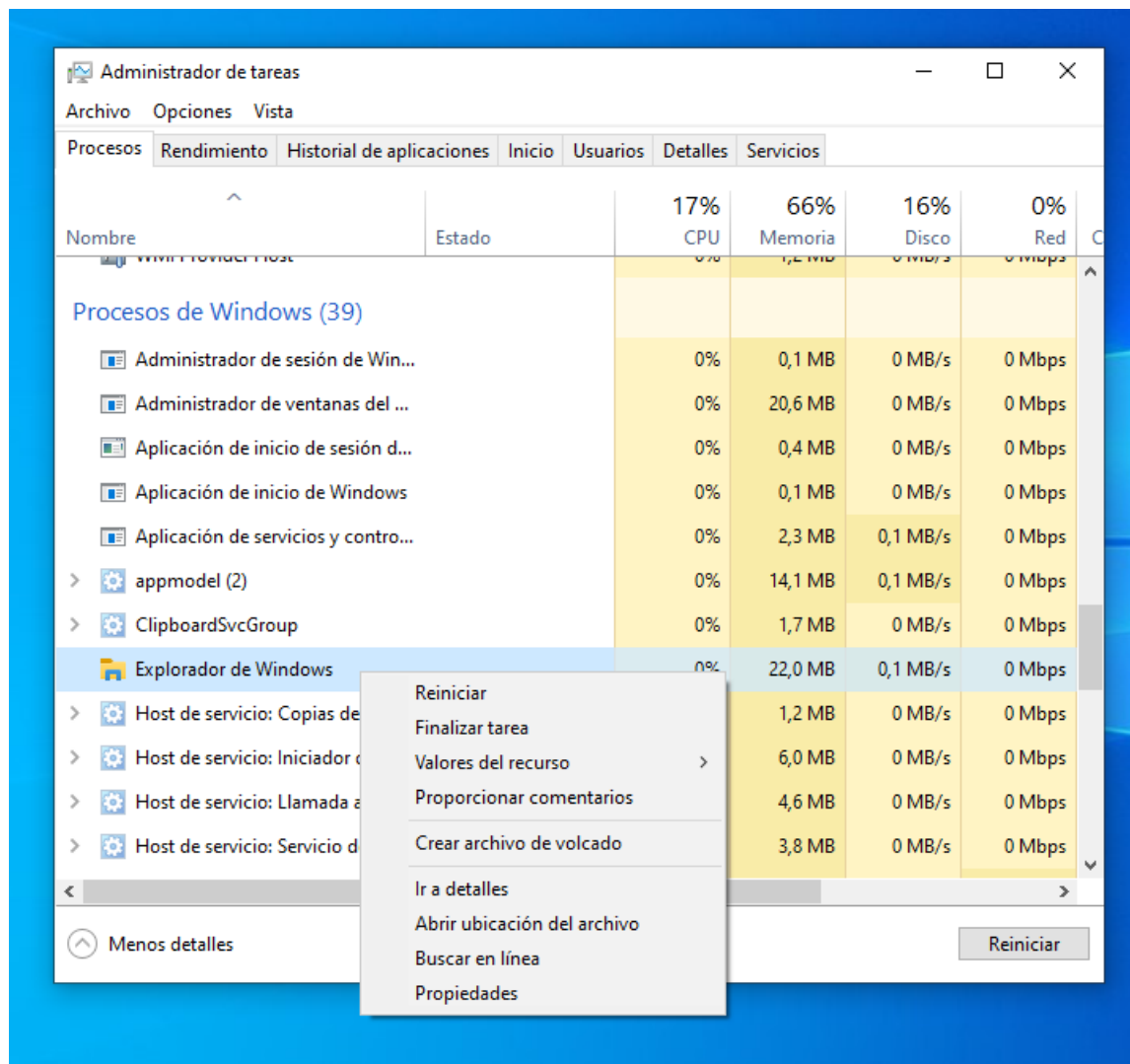
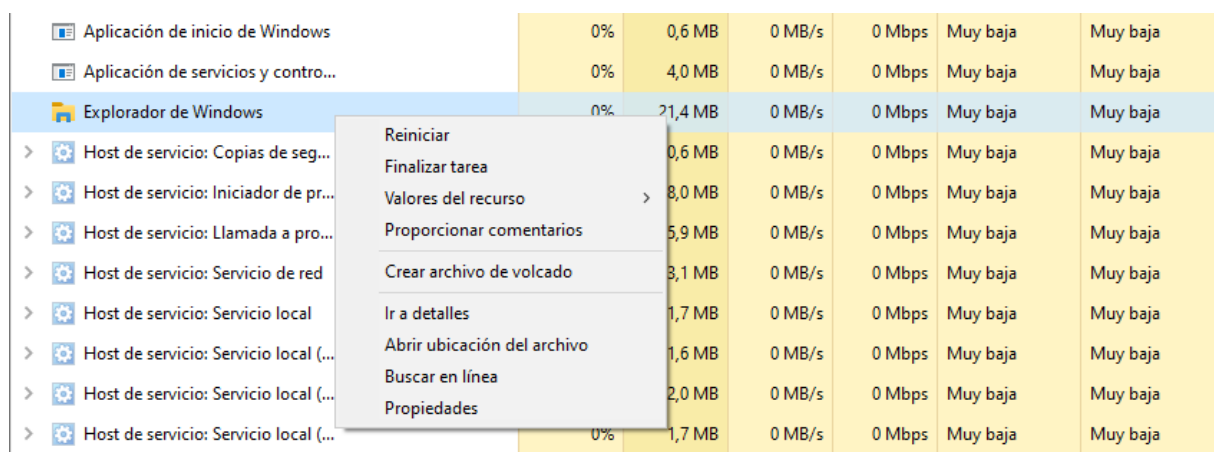


