

## **Practica: 2.1 Procesos en Windows**

### **Sistemas Operativos – Kevin Zamora Amela**

Un proceso puede definirse como un programa en ejecución. Los sistemas operativos multitarea, como Windows, permiten la ejecución simultánea de múltiples procesos. En estos sistemas, la CPU se va repartiendo entre los diferentes procesos, de modo que todos ellos se vayan ejecutando en “tiempo compartido”. Para observar y llevar el control de los procesos que se encuentran en ejecución en el sistema, Windows proporciona una herramienta denominada *Administrador de tareas*. Ahora, utilizando esta herramienta, vamos a observar algunos procesos muy importantes que están presentes en todo sistema Windows.

El administrador de tareas de Windows se puede ejecutar desde el comando taskmgr o desde la unión de las teclas Ctrl+Alt+Supr, aparece directamente la opción administrador de tareas.

Aparecen los procesos en segundo plano y las opciones más importantes aparecen **más detalles**. Las pestañas, las más importantes para nosotros serán procesos, usuarios y detalles.

En la segunda pestaña aparecen los procesos, una serie de características de los procesos, por defecto, el nombre del ejecutable, el propietario, los ciclos de CPU y el uso de memoria. Desde el menú ver seleccionar columnas, pueden verse muchos mas datos de los procesos como por ejemplo el PID del proceso.

1. Escoge una aplicación que tengas abierta (por ejemplo, chrome) y descubre características de ese proceso en ir al detalle. Anota las siguientes características.

Aplicación: **Mozilla Firefox**

Nombre del proceso: **Firefox**

PID del proceso: **5888, 352, 3192, 7668, 1160, 52, 3828, 2060,1492**

Estado: **Running**

## SI02

2. Aparecen procesos de sistema y de usuario. Sobre los procesos de sistema (System), no pueden ser modificados (terminarlos o cambiarles la prioridad). Hay procesos de sistema que deben estar ejecutándose, por ejemplo, el proceso Winlogon, controla las sesiones de usuario. Anota

PID WINLOGON:

¿Tiene un PID grande o pequeño con respecto al resto?

**Un PID pequeño, concretamente el 552.**

¿A qué se debe?

**Se relaciona con la prioridad y el orden de ejecución de la tarea/proceso que se encuentra en ejecución, almacenado y procesado mediante este, mejor dicho: nos indica el orden en el que las diferentes tareas/procesos se han ido ejecutando desde el arranque de nuestro sistema operativo.**

Intenta terminar el proceso. ¿Qué ocurre?

**Se cierra la sesión, nos redirige a la pantalla de inicio de sesión, nos requiere volver a iniciar una nueva sesión y se reinicia el proceso winlogon.exe, supuesta y teóricamente. Acto seguido, procedemos a comprobar si dicha tarea sigue localizándose y procesándose mediante el mismo PID (552); Tras dicha comprobación, confirmamos que dicha tarea ha cambiado de PID: ahora se localiza en el PID número 6868.**

3. Otro proceso importante es Explorer.exe, que gestiona la interfaz gráfica del sistema.

PID Explorer:

