

**UNIVERSIDAD AUTÓNOMA “TOMAS FRÍAS”**  
**CARRERA DE INGENIERÍA DE SISTEMAS**

**ESTUDIANTE: HERSON JOSE CANAZA DELGADO**

<b>Materia:</b>	Arquitectura de computadoras (SIS-522)			 Nº Práctica
<b>Docente:</b> <b>Auxiliar:</b>	Ing. Gustavo A. Puita Choque Univ. Aldrin Roger Perez Miranda			
<b>23/09/2024</b>	<b>Fecha publicación</b>			3
<b>08/09/2024</b>	<b>Fecha de entrega</b>			
<b>Grupo:</b>	1	Sede	Potosí	

**PARTE TEÓRICA (50 pts)**

**1) ¿Cuál es la diferencia fundamental entre una memoria RAM y una memoria ROM en términos de accesibilidad y volatilidad? (2 pts)**

R.- La RAM (Memoria de Acceso Aleatorio) es volátil, lo que significa que pierde su contenido cuando se apaga el dispositivo. Permite lectura y escritura rápida de datos. La ROM (Memoria de Sólo Lectura) es no volátil, conservando su contenido incluso sin energía. Como su nombre indica, generalmente sólo permite la lectura de datos, no la escritura.

**2) ¿Qué ventajas y desventajas presentan las memorias estáticas y dinámicas en términos de velocidad, densidad y costo? (2 pts)**

R.-

- Memoria Estática:

Ventajas: Mayor velocidad, No necesita refrescamiento, Menor consumo de energía

Desventajas: Más cara, Menor densidad (ocupa más espacio), Costo por bit más alto

- DRAM (Memoria Dinámica): Ventajas: Mayor densidad (más capacidad en menos espacio), Más económica, Menor costo por bit

Desventajas: Más lenta que SRAM, Requiere refrescamiento constante, Mayor consumo de energía

**3) ¿Por qué se utiliza la tecnología de Video RAM (VRAM) en los controladores de video de las computadoras y cuál es su función principal? (2 pts)**

R.- Se utiliza en los controladores de video de las computadoras porque permite almacenar y acceder rápidamente a los datos gráficos, como texturas e imágenes, que se necesitan para renderizar la pantalla. Su función principal es mejorar el rendimiento gráfico, al reducir la latencia.

**4) Dibuja un diagrama que represente la jerarquía de memoria en un sistema informático típico y etiqueta cada nivel con el tipo correspondiente de memoria. (2 pts)**



R.-

**5) ¿Qué diferencias existen entre la memoria caché L1, L2 y L3 en términos de tamaño, velocidad y proximidad al procesador? (2 pts)**

R.- Caché L1:

- La más cercana al procesador (integrada en el núcleo)
- Tamaño más pequeño (típicamente 32-64 KB por núcleo)
- Velocidad más rápida (acceso en 2-4 ciclos de reloj)
- Una por núcleo del procesador

Caché L2:

- Segunda más cercana al procesador
- Tamaño medio (256 KB - 1 MB por núcleo)
- Velocidad intermedia (acceso en 10-20 ciclos)
- Puede ser compartida entre pares de núcleos

