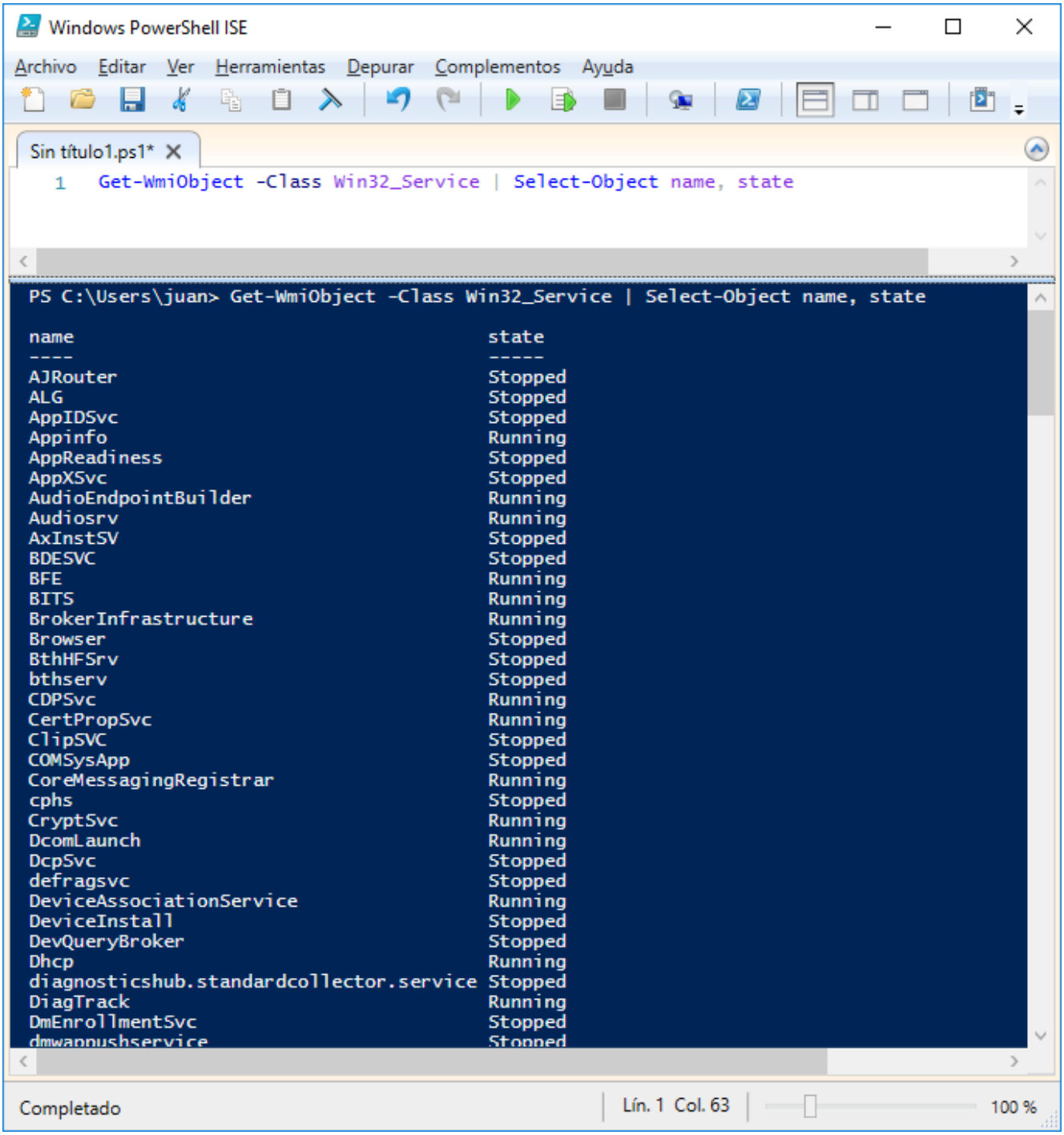
Analizar servicios con PowerShell

Ver estado de servicios

```
#Ver estado de servicios
Get-WmiObject -Class Win32_Service | Select-Object name, state
```



Ver servicios que están «Running»

```
#Ver servicios que están "Running"
Get-WmiObject -Class Win32_Service | Where-Object State -EQ
'Running'
```

Mostrar los procesos que se están ejecutando en relación con los servicios

```
#Mostrar los procesos que se están ejecutando en relación con
los servicios
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ
'Running') | %{
Write-Host  $_.Name,$_.ProcessId,$_.State,(Get-Process  -Id
$_.ProcessId).Name
}
```

Mostrar los procesos que se están ejecutando en relación con los servicios (solo llamadas WMI)

```
#Mostrar los procesos que se están ejecutando en relación con
los servicios (solo llamadas WMI)
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ
'Running') | %{
Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class
win32_process   |   Where-Object   ProcessId   -EQ
$_.ProcessId).ProcessId
}
```

Mostrar los procesos que se están ejecutando en relación con los servicios (solo llamadas WMI y más información)

```
#Mostrar los procesos que se están ejecutando en relación con los servicios (solo llamadas WMI y más información)
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{
Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class win32_process | Where-Object ProcessId -EQ  $_.ProcessId | select name, Path, ExecutablePath, CommandLine)
}
```

Mostrar los servicios que se están ejecutando en relación con los procesos y los hilos

```
#Mostrar los servicios que se están ejecutando en relación con los procesos y los hilos
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{
Write-Host  $_.Name,$_.ProcessId,$_.State,(Get-Process  -Id $_.ProcessId).Name,(Get-WmiObject -Class Win32_Thread | Where-Object ProcessHandle -EQ $_.ProcessId)
}
```

Mostrar los hilos que se están

ejecutando en relación con los servicios y los procesos

```
#Mostrar los hilos que se están ejecutando en relación con los servicios y los procesos
$i=0
(Get-WmiObject -Class Win32_Thread) | %{
$i++
Write-Host $i,$_.Handle,$_.ProcessHandle,(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running' | Where-Object ProcessId -EQ $_.ProcessHandle),(Get-Process -Id $_.ProcessHandle).ProcessName
}
```

Obtener información sobre el comando ejecutado analizando procesos con una llamada WMI

```
#Obtener información sobre el comando ejecutado analizando procesos con una llamada WMI
Get-WmiObject -Class win32_process | select name, Path, ExecutablePath, CommandLine | Format-Custom
```

Mostrar información avanzada de los procesos (Path, ExecutablePath, CommandLine) que se están ejecutando en relación con los

servicios

```
#Mostrar información avanzada de los procesos (Path, ExecutablePath, CommandLine) que se están ejecutando en relación con los servicios
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{
#Write-Host  $_.Name,$_.ProcessId,$_.State,(Get-Process  -Id $_.ProcessId  | Select-Object name, Path, ExecutablePath, CommandLine)
Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class win32_process | Where-Object ProcessId -EQ  $_.ProcessId | select name, Path, ExecutablePath, CommandLine)
Write-Host "################################################"
}
```