

# Obtener valores de la memoria en PowerShell utilizando la clase Marshal

Hay que tener en cuenta que cuando un proceso se ejecuta, el sistema operativo le asigna un espacio de direcciones y lo añade a una tabla de procesos. El espacio de direcciones de cada proceso contiene las instrucciones y datos del programa, además tiene una pila que lleva la cuenta de las llamadas a procedimientos. En el siguiente script de ejemplo podemos ver información sobre la memoria de ese proceso que se está ejecutando y que es PowerShell, en él que se almacenan valores en variables (datos del programa).

```
# StringToHGlobalAnsi: Copia el contenido de un String administrado en la memoria no administrada, convirtiéndolo en formato ANSI mientras realiza la copia.
```

```
# PtrToStringAnsi: Asigna un String administrado y copia en él total o parcialmente una cadena ANSI (en Windows) o UTF-8 (en Unix) no administrada.
```

```
$a = "hola"
```

```
# Dirección del primer carácter de la cadena no administrada. Dirección, en memoria no administrada, donde se copió la cadena o 0 si $a es null.
```

```
$ptr = [Runtime.InteropServices.Marshal]::StringToHGlobalAnsi($a);  
$ptr
```

```
1..10000 | %{
```

```
    # Obtener el valor de una variable en base a una dirección  
    Ptr más un variable contador
```

```
[Runtime.InteropServices.Marshal]::PtrToStringAnsi($ptr.ToInt64()+$_)  
}
```

Windows PowerShell ISE

Archivo Editar Ver Herramientas Depurar Complementos Ayuda

Sin título1.ps1 X

```
1 # StringToHGlobalAnsi: Copia el contenido de un String administrado en la memoria no administrada, convirtiéndolo en formato ANSI mientras realiza la copia.
2 # PtrToStringAnsi: Asigna un String administrado y copia en él total o parcialmente una cadena ANSI (en windows) o UTF-8 (en unix) no administrada.
3
4 $a = "hola"
5
6 # Dirección del primer carácter de la cadena no administrada. Dirección, en memoria no administrada, adonde se copió la cadena o 0 si s es null.
7 $ptr = [Runtime.InteropServices.Marshal]::StringToHGlobalAnsi($a); $ptr
8
9 [1..10000] | %{
10     # Obtener el valor de una variable en base a una dirección Ptr más un variable contador
11     [Runtime.InteropServices.Marshal]::PtrToStringAnsi($ptr.ToInt64()+$_)
12 }
```

2kI  
kI  
I

System.Runtime.Serialization.dll  
ystem.Runtime.Serialization.dll  
stem.Runtime.Serialization.dll  
tem.Runtime.Serialization.dll  
em.Runtime.Serialization.dll  
m.Runtime.Serialization.dll  
.Runtime.Serialization.dll  
Runtime.Serialization.dll  
untime.Serialization.dll  
ntime.Serialization.dll  
time.Serialization.dll  
ime.Serialization.dll  
me.Serialization.dll  
e.Serialization.dll  
.Serialization.dll  
Serialization.dll  
erialization.dll  
rialization.dll

Detenido Lin. 11 Col. 75 110 %