

INSTITUTO TECNOLÓGICO AUTÓNOMO DE MÉXICO
PRÁCTICAS de SISTEMAS OPERATIVOS

PRÁCTICA #1

<Información de procesos, en Windows>

Grupo

<G5>

Integrantes

<Rebeca Baños García – 157655>

<Víctor Hugo Flores Pineda– 155990>

<Humberto Martínez Barrón y Robles – 166056>

Fecha (s) de elaboración de la práctica

<28 de enero del 2020>

Práctica 01

Información de procesos, en Windows.

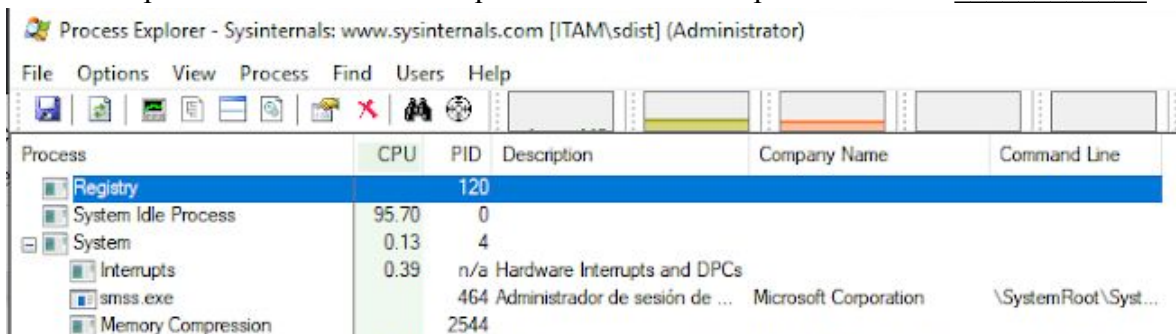
INDICACIONES SOBRE EL DESARROLLO

En los puntos que sigue, donde aparece _____, tendrá que explicar con detalle cómo logró llevar a cabo lo pedido, indicando trayectorias, comandos, cálculos y / o acciones realizadas. En el caso de despliegue de comandos explique el significado de lo desplegado.

DESARROLLO

- 1) Usaremos la aplicación *ProcessExplorer*, que instalamos el martes (matAA) pasado, que es un software para administrar procesos al estilo del *Task Manager de Windows* o *Administrador de Tareas*.
- 2) Ejecute *procexp64.exe* en modo “Ejecutar como administrador”, abriéndose la aplicación. Una de las ventajas de esta aplicación es que muestra la relación padre – hijo entre los procesos, de manera arborescente. En caso de no estar seleccionado la facilidad del despliegue arborescente asegúrese mediante *View->Show Process Tree*, que activa esta facilidad.
- 3) Haga lo necesario para que *ProcessExplorer* despliegue las siguientes columnas, mediante el menu *View->Select Columns*. en las diferentes pestañas *Process Image*, *Process Performance* y *Process Memory*.:
 - Process – nombre del proceso, _____
 - PID (Process ID) – Identificación del proceso ante el sistema operativo _____
 - CPU usage – porcentaje de uso del proceso en un momento dado _____
 - Description - Breve descripción sobre la funcionalidad del proceso _____
 - Company name – Compañía del fabricante del software del proceso _____
 - Command Line – Línea de comando ejecutada para arrancar el proceso _____

Si aparecen columnas extras quítelas con el mismo procedimiento. _____



- 4) Ahora despliegue 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. _____

Process Explorer - Sysinternals: www.sysinternals.com [ITAM\sdist] (Administrator)