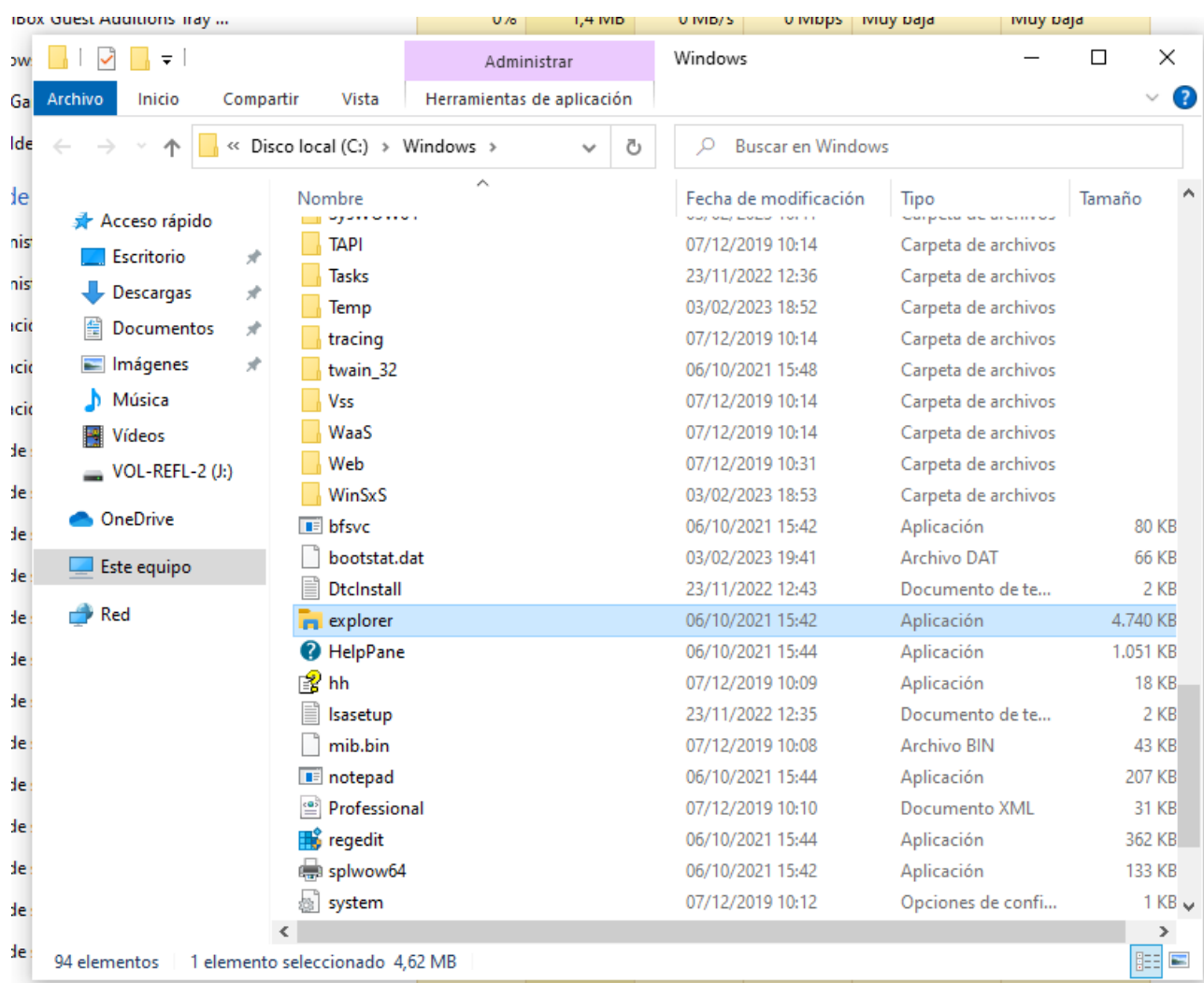
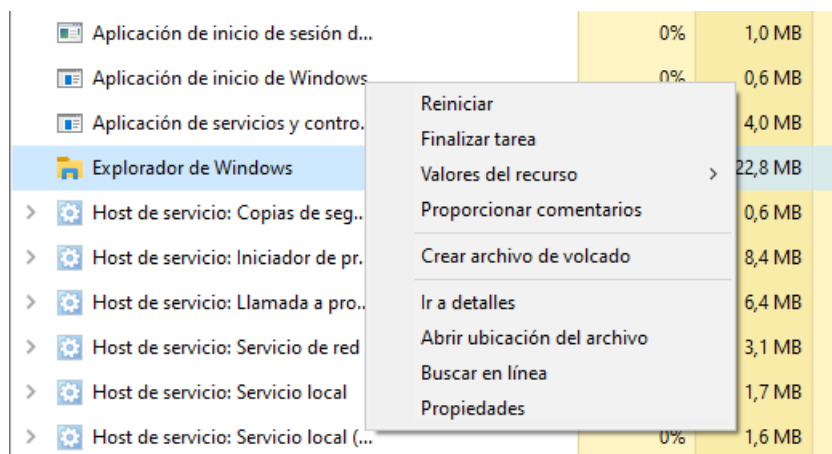
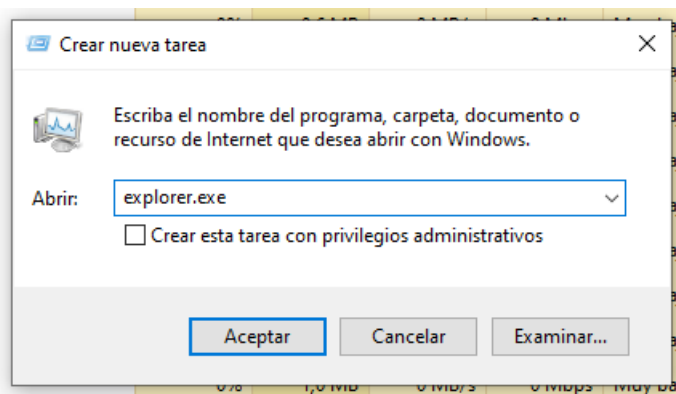
Ejercicio 2

1. Abre el Administrador de tareas en tu máquina virtual y reinicia el proceso "Explorador de Windows" (0,5 p)



2. Encuentra en la pestaña adecuada del Administrador de tareas el proceso explorer.exe y finalízalo. A continuación, vuelve a iniciar este proceso desde la opción "Ejecutar nueva tarea". Desde el Administrador de tareas, averigua la ubicación del programa explorer.exe en disco. (0,75 p)





