

INSTITUTO TECNOLÓGICO AUTÓNOMO DE MÉXICO

LABORATORIO: Sistemas Operativos

Práctica 1

Información de procesos en Windows

LosDos

Integrantes:

Amanda Velasco Gallardo - 154415
Carlos Octavio Ordaz Bernal - 158525

Fecha(s) de elaboración de la práctica:

18 de enero de 2019

Introducción

Una parte fundamental al momento de querer entender el funcionamiento de una computadora es el estudio de los sistemas operativos. Un **sistema operativo** es esa capa intermediaria dentro de un sistema de cómputo que consiste en el conjunto de programas que gestionan los recursos de *hardware* para proveer servicios a las aplicaciones. Cabe resaltar que los sistemas operativos no se encuentran solamente en las computadoras sino que también forman parte de múltiples aparatos tales como automóviles y televisores.

Entre las funciones de un sistema operativo se encuentran la gestión de procesos y la gestión de recursos. Un **proceso** es un programa en ejecución que requiere de tiempo de CPU, memoria, archivos y dispositivos de Entrada/Salida. El sistema operativo, entonces, debe encargarse de crear y destruir, interrumpir y reanudar y, si es el caso, alternar procesos.

Existen herramientas cuyo propósito es mostrar información sobre los procesos que se están ejecutando en la computadora. Estos programas se conocen como **administradores de tareas**. En esta práctica se utilizó un administrador de tareas para Windows llamado *Process Explorer*, el cual permite obtener información mucho más rica que el administrador de tareas predeterminado del sistema. Algunas de las funcionalidades de *Process Explorer* que se utilizaron en esta práctica son:

- Opción de seleccionar de entre una amplia gama qué información o características sobre los procesos se desea desplegar (PID, compañía fabricante, línea de comando, etc.).
- Vista jerárquica de los procesos.
- La arboresencia de los procesos permite realizar acciones sobre ramas enteras.
- Guardar el estado a un archivo de texto.
- Opción de elegir la frecuencia de muestreo.

Además de los administradores de tareas, Windows cuenta con el comando **tasklist**. Al ser ejecutado, éste muestra una lista de los procesos que se están ejecutando en la computadora junto con información o en formato adicionales dados ciertos parámetros.

Por último, también existe el comando **wmic**, el cual establece una interfaz de

línea de comando de **WMI** (*Windows Management Instrumentation*). WMI es una infraestructura que permite gestionar datos y operaciones administrativas en sistemas operativos de Windows [1].

Desarrollo

3. Hacer lo necesario para que ProcessExplorer despliegue las siguientes columnas, mediante el menú *View/Select Columns*, en las diferentes pestañas *Process Image*, *Process Performance* y *Process Memory*.

Para lograr lo anterior, seleccionamos la opción del menú *View/Select Columns* y navegamos entre sus diferentes pestañas para seleccionar cada una de las opciones indicadas.

4. Desplegar una imagen donde se pueda ver, de ProcessExplorer, el área de menús, la barra de los nombres de las columnas y las 10 primeras líneas de los procesos.

Como se puede observar en la siguiente figura 1, mostramos las primeras diez líneas de procesos que se encontraron con ayuda del programa. Además, es posible identificar los campos solicitados en la pregunta del inciso anterior.

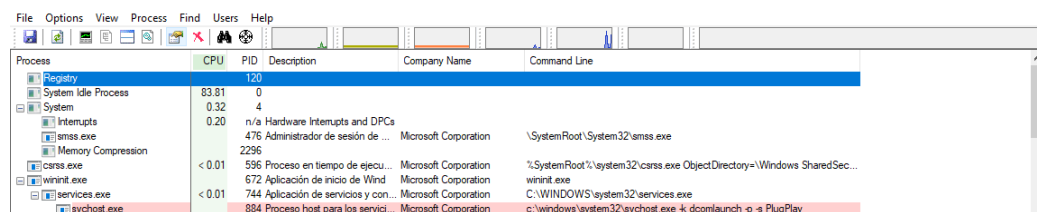


Fig. 1: Ventana del programa Process Explorer.

5.

