David Alejandro Rodríguez García 1814035

# PARTE1

## 1.- Navegar en los registros hasta la siguiente ruta:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

**¿Qué información contiene los Profiles?**

RESPUESTA: Información de los perfiles de red (Category, DateCreated, DateLastConnected, Description, Managed, NameType, ProfileName)

2.- Navegar en los registros hasta la siguiente ruta:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

**¿Qué información contiene los registros en RecentDocs?**

RESPUESTA: Registros de los documentos abiertos recientemente

**¿Podemos identificar los últimos archivos PDF que se accedieron?**

RESPUESTA: A simple vista no, pero si entramos a la opción de modificar se puede ver la sección de la información codificada que corresponde al nombre del archivo PDF.

3.- Navegar en los registros hasta la siguiente ruta:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

## ¿Qué información encuentro en ese registro?

RESPUESTA: Las URLs ingresadas en el Internet Explorer

4.- Navegar en los registros hasta la siguiente ruta:

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interface

s

**¿Es importante la información que se encuentra en esta ruta del registro?**

RESPUESTA: Si

**¿De qué información se trata?**

RESPUESTA: Información del servidor DHCP (DhcpIPAddress, Domain, DhcpNameServer, etc).

5.- Navegar en los registros hasta la siguiente ruta:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

**¿Qué indicios nos da la información que se almacena en esta ruta?**

RESPUESTA: Que es información relacionada con la seguridad del sistema.

**¿es importante?**

RESPUESTA: Si, es parte de los servicios de seguridad de Windows.

6.- Navegar en los registros hasta la siguiente ruta:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

**¿Qué indicios nos da la información que se almacena en los subregistros de "Services"?**

RESPUESTA: Se almacenan registros de servicios del sistema y terceros

7.-Navegar en los registros hasta la siguiente ruta:

HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR

**¿Qué información guardan los subregistros de esta ruta?**

RESPUESTA: Address, Capabilities, ClassGUID, CompatibleIDs, Driver, HardwareID, etc.

8.- Navegar en los registros hasta la siguiente ruta:

HKEY_LOCAL_MACHINE\System\MountedDevices

**¿Qué información podemos determinar de los registros almacenados en esa ruta?**

RESPUESTA: información de los dispositivos conectados

## PARTE 2

5.- Ahora naveguemos a la siguiente ruta:

**¿cómo obtenemos las subclaves usando PowerShell?**

RESPUESTA: Get-ChildItem