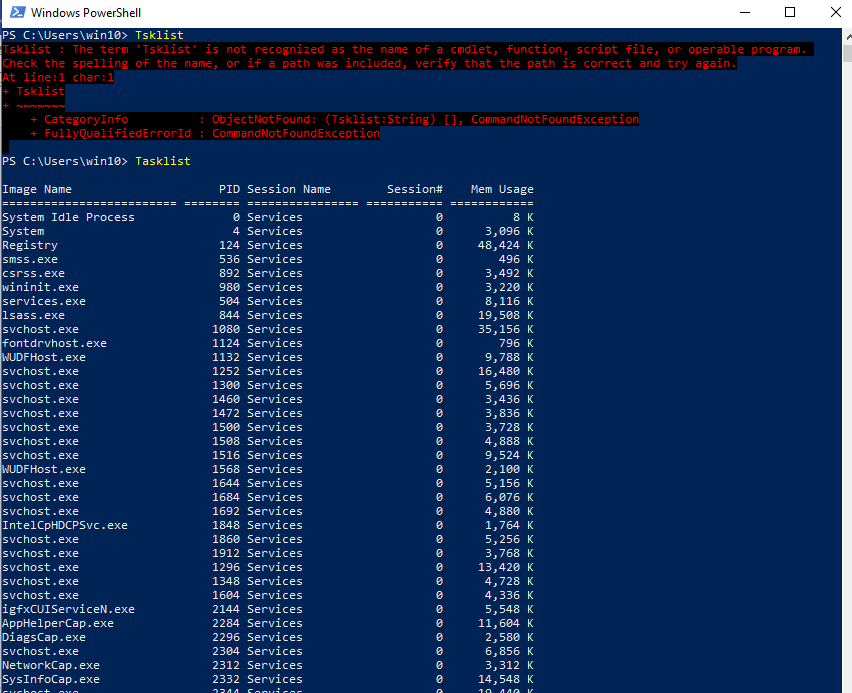
* Search
* Task mgr.exe
* Ctrl-Shift-Esc