- ¿Cuál es el PID del proceso *ProcessExplorer*? Su PID es 2740.
- ¿Cómo se llama el proceso que es padre del *ProcessExplorer* y cuál es su y respectivo PID? El proceso padre es *Explorer.exe* y su PID es 11408.
- Desplegar la línea de comando de *ProcessExplorer*: `C:/Users/sdist/SistemasOperativos/matAA/procexp64.exe`

6. Arancar los programas Word y dos instancias de Internet Explorer.

- *¿Cuáles son sus respectivos nombres de proceso y PID?:* Para Word, el nombre del proceso es `WINWORD.EXE` y su PID es 11764. Para la primera instancia de Internet Explorer, el nombre del proceso es `iexplorer.exe` y su PID es 5620. Para la segunda instancia el nombre es el mismo, pero su PID es 5080.
- *¿Quiénes son los procesos padres de estos dos procesos (nombre y PID)?:* El padre el proceso de Word es `explorer.exe` y su PID es 11408. Mientras que, para los dos procesos de Internet Explorer, su padre es `iexplore.exe` con PID 1416.
- *¿Pasa algo raro con el Internet Explorer?:* Sí, hay una instancia de Internet Explorer que es padre de las otras dos instancias abiertas.

7. De los incisos anteriores, se observa que el proceso padre tanto de ProcessExplorer, como de Word, es el mismo proceso. ¿Qué función o funciones del Sistema Operativo realiza este proceso dentro de Windows?

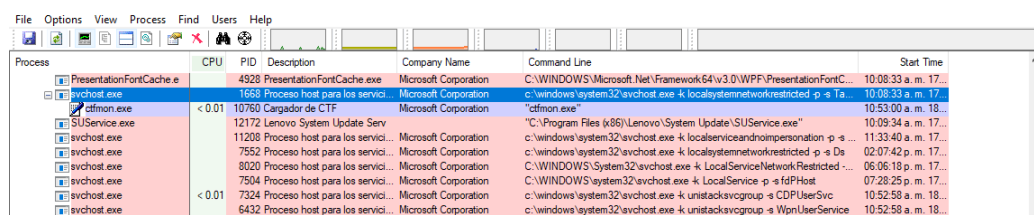
Las funciones que realiza dentro del sistema operativo son: interprete de comandos, administrador de procesos y administrador de archivos.

8. ¿Cuál es el tiempo de muestreo en este momento (Update Speed) y cuáles otras opciones de muestro hay?

Actualmente, se tiene una frecuencia de 1 segundo. Sin embargo, hay opciones de 0.5, 1, 2, 5, y 10 segundos.

9. ¿Es posible conocer el momento en que arrancó cada proceso? En caso que se pueda explique qué habría que hacer en ProcessExplorer para ver este valor, desplegar el pedazo de imagen donde se muestran estos dos valores para diez procesos.

Sí, es posible. Para lograrlo es necesario ir a la pestaña *View*, hacer clic en *Select Columns*, luego en la pestaña *Process Performance* y seleccionar la opción de *Start Time*. La figura 2 muestra el resultado.



Process	CPU	PID	Description	Company Name	Command Line	Start Time
PresentationFontCache.exe		4528	PresentationFontCache.exe	Microsoft Corporation	C:\WINDOWS\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontC...	10:08:33 a. m. 17...
svchost.exe		1668	Proceso host para los servi...	Microsoft Corporation	c:\windows\system32\svchost.exe -k localSystemNetworkRestricted -p -s Ta...	10:08:33 a. m. 17...
ctfmon.exe	< 0.01	10760	Cargador de CTF	Microsoft Corporation	"ctfmon.exe"	10:53:00 a. m. 18...
SUService.exe		12172	Lenovo System Update Serv...	Microsoft Corporation	"C:\Program Files (x86)\Lenovo\System Update\SUService.exe"	10:59:34 a. m. 17...
svchost.exe		11208	Proceso host para los servi...	Microsoft Corporation	c:\windows\system32\svchost.exe -k localServiceAndImpersonation -p -s ...	11:33:40 a. m. 17...
svchost.exe		7552	Proceso host para los servi...	Microsoft Corporation	c:\windows\system32\svchost.exe -k localSystemNetworkRestricted -p -s Ds...	02:07:42 p. m. 17...
svchost.exe		8020	Proceso host para los servi...	Microsoft Corporation	C:\WINDOWS\System32\svchost.exe -k LocalServiceNetworkRestricted ...	06:06:18 p. m. 17...
svchost.exe		7504	Proceso host para los servi...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe -k LocalService -p -s fdHost	07:28:25 p. m. 17...
svchost.exe	< 0.01	7324	Proceso host para los servi...	Microsoft Corporation	c:\windows\system32\svchost.exe -k unistacksvcgroup -s CDPUserSvc	10:52:58 a. m. 18...
svchost.exe		6432	Proceso host para los servi...	Microsoft Corporation	c:\windows\system32\svchost.exe -k unistacksvcgroup -s WpnUserService	10:52:58 a. m. 18...

Fig. 2: Ventana del programa Process Explorer con la opción de *Start Time*.

10. Seleccionando un proceso, con el botón derecho del mouse, mencionar qué operaciones básicas se pueden llevar a cabo sobre un proceso desde ProcessExplorer.

Las opciones son: Kill Process, Kill Process Tree, Restart, y Suspend.

11.

- ¿Cuál es el objetivo del proceso “System Idle Process” o “Proceso Inactivo del Sistema”? Es el porcentaje de CPU que no está siendo utilizado.

- ¿Cuál es su PID?: Su PID es 0.

12.

- ¿A qué se refiere, en la columna de procesos “Interrupts”? Es un proceso que mantiene la lista de procesos que están encolados.
- ¿Es un proceso?, ¿por qué?: Sí, sí es un proceso. Porque está en la columna de procesos del programa.

13. Vaciar toda la información desplegada por ProcessExplorer sobre los procesos en un archivo de texto. ¿Cómo llevó a cabo esta actividad?

En el menú de *File*, dar clic en *Save As* y seleccionar el directorio donde se guardará el archivo.

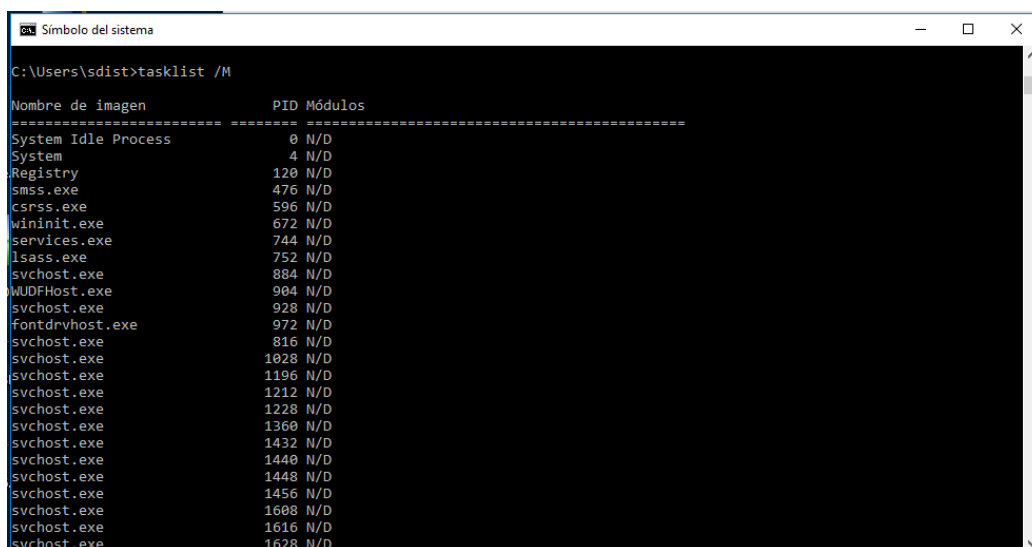
14. ¿Cómo nota usted la relación jerárquica padre-hijo, en el archivo de texto?

Por la indentación del archivo.

15. Cambiar al ámbito de la ventana DOS por medio del comando CMD.

- *¿Cuál es la utilidad del comando “tasklist”?:* Muestra los procesos, su PID, el nombre de la sesión, el número de la sesión, y el uso de memoria.
- *Explicar la funcionalidad de este comando para dos de sus diferentes parámetros.:* En primer lugar probamos, `tasklist /M` que devuelve la lista de archivos y extensiones `.dll` para cada proceso. En segundo lugar, el comando `tasklist /FO CSV` el cual lista la información de los procesos en formato CSV, valores separados por comas.