**PID → 2840**

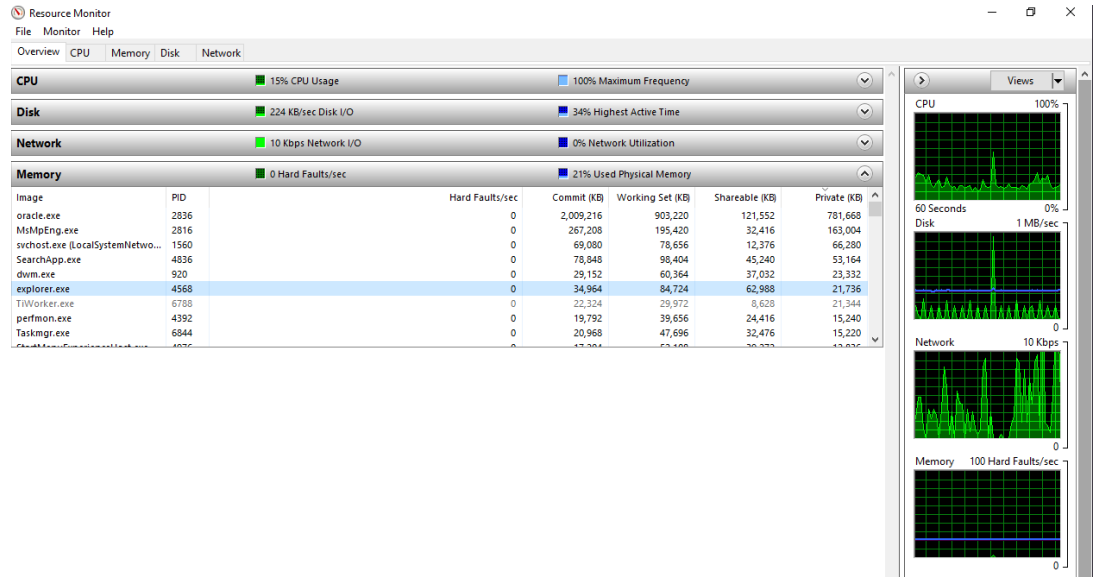
¿Qué ocurre al terminar el proceso?

**Se cierra el entorno gráfico principal de nuestro Windows 10 y sólo se mantienen abiertas las ventanas de navegación que teníamos abiertas, quedándose “bloqueado” desde nuestro punto de vista y sin permitirnos realizar apenas ninguna opción para lograr actuar sobre nuestro sistema operativo.**

Reinicia de nuevo el Explorador de Windows, el Explorer.exe. ¿Qué PID tiene ahora? **Ahora tiene el 4568 ¿Es el mismo? No.**

1. Los procesos usan memoria, característica que figura en una columna del administrador de tareas. Mira el proceso Explorer.exe y apunta cuanta memoria está usando en este instante.

Memoria utilizada:  $34,964 + 84,724 + 62,988 + 21,736 = 204,412 \text{ KB}$



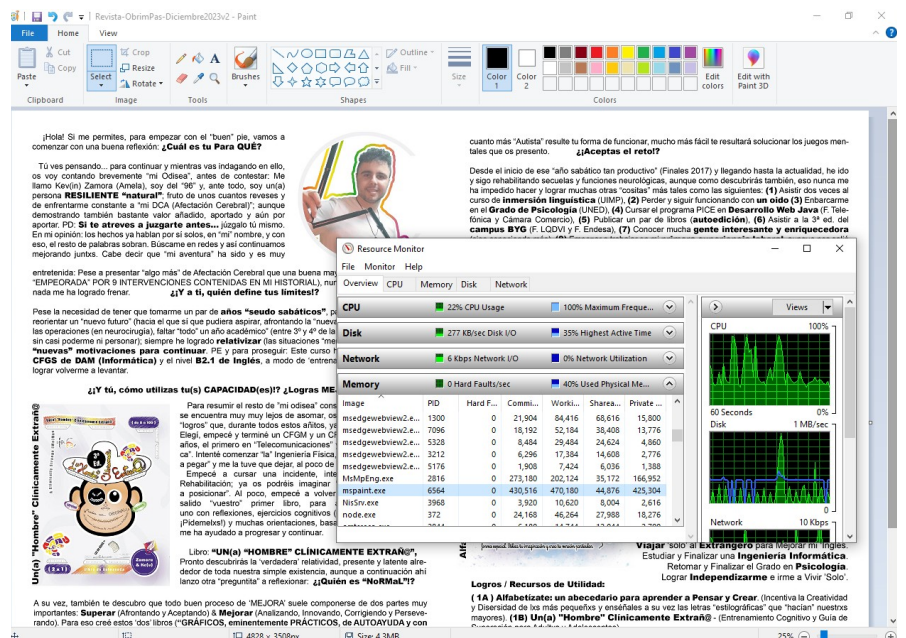
Abre un paint sin ningún archivo y anota cuanta memoria utiliza y ahora abre una imagen desde paint, y anota cuanto ocupa ahora.