To identify PID in Windows TaskManager->Details



To Access PID from Powershell use command

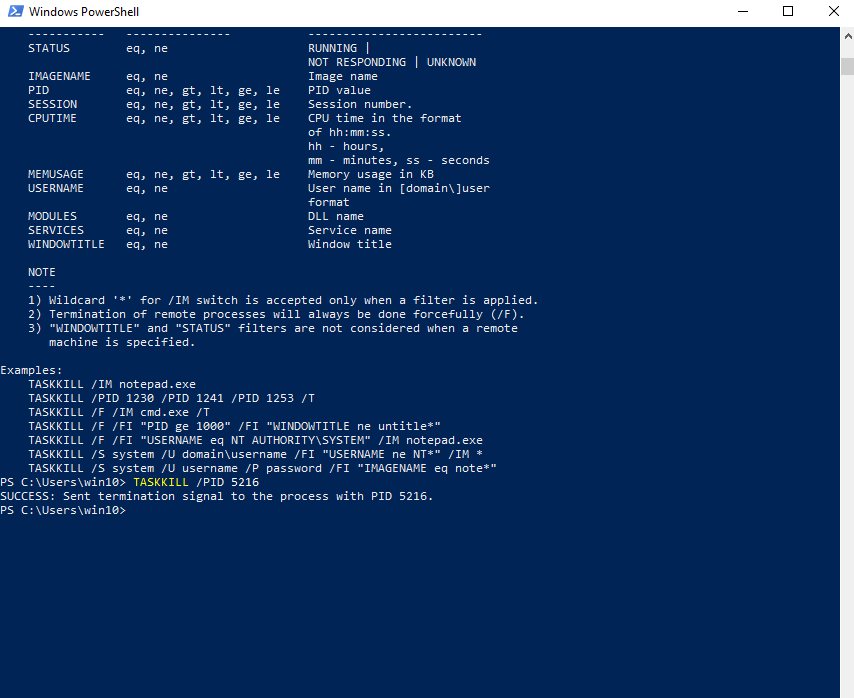
**Tasklist**

****

1. Command :

**taskkill /PID 5865**

**Eg taskill /PID 5856**

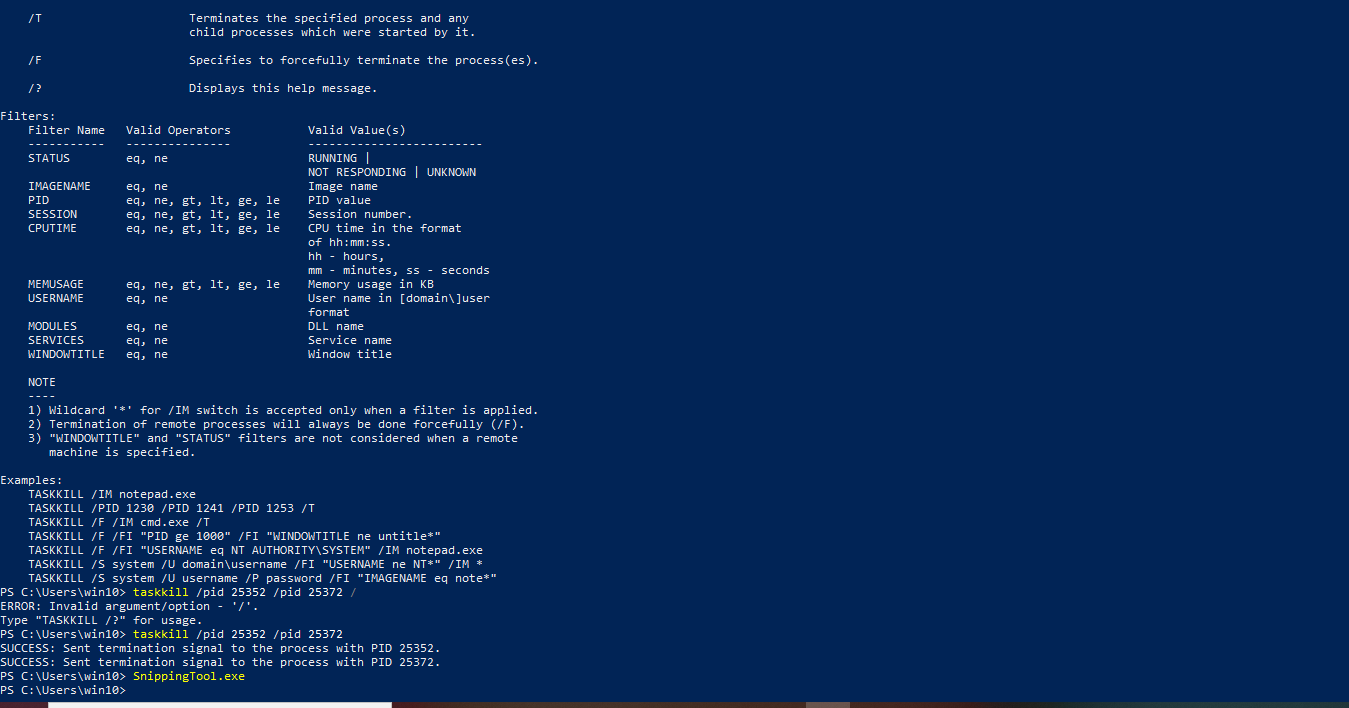
****

**To Kill Multiple Processes**

1. First, launch the PowerShell application. This can be done by pressing the **[Windows Key]** + **[R]** and then typing powershell  in the run box.
2. Type tasklist in the PowerShell window. Soon you’ll see a list of all the processes running on your operating system, along with relevant info such as session number and PID, and memory usage.
3. Make note of the PID on the process that you want to kill and then execute the following command: taskkill /f /PID 00000. Replace the zeros with the PID you want to kill.

For many Processes

For example, taskkill /IM loom.exe /F will kill all processes that are associated with the Loom service.

****

**Signals**

1.To tell a process to quit at the system level

We use something called Signal.

2.Signal

A signal is a way to tell a process that something just happened.