La figura 3 muestra el resultado del comando `tasklist /M`, y la figura 4 muestra el resultado del comando `tasklist /FO CSV`.



```
C:\Users\sdist>tasklist /M

Nombre de imagen          PID  Módulos
=====
System Idle Process       0    N/D
System                    4    N/D
Registry                  120  N/D
smss.exe                  476  N/D
csrss.exe                 596  N/D
wininit.exe               672  N/D
services.exe              744  N/D
lsass.exe                 752  N/D
svchost.exe               884  N/D
WUDFHost.exe              904  N/D
svchost.exe               928  N/D
fontdrvhost.exe           972  N/D
svchost.exe               816  N/D
svchost.exe              1028  N/D
svchost.exe              1196  N/D
svchost.exe              1212  N/D
svchost.exe              1228  N/D
svchost.exe              1360  N/D
svchost.exe              1432  N/D
svchost.exe              1440  N/D
svchost.exe              1448  N/D
svchost.exe              1456  N/D
svchost.exe              1608  N/D
svchost.exe              1616  N/D
svchost.exe              1628  N/D
```

Fig. 3: Resultado del comando `tasklist /M`.

```

C:\Users\sdist>tasklist /FO CSV
"Nombre de imagen","PID","Nombre de sesión","Núm. de sesión","Uso de memoria"
"System Idle Process","0","Services","0","8 KB"
"System","4","Services","0","140 KB"
"Registry","120","Services","0","43,472 KB"
"smss.exe","476","Services","0","1,132 KB"
"csrss.exe","596","Services","0","5,728 KB"
"wininit.exe","672","Services","0","7,028 KB"
"services.exe","744","Services","0","14,248 KB"
"lsass.exe","752","Services","0","23,136 KB"
"svchost.exe","884","Services","0","3,868 KB"
"WUDFHost.exe","904","Services","0","8,172 KB"
"svchost.exe","928","Services","0","37,268 KB"
"fontdrvhost.exe","972","Services","0","4,148 KB"
"svchost.exe","816","Services","0","16,448 KB"
"svchost.exe","1028","Services","0","9,508 KB"
"svchost.exe","1196","Services","0","11,620 KB"
"svchost.exe","1212","Services","0","7,460 KB"
"svchost.exe","1228","Services","0","8,728 KB"
"svchost.exe","1360","Services","0","7,020 KB"
"svchost.exe","1432","Services","0","15,840 KB"
"svchost.exe","1440","Services","0","11,684 KB"
"svchost.exe","1448","Services","0","10,040 KB"
"svchost.exe","1456","Services","0","8,704 KB"
"svchost.exe","1608","Services","0","9,308 KB"
"svchost.exe","1616","Services","0","5,888 KB"
"svchost.exe","1628","Services","0","7,824 KB"
"svchost.exe","1692","Services","0","11,848 KB"
"svchost.exe","1756","Services","0","26,928 KB"
"svchost.exe","1828","Services","0","9,348 KB"

```

Fig. 4: Resultado del comando `tasklist /FO CSV`.

16. Cambiar al ámbito de la ventana DOS por medio del comando CMD.

- *¿Cuál es la utilidad del comando `wmic`?*: Activa la interfaz de línea de comandos del sistema de instrumentación de Windows Management.
- *Aplicar el comando `wmic` con los siguientes parámetros y explicar lo desplegado: `wmic process get description, processid, parentprocessid, commandline, osname`*: Despliega en línea de comando, los distintos procesos que se encuentran. El comando nos permite mostrar la descripción, el id del proceso, su padre, el sistema operativo y la línea de comando.
- *Aplique el comando `wmic` con los siguientes parámetros y explicar lo desplegado: `wmic memorychip get description, manufacturer, banklabel, capacity`*: Despliega la información de la memoria RAM y su uso.
- *¿Cuál es el tamaño total de la memoria, expresado en gigabytes?*: El comando muestra dos memorias de 8.589934592 Gigabytes cada una. El tamaño total es de 16 GB.

Conclusiones

En esta práctica comenzamos a familiarizarnos con el programa *Process Explorer* y con ello se logró afianzar los conceptos sobre procesos vistos en clase. El uso de este programa y de los comandos `tasklist` y `wmic` nos permitió comprender la utilidad y las diferencias de cada uno para analizar a fondo los procesos que se están ejecutando en la computadora así como la forma en que la información obtenida puede ser usada. También se pudieron observar las distintas características, acciones y valores asociados a un proceso y la jerarquía en que se encuentra. En conclusión, todo esto facilitó un primer acercamiento a los sistemas operativos y sus funciones de gestión.

Referencias

- [1] “Windows Management Instrumentation,” 2018, [Accedido el 24-01-2019]. [Online]. Available: <https://docs.microsoft.com/en-us/windows/desktop/wmisdk/wmi-start-page>