

Ejercicios de PowerShell: analizar procesos

Ruta donde se ejecutan los procesos

```
Get-Process -FileVersionInfo
```

Buscar un proceso que se está ejecutando

```
(Get-Process).Where{$_.Name -like "chrome"}
```

Ver el padre de los procesos

```
(Get-WmiObject win32_process) | Select-Object  
ProcessId,Description,ParentProcessId
```

Obtener más información sobre los procesos (línea de comandos)

```
(Get-WmiObject win32_process) | Select-Object  
ProcessId,Name,CommandLine
```

Ejercicio sobre analizar procesos y relacionarlos con los paquetes instalados

Ideas

- Información sobre paquetes

```
Get-ChildItem .\172adf28.msi | select *
```

- Descomprimir el paquete
- Instalar el paquete y detectarlo en C:\Program Files
- Relación de nombre de proceso con nombre de paquete

Solución 1

```
# Extraer contenido de instalador .msi a una carpeta
```

```
msiexec /a C:\windows\Installer\9ec68a07.msi /qb  
TARGETDIR=C:\users\clase\descompresion.msi  
# Localizar proceso del que queremos sacar el instalador y  
meterlo en un fichero  
(ps | select name).Where{$_.Name -like "DolbyDax2TrayIcon"} |  
Out-File fichero.txt  
# Buscar ruta del proceso que se esta ejecutando  
ls -Recurse | Select-String (gc .\fichero.txt)[3]
```

Solución 2

```
# Instalar un paquete .msi  
msiexec.exe /package C:\windows\Installer\9ec68a07.msi  
# Irnos a la carpeta de Archivos de programa  
C:\ProgramFiles  
# Listar todas las carpeta y sacar la última instalada  
ls | sort -Descending CreationTime | select -last 1  
# Localizar proceso del que queremos sacar el instalador y  
meterlo en un fichero  
(ps | select name).Where{$_.Name -like "DolbyDax2TrayIcon"} |  
Out-File fichero.txt  
# Buscar ruta del proceso que se está ejecutando  
ls -Recurse | Select-String (gc .\fichero.txt)[3]
```