Process	CPU	PID	Description	Company Name	Command Line
Registry		120			
System Idle Process	96.92	0			
System	0.09	4			
Interrupts	0.31	n/a	Hardware Interrupts and DPCs		
smss.exe		464	Administrador de sesión de ...	Microsoft Corporation	\SystemRoot\Syst...
Memory Compression		2544			
csrss.exe	< 0.01	708	Proceso en tiempo de ejecu...	Microsoft Corporation	%SystemRoot%\s...
wininit.exe		796	Aplicación de inicio de Wind...	Microsoft Corporation	wininit.exe
services.exe	< 0.01	868	Aplicación de servicios y con...	Microsoft Corporation	C:\Windows\syst...
svchost.exe		552	Proceso host para los servi...	Microsoft Corporation	C:\Windows\syst...
svchost.exe		732	Proceso host para los servi...	Microsoft Corporation	C:\Windows\syst...
WmiPrvSE.exe		8468	WMI Provider Host	Microsoft Corporation	C:\Windows\syst...
WmiPrvSE.exe		14108	WMI Provider Host	Microsoft Corporation	C:\Windows\syst...
WmiPrvSE.exe		13708	WMI Provider Host	Microsoft Corporation	C:\Windows\syst...
dhllhost.exe		10744	COM Surrogate	Microsoft Corporation	C:\WINDOWS\S...
WmiPrvSE.exe		2868	WMI Provider Host	Microsoft Corporation	C:\Windows\syst...
ShellExperienceHost...	Susp...	9328	Windows Shell Experience H...	Microsoft Corporation	"C:\Windows\Sys...
dhllhost.exe		10444	COM Surrogate	Microsoft Corporation	C:\WINDOWS\S...
SearchUI.exe	Susp...	8148	Search and Cortana applicati...	Microsoft Corporation	"C:\Windows\Sys...
RuntimeBroker.exe		3680	Runtime Broker	Microsoft Corporation	C:\Windows\Syst...
RuntimeBroker.exe		11920	Runtime Broker	Microsoft Corporation	C:\Windows\Syst...
RuntimeBroker.exe		13608	Runtime Broker	Microsoft Corporation	C:\Windows\Syst...
RuntimeBroker.exe		6728	Runtime Broker	Microsoft Corporation	C:\Windows\Syst...
dhllhost.exe		2148	COM Surrogate	Microsoft Corporation	C:\WINDOWS\S...
ApplicationFrameHost...		14712	Application Frame Host	Microsoft Corporation	C:\Windows\syst...
WinStore.App.exe	Susp...	13356	Store	Microsoft Corporation	"C:\Program Files...
dhllhost.exe		8260	COM Surrogate	Microsoft Corporation	C:\WINDOWS\S...
SystemSettings.exe	Susp...	15784	Configuración	Microsoft Corporation	"C:\Windows\Im...
WindowsInternal.Com...	Susp...	10192	WindowsInternal Composabl...	Microsoft Corporation	"C:\Windows\Sys...
svchost.exe		1100	Proceso host para los servi...	Microsoft Corporation	C:\Windows\syst...

- 5) ¿Cuál es el PID del proceso *ProcessExplorer*? 16132
 ¿Cómo se llama el proceso que es padre del *ProcessExplorer*? explorer.exe y ¿cuál su respectivo PID? 10364
 Despliegue la línea de comando de *ProcessExplorer*: "C:\Sistemas Operativos\matAA\procexp64.exe"
- 6) Si tiene abiertos programas de Internet Explorer por favor ciérrelos. Ahora arranque los programas WORD e Internet Explorer, también arranque una segunda instancia de Internet Explorer, ¿cuáles son sus respectivos nombres de proceso y PID?
WORD: WINWORD.EXE 8832
INTERNET EXPLORER 1: ieexplore.exe 12072
INTERNET EXPLORER 2: ieexplore.exe 4324
 ¿Quiénes son los procesos padres de estos dos procesos (nombre y PID)? ieexplore.exe 9112
 ¿Pasa algo raro con el Internet Explorer? Ambos procesos, así como el padre, tienen el mismo nombre.
- 7) De los incisos anteriores, vemos 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? explorer.exe. Actúa como:
 Command Interpreter
 Process Manager
 File Manager

- 8) Ahora cierre tanto Word como los Internet Explorer. Abra el browser Chrome. ¿Qué diferencia nota comparado con el Internet Explorer? El padre de Chrome tiene más hijos que ventanas o pestañas ejecutadas.
- 9) ¿Cuál es el tiempo de muestreo en este momento (Update Speed)? 1 segundo Cuáles otras opciones de muestreo hay? 0.5, 2, 5 y 10 segundos
- 10) ¿Es posible conocer el momento en que arrancó cada proceso? Sí En caso que se pueda explique que habría que hacer en *ProcessExplorer* para ver este valor: Agregar la columna de Start Time en View->Select Columns->Process Performance->Start Time. En caso de ser factible, despliegue el pedazo de imagen donde se muestran estos dos valores para diez procesos.

