[AF]Comandos Importantes Prácticas

Se recomienda trabajar con el sistema operativo instalado en hardware real, se deben evitar las máquinas virtuales ya que nos pueden traer problemas. Se recomienda empezar con linux y luego pasar a Windows.

Comandos para comprobar automontado

Linux

El comando lsblk muestra los dispositivos conectados, estén montados o no

```
lsblk
```

Mount muestra todo lo que está montado

```
mount
```

Si el dispositivo está montado muestra el punto de montaje, en caso contrario, no muestra nada

```
findmnt
```

Muestra espacio libre, si el dispositivo no está montado no aparece

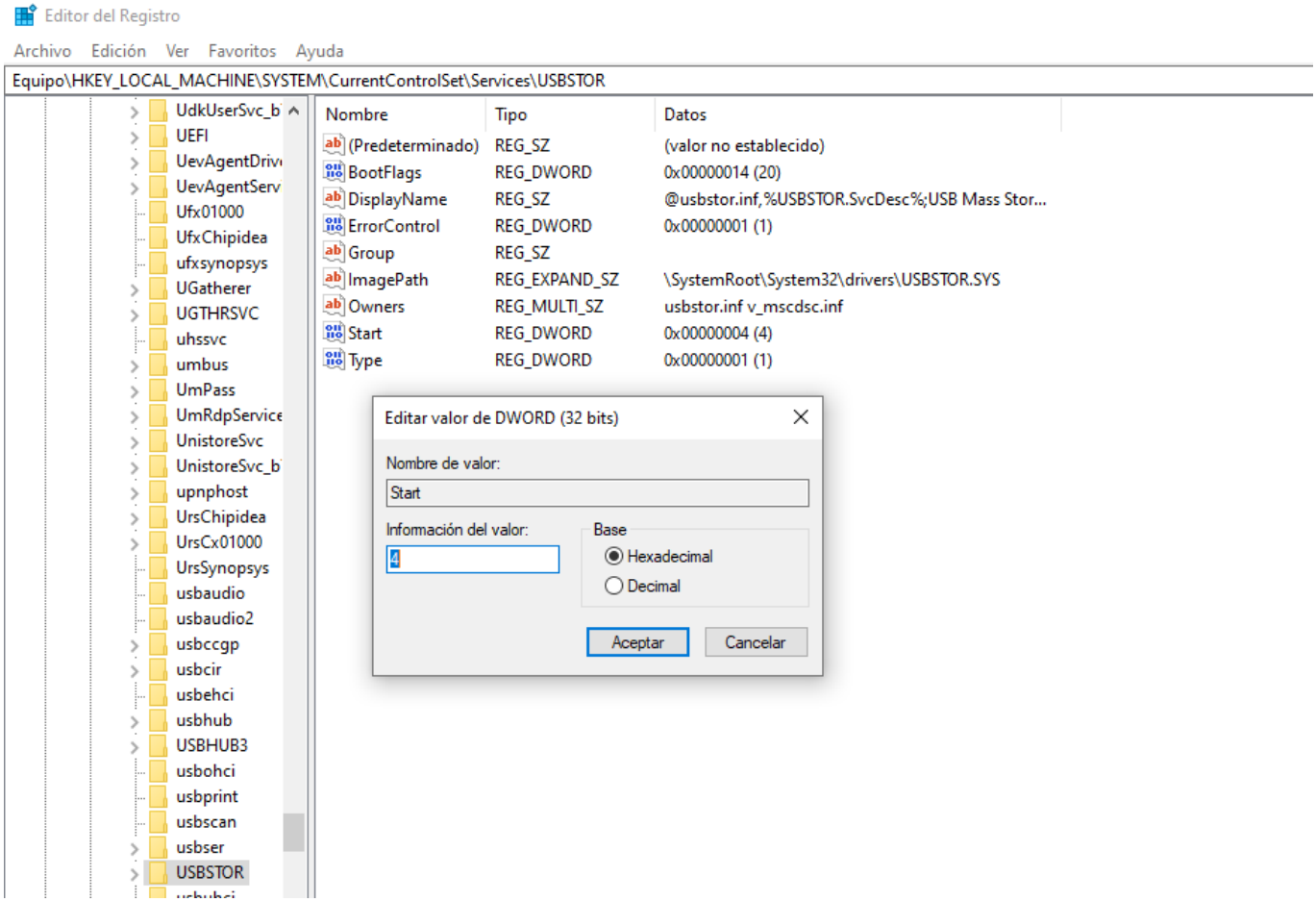
```
df
```

Windows

Para bloquear el montaje automático de USBs en windows tenemos que ir a la siguiente sección del registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
```

y modificar la REG_DWORD Start, con un valor inicial de 3, al valor 4 como se ve en la siguiente imagen:



Comandos para obtener información

Muestra información sobre los discos, pero no nos permite saber si están montados o no

```
fdisk
```

Permite obtener información de los dispositivos

```
parted
```

Bersión gráfica de parted

```
gparted
```

Muestra los mensajes del buffer del kernel, cuando se conecta un dispositivo muestra un mensaje aunque no se monte. Puede dar bastantes datos identificativos sobre un medio de almacenamiento.

```
dmesg
```

Comando para mostrar dispositivos USB conectados

```
lsusb
```

Comando que tiene una opción para mostrar información sobre un dispositivo que le indiquemos

```
udevadn
```

Comandos para recuperar información de un dispositivo

Para bloquear el montaje de un dispositivo hay varios métodos:

reglas udev

Se encuentran en /lib/udev/rules.dev y /etc/udev/rules.d, dentro encontraremos documentos con nombres como 90-usb_lock.rules, dentro encontraremos los siguientes campos (Todos en una línea, separados por motivos explicativos):

```