3. Desde Powershell, usando los comandos de gestión de procesos adecuados, inicia el programa Paint (mspaint.exe), averigua su identificador de proceso y la ubicación del programa en disco. Finaliza el programa desde la línea de comandos. (0,75 p)

```
PS C:\Users\Javier> get-process -name mspaint
```

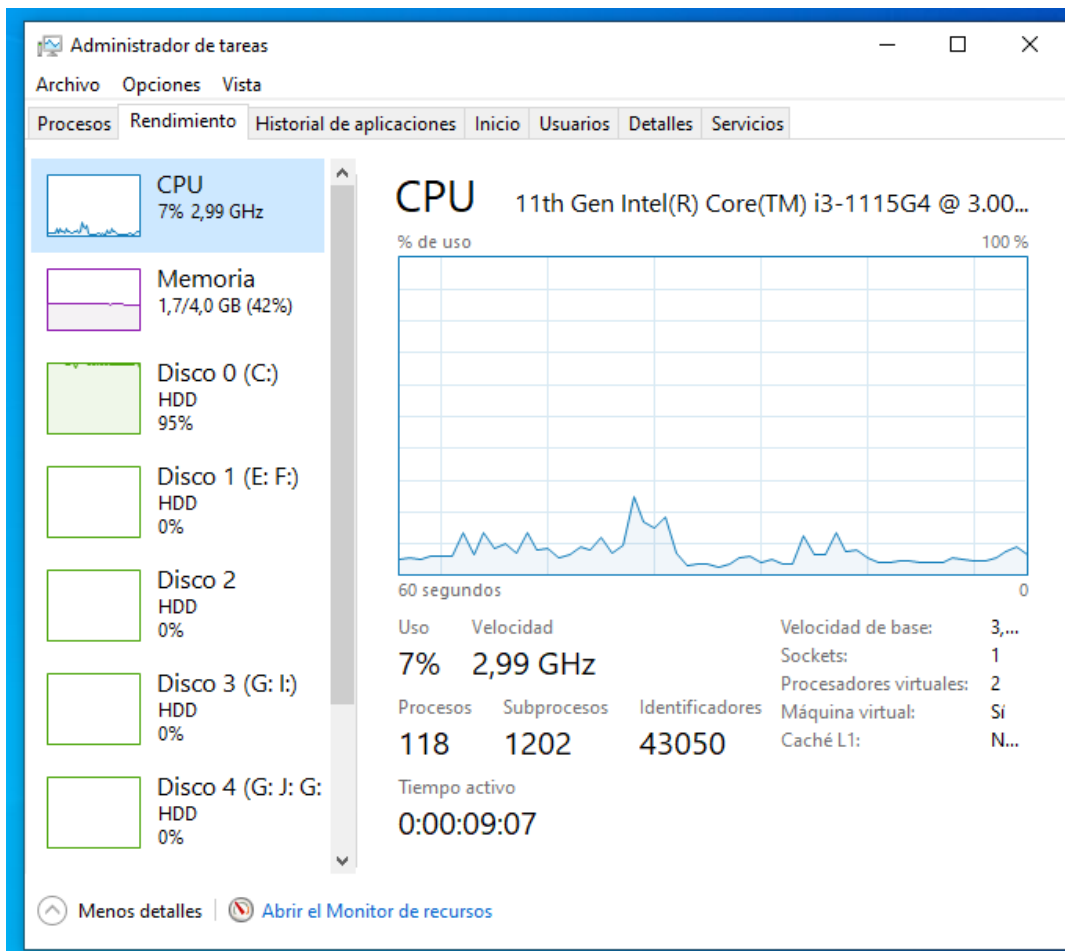
Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
311	48	8860	29828	0,42	2668	1	mspaint

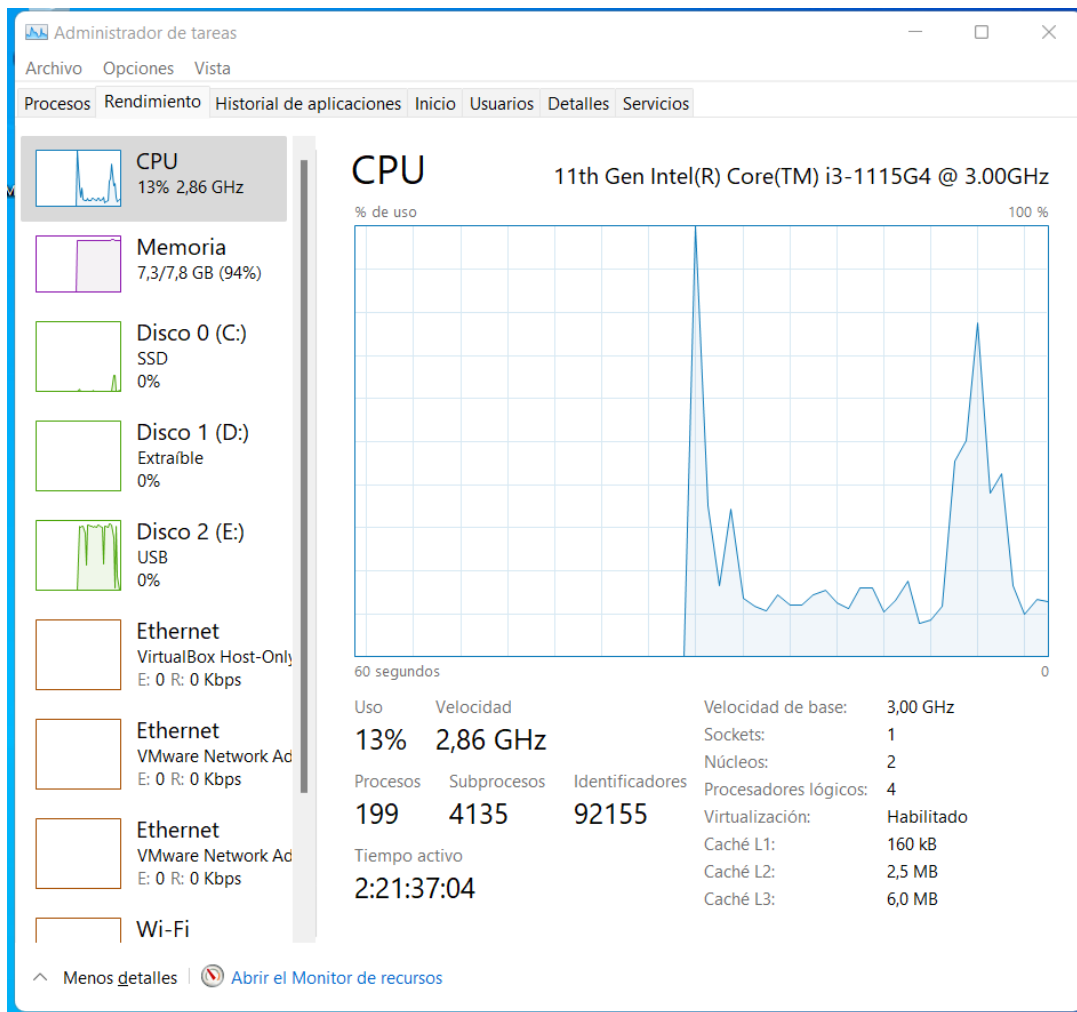
```
PS C:\Users\Javier> get-process -name mspaint -fileversioninfo
```