3.**SIGINT**- Signal Interrupt or Ctrl-C

**Managing Processes**

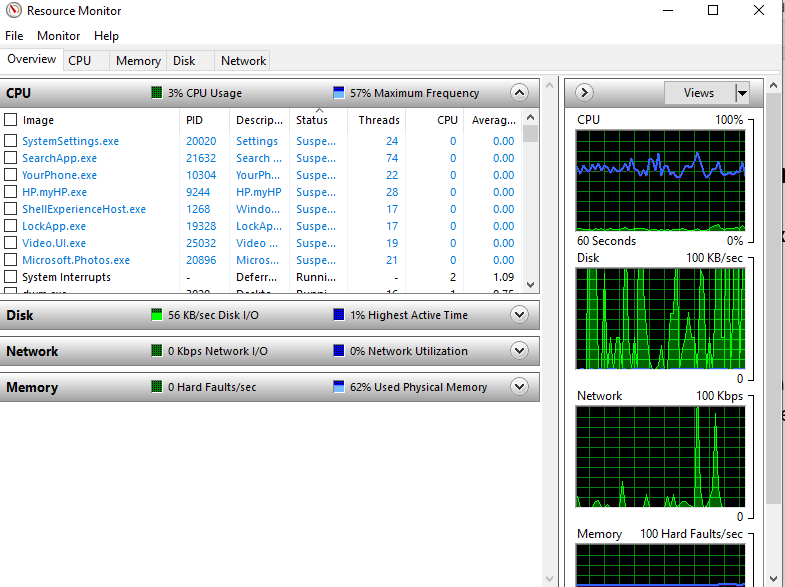
1. When you click open on an application, OS turns the resting code of program into running,responding, working applications.
2. It becomes a process.
3. Task Manager shows you the detail.
4. Now, the tool that allows you to restart or pause a process is called Process Explorer in Windows.
5. **Process Explorer**: It is a Microsoft utility created to let IT support specialists,system administrators and other users to look at the details of running process.
6. It has to be downloaded.
7. It is a very useful tool if you want to know the details of the process at depth.
8. Options/commands like **kill process**(kills the process) and **kill process tree**(which along with program kills all its descendants as well ) are given.
9. **Restart** – kills the program ,restarts again .**Suspend-** option used for pausing the process
10. Process name for process explorer **is procexp.exe**.

**Process Utilization**

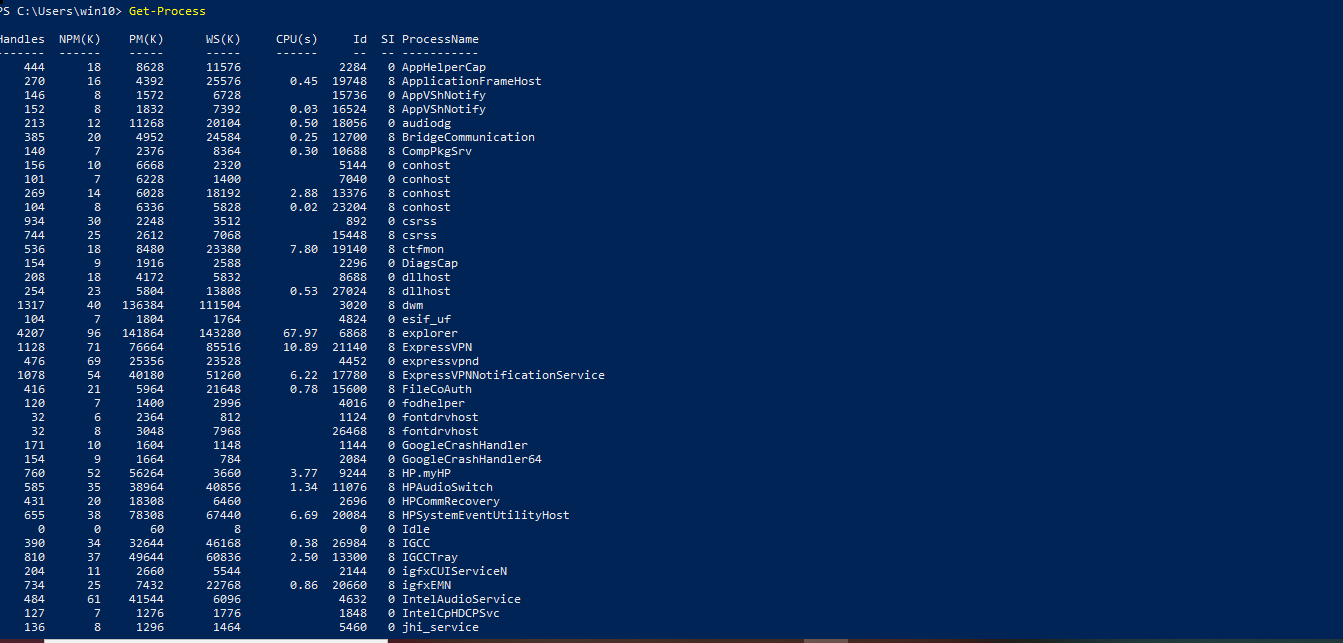
**Resource Monitoring**

Resource Monitoring Tools helps monitoring and gathering information about the resources available and the one’s involved in the processes.