ACTION=="add|change", #Cada vez que se conecta o cambia algo en el
dispositivo, se lanza esta regla
SUBSYSTEM=="block", #Indica el tipo, no se debe confundir con SUBSYSTEMS.
ENV{UDISKS_AUTO}="0" #Evita el automontaje de la unidad
ENV{UDISKS_INFNORE}="1" #Esta sería una alternativa a la línea anterior, no
deben estar las dos a la vez, esta regla indica que se ignora el dispositivo
```

En resumidas cuentas, el contenido puede ser si fuera poco restrictivo como:

```
ACTION=="add|change", SUBSYSTEM=="block", ENV{UDISKS_AUTO}="0"
```

Y si fuera muy restrictivo como:

```
ACTION=="add|change", SUBSYSTEM=="block", ENV{UDISKS_INFNORE}="1"
```

Para aplicar los cambios a las reglas se usa el siguiente comando:

```
sudo udevadm control --reload-rules
```

UDISKS2

Paramos el servicio de udisks2 para prevenir el montaje automático

```
sudo systemctl stop udisks2.service
```

OJO: Cada vez que se reinicie el dispositivo este servicio se reiniciará.

GSettings

No es recomendable su uso, es muy fácil que falle. Depende del entorno en el que estemos (GNOME, KDE, etc…). Este ejemplo se aplica a GNOME.

```
gsettings get org gnome desktop media-handling automount
```

Si se ejecuta este comando, debería decir TRUE para indicar que esta el montaje automático montado. Para cambiar eso usamos el siguiente comando:

```
gsettings set org gnome desktop media-handling automount false
```

OJO: solo funciona al usuario que tiene iniciada la sesión, si se usa SUDO no funcionará.

Como configurar Windows en equipos de investigación

Primero debemos deshabilitar el AutoRun o el AutoPlay desde ciertas claves de registro. Hacer que los USB sean de solo lectura. Usando la opción diskpart de automount podemos deshabilitar el montaje automático.

OJO: Cada vez que se acutalice una máquina hay que comprobar que no se hayan revertido estos cambios.

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:analisis_forense:cmdimportant&rev=1741544622

Last update: **2025/03/09 18:23**