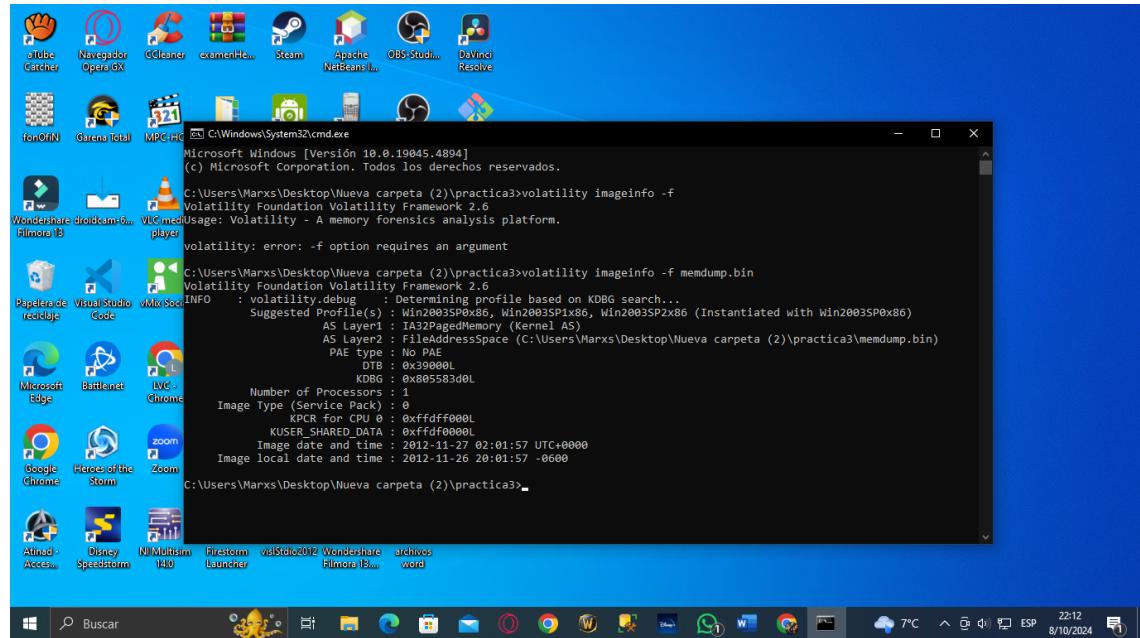
Caché L3:

- La más alejada del procesador
- Tamaño más grande (varios MB, compartidos)
- Velocidad más lenta de las tres (20-60 ciclos)
- Compartida entre todos los núcleos

6) Resolver el siguiente laboratorio paso a paso con capturas propias mostrando su barra de tareas de su pc (40 pts)

## ANALISIS DE MEMORIA RAM CON VOLATILITY

### PASO 3



### Paso 4

```
C:\Windows\System32\cmd.exe
OSXPMemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 pslist
Volatility Foundation Volatility Framework 2.6
-----
Offset(V) Name PID PPID Thds Hnds Sess Wow64 Start Exit
-----
0x822b07a8 System 4 0 52 842 ----- 0
0x820c6028 smss.exe 372 4 3 17 0 0 2012-11-03 20:18:29 UTC+0000
0x82031020 csrss.exe 420 372 11 505 0 0 2012-11-03 20:18:30 UTC+0000
0x820496c8 winlogon.exe 444 372 19 613 0 0 2012-11-03 20:18:30 UTC+0000
0x8203fa00 services.exe 488 444 21 422 0 0 2012-11-03 20:18:31 UTC+0000
0x82022920 lsass.exe 500 444 58 959 0 0 2012-11-03 20:18:31 UTC+0000
0x822bc770 svchost.exe 740 488 12 230 0 0 2012-11-03 20:18:33 UTC+0000
0x821fdfe0 svchost.exe 884 488 9 133 0 0 2012-11-03 20:18:44 UTC+0000
0x81ffdaf8 svchost.exe 904 488 5 78 0 0 2012-11-03 20:18:44 UTC+0000
0x81fcfa98 spoolsv.exe 934 488 47 1992 0 0 2012-11-03 20:18:44 UTC+0000
0x81fcfa00 spoolsv.exe 1216 488 9 155 0 0 2012-11-03 20:19:12 UTC+0000
0x81810000 mediatomb.exe 1408 488 15 160 0 0 2012-11-03 20:19:12 UTC+0000
0x81c32d88 mfcv.dll 1513 488 10 106 0 0 2012-11-03 20:19:12 UTC+0000
0x81c19900 svchost.exe 1494 488 2 69 0 0 2012-11-03 20:19:12 UTC+0000
0x81c2d288 ismservr.exe 1436 488 11 276 0 0 2012-11-03 20:19:12 UTC+0000
0x81c1b0120 ntfrs.exe 1452 488 19 282 0 0 2012-11-03 20:19:12 UTC+0000
0x81c71020 svchost.exe 1512 488 2 34 0 0 2012-11-03 20:19:13 UTC+0000
0x81c46288 svchost.exe 1736 488 16 127 0 0 2012-11-03 20:19:27 UTC+0000
0x81c4bd88 explorer.exe 188 1996 11 337 0 0 2012-11-03 21:32:30 UTC+0000
0x81c4ad88 dns.exe 340 488 12 163 0 0 2012-11-03 21:41:26 UTC+0000
0x81bf9020 wins.exe 756 488 19 214 0 0 2012-11-04 17:02:07 UTC+0000
0x81be0108 wuauctl.exe 1092 932 5 74 0 0 2012-11-04 18:57:32 UTC+0000
0x81be1b18 dllhost.exe 3292 488 18 254 0 0 2012-11-24 17:47:12 UTC+0000
0x81b4b9d0 appmgr.exe 2992 488 4 102 0 0 2012-11-24 17:47:40 UTC+0000
0x81b1bb08 srvcsrcs.exe 1496 488 3 87 0 0 2012-11-24 17:47:40 UTC+0000
0x81b1bf348 netinfo.exe 308 488 25 515 0 0 2012-11-24 17:47:51 UTC+0000
0x81b17188 wmprvse.exe 2116 748 7 208 0 0 2012-11-24 17:48:40 UTC+0000
0x81b154d8 POP3svc.exe 2260 488 8 208 0 0 2012-11-24 17:55:08 UTC+0000
0x81a6e200 cmd.exe 2976 188 1 22 0 0 2012-11-24 18:01:57 UTC+0000
0x81c25b08 mud.exe 5468 2076 1 25 0 0 2012-11-27 02:01:56 UTC+0000

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>
```