ProductVersion	FileVersion	FileName
10.0.19041.2364	10.0.19041.23...	C:\Windows\system32\mspaint.exe

Para finalizar el proceso se usa el comando “Stop-process -name mspaint”

4. Consulta la pestaña adecuada del Administrador de tareas de la máquina anfitriona y del de la máquina virtual para responder a las siguientes preguntas. ¿Cuántos procesadores virtuales tiene cada una? ¿Y cuánta RAM? Teniendo en cuenta las limitaciones de la máquina anfitriona, ¿crees que podrías optimizar la configuración de tu máquina virtual? Justifica tu respuesta. (1 p)





Procesadores virtuales

Host – 4 procesadores

Máquina virtual – 2 procesadores virtuales

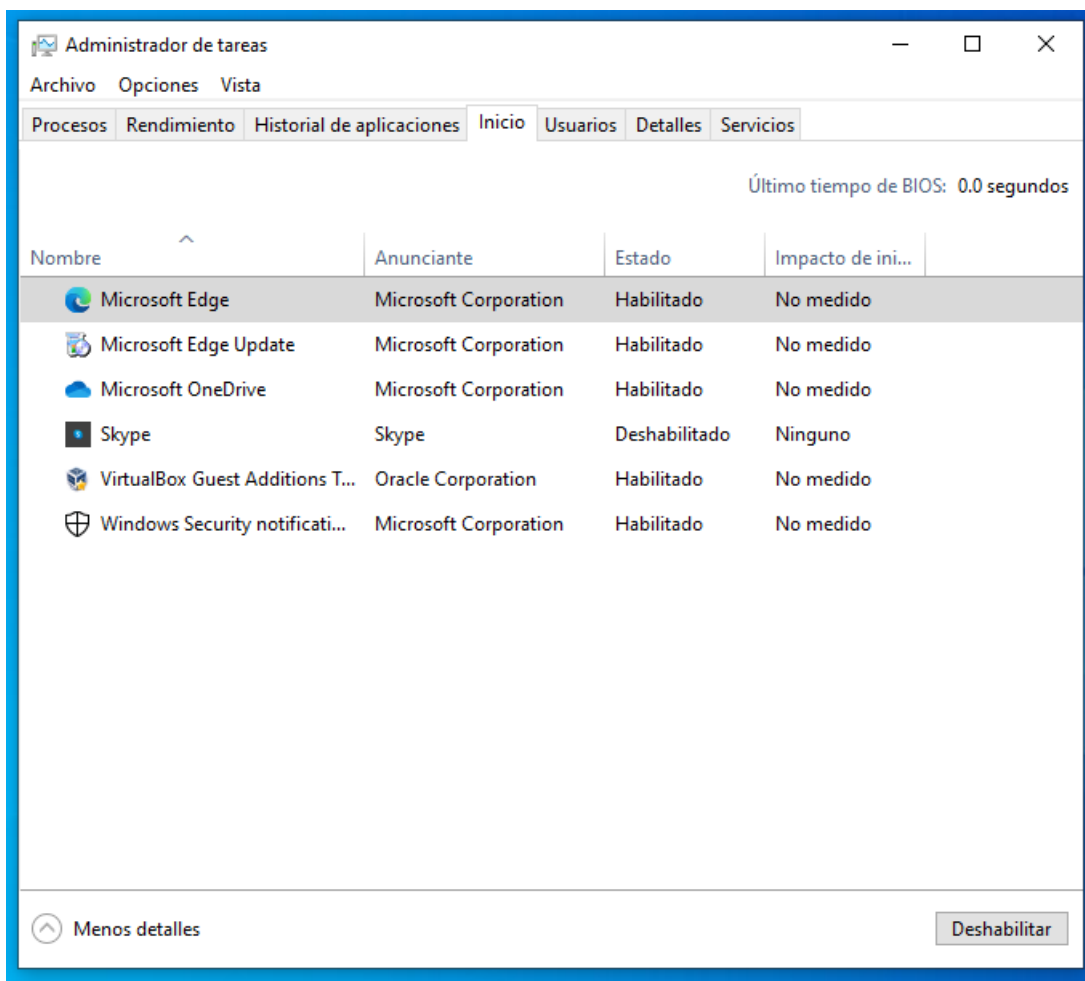
Memoria RAM

Host – 8 GB

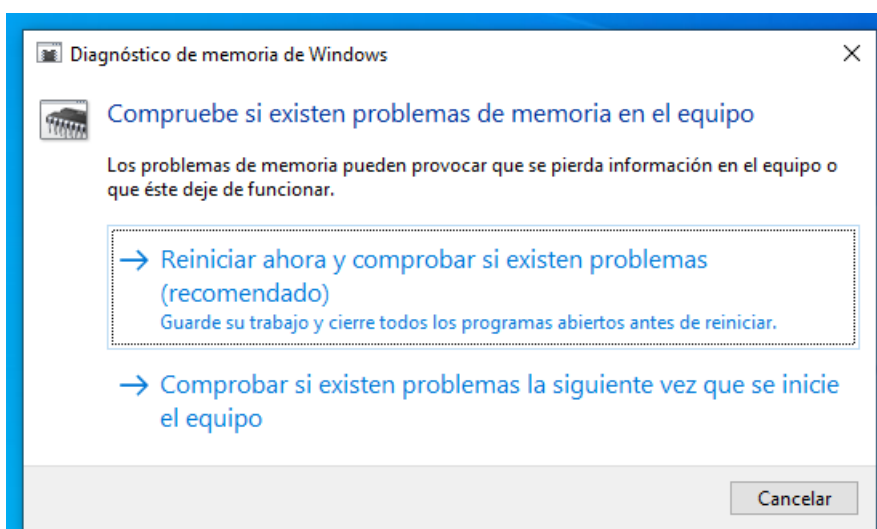
Máquina virtual – 4 GB

Creo que si se podrían optimizar las configuraciones, ya sea añadiéndole algún procesador virtual más, añadiéndole algo más de RAM y asignándole un poco de VRAM virtual.

5. Averigua qué programas arranca Windows automáticamente al iniciar sesión y optimiza el arranque del sistema deshabilitando los que consideres innecesarios. (0,5 p)



6. Investiga qué herramienta propia de Windows nos permite hacer un diagnóstico de la memoria y ejecútalo. Menciona al menos dos situaciones en las que sería conveniente hacer esta comprobación. (1 p)



Herramienta de diagnóstico de memoria de Windows

Windows está comprobando si hay problemas en la memoria...
Esto puede tardar varios minutos.

Ejecutando paso de prueba 1 de 2: 04% completado

Estado general de la prueba: 02% completado



Estado:

Aún no se detectó ningún problema.

Aunque a veces parezca que la prueba está inactiva, sigue ejecutándose.
Espere a que se completen las pruebas...

Windows reiniciará el equipo automáticamente. Los resultados de las pruebas se mostrarán de nuevo después de que inicie sesión.

F1=Opciones

Esc

7. Averigua los requisitos hardware recomendados para instalar la última versión de XAMPP en tu máquina virtual. Ten en cuenta que tú serás el único usuario de sus servicios, por lo que puedes guiarte por los valores mínimos que encuentres (0,5 p).