Memoria Paint (antes):

$9.592 + 31.412 + 22.940 + 8.472 = 72.416 \text{ KB}$

Memoria Paint (después):

$430.516 + 470.180 + 44.876 + 425.304 = 1.370,876 \text{ KB}$



2. Un mismo programa puede generar varios procesos, por ejemplo, el bloc de notas, genera un proceso notepad.exe, cada vez que se ejecuta. Ejecuta 2 veces Bloc de notas y anota los PID de los procesos.

PID: **2588**

PID: **2448**

Prueba desde el bloc de notas a abrir un nuevo documento. ¿Qué ocurre?

Este nuevo archivo/documento también tiene asignado otro PID: **6976**

Pero también existen programas que emplean hilos o hebras (característica que permite a una aplicación realizar varias tareas concurrentemente), donde un solo proceso puede tener varias aplicaciones abiertas.

3. Abre varios documentos Word, ¿Cuántos procesos Winword.exe están ejecutándose? También hay varios (2 archivos y 2 procesos Winword.exe)

¿Cómo se puede explicar eso?

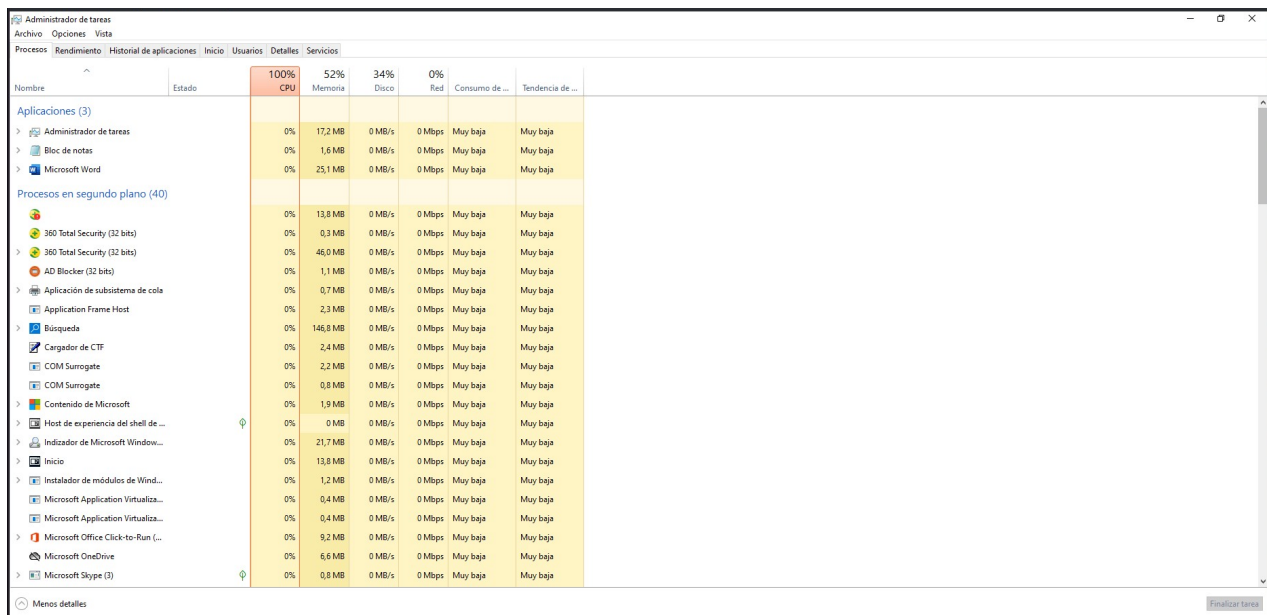
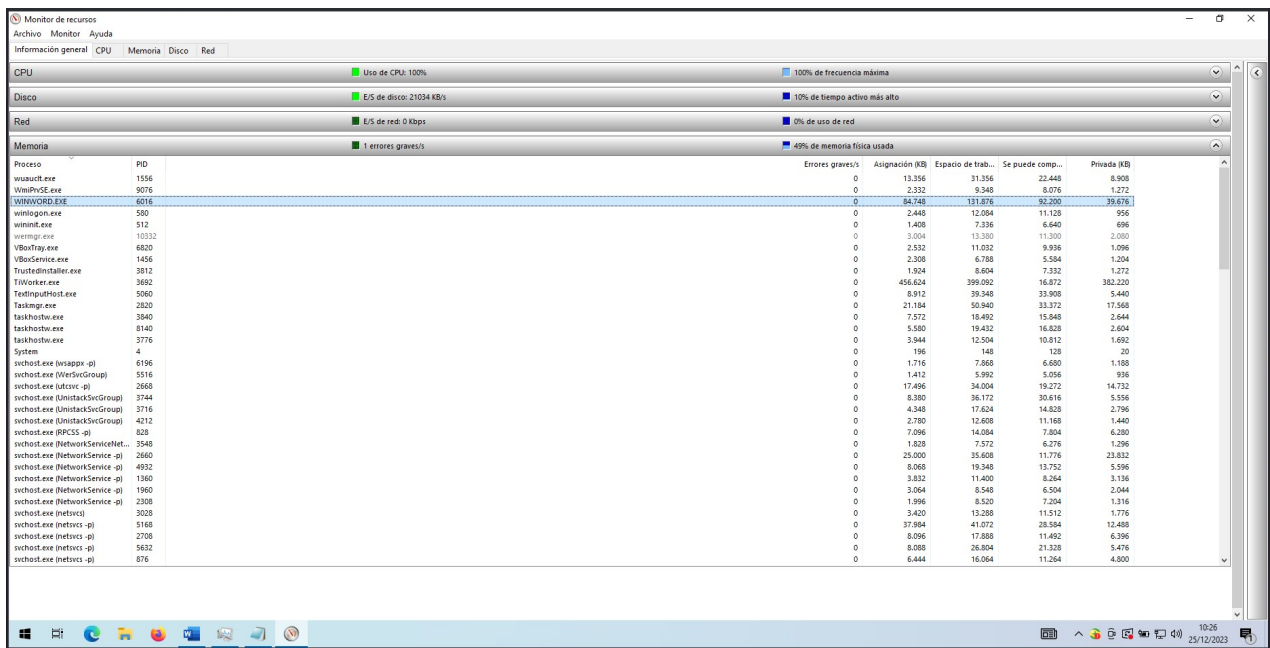
**Esto sucede debido a que cada archivo, cada ventana, se ejecuta de forma independiente, como 'dos' procesos diferentes. De esta forma, logramos dividir la carga del procesamiento y manipulación de estos incidente sobre nuestra CPU y a su vez, esta resulta capaz de gestionar mejor los recursos de nuestro PC y balancearlos entre ellos y en consecuencia, según los que requiera cada tarea y siguiendo también cierto orden de prioridad de ejecución.**