### Paso 5

```
C:\Windows\System32\cmd.exe
0x81b8f348 inetinfo.exe      308   488   25    515   0     0 2012-11-24 17:47:51 UTC+0000
0x81b71788 wminprvse.exe    2116   740    7    208   0     0 2012-11-24 17:48:48 UTC+0000
0x81bda4d8 POP3svc.exe     2260   488    7    142   0     0 2012-11-24 17:55:08 UTC+0000
0x81ae2020 cmd.exe        2076   188    1    22   0     0 2012-11-27 01:37:57 UTC+0000
0x81c5b68 mdd.exe         3468   2076   1    25   0     0 2012-11-27 02:01:56 UTC+0000

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 pstrace
Volatility Foundation Volatility Framework 2.6
Name          Pid  PPid Thds Hnds Time
-----
0x822bb7a8:System          4    0    52   842 1970-01-01 00:00:00 UTC+0000
0x820c6020:smsvc.exe      372    4    3   17 2012-11-03 20:18:29 UTC+0000
0x82031020:csrss.exe      420    372   11   505 2012-11-03 20:18:30 UTC+0000
0x820494c8:winlogon.exe    444    372   19   613 2012-11-03 20:18:30 UTC+0000
0x82022920:lsass.exe      500    444   58   959 2012-11-03 20:18:31 UTC+0000
0x8203fd0:services.exe    488    444   21   422 2012-11-03 20:18:31 UTC+0000
0x81f1daff:svchost.exe    904    488   5    78 2012-11-03 20:18:44 UTC+0000
0x81b0bb0:svrscung.exe   1496   488   3    87 2012-11-24 17:47:48 UTC+0000
0x81b182d88:ismserv.exe   1436   488   11   276 2012-11-03 20:19:12 UTC+0000
0x81f1df2e0:svchost.exe   884    488   9    133 2012-11-03 20:19:44 UTC+0000
0x81ca3d68:dfssvc.exe    1312   488   16   106 2012-11-03 20:19:12 UTC+0000
0x81c0400:ntfrs.exe       1452   488   19   282 2012-11-03 20:19:44 UTC+0000
0x81b0400:spoolsvr.exe    2997   488   4    602 2012-11-24 17:47:49 UTC+0000
0x81b18f74d8:inetinfo.exe 3088   488   25   515 2012-11-24 17:47:51 UTC+0000
0x81cafd2d8:spoolsv.exe  1216   488   9    135 2012-11-03 20:19:12 UTC+0000
0x81c1462e8:svchost.exe  1736   488   16   127 2012-11-03 20:19:27 UTC+0000
0x81c144d88:dns.exe      340    488   12   163 2012-11-03 21:41:26 UTC+0000
0x81c1bad88:sdts.exe     1240   488   15   169 2012-11-03 20:19:12 UTC+0000
0x81f1d6968:svchost.exe  932    488   47   1092 2012-11-03 20:19:44 UTC+0000
0x81be0108:wuauclt.exe   1092   932    5   74 2012-11-04 18:57:32 UTC+0000
0x81b61b18:dlldhost.exe  3292   488   18   254 2012-11-24 17:47:12 UTC+0000
0x822bc770:svchost.exe  740    488   12   230 2012-11-03 20:18:33 UTC+0000
0x81b71788:wminprvse.exe 2116   740    7    208 2012-11-24 17:48:48 UTC+0000
0x81c71020:svchost.exe  1512   488    2   34 2012-11-03 20:19:13 UTC+0000
0x81b1f0020:wins.exe     756    488   19   214 2012-11-03 17:02:01 UTC+0000
0x81b16a4d8:POP3svc.exe  2260   488    7   142 2012-11-24 17:55:08 UTC+0000
0x81c199020:svchost.exe  1404   488    2   66 2012-11-03 20:19:12 UTC+0000
0x81c4b088:explorer.exe 188    1996   11   337 2012-11-03 21:32:38 UTC+0000
0x81ae2020:cmd.exe      2076   188    1    22 2012-11-27 01:37:57 UTC+0000
0x81c25b68:mdd.exe      3468   2076   1    25 2012-11-27 02:01:56 UTC+0000

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>
```