85 MB de espacio libre en disco

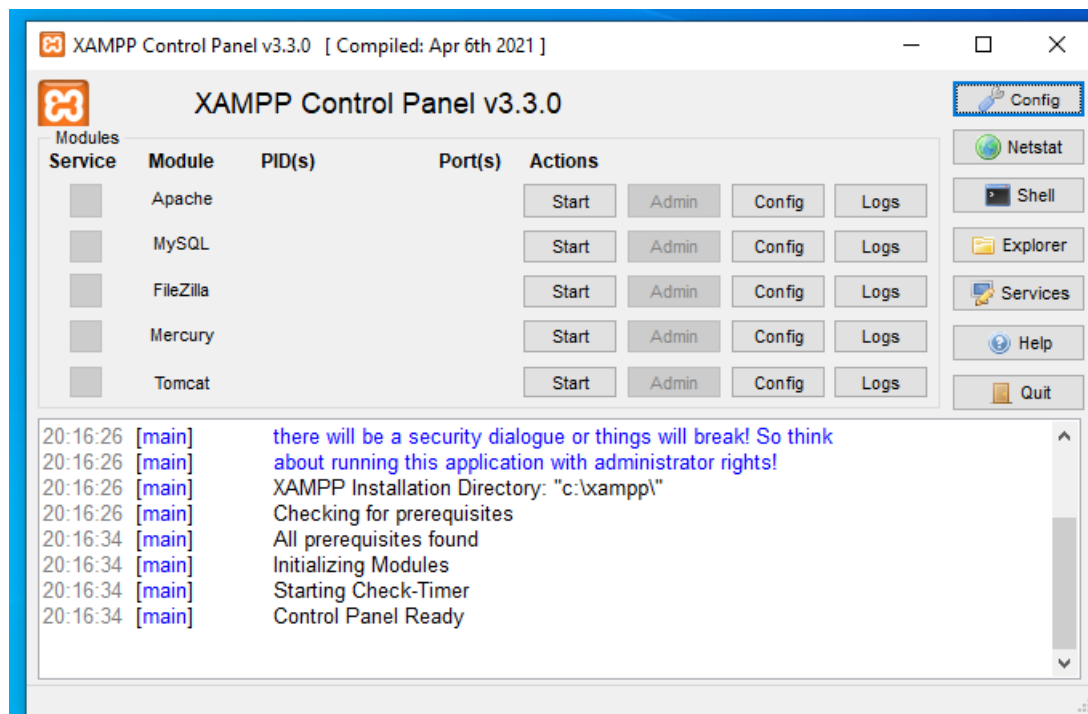
256 MB de RAM

Procesador Pentium o superior

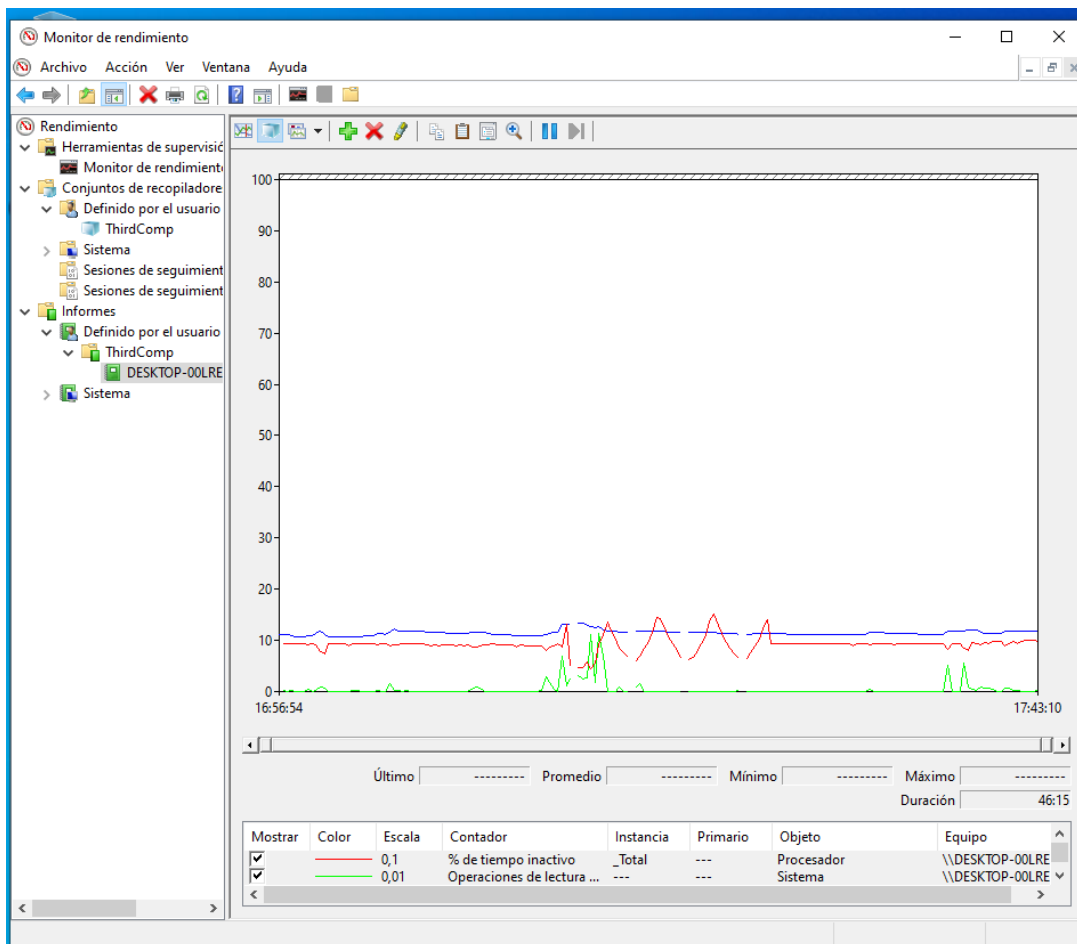
Tener Windows, Linux o MacOS

8. Sigue los primeros pasos de la siguiente guía para realizar la instalación. No te preocupes por documentar este apartado (ya están en el tutorial) y tampoco es necesario que configures por completo todos los servicios, sólo asegúrate de poder gestionarlos desde la herramienta Servicios de Windows.

<https://www.solvetic.com/tutoriales/article/8154-como-instalar-y-configurar-xampp-en-windows-10/>



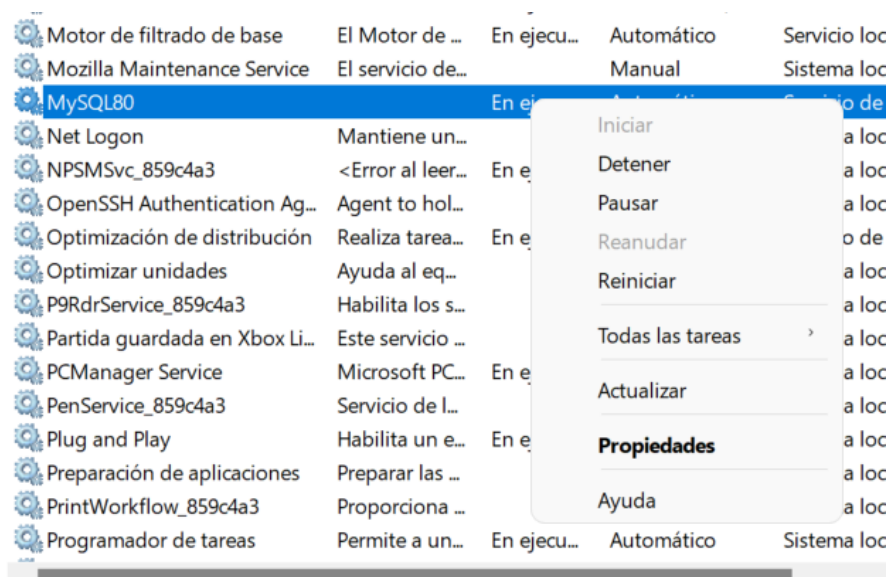
9. Abre el monitor de rendimiento de Windows agrega 3 componentes (procesador - % tiempo inactivo, sistema – procesos y operaciones de lectura de archivo/s) para realizar su seguimiento. Observa la gráfica. (0,75 p)