Ejecuta el programa bloc de notas y un solo documento Word y mira cuanta memoria usa cada uno.

Bloc de notas:

Proceso	PID	CPU	Memoria Privada (KB)	Conjunto de trabajo (KB)
ApplicationFrameHost.exe	3076	0	25,668	23,092
AppHostHelper.exe	10016	0	1,700	8,152
AppHostHelper.exe	9980	0	1,592	7,420
backgroundTaskHost.exe	4536	0	3,612	16,540
backgroundTaskHost.exe	10832	0	5,208	16,424
backgroundTaskHost.exe	6660	0	2,220	11,612
csrss.exe	520	0	2,156	5,776
csrss.exe	444	0	1,672	5,712
csrss.exe	4040	0	3,972	20,792
dllhost.exe	10932	0	3,328	12,436
dllhost.exe	5540	0	3,204	11,504
dmoc.exe	952	0	51,712	113,844
explorer.exe	3316	0	70,172	181,456
fontdrvhost.exe	732	0	3,776	9,284
fontdrvhost.exe	740	0	1,272	3,500
GenHost.exe	8964	0	3,360	10,896
lsass.exe	616	0	8,412	20,972
Memory Compression	1612	0	92	2,624
ModHost.exe	5704	0	26,860	50,828
MustacheHost.exe	10656	0	4,372	316
notepad.exe	9736	0	2,700	15,732
OfficeClickToRun.exe	3732	0	28,464	55,140
OneDrive.exe	9952	0	41,084	103,306
perfmom.exe	9444	0	79,504	102,752
PopUp.exe	6100	0	736	2,392
PopUp.exe	7420	0	8,296	22,604
QHActiveDefense.exe	2000	0	92,364	120,164
QHSafeRay.exe	7336	0	33,116	70,156
QHVatHost.exe	3436	0	920	5,300
Registry	72	0	10,404	137,928
RuntimeBroker.exe	5972	0	13,244	43,728
RuntimeBroker.exe	5392	0	5,600	24,512
RuntimeBroker.exe	6992	0	4,504	22,276
RuntimeBroker.exe	3372	0	2,376	15,728

