DU1 – Windows processes

Windows Task Manager

Task Manager is a built-in system **moritoring tool** in Windows that provides real-time information about the performance, processes, and resource usage of the operating system. It helps identify and manage programs or processes that may be consuming excessive resources or causing system issues.

The easiest way to open the Windows Task Manager is pressing **Ctrl+Shift+Esc** together at the same time and Task Manager will launch.

Processes tab

This tab provides a list of all running processes on a computer, including apps, background processes and Windows processes. It provides details such as the process name, CPU and memory usage, disk and network activity, and user associated with each process. We can end processes, change their priority, or open their file locations from this tab.

Details tab

The Details tab provides detailed information about the processes running on a system, giving a more extensive view than the information in the Processes tab. Similar to the Processes tab, we can right click on a process to access options such as ending the process, changing its priority, or searching online for more information about it.

List of processes on the command line

All processes in Windows can be listed on the command line prompt (cmd) using the **tasklist** command.

The **tasklist** command in **Windows** is the **Linux ps** command equivalent.

To get the list of **all running processes** in **Windows** we can run:

```
C:\> tasklist
```

If we want to filter the list of processes by a process name (case insensitive) we can use:

```
C:\> tasklist /NH | findstr /I myProcess
```

The option **/NH** is used to hide header column names from the result set output.

The command **findstr** searches for patterns of text. Using it with the **/I** option makes the search **case-insensitive**.

List of processes in PowerShell

We can use the **Get-Process** cmdlet in PowerShell to show a list of running processes on a Windows machine.

This cmdlet gives useful information related to each process, such as process ID, name, memory usage, etc.

When we want to filter the running processes to get only the information about a process whose name we know, we can use:

```
Get-Process processName
```

Kill a process on the cmd

We can use the taskkill command to kill a process from the command line.

If you know the process ID (PID), you can use the following command:

```
taskkill /F /PID <pid>
```

The option **/F** is used to **forcibly** kill the process. If not used, it would ask a user confirmation.

Taskkill also supports killing a process by its name. To do so, you can use the following command:

```
taskkill /F /IM <process_name>
```

The option **/IM** represents the **image name** and corresponds to the name brought up by tasklist.

Kill a process in PowerShell

PowerShell offers a **Stop-Process** cmdlet to terminate processes by their **ID** or **Name**.

You can use the Get-Process cmdlet to find the process ID (PID) of a specific process.

If a process does not terminate with a standard **Stop-Process** command, using the **-Force** parameter might be necessary.