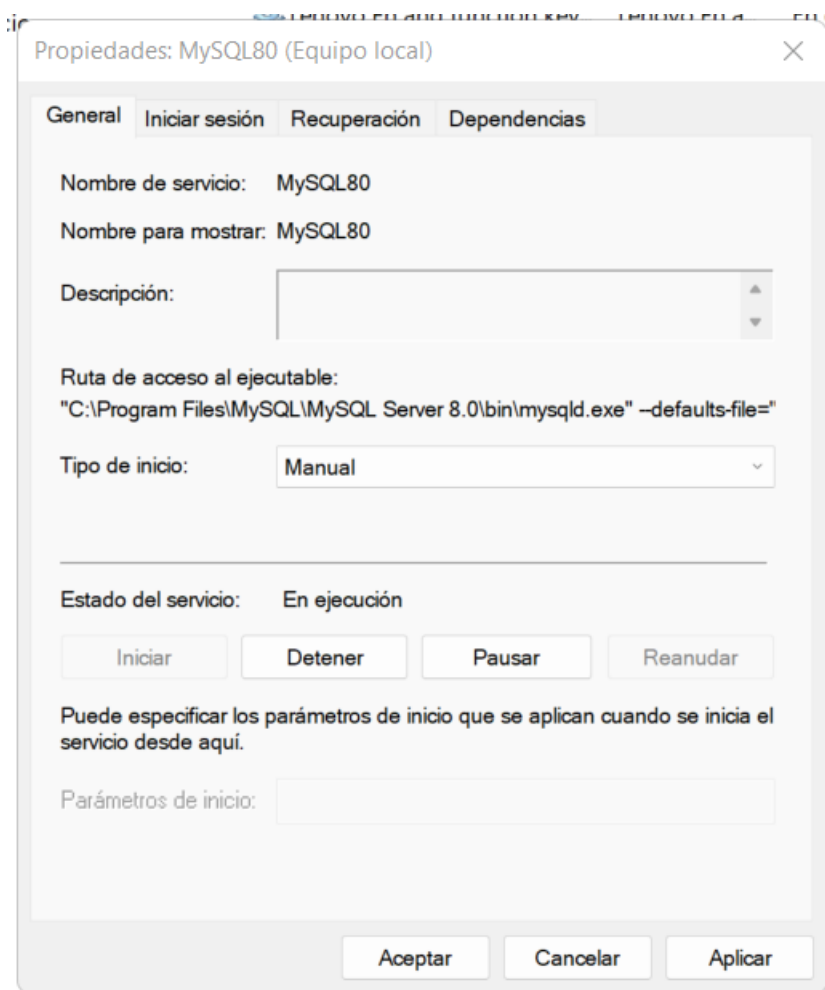
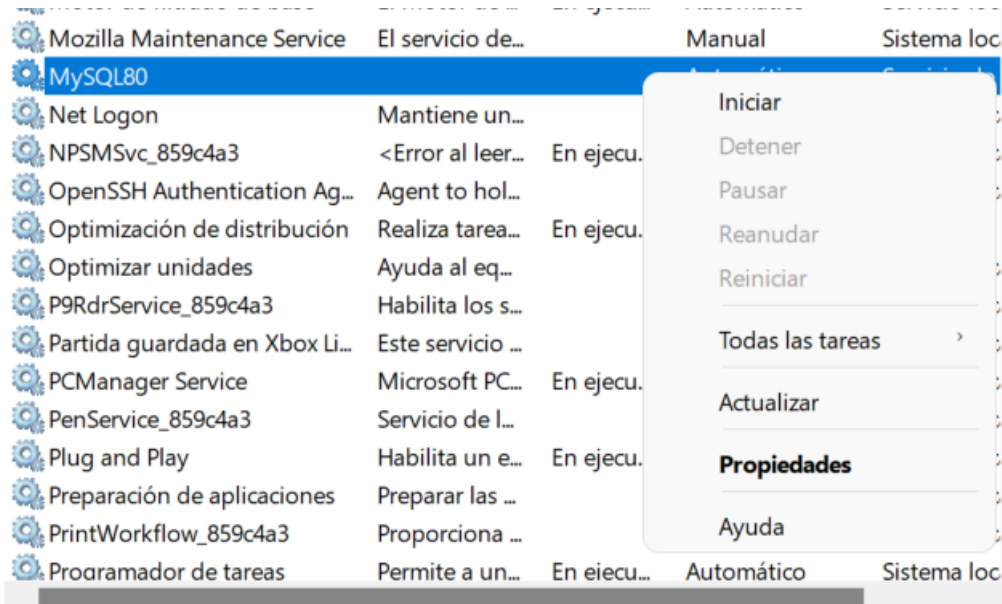


10. ¿Qué servicios se han instalado en el apartado 8? (0,75 p)

Se han instalado Apache, Mysql, PHP y Perl

11. Desde Servicios, inicia y detén (o viceversa) alguno de los servicios instalados anteriormente. Cambia el tipo de inicio. (0,75 p)





12. Desde línea de comandos, inicia y detén (o viceversa) el servicio anterior. Vuelve a cambiar el tipo de inicio para dejarlo como estaba antes del apartado anterior. (0,75 p)