WORD:



## SI02

Ahora abre 10 documentos con el bloc de notas y 10 archivos Word (pueden ser en blanco) y mira cuanta memoria ocupa todos los bloc de notas juntos y todos Word juntos.

10 Bloc de notas:

Proceso	PID	Errores graves/s	Asignación (KB)	Espacio de trab...	Se puede comp...	Privada (KB)
ApplicationFrameHost.exe	3076	0	4.860	25.668	23.092	2.576
AppVSNHost.exe	10016	0	1.700	8.152	7.264	888
AppVSNHost.exe	9980	0	1.592	7.420	6.544	876
backgroundTaskHost.exe	10832	1	5.260	17.696	15.784	1.912
backgroundTaskHost.exe	4536	0	3.612	15.396	13.492	1.904
csrss.exe	520	0	2.140	5.584	4.888	696
csrss.exe	444	0	1.672	5.516	4.804	592
ctfmon.exe	4048	0	4.224	21.112	17.592	3.520
dllhost.exe	10932	0	3.276	12.440	10.552	1.888
dllhost.exe	5540	0	3.204	11.504	10.368	1.116
dwm.exe	952	0	141.732	223.336	91.672	131.664
explorer.exe	3316	0	71.148	182.564	131.712	50.852
fontdrvhost.exe	732	0	3.888	9.100	6.364	2.736
fontdrvhost.exe	740	0	1.272	2.816	2.564	252
GenuineUI.exe	8964	0	3.360	10.896	7.936	2.960
lsass.exe	616	0	8.488	19.148	14.520	4.628
Memory Compression	1612	0	92	2.044	0	2.044
MusNotifCon.exe	5704	0	26.560	50.828	26.968	23.060
MusNotifCon.exe	10656	0	4.372	352	256	96
notepad.exe	9736	0	3.700	24.456	22.088	2.368
notepad.exe	10336	0	3.676	24.088	21.732	2.356
notepad.exe	544	0	3.664	24.088	21.736	2.352
notepad.exe	4584	0	3.684	24.084	21.732	2.352
notepad.exe	9200	0	3.676	24.080	21.728	2.352
notepad.exe	4112	0	3.680	24.128	21.776	2.352
notepad.exe	9144	0	3.676	24.068	21.720	2.348
notepad.exe	3608	0	3.680	24.084	21.736	2.348
notepad.exe	8976	0	3.672	24.076	21.732	2.344
notepad.exe	5364	0	3.660	14.320	12.448	1.672
OfficeClickToRun.exe	3732	0	28.676	55.836	35.320	20.516
OneDrive.exe	9952	0	41.076	103.292	80.336	22.956
perfmon.exe	9444	0	84.456	107.816	25.320	81.088
PopWinLog.exe	7460	0	8.264	22.612	18.364	4.248
QHActiveDefense.exe	2000	0	93.544	119.824	51.168	68.656

