Cambridge Small (2025), , 1–6

CAMBRIDGE
UNIVERSITY PRESS

ARTICULO CIENTIFICO

Universidad Mayor de San Simón

Merino Vidal Mateo Alejandro

Cochabamba, Bolivia
202301308@est.umss.edu

Abstract

El presente informe tiene como objetivo demostrar la ejecución de procesos en el sistema operativo Windows 11. Para una correcta visualización en cuanto a la jerarquía de procesos se requirió el uso de una aplicación o programa denominado Procmon. Se comparan dos escenarios: uno en donde se observa el árbol de procesos correspondiente a un solo usuario y otro cuando se están ejecutando dos usuarios a la vez.

Keywords: proceso, jerarquía, sistema operativo, cambio de contexto

1. Introducción

Actualmente, muchas personas creen que la computadora trabaja de forma simultanea al momento de realizar diversos procesos, es decir, que ejecuta múltiples acciones a la vez. Sin embargo, esto no es verdad, ya que a pesar de que la computación ha evolucionado a lo largo de la historia, las computadoras siguen estando limitadas.

Los microprocesadores actuales ejecutan un solo proceso a la vez, pero lo hacen a una velocidad tan alta que el ser humano no puede percibir cuándo comienza o termina cada uno. Como resultado, da la impresión de que todos los procesos se ejecutan a la vez.

Cada acción realizada en la computadora, desde abrir una aplicación hasta ejecutar un simple comando, implica por lo menos la ejecución de un proceso.

Proceso: Actividad que se ejecuta de manera independiente dentro de un programa, pero que forma parte del conjunto de tareas necesarias para su funcionamiento. Cada proceso utiliza sus propios datos y recursos durante su ejecución.

Cuando el procesador atiende un proceso en cola, está en ejecución. Sin embargo, si la tarea ocupa demasiado tiempo, el procesador no puede asignar todo su tiempo de ejecución a esta actividad, ya que existen otras que están esperando en cola. En este caso, se guarda el estado del proceso mediante el contador del programa y el procesador pasa al siguiente proceso. A esta transición entre procesos o actividades se le denomina cambio de contexto.

Cambio de Contexto: Procedimiento en el cual el procesador interrumpe la ejecución de un proceso y guarda su estado para poder ejecutar el siguiente en espera. Sin embargo, este cambio requiere tiempo para guardar y restaurar la información del proceso, siendo considerado como "tiempo perdido" o "tiempo muerto", ya que no contribuye directamente con la ejecución de las tareas.

Cada proceso al momento de crearse, sigue una jerarquía, pudiendo representarla a través de un árbol de procesos, cuya estructura es similar a la de un árbol genealógico, por lo que es necesario emplear términos como padre, hijo, abuelo.

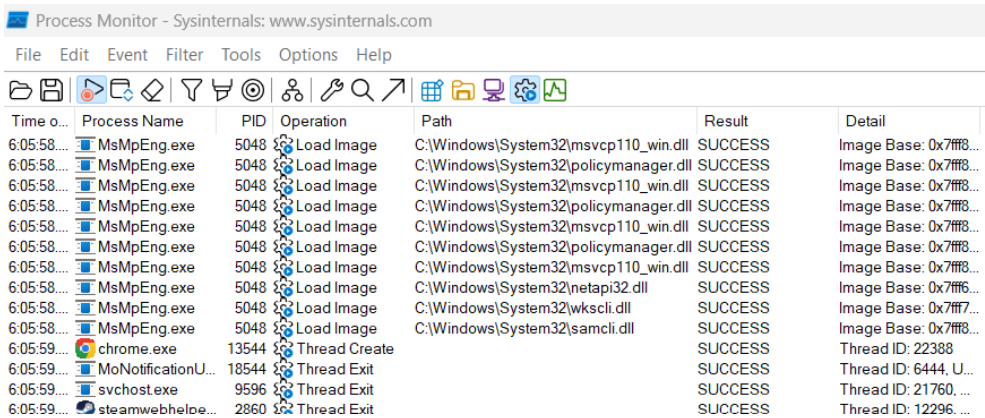
En el caso de Windows, los procesos del sistema operativo no siguen como tal una jerarquía, pero gracias a la aplicación Procmon es posible observar cuales son los principales. Al iniciar el sistema, los primeros procesos que se ejecutan son los encargados de la administración básica de los recursos del sistema. Entre ellos se encuentran:

1. `System`: Núcleo de Windows, responsable de gestionar los recursos del sistema.
2. `Winlogon`: Se encarga de la administración y autentificación del usuario.
3. `Explorer (Shell)`: Interfaz gráfica para interactuar con el sistema.

2. Desarrollo

Para el presente proyecto, se llevaron a cabo una serie de pasos e instrucciones que permitieron estructurar y ejecutar de manera adecuada las tareas necesarias para el análisis de los procesos en el sistema operativo Windows 11.

1. Instalación de la aplicación Procmon, ya que Windows por defecto no nos permite ver de forma clara la jerarquía de los procesos que se están ejecutando.