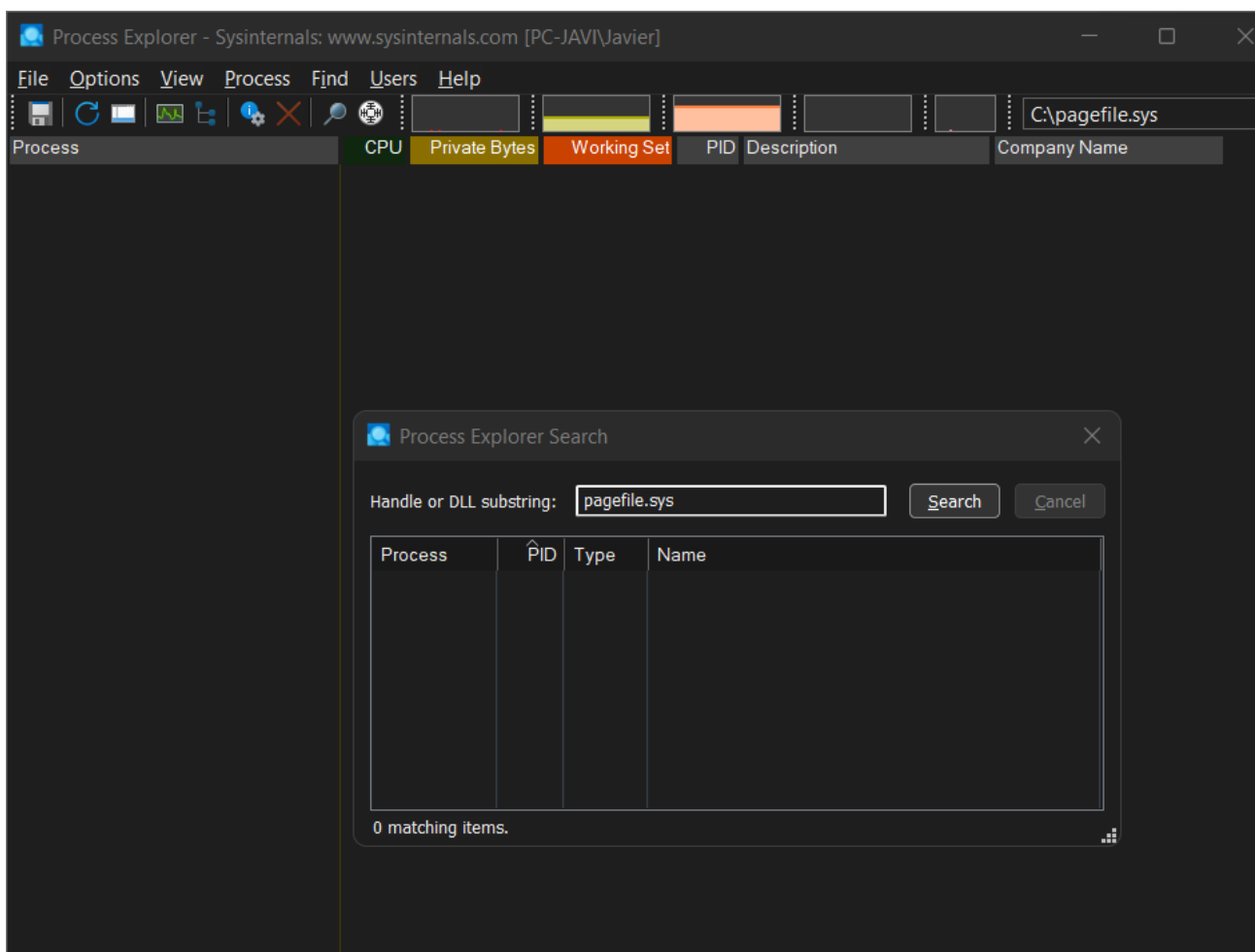
```
PS C:\Windows\system32> stop-service -name MySQL80
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> stop-service -name MySQL80
PS C:\Windows\system32> start-service -name MySQL80
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> set-service -name MySQL80 -startuptype manual
PS C:\Windows\system32>
```

```
PS C:\Windows\system32> set-service -name MySQL80 -startuptype automatic
PS C:\Windows\system32>
```