Start->Resource Monitor

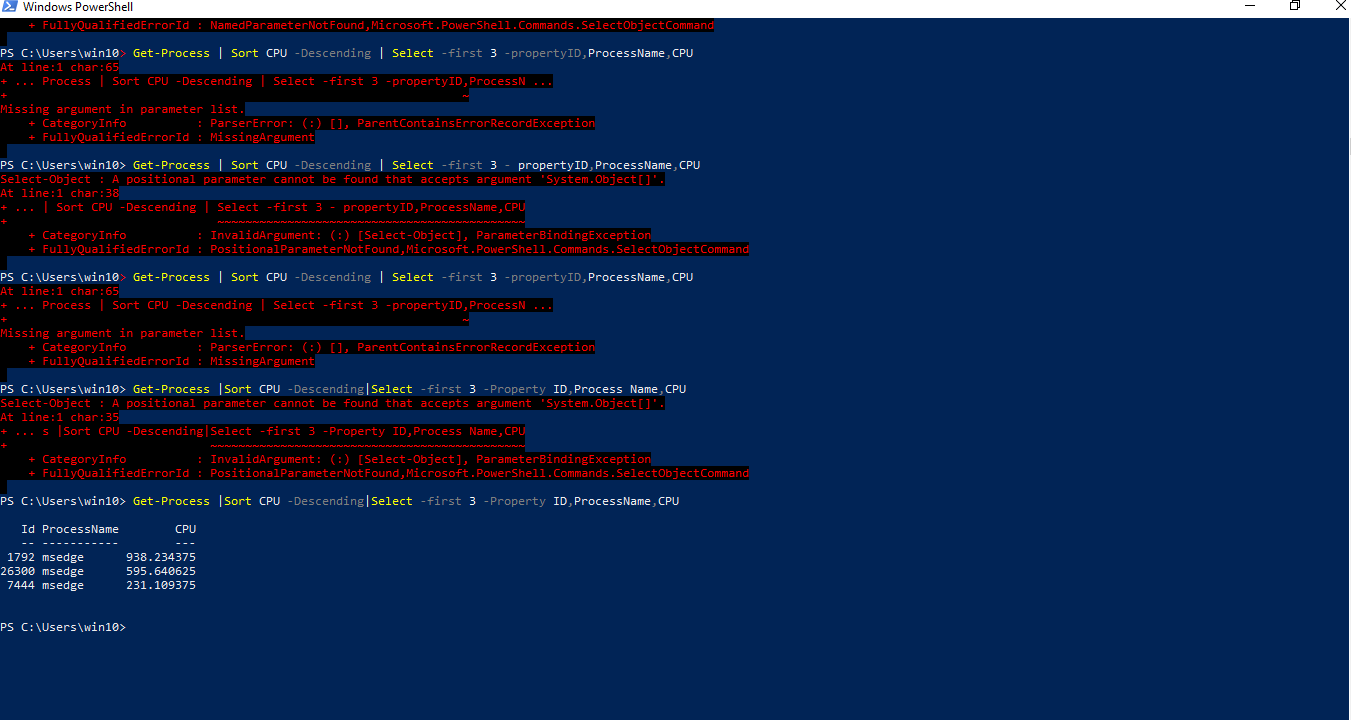


**Command Get-Process:**This command gives details about the processes going on your system.



These commands can be used to filter out the list as per our requirements.

For example we need to know the top 3 processes which are consuming or the CPU is busy with we type the following command:

**Get-Process |Sort CPU -Descending|Select -first 3 -propertyID,processname,CPU**

This can be used as a good trouble-shooting method incase we face any slow or CPU related or any other fatalities.

**Explanation of the Command used for better understanding of each command used.**

**Get-Process |Sort CPU -Descending|Select -first 3 -propertyID,processname,CPU**

**Get-Process -**To obtain all the process details/info of ongoing processes from OS

Then we use | or pipe to connect the output of Get-process to sort command

**|Sort CPU -Descending-** We sort our CPU column in a descending manner to find out top 3 CPU consuming processes

**|Select -first 3 -propertyID,processname,CPU -** Then we pipe the info with select command to pick the first 3 rows from the sorted output and display only the Property ID, Process name and CPU amount to display as output.