Process Explorer - Sysinternals: www.sysinternals.com [ITAM\sdist] (Administrator)

File Options View Process Find Users Help

Process	CPU	PID	Description	Company Name	Command Line	Start Time
Registry		120				07:04:53 p. m. 27...
System Idle Process	95.29	0				07:04:55 p. m. 27...
System	0.06	4				07:04:55 p. m. 27...
csrss.exe	< 0.01	708	Proceso en tiempo de ejecu...	Microsoft Corporation	%SystemRoot%\s...	07:04:58 p. m. 27...
wininit.exe		796	Aplicación de inicio de Wind...	Microsoft Corporation	wininit.exe	07:04:59 p. m. 27...
csrss.exe	0.07	2016	Proceso en tiempo de ejecu...	Microsoft Corporation	%SystemRoot%\s...	01:00:26 p. m. 28...
winlogon.exe		12956	Aplicación de inicio de sesi...	Microsoft Corporation	winlogon.exe	01:00:26 p. m. 28...
explorer.exe	0.23	10364	Explorador de Windows	Microsoft Corporation	C:\Windows\Expl...	01:11:56 p. m. 28...
SecurityHealthSystray.exe		14140	Windows Security notificatio...	Microsoft Corporation	"C:\Windows\Sys...	01:12:09 p. m. 28...
Skd8821.exe		11772	Lenovo Slim USB Keyboard	LITE-ON TECHNOLOGY ...	"C:\Program Files...	01:12:10 p. m. 28...
hAgentTray.exe	0.01	224				01:12:11 p. m. 28...
OneDrive.exe		8212	Microsoft OneDrive	Microsoft Corporation	"C:\Users\sdist.IT...	01:12:11 p. m. 28...
Docker Desktop.exe		2220	Docker Desktop	Docker Desktop	"C:\Program Files...	01:12:14 p. m. 28...
chrome.exe	0.29	12676	Google Chrome	Google LLC	"C:\Program Files ...	01:16:20 p. m. 28...
WINWORD.EXE	< 0.01	8832	Microsoft Word	Microsoft Corporation	"C:\Program Files...	02:10:19 p. m. 28...
procexp64.exe	0.62	16132	Sysinternals Process Explorer	Sysinternals - www.sysinter...	"C:\Sistemas Ope...	02:15:38 p. m. 28...
usched.exe		10616	Java Update Scheduler	Oracle Corporation	"C:\Program Files ...	01:12:17 p. m. 28...
jucheck.exe		15372	Java Update Checker	Oracle Corporation	"C:\Program Files ...	01:17:17 p. m. 28...
NSConnSvrUI.exe		12668	NetSupport gateway dll	NetSupport Ltd	"C:\Program Files ...	01:12:17 p. m. 28...
DSATray.exe	0.03	6928	Intel Driver & Support Assista...	Intel	"C:\Program Files ...	01:12:18 p. m. 28...
IAStorIcon.exe	< 0.01	13396	IAStorIcon	Intel Corporation	"C:\Program Files...	01:13:10 p. m. 28...
PrivacyIconClient.exe	0.02	4180	Intel(R) Management and Se...	Intel Corporation	"C:\Program Files ...	01:15:16 p. m. 28...

- 11) Seleccionando un proceso, con el botón derecho del mouse, diga qué operaciones básicas se pueden llevar a cabo sobre un proceso desde *ProcessExplorer*. Set Affinity, Set Priority, Kill Process, Kill Process Tree, Restart, Suspend, Debug, Create Dump, Check Virus Total, Properties, Search Online
- 12) ¿Cuál es el objetivo del proceso "System Idle Process" o "Proceso Inactivo del Sistema"? Describa: Es dónde checas el tiempo en el que el procesador no está haciendo nada. ¿Cuál es su PID? 0.
- 13) ¿A qué se refiere, en la columna de procesos, "Interrupts"? Hardware Interrupts y DPC (Differ Procedure Call). Permite diferenciar los procesos de importancia alta a los de importancia baja. ¿Es un proceso? No. Si o no, ¿por qué? Porque no tiene ID de Proceso (PID=n/a).
- 14) Vacíe toda la información desplegada por *ProcessExplorer* sobre los procesos en un archivo de texto que entregara adjunto a este reporte. ¿Cómo llevo a cabo esta actividad? File>Save as> .txt

- 15) ¿Cómo nota usted la relación jerárquica padre-hijo, en el archivo de texto? Describa: Con sangrías, cuando esta un proceso abajo de otro con más sangría significa que es un hijo.
- 16) Cambiando al ámbito de la ventana DOS por medio del comando CMD.
 ¿Cuál es la utilidad del comando “tasklist”? Te despliega la lista de procesos con las siguientes columnas:
- Nombre de imagen (equivalente a nombre de proceso en process explorer)
 - PID
 - Nombre de sesión
 - Número de sesiones
 - Uso de memoria

Además explique la funcionalidad de este comando para dos de sus diferentes parámetros.

/s <Computer>: Nombre o dirección IP de una computadora robot. Si no se especifica se inicializa en el IP de la computadora actual.

/u <Username>: Va a correr el comando con los permisos de cuenta del usuario especificado en username. Si no se especifica se usan los permisos del usuario actual, es decir, el que está corriendo el comando.