13. Descarga la utilidad Process Explorer desde la web Microsoft SysInternals. Úsala para averiguar qué proceso está usando el fichero C:\pagefile.sys (1 p)




Actualmente, ningún proceso usa pagefile.sys

14. Descarga otra utilidad de SysInternals de tu elección. Descríbela brevemente, prueba y documenta un caso de uso que te parezca interesante. (1 p)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time o...	Process Name	PID	Operation	Path	Result	Detail
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
16:16:40...	Explorer.EXE	42296	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:16:40...	Explorer.EXE	42296	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
16:16:40...	Explorer.EXE	42296	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKCU\Software\Classes\Applications\Pr...	NAME NOT FOUND	Desired Access: R...
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
16:16:40...	ctfmon.exe	38356	ReadFile	C:\Windows\System32\CoreUICompon...	SUCCESS	Offset: 2.802.176, Le...
16:16:40...	ctfmon.exe	38356	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:16:40...	Explorer.EXE	42296	CreateFile	C:\Users\xxelb\Downloads\SysIntern...	SUCCESS	Desired Access: R...
16:16:40...	ctfmon.exe	38356	RegOpenKey	HKLM\Software\Microsoft\Input\Locales\...	SUCCESS	Desired Access: R...
16:16:40...	Explorer.EXE	42296	ReadFile	C:\Windows\System32\windows.storage...	SUCCESS	Offset: 7.761.920, Le...
16:16:40...	Explorer.EXE	42296	QueryBasicInfo...	C:\Users\xxelb\Downloads\SysIntern...	SUCCESS	CreationTime: 06/0...
16:16:40...	Explorer.EXE	42296	CloseFile	C:\Users\xxelb\Downloads\SysIntern...	SUCCESS	
16:16:40...	ctfmon.exe	38356	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Loca...	SUCCESS	Type: REG_DWO...
16:16:40...	ctfmon.exe	38356	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Loca...	SUCCESS	
16:16:40...	ctfmon.exe	38356	QueryNameInfo...	C:\Users\xxelb\Downloads\SysIntern...	SUCCESS	Name: \Users\xxel...
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
16:16:40...	Explorer.EXE	42296	RegOpenKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	Desired Access: Q...
16:16:40...	svchost.exe	3396	ReadFile	C:\Windows\System32\Windows.StateR...	SUCCESS	Offset: 6.328.320, Le...
16:16:40...	Explorer.EXE	42296	RegQueryValue	HKLM\System\CurrentControlSet\Control...	NAME NOT FOUND	Length: 24
16:16:40...	Explorer.EXE	42296	RegCloseKey	HKLM\System\CurrentControlSet\Control...	SUCCESS	
16:16:40...	ctfmon.exe	38356	ReadFile	C:\Windows\System32\InputService.dll	SUCCESS	Offset: 4.182.016, Le...
16:16:40...	Explorer.EXE	42296	ReadFile	C:\Windows\System32\thumbcache.dll	SUCCESS	Offset: 360.448, Len...
16:16:40...	svchost.exe	3396	LockFile	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Exclusive: False, Of...
16:16:40...	svchost.exe	3396	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\Ap...	SUCCESS	Offset: 123, Length: 1
16:16:40...	ctfmon.exe	38356	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
16:16:40...	ctfmon.exe	38356	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
16:16:40...	ctfmon.exe	38356	RegQueryValue	HKCU\Software\Microsoft\Input\Settings\...	NAME NOT FOUND	Length: 16
16:16:40...	ctfmon.exe	38356	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
16:16:40...	Explorer.EXE	42296	ReadFile	C:\Windows\System32\Taskbar.dll	SUCCESS	Offset: 2.494.464, Le...
16:16:40...	ctfmon.exe	38356	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
16:16:40...	ctfmon.exe	38356	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Desired Access: R...
16:16:40...	ctfmon.exe	38356	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Setti...	SUCCESS	Type: REG_DWO...

Showing 130.660 of 442.475 events (29%) Backed by virtual memory

Process Monitor es una aplicación de la suite de Microsoft Sysinternal en cual te permite ver todos los procesos actuales y monitorearlos, indicándote datos muy detallados como si son un archivo, una clave de registro, su ruta de acceso, su resultado de ejecución, etc.

Este programa se podría usar a la hora de escanear y ver en busca de virus, pudiendo ve el comportamiento de todos los procesos del equipo y así poder eliminar el malware.