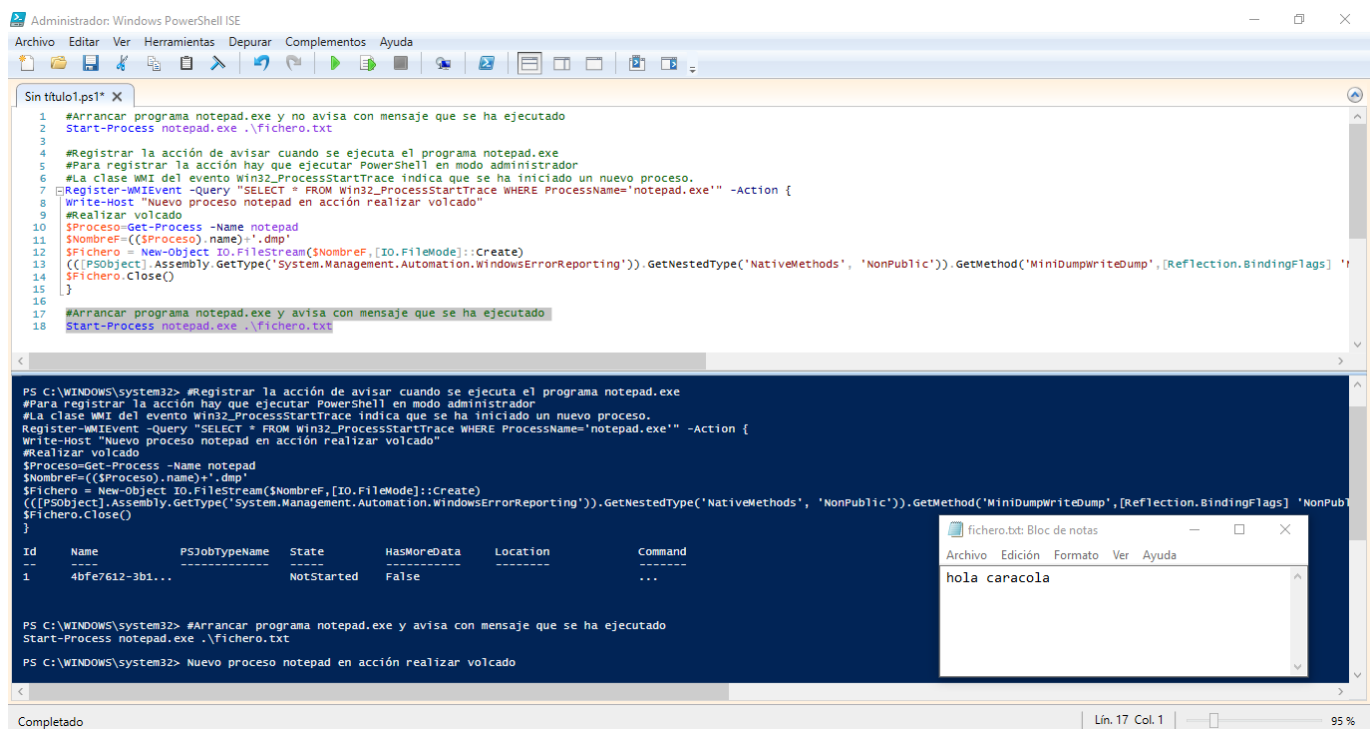


Realizar un volcado de memoria de un proceso cuando se empieza a ejecutar

[crayon-6a9d4f85dca0d668847096/]

En el siguiente ejemplo vemos que se ha realizado el volcado



```
Sin título1.ps1* X
1 #Arrancar programa notepad.exe y no avisa con mensaje que se ha ejecutado
2 Start-Process notepad.exe .\fichero.txt
3
4 #Registrar la acción de avisar cuando se ejecuta el programa notepad.exe
5 #Para registrar la acción hay que ejecutar PowerShell en modo administrador
6 #La clase WMI del evento Win32_ProcessStartTrace indica que se ha iniciado un nuevo proceso.
7 [Register-WMIEvent -Query "SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName='notepad.exe'" -Action {
8   Write-Host "Nuevo proceso notepad en acción realizar volcado"
9   #Realizar volcado
10  $Proceso=Get-Process -Name notepad
11  $NombreF=((($Proceso).Name)+'.dmp')
12  $Fichero = New-Object IO.FileStream($NombreF,[IO.FileMode]::Create)
13  ((([PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting')).GetNestedType('NativeMethods', 'NonPublic')).GetMethod('MiniDumpWriteDump',[Reflection.BindingFlags] 'NonPublic', $Fichero).Invoke($Proceso,$Fichero))
14  $Fichero.Close()
15 }
16
17 #Arrancar programa notepad.exe y avisa con mensaje que se ha ejecutado
18 Start-Process notepad.exe .\fichero.txt
```

```
PS C:\WINDOWS\system32> #Registrar la acción de avisar cuando se ejecuta el programa notepad.exe
#Para registrar la acción hay que ejecutar PowerShell en modo administrador
#La clase WMI del evento Win32_ProcessStartTrace indica que se ha iniciado un nuevo proceso.
Register-WMIEvent -Query "SELECT * FROM Win32_ProcessStartTrace WHERE ProcessName='notepad.exe'" -Action {
  Write-Host "Nuevo proceso notepad en acción realizar volcado"
  #Realizar volcado
  $Proceso=Get-Process -Name notepad
  $NombreF=((($Proceso).Name)+'.dmp')
  $Fichero = New-Object IO.FileStream($NombreF,[IO.FileMode]::Create)
  ((([PSObject].Assembly.GetType('System.Management.Automation.WindowsErrorReporting')).GetNestedType('NativeMethods', 'NonPublic')).GetMethod('MiniDumpWriteDump',[Reflection.BindingFlags] 'NonPublic', $Fichero).Invoke($Proceso,$Fichero))
  $Fichero.Close()
}

Id      Name      PSJobTypeName State      HasMoreData Location      Command
--      -
1       4bfe7612-3b1... NotStarted False      C:\WINDOWS\system32\notepad.exe
```

```
PS C:\WINDOWS\system32> #Arrancar programa notepad.exe y avisa con mensaje que se ha ejecutado
Start-Process notepad.exe .\fichero.txt

PS C:\WINDOWS\system32> Nuevo proceso notepad en acción realizar volcado
```

Completado | Lín. 17 Col. 1 | 95 %

Buscamos la cadena «caracola» en el fichero de volcado de esa forma confirmamos que se ha realizado correctamente la acción del volcado en cuanto se ejecutó el programa notepad