Time o...	Process Name	PID	Operation	Path	Result	Detail
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\msvcp110_win.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\policymanager.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\msvcp110_win.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\policymanager.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\msvcp110_win.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\policymanager.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\msvcp110_win.dll	SUCCESS	Image Base: 0x7fff8...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\netapi32.dll	SUCCESS	Image Base: 0x7fff6...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\wkscli.dll	SUCCESS	Image Base: 0x7fff7...
6:05:58....	MsMpEng.exe	5048	Load Image	C:\Windows\System32\samcli.dll	SUCCESS	Image Base: 0x7fff8...
6:05:59....	chrome.exe	13544	Thread Create		SUCCESS	Thread ID: 22388
6:05:59....	MoNotificationU...	18544	Thread Exit		SUCCESS	Thread ID: 6444, U...
6:05:59....	svchost.exe	9596	Thread Exit		SUCCESS	Thread ID: 21760, ...
6:05:59....	steamwebhelpe...	2860	Thread Exit		SUCCESS	Thread ID: 12296, ...

Figure 1. Procmon

2. Ir al apartado de "Tools" en la aplicación y seleccionar Process Tree, el cual nos mostrara la jerarquía de los procesos que están actualmente en ejecución. Esto hace

posible observar los procesos, con sus respectivos PID (Process Identifier) cada uno, los cuales nos indican que procesos están por encima de otros en la jerarquía, es decir, cuales son padres y cuales son hijos.
Entre los primeros procesos como se observa en la fig, 2 , se encuentran:

System –> Winnit –> WinLogon –> Explorer (Iniciado por Winlogon).

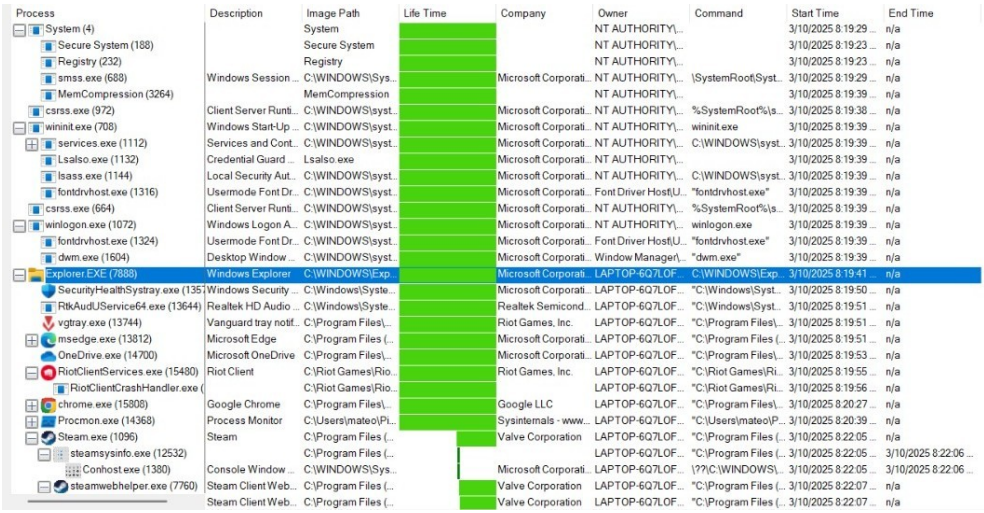


Figure 2. Process Tree de 1 Usuario

Como se puede observar, el proceso explorer.exe gestiona la interfaz gráfica del usuario en Windows, y dentro de esta interfaz, se muestran procesos de aplicaciones abiertas como Steam, Edge, Google, etc.

3. Se procede a la creación de un segundo usuario, con el fin de demostrar la existencia de dos sesiones de usuario activas, cada una con su propio proceso de WinLogon y Explorer.

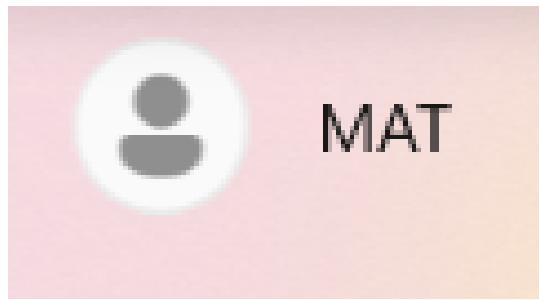


Figure 3. Usuario Principal

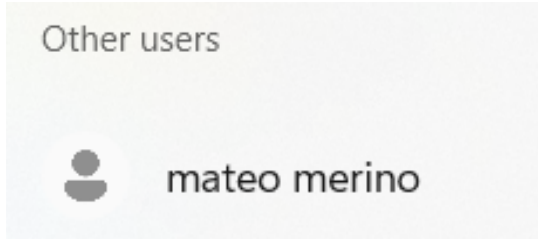


Figure 4. Usuario Secundario

4. Se inicia sesión en la cuenta del segundo usuario y se procede a abrir aplicaciones para generar nuevos procesos. Posteriormente se regresa a la sesión del primer usuario y se procede a generar nuevamente el Process Tree en la aplicación Procmon.