Para ayuda de parámetros en la ventana aplique “tasklist /?” También se puede ayudar en la Web. Muestre despliegues del uso del comando.

```

C:\Windows\system32>tasklist /?

TASKLIST [/S sistema [/U usuario [/P [contraseña]]] [/M [modulo] | /SVC | /V] [/FI filtro] [/FO formato] [/NH]]

Descripción:
  Esta herramienta muestra una lista de procesos que se están ejecutando
  en un equipo local o remoto.

Lista de parámetros:
/S sistema      Especifica el sistema remoto al que conectarse.
/U [dominio]usuario Especifica el contexto de usuario en el que
                  el comando debe ejecutarse.
/P [contraseña]  Especifica la contraseña para el contexto
                  de usuario dado. Pide entrada si se omite.
/M [module]      Enumera todas las tareas que actualmente usan
                  el nombre exe/dll dado. Si el nombre del módulo
                  no se especifica, se muestran todos los módulos
                  cargados.
/SVC             Muestra los servicios hospedados en cada proceso.
/APPS           Muestra las aplicaciones de Store y sus procesos asociados.
/V             Muestra información detallada de tareas.
/FI filtro      Muestra un conjunto de tareas que coinciden
                  con el criterio especificado por el filtro.
/FO formato      Especifica el formato de salida.
                  Valores válidos: "TABLE", "LIST", "CSV".
/NH            Especifica que el "encabezado de columna"
                  no debe mostrarse en la salida.
                  Válido solo para formatos "TABLE" y "CSV".
/?             Muestra este mensaje de ayuda.

Filtros:
  Nombre filtro  Operadores válidos  Valores válidos
  -----
STATUS          eq, ne          RUNNING | SUSPENDED
                  NOT RESPONDING | UNKNOWN
IMAGENAME        eq, ne          Nombre de imagen
PID              eq, ne, gt, lt, ge, le Valor del PID
SESSION          eq, ne, gt, lt, ge, le Número de sesión
SESSIONNAME      eq, ne          Nombre de sesión
CPUTIME          eq, ne, gt, lt, ge, le Tiempo de la CPU en el formato
                  hh:mm:ss.
MEMUSAGE         eq, ne, gt, lt, ge, le Uso de memoria en KB
USERNAME        eq, ne          Nombre de usuario en formato
                  [dominio]usuario
SERVICES         eq, ne          Nombre de servicio
WINDOWTITLE     eq, ne          Título de ventana
MODULES         eq, ne          DLL name

NOTA: los filtros "WINDOWTITLE" y "STATUS" no se tienen en cuenta cuando se consultan
equipos remotos.

Ejemplos:
TASKLIST
TASKLIST /M
TASKLIST /V /FO CSV
  
```

- 17) Cambiando al ámbito de la ventana DOS por medio del comando CMD.
¿Cuál es la utilidad del comando “*wmic*”? Permite a los usuarios hacer operaciones de Windows Management Instrumentation (WMI) desde el ámbito de la ventana DOS.
“*wmic*” significa *Windows Management Instrumentation Console*.
Aplique el comando *wmic* con los siguientes parámetros y explique lo desplegado
- *>wmic process get description*: Despliega las descripciones de todos los procesos que están corriendo.
 - *processid*: Despliega los ID de los procesos que se están ejecutando.
 - *parentprocessid*: Despliega los ID de los padres de cada proceso.
 - *commandline*: Despliega las líneas de comando de los procesos que la tienen disponible. Los que no tienen una línea de comando disponible se representan con espacios en blanco.
 - *osname*: Dice el sistema operativo, el dispositivo y la partición a la que pertenece ese proceso.
- 18) Manteniéndose en la ventana de DOS.
Aplique el comando *wmic* con los siguientes parámetros y explique lo desplegado
- *>wmic memorychip get description*: Despliega la descripción del chip de memoria, en este caso ambos chips de memoria parecen ser de memoria física.
 - *manufacturer*: La empresa manufacturera del chip de memoria, en este caso ambas son Samsung.
 - *banklabel*: Muestra la etiqueta del banco físico donde se encuentra la memoria.
 - *capacity*: Muestra la capacidad del chip de memoria en bytes.
- Además ¿Cuál es el tamaño total de la memoria, expresado en gigabytes? 8 Gigabytes
Muestre como de los desplegados hace la conversión para el cálculo final en GBytes. 1 Gbyte=2³⁰ Bytes
- 19) Al final forme un archivo zip con este reporte, el archivo de texto, y súbalo a Comunidad en la parte del Exámenes y Tareas. El nombre del reporte y del zip seguirán el formato de la Guía de Reportes.