

1. Formas de abrir Task Manager:
 - a. Clic derecho en la barra de tareas y seleccionar: **Task Manager**
 - b. Presionar Ctrl+Alt+Delete y seleccionar: **Start Task Manager**
 - c. Presionar Ctrl+Shift+Esc
2. TList.exe: Puede mostrar los procesos en forma de árbol para identificar al proceso padre usando el parámetro /t. Tlist.exe se encuentra con la instalación de "Debugging Tools for Windows".



```
C:\Program Files\Debugging Tools for Windows (x64)>tlist.exe /t
System Process (0)
System (4)
  smss.exe (280)
  csrss.exe (376)
  csrss.exe (436)
    conhost.exe (2332) CicMarshalWnd
  wininit.exe (444)
    services.exe (540)
      svchost.exe (660)
        WmiPrvSE.exe (2712)
        WmiPrvSE.exe (4056)
        wlcomm.exe (3504) PresenceSignIn
        MOMHost.exe (3720)
      svchost.exe (740)
      MsMpEng.exe (832)
      svchost.exe (928)
        audiodg.exe (4068)
      svchost.exe (960)
        dwm.exe (1360) DWM Notification Window
      svchost.exe (988)
      svchost.exe (552)
      svchost.exe (1124)
      spoolsv.exe (1296)
      svchost.exe (1332)
      FcsSas.exe (1544)
      vmware-usbarbitrator.exe (1668)
```

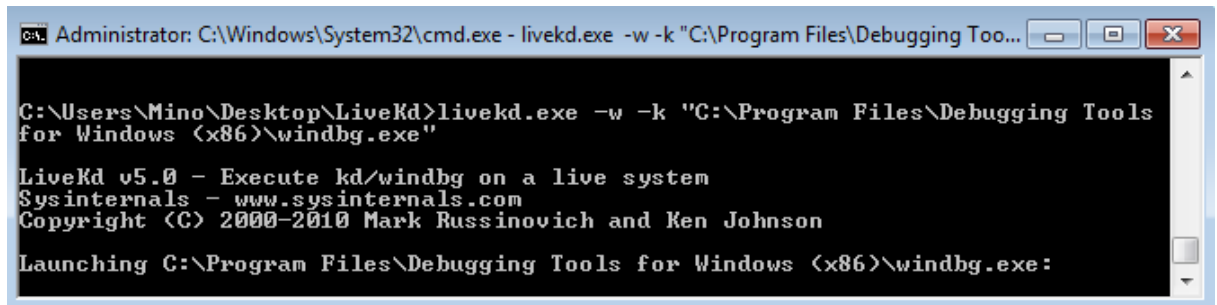
3. Demostración que en Windows solo mantiene ID del proceso padre y no del proceso abuelo.
 - a. Abrir un símbolo de sistema
 - b. Escribir: **start cmd** (se abrirá un segundo símbolo de sistema)
 - c. En el segundo símbolo de sistema escribir: **mspaint**
 - d. **Cerrar** el segundo símbolo de sistema
 - e. Abrir el administrador de tareas (**Task Manager**)
 - f. Ir a la pestaña de aplicaciones
 - g. Clic derecho en la aplicación de símbolo de sistema y seleccionar: Go To Process
 - h. Clic derecho en el proceso y seleccionar: End Process Tree
 - i. Aceptar el mensaje de advertencia

NOTA: Paint sigue abierto, Windows no tiene forma de relacionar un proceso nieto con el proceso abuelo.

4. **Process Explorer:** Es una herramienta del sysinternals que muestra información detallada de lo que son los procesos e hilos.

TIPS:

- a. Procesos alojando servicios se muestran en color rosado
 - b. Procesos propios están de color azul
 - c. Nuevos procesos se muestra momentáneamente en color verdes
 - d. Procesos cerrándose se muestra momentáneamente en color rojo
 - e. Poner el mouse encima de un proceso te mostrara el full path
 - f. Apretar en la columna de procesos cambiara la forma en que se muestra los procesos
 - g. Doble clic en un proceso mostrara una ventana con las propiedades del proceso
5. Cargar Windows Debugger localmente
- a. Descargar **LiveKD** (<http://technet.microsoft.com/en-us/sysinternals/bb897415>)
 - b. Ejecutar **livekd.exe** en un símbolo de sistema como administrador:



```
Administrator: C:\Windows\System32\cmd.exe - livekd.exe -w -k "C:\Program Files\Debugging Tools for Windows (x86)\windbg.exe"

C:\Users\Mino\Desktop\LiveKd>livekd.exe -w -k "C:\Program Files\Debugging Tools for Windows (x86)\windbg.exe"

LiveKd v5.0 - Execute kd/windbg on a live system
Sysinternals - www.sysinternals.com
Copyright (C) 2000-2010 Mark Russinovich and Ken Johnson

Launching C:\Program Files\Debugging Tools for Windows (x86)\windbg.exe:
```

Nota: Lo siguientes parámetros sirven para:

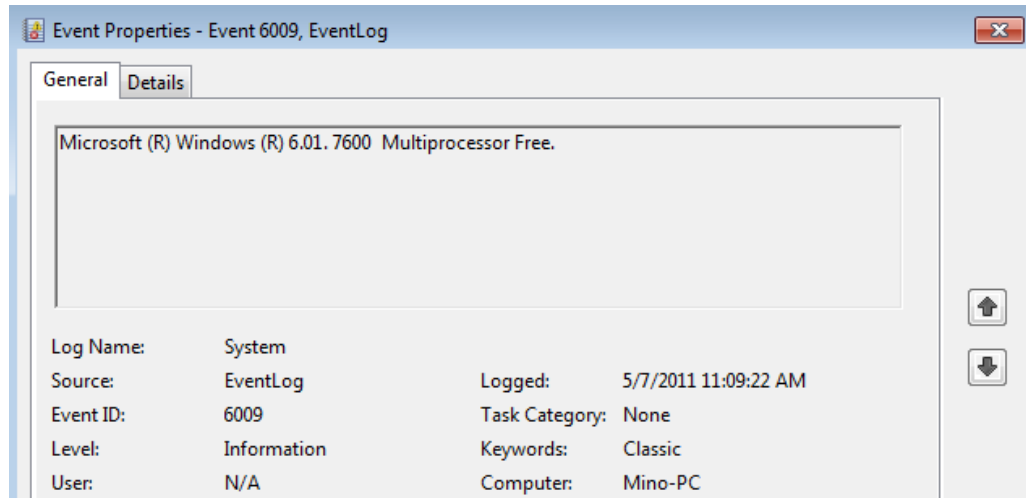
–w: lanzar “windbg.exe”.

–k: path del debugger.

- c. Seleccionar descargar símbolos (por defecto **c:\Symbols**)
- d. Tardara un poco para que Windbg se ejecute porque tiene que tener ciertos símbolos descargados
- e. **Windbg** será abierto
- f. Mostrar estructuras del Kernel: **dt nt!_***
- g. Usar wildcards con el comando dt para encontrar estructuras específicas: **dt nt!_*interrupt***
- h. Mostrar subestructuras (por defecto no muestra, usar –r para mostrar): **dt nt!_kinterrupt –r**

6. Versión del Kernel

- a. En Windows debugger escribir: **lm vm nt**
- b. También es posible identificar la versión del Kernel desde event viewer (**Start Menu->Programs->Administrative Tools->Event Viewer**). Cuando Windows se inicializa escribe el evento 6009 (System event) con información del Kernel:



7. Versión del HAL

- a. En Windows debugger escribir: **lm vm hal**

8. Ver características habilitadas por licencia de Windows

- a. **SIPolicy.exe**

9. Identificar checked build

- a. Guardar el siguiente script como .vbs (checkedbuild.vbs)

```
strComputer = "."  
Set objWMIService = GetObject("winmgmts:" _  
& "{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")  
Set colOperatingSystems = objWMIService.ExecQuery _  
("SELECT * FROM Win32_OperatingSystem")  
For Each objOperatingSystem in colOperatingSystems  
Wscript.Echo "Caption: " & objOperatingSystem.Caption  
Wscript.Echo "Debug: " & objOperatingSystem.Debug  
Wscript.Echo "Version: " & objOperatingSystem.Version  
Next
```

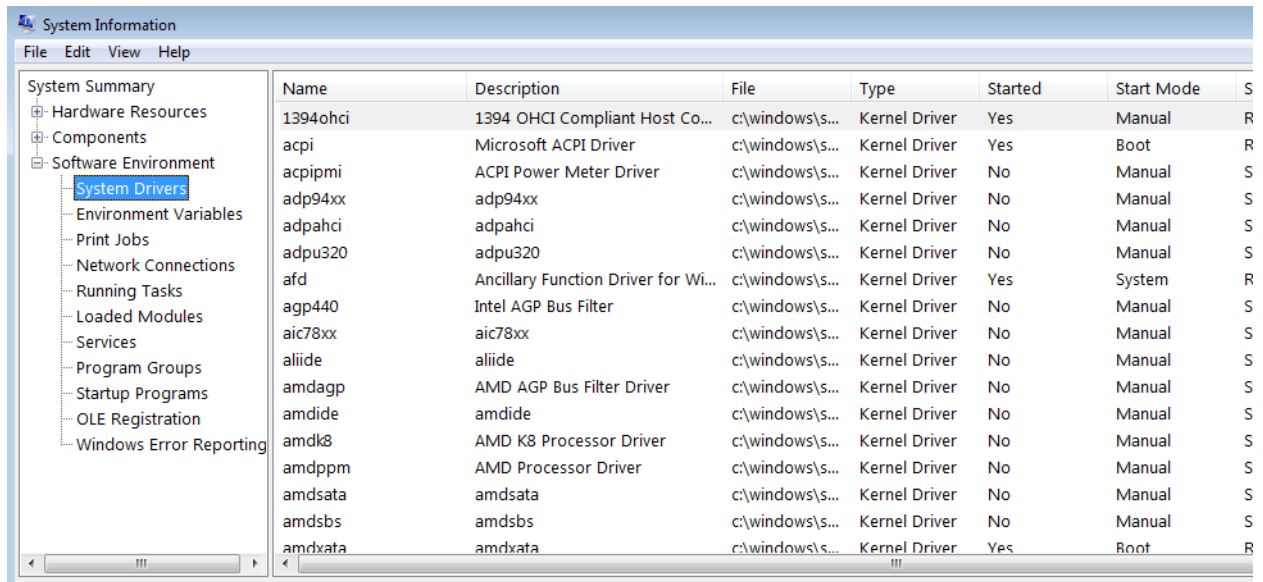
- b. Doble clic en el archivo guardado (checkedbuild.vbs)
- c. También es posible identificar si es una instalación checked o free desde el event log (**Start Menu->Programs->Administrative Tools->Event Viewer**). Cuando Windows se inicializa escribe el evento 6009 (System event).

10. Depends.exe

- Select File->Open
- Abrir cada uno de las imágenes (cmd.exe, notepad.exe, Ntoskrnl.exe)
- Ver el listado de librerías

11. Mostrar Device drivers instalados

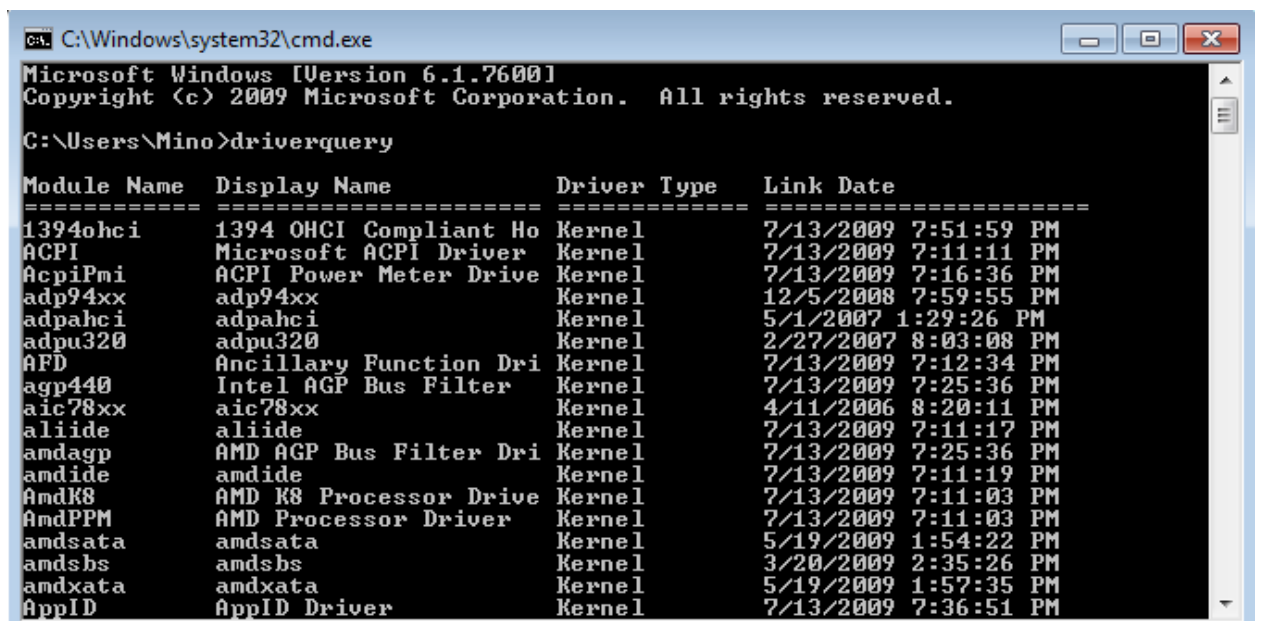
- Menú inicio->Run
- Escribir: **Msinfo32**



The screenshot shows the 'System Information' window with the 'System Drivers' tab selected. The left sidebar shows a tree view with 'System Drivers' highlighted. The main pane displays a table of installed drivers.

Name	Description	File	Type	Started	Start Mode	S
1394ohci	1394 OHCI Compliant Host Co...	c:\windows\s...	Kernel Driver	Yes	Manual	R
acpi	Microsoft ACPI Driver	c:\windows\s...	Kernel Driver	Yes	Boot	R
acpimmi	ACPI Power Meter Driver	c:\windows\s...	Kernel Driver	No	Manual	S
adp94xx	adp94xx	c:\windows\s...	Kernel Driver	No	Manual	S
adpahci	adpahci	c:\windows\s...	Kernel Driver	No	Manual	S
adpu320	adpu320	c:\windows\s...	Kernel Driver	No	Manual	S
afd	Ancillary Function Driver for Wi...	c:\windows\s...	Kernel Driver	Yes	System	R
agp440	Intel AGP Bus Filter	c:\windows\s...	Kernel Driver	No	Manual	S
aic78xx	aic78xx	c:\windows\s...	Kernel Driver	No	Manual	S
aliide	aliide	c:\windows\s...	Kernel Driver	No	Manual	S
amdagp	AMD AGP Bus Filter Driver	c:\windows\s...	Kernel Driver	No	Manual	S
amdide	amdide	c:\windows\s...	Kernel Driver	No	Manual	S
amdk8	AMD K8 Processor Driver	c:\windows\s...	Kernel Driver	No	Manual	S
amdppm	AMD Processor Driver	c:\windows\s...	Kernel Driver	No	Manual	S
amdsata	amdsata	c:\windows\s...	Kernel Driver	No	Manual	S
amdsbs	amdsbs	c:\windows\s...	Kernel Driver	No	Manual	S
amdxdta	amdxdta	c:\windows\s...	Kernel Driver	Yes	Boot	R

- También es posible ver los drivers instalados ejecutando “**driverquery**” desde el símbolo de sistema.

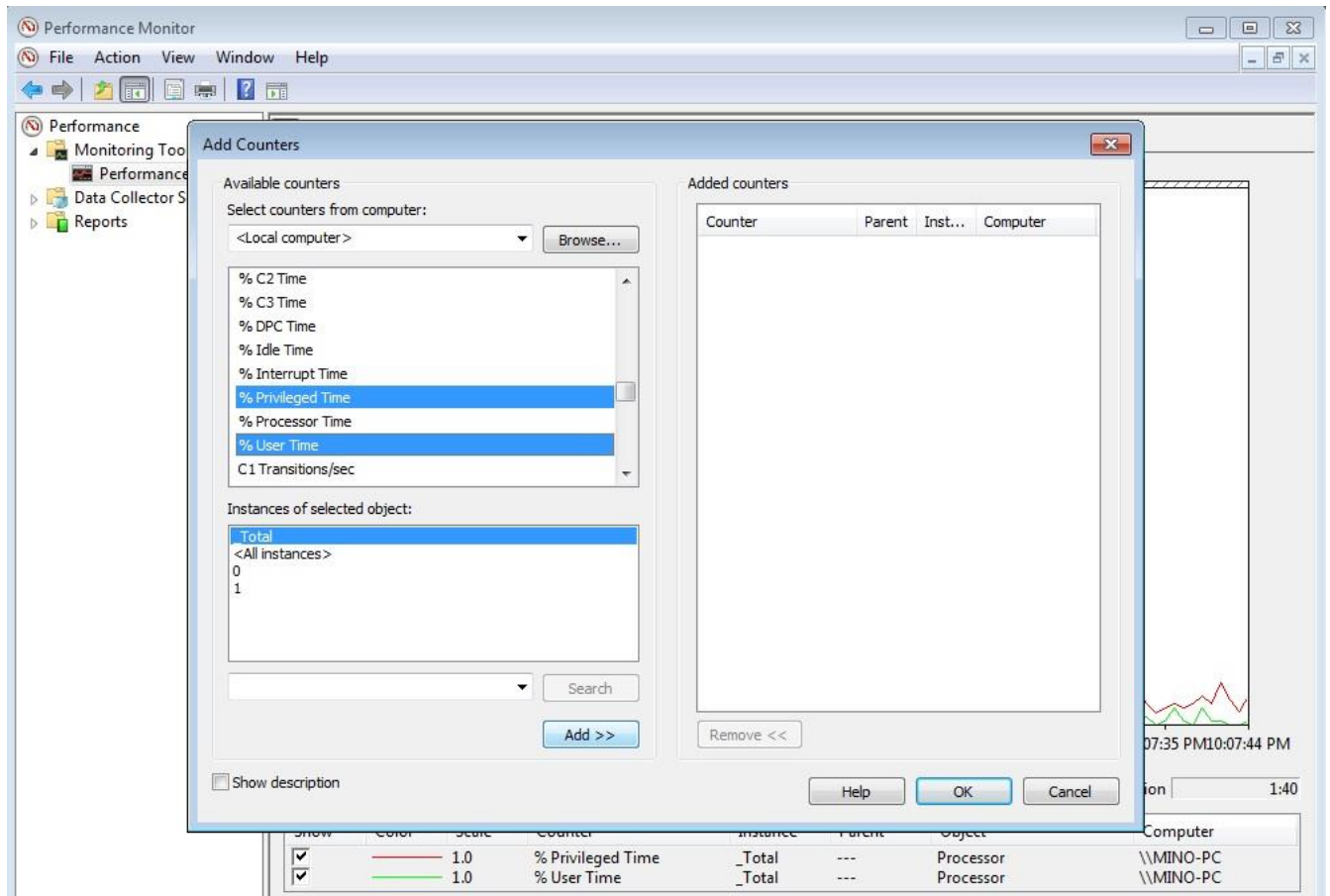


The screenshot shows a Windows command prompt window with the command 'driverquery' executed. The output is a table of installed drivers.

Module Name	Display Name	Driver Type	Link Date
1394ohci	1394 OHCI Compliant Ho	Kernel	7/13/2009 7:51:59 PM
ACPI	Microsoft ACPI Driver	Kernel	7/13/2009 7:11:11 PM
AcpiPmi	ACPI Power Meter Drive	Kernel	7/13/2009 7:16:36 PM
adp94xx	adp94xx	Kernel	12/5/2008 7:59:55 PM
adpahci	adpahci	Kernel	5/1/2007 1:29:26 PM
adpu320	adpu320	Kernel	2/27/2007 8:03:08 PM
AFD	Ancillary Function Dri	Kernel	7/13/2009 7:12:34 PM
agp440	Intel AGP Bus Filter	Kernel	7/13/2009 7:25:36 PM
aic78xx	aic78xx	Kernel	4/11/2006 8:20:11 PM
aliide	aliide	Kernel	7/13/2009 7:11:17 PM
amdagp	AMD AGP Bus Filter Dri	Kernel	7/13/2009 7:25:36 PM
amdide	amdide	Kernel	7/13/2009 7:11:19 PM
AmdK8	AMD K8 Processor Drive	Kernel	7/13/2009 7:11:03 PM
AmdPPM	AMD Processor Driver	Kernel	7/13/2009 7:11:03 PM
amdsata	amdsata	Kernel	5/19/2009 1:54:22 PM
amdsbs	amdsbs	Kernel	3/20/2009 2:35:26 PM
amdxdta	amdxdta	Kernel	5/19/2009 1:57:35 PM
AppID	AppID Driver	Kernel	7/13/2009 7:36:51 PM

12. Tiempo procesador en Kernel Mode vs User Mode

- Escribir Performance monitor en menú de inicio
- Apretar el botón + de la barra de herramientas
- En el objeto **procesador** seleccionar: **%Privileged Time** y **%User Time**



- Mover el ratón y ver como los contadores incrementan

NOTA: Se podrá observar los mismos contadores desde el administrador de tareas en la pestaña de performance. (Menú->View->Show Kernel Time).