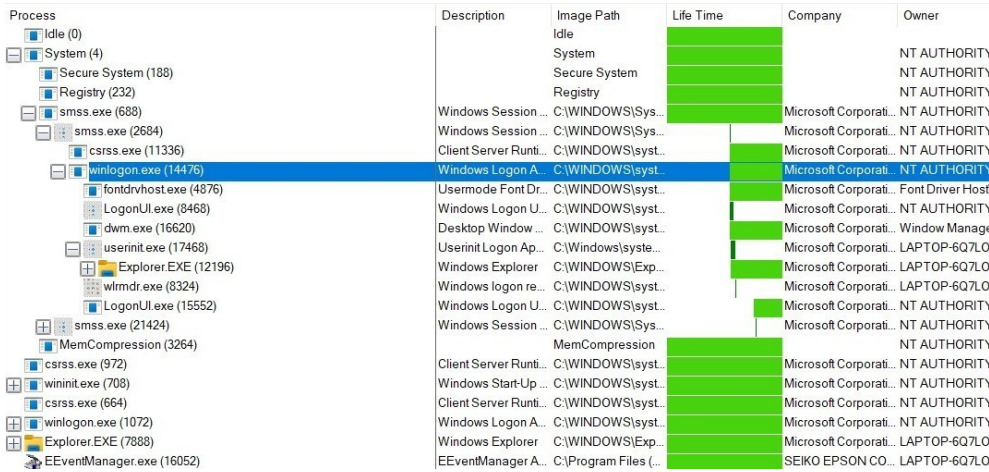
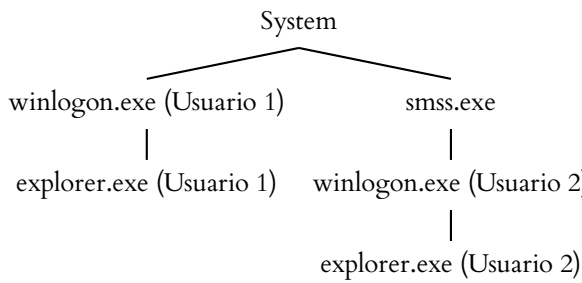


Figure 5. Process Tree de los dos usuarios

Tal y como se observa en la fig. 5, ambos usuarios cuentan con sus propios procesos en cuanto al Winlogon y Explorer, teniéndose una estructura:



Cabe mencionar que el Winlogon y Explorer del usuario secundario ha pasado a estar contenido dentro de smss.exe. Esto ocurre porque, al iniciar una segunda sesión de usuario, el sistema reorganiza la jerarquía de procesos, y smss.exe asume el control de la administración de sesiones activas.
Por otro lado, el Winlogon y Explorer del usuario principal se muestra como un proceso independiente, es decir, que no esta contenido dentro del smss.exe como el usuario secundario.

A continuación, se puede observar en la fig.6 y fig 7 los procesos correspondientes a cada usuario, pero de forma mucho mas detallada.

Figure 6. Procesos del Usuario Principal

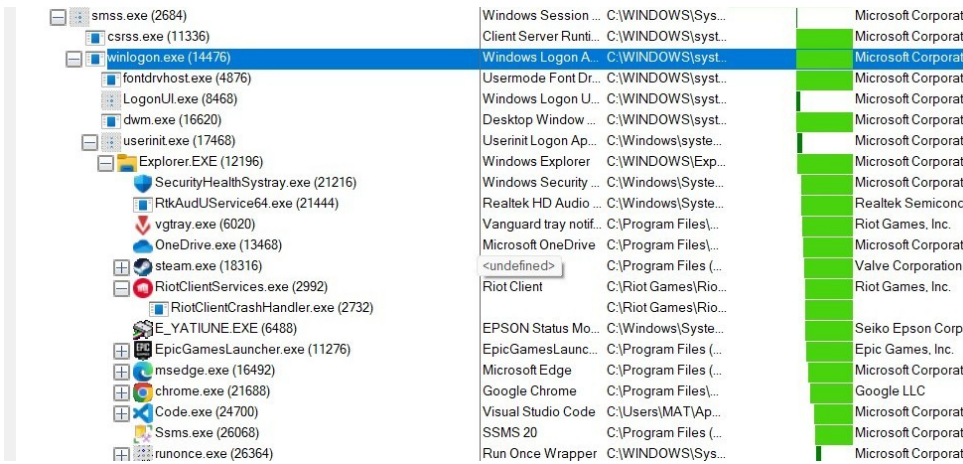


Figure 7. Procesos del Usuario Secundario

3. Conclusión

- Aunque el procesador ejecuta muchos procesos a alta velocidad, lo que da la impresión de que los realiza simultáneamente, en realidad solo puede ejecutar un proceso a la vez.

- Windows no mantiene como tal una jerarquía de procesos, pero, mediante la herramienta Procman, se ha observado que entre los primeros procesos se encuentran System, Winlogon y Explorer.
  Cuando se inicia sesión en un usuario secundario, se crea un segundo Winlogon y Explorer para ese usuario, lo que modifica la estructura del Process Tree.