## Paso 6

```
C:\Windows\System32\cmd.exe
, 0x81ae2020:cmd.exe      2076   188    1    22 2012-11-27 01:37:57 UTC+0000
, 0x81c25b68:mdd.exe      3468   2076   1    25 2012-11-27 02:01:56 UTC+0000

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>volatility -f memdump.bin --profile=Win2003SP0x86 dlllist
Volatility Foundation Volatility Framework 2.6
*****
System pid:          4
Unable to read PEB for task.
*****
smss.exe pid:        372
Command line : \SystemRoot\System32\smss.exe

Base      Size LoadCount Path
-----
0x48580000 0xfffff 0xfffff \SystemRoot\System32\smss.exe
0x77f40000 0xb000 0xfffff C:\WINDOWS\system32\ntdll.dll
*****
csrss.exe pid:       420
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,3072,512 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDlInitialization,3 ServerDll=conservDlInitialization,2 ProfileControl=Off MaxRequestThreads=6

Base      Size LoadCount Path
-----
0x44680000 0x4000 0xfffff ?>C:\WINDOWS\system32\csrss.exe
0x77f40000 0xb000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x75a50000 0xb000 0xfffff C:\WINDOWS\system32\CSRSRV.dll
0x75a60000 0xf000 0x3 C:\WINDOWS\system32\basesrv.dll
0x75a80000 0x4c000 0x2 C:\WINDOWS\system32\winsrv.dll
0x77e40000 0x14000 0x10 C:\WINDOWS\system32\KERNELE32.dll
0x77d60000 0x5f000 0x6 C:\WINDOWS\system32\USER32.dll
0x77d70000 0x20000 0x3 C:\WINDOWS\system32\GDI32.dll
0x75d40000 0x2a000 0x1 C:\WINDOWS\system32\xps.dll
0x77d30000 0x20000 0x3 C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x4000 0x3 C:\WINDOWS\system32\RPCRT4.dll
0x75e60000 0x22000 0x1 C:\WINDOWS\system32\apphelp.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
*****
winlogon.exe pid:      444
Command line : winlogon.exe

Base      Size LoadCount Path
-----
```

```
C:\Windows\System32\cmd.exe
winlogon.exe pid: 444
Command line : winilogon.exe

Base           Size  LoadCount Path
0x0100000000 0x8b0000 0xfffff :\?;c:\WINDOWS\system32\winlogon.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ha0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x2f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c60000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x75970000 0xba000 0xfffff C:\WINDOWS\system32\USERENV.dll
0x75810000 0x7000 0xfffff C:\WINDOWS\system32\NDR32.dll
0x761b0000 0x98000 0xfffff C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0xfffff C:\WINDOWS\system32\MSASN1.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Searur32.dll
0x76260000 0x10000 0xfffff C:\WINDOWS\system32\WINSTA.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x75860000 0x6000 0xfffff C:\WINDOWS\system32\PEFMAP.dll
0x77d70000 0x1f000 0xfffff C:\WINDOWS\system32\OLE32.dll
0x71c00000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71b70000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x76b70000 0xb000 0xfffff C:\WINDOWS\system32\PSAPI.dll
0x77b90000 0x8000 0xfffff C:\WINDOWS\system32\VERSION.dll
0x765a0000 0x100000 0xfffff C:\WINDOWS\system32\SETUPAPI.dll
0x75840000 0x128000 0x2 C:\WINDOWS\system32\MSGINA.dll
0x76b40000 0x21000 0x1 C:\WINDOWS\system32\SHSVCS.dll
0x77290000 0x49000 0x29 C:\WINDOWS\system32\SHLWAPI.dll
0x76b10000 0x5000 0x2 C:\WINDOWS\system32\sfc.dll
0x76be0000 0x2a000 0x5 C:\WINDOWS\system32\sfc_os.dll
0x76bb0000 0x2b000 0x5 C:\WINDOWS\system32\WINTRUST.dll
0x77160000 0x124000 0x2a C:\WINDOWS\system32\ole32.dll
0x76c10000 0x28000 0x5 C:\WINDOWS\system32\imghelp.dll
0x76ad0000 0x6e000 0xa C:\Windows\Win32\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-wv_8417450B\Comctl32.dll