10 Word:

Nombre	Estado	100% CPU	51% Memoria	40% Disco	0% Red	Consumo de ...	Tendencia de ...
<b>Aplicaciones (12)</b>							
Administrador de tareas		0%	17,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	1,6 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,2 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,2 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,2 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,2 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Microsoft Word		0%	70,7 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
<b>Procesos en segundo plano (38)</b>							
360 Total Security (32 bits)		0%	14,0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
360 Total Security (32 bits)		0%	0,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
360 Total Security (32 bits)		3,1%	45,6 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
AD Blocker (32 bits)		0%	1,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Aplicación de subsistema de cola		0%	0,7 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Application Frame Host		0%	2,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Búsqueda		0%	143,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Cargador de CTF		0%	2,4 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
COM Surrogate		0%	1,8 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
COM Surrogate		0%	0,8 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Contenido de Microsoft		0%	1,9 MB	0 MB/s	0 Mbps	Muy baja	Muy baja

Monitor de recursos					
Archivo Monitor Ayuda					
Información general CPU Memoria Disco Red					
CPU		Uso de CPU: 100%		100% de frecuencia máxima	
Disco		E/S de disco: 14939 KB/s		38% de tiempo activo más alto	
Red		E/S de red: 0 Kbps		0% de uso de red	
Memoria		0 errores graves/s		50% de memoria física usada	
Proceso	PID	Errores graves/s	Asignación (KB)	Espacio de trab...	Se puede comp...
svchost.exe	1556	0	13.356	31.356	22.448
WmiPvse.exe	9076	0	2.328	9.088	8.076
WINWORD.EXE	6016	0	87.024	154.568	82.844
winlogon.exe	580	0	2.448	11.748	11.128
svchost.exe	512	0	1.408	7.632	6.640
VBoxTray.exe	6820	0	2.556	10.748	9.940
VBoxService.exe	1456	0	2.304	6.552	5.584
Trustcmdstales.exe	3812	0	1.904	8.600	7.332
TIWorker.exe	3892	0	483.932	417.544	16.888
TextinputHost.exe	5060	0	8.960	37.540	34.060
Taskmgr.exe	2820	0	21.284	47.692	33.504
taskhost.exe	3840	0	7.572	18.288	15.848
taskhost.exe	8140	0	5.316	16.180	14.032
taskhost.exe	3776	0	3.944	12.468	10.812
System	4	0	196	148	128
svchost.exe (svsappx -p)	8524	0	1.704	7.860	6.680
svchost.exe (utconv -p)	2668	0	17.540	32.664	19.288
svchost.exe (UnistackSvcGroup)	3744	0	8.428	34.496	30.688
svchost.exe (UnistackSvcGroup)	3716	0	4.580	17.248	14.828
svchost.exe (UnistackSvcGroup)	4212	0	2.780	11.948	11.176
svchost.exe (RPCSS -p)	828	0	6.972	13.532	7.820
svchost.exe (NetworkServiceNet...	3548	0	1.772	7.220	6.276
svchost.exe (NetworkService -p)	2680	0	24.896	34.688	11.776
svchost.exe (NetworkService -p)	4932	0	7.912	18.164	13.752
svchost.exe (NetworkService -p)	1960	0	3.068	8.028	6.504
svchost.exe (NetworkService -p)	2368	0	1.882	7.938	7.204
svchost.exe (NetworkService -p)	1360	0	3.832	8.940	8.264
svchost.exe (netvcs)	3028	0	3.368	12.356	11.512
svchost.exe (netvcs -p)	5168	0	37.716	89.712	28.812
svchost.exe (netvcs -p)	2708	0	8.044	16.972	11.492
svchost.exe (netvcs -p)	876	0	6.156	15.048	11.264
svchost.exe (netvcs -p)	5632	0	7.412	23.908	21.364
svchost.exe (netvcs -p)	1094	0	3.600	13.188	11.100
svchost.exe (netvcs -p)	2832	0	4.460	20.208	18.264
					1.944

¿Cuánta diferencia existe entre la memoria usada por 10 procesos notepad y un proceso word con 10 hilos abiertos?

**70,7 – 22 = 48,7 MB**

Entre la carga en memoria de los 10 archivos de Word y los 10 del Bloc de Notas, existe una diferencia notable de casi 50MB. Si sólo estuvieran consumiendo memoria estos dos conjuntos de tareas, el bloc de notas consumiría el 23% de la memoria total y Word estaría consumiendo 77% restante.