0x72430000 0x1c000 0x1 C:\WINDOWS\system32\WINSCARD.DLL
0x76f80000 0x8000 0x7 C:\WINDOWS\system32\WTSAPI32.dll
0x75d40000 0x10000 0x1 C:\WINDOWS\system32\WTSAPI32.dll
0x77f70000 0x9000 0x9 C:\WINDOWS\system32\hel1132.dll
0x71b30000 0x9000 0x1 C:\WINDOWS\system32\wsock32.dll
0x76c70000 0x17000 0x4 C:\WINDOWS\system32\iphlpapi.dll
0x74010000 0x5000 0x1 C:\WINDOWS\system32\icmp.dll
```

```
C:\Windows\System32\cmd.exe
0x75d40000 0xb0000 0x1 C:\WINDOWS\system32\sxs.dll
0x77380000 0x7dd000 0x8c C:\WINDOWS\system32\shell32.dll
0x71b40000 0x9000 0x1 C:\WINDOWS\system32\wsock32.dll
0x76cf0000 0x17000 0x4 C:\WINDOWS\system32\iphlpapi.dll
0x74030000 0x5000 0x1 C:\WINDOWS\system32\icmp.dll
0x0ff40000 0x2d000 0x1 C:\WINDOWS\system32\raenh.dll
0x76c60000 0x17000 0x1 C:\WINDOWS\system32\MPRAPI.dll
0x76d70000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adsldpc.dll
0x76f10000 0x2f000 0x10 C:\WINDOWS\system32\WLDAP32.dll
0x76b30000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x76a80000 0x18000 0x1 C:\WINDOWS\system32\ATL.dll
0x770e0000 0x7d000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0x20000 0x1 C:\WINDOWS\system32\VTUTILS.dll
0x75c50000 0x16000 0x3 C:\WINDOWS\system32\ASync.dll
0x71b20000 0x3f000 0x4 C:\WINDOWS\system32\ws2sock.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\system32\rsashdrp.dll
0x71ca0000 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x766a0000 0xc000 0x1 C:\WINDOWS\system32\crypt32.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshftp.dll
0x76f60000 0x16000 0x3 C:\WINDOWS\system32\NTDSAPI.dll
0x75e00000 0x27000 0x4 C:\WINDOWS\system32\DNSAPI.dll
0x76520000 0x1d000 0x2 C:\WINDOWS\system32\scsd11.dll
0x75820000 0x1a000 0x6 C:\WINDOWS\system32\WINotify.dll
0x76a60000 0x2c000 0x7 C:\WINDOWS\system32\WINMM.dll
0x73070000 0x26000 0x6 C:\WINDOWS\system32\WINSPPOOL.DRV
0x71b00000 0x11000 0x7 C:\WINDOWS\system32\WPR.dll
0x76bc0000 0x90000 0x1 C:\Windows\Win32\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-wv_8A69BA05\COMCTL32.dll
0x71b70000 0x33000 0x2 C:\WINDOWS\system32\UXTheme.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0x6c000 0x1 C:\WINDOWS\system32\COMRes.dll
0x74c40000 0x8000 0x1 C:\WINDOWS\system32\wbem\wbemprox.dll
0x73230000 0x38000 0x2 C:\WINDOWS\system32\wbem\wbemcom.dll
0x74c10000 0x10000 0x1 C:\WINDOWS\system32\wbem\wbemserv.dll
0x75550000 0x71000 0x1 C:\WINDOWS\system32\wbem\fastprox.dll
0x78900000 0x61000 0x1 C:\WINDOWS\system32\MSVCP60.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x75540000 0x50000 0x1 C:\WINDOWS\system32\scsi1.dll
0x76fa0000 0x3e000 0x1 C:\WINDOWS\system32\ES.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WTMARTA.dll
0x74fa0000 0x14000 0x1 C:\WINDOWS\system32\Cabinet.dll
0x73ca0000 0x12000 0x1 C:\WINDOWS\system32\cryptnet.dll
0x722f0000 0x5000 0x1 C:\WINDOWS\system32\Sensa.dll
```

```
C:\Windows\System32\cmd.exe
=====
0x722f0000 0x5000 0xa C:\WINDOWS\system32\SensApi.dll
***** services.exe pid: 488
Command line : C:\WINDOWS\system32\services.exe

Base      Size  LoadCount Path
0x01000000 0x1b000 0xfffff C:\WINDOWS\system32\services.exe
0x77fa0000 0x9a000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c5d000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d0d000 0xb7000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c6c000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x75970000 0xba000 0xfffff C:\WINDOWS\system32\USERENV.dll
0x757a0000 0x52000 0xfffff C:\WINDOWS\system32\SCSERV.dll
0x76c4c000 0x14000 0xfffff C:\WINDOWS\system32\AUTHZ.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x75770000 0x21000 0xfffff C:\WINDOWS\system32\umnpngr.dll
0x762c0000 0x16000 0xfffff C:\WINDOWS\system32\WINSTA.dll
0x75f10000 0x10000 0xfffff C:\WINDOWS\system32\ole32.dll
0x75800000 0x51000 0xfffff C:\WINDOWS\system32\MSVCP60.dll
0x76f50000 0x13000 0x6 C:\WINDOWS\system32\sec32.dll
0x75750000 0x12000 0x1 C:\WINDOWS\system32\eventlog.dll
0x71c80000 0x18000 0x7 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x76f60000 0x8000 0x1 C:\WINDOWS\system32\wtsapi32.dll
0x74190000 0x30000 0x1 C:\WINDOWS\system32\secl1.dll
0x765a0000 0x10000 0x2 C:\WINDOWS\system32\SETUPAPI.dll
0x74fa0000 0x14000 0x1 C:\WINDOWS\system32\Cabinet.dll
0x77160000 0x124000 0x2 C:\WINDOWS\system32\ole32.dll
0x5ccf0000 0x10000 0x2 C:\WINDOWS\system32\SAMLIB.dll
0x69750000 0x108000 0x1 C:\WINDOWS\system32\ESSENT.dll
0x76c00000 0x20000 0x1 C:\WINDOWS\system32\MTMARTA.dll
0x76f10000 0x2f000 0x3 C:\WINDOWS\system32\WLDAP32.dll
0x71b20000 0x43000 0x2 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\winhttp.dll
0x76f60000 0x10000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x76e60000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x71ca0000 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x76660000 0xc000 0x1 C:\WINDOWS\system32\crypt.dll
0x76660000 0x2c000 0x1 C:\WINDOWS\system32\crypt.dll
```

```
C:\Windows\System32\cmd.exe
=====
lsass.exe pid: 500
Command line : C:\WINDOWS\system32\lsass.exe

Base      Size  LoadCount Path
0x01000000 0x6000 0xfffff C:\WINDOWS\system32\lsass.exe
0x77fa0000 0x9a000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c5d000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x742c0000 0x8c000 0xfffff C:\WINDOWS\system32\LSASRV.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x77d0d000 0xb7000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c6c000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x741a0000 0x76000 0xfffff C:\WINDOWS\system32\SAMSRV.dll
0x76660000 0xcc000 0xfffff C:\WINDOWS\system32\crypt.dll
0x76e60000 0x27000 0xfffff C:\WINDOWS\system32\DNSAPI.dll
0x71c60000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x76190000 0x12000 0xfffff C:\WINDOWS\system32\WTSNSI.dll
0x71c40000 0x10000 0xfffff C:\WINDOWS\system32\WNETAPI.dll
0x765a0000 0x10000 0xfffff C:\WINDOWS\system32\SAMLIB.dll
0x71bd0000 0x11000 0xfffff C:\WINDOWS\system32\WPR.dll
0x766f0000 0x16000 0xfffff C:\WINDOWS\system32\WTDSSAP.dll
0x76f10000 0x2f000 0xfffff C:\WINDOWS\system32\WLDAP32.dll
0x7413a000 0xe000 0x1 C:\WINDOWS\system32\msprivs.dll
0x71ca0000 0x56000 0x6 C:\WINDOWS\system32\kerberos.dll
0x76c90000 0x24000 0xf C:\WINDOWS\system32\msv1_0.dll
0x74250000 0x68000 0x8 C:\WINDOWS\system32\netlogon.dll
0x76730000 0x38000 0x8 C:\WINDOWS\system32\w32time.dll
0x780c0000 0x61000 0x8 C:\WINDOWS\system32\MSVCP60.dll
0x76c50000 0x17000 0xa C:\WINDOWS\system32\iphlpapi.dll
0x75970000 0xba000 0xfffff C:\WINDOWS\system32\USERENV.dll
0x76c40000 0x14000 0x17 C:\WINDOWS\system32\AUTHZ.dll
0x76750000 0x28000 0x7 C:\WINDOWS\system32\sschannel.dll
0x761b0000 0x98000 0x1a C:\WINDOWS\system32\CRYPT32.dll
0x741b0000 0x12000 0x3 C:\WINDOWS\system32\wdigest.dll
0x0ff00000 0xd2000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb7000 0x2 C:\WINDOWS\system32\PSAPI.dll
0x720e0000 0x19a000 0xa C:\WINDOWS\system32\WTDSSA.dll
0x71f00000 0xb000 0xe C:\WINDOWS\system32\WTDSSATQ.dll
```

```

C:\Windows\System32\cmd.exe
0x77160000 0x124000 0x12 C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0x9 C:\WINDOWS\system32\OLEAUT32.dll
0x63a80000 0x3a000 0x4 C:\WINDOWS\system32\KDSVC.dll
0x5d9f0000 0x9000 0x1 C:\WINDOWS\system32\RASSPSP.dll
0x74190000 0x38000 0x3 C:\WINDOWS\system32\RPCRT4.dll
0x72e20000 0x38000 0x5 C:\WINDOWS\system32\SETUPAPI.dll
0x712a0000 0x8000 0x1 C:\WINDOWS\system32\wshTCPip.dll
0x5de80000 0x7000 0x1 C:\WINDOWS\system32\pwdsp.dll
0x71e00000 0x14000 0x1 C:\WINDOWS\system32\msaspsspc.dll
0x78880000 0x11000 0x1 C:\WINDOWS\system32\MSVCRT40.dll
0x720a0000 0x1f000 0x1 C:\WINDOWS\system32\WTSKCC.dll
0x71f30000 0xa000 0x1 C:\WINDOWS\system32\W32TPL.dll
0x74160000 0xb2000 0x1 C:\WINDOWS\system32\lipsccsvc.dll
0x74390000 0xce000 0x1 C:\WINDOWS\system32\Oakley.DLL
0x740f0000 0xc000 0x1 C:\WINDOWS\system32\WINIPSEC.DLL
0x74120000 0x9000 0x1 C:\WINDOWS\system32\psotrsvc.dll
0x74140000 0x17000 0x1 C:\WINDOWS\system32\psbase.dll
0x0fffa0000 0x22000 0x1 C:\WINDOWS\system32\dssenh.dll
0x56f40000 0x17000 0x1 C:\WINDOWS\system32\wlbsctrl.dll
0x77290000 0x49000 0x6 C:\WINDOWS\system32\SHLWAPI.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77020000 0x7e000 0x2 C:\WINDOWS\system32\CRYPTERS.dll
0x76d00000 0x6000 0x1 C:\WINDOWS\system32\cryptui.dll
0x76f90000 0x5000 0x1 C:\WINDOWS\system32\rasadhlp.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\system32\winrnr.dll
0x76cfa0000 0x20000 0x1 C:\WINDOWS\system32\WTMARTA.dll
0x76c10000 0x17000 0x1 C:\WINDOWS\system32\WPRAPI.dll
0x76df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adsldpc.dll
0x76b20000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x77380000 0x7dd000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x76e30000 0xb000 0x1 C:\WINDOWS\system32\rtrutils.dll
0x78ad0000 0xe6000 0x2 C:\Windows\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-wv_84174508\comctl32.dll
0x5b640000 0x15000 0x2 C:\WINDOWS\system32\strmfilter.dll
0x67150000 0xa000 0x2 C:\WINDOWS\system32\HTTPAPI.dll
*****svchost.exe pid: 748
Command line : C:\WINDOWS\system32\svchost -k rpcss

Base Size LoadCount Path
----- -----
Windows Taskbar

C:\Windows\System32\cmd.exe
0x67150000 0xa000 0x2 C:\WINDOWS\system32\HTTPAPI.dll
*****svchost.exe pid: 748
Command line : C:\WINDOWS\system32\svchost -k rpcss

Base Size LoadCount Path
----- -----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xba000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x75700000 0x48000 0x1 c:\windows\system32\rpcss.dll
0x77ba0000 0x54000 0xf C:\WINDOWS\system32\msvcrtd.dll
0x71c00000 0x18000 0x6 c:\windows\system32\WS2_32.dll
0x71bf0000 0x8000 0x9 c:\windows\system32\WS2HELP.dll
0x77d00000 0x2f000 0x4 C:\WINDOWS\system32\USER32.dll
0x77c70000 0x44000 0x8 C:\WINDOWS\system32\GDI32.dll
0x76f50000 0x13000 0x2 c:\windows\system32\SeHun32.dll
0x71b20000 0x43000 0x3 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshTCPip.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77710000 0x24000 0x1 C:\WINDOWS\system32\ole32.dll
0x77160000 0x56000 0x3 C:\WINDOWS\system32\RPCRT4.dll
0x77010000 0x65000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
*****svchost.exe pid: 884
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService

Base Size LoadCount Path
----- -----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xba000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x76d10000 0x1c000 0x3 c:\windows\system32\dhcpsvc.dll
0x77b30000 0x54000 0x1167 C:\WINDOWS\system32\msvcrtd.dll
0x76ed0000 0x27000 0x5 c:\windows\system32\DNSAPI.dll
0x71c60000 0x18000 0x8ce c:\windows\system32\WS2_32.dll
0x71bf0000 0x8000 0x8c7 c:\windows\system32\WS2HELP.dll
Windows Taskbar

```

```
C:\Windows\System32\cmd.exe
0x76df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adl1pc.dll
0x71c40000 0x53000 0x9 C:\WINDOWS\system32\NEAPI32.dll
0x76f80000 0x2f000 0x3 C:\WINDOWS\system32\WLDAP32.dll
0x76f90000 0x10000 0x1 C:\WINDOWS\system32\ole32.dll
0x77380000 0x7dd000 0x2 C:\WINDOWS\system32\SHLWAPI.dll
0x77290000 0x49000 0x7 C:\WINDOWS\system32\SHLWAPI.dll
0x76a80000 0x18000 0x1 C:\WINDOWS\system32\ATL.dll
0x77160000 0x124000 0x6 C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0x4 C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb0000 0x4 C:\WINDOWS\system32\rutil.dll
0x5cf00000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x765a0000 0x100000 0x1 C:\WINDOWS\system32\SETUPAPI.dll
0x76e90000 0x3b000 0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e40000 0x11000 0x2 C:\WINDOWS\system32\rasman.dll
0x76e60000 0x2e000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76aa0000 0x2c000 0x2 C:\WINDOWS\system32\WINMM.dll
0x761b0000 0x98000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x2 C:\WINDOWS\system32\MSASN1.dll
0x76d30000 0x47000 0x1 C:\WINDOWS\system32\WZCsvc.dll
0x76cc0000 0x5000 0x1 C:\WINDOWS\system32\WMI.dll
0x76fb0000 0x8000 0x1 C:\WINDOWS\system32\WINSAP32.dll
0x76f20000 0x10000 0x2 C:\WINDOWS\system32\WIN32A.dll
0x69750000 0x8000 0x1 C:\WINDOWS\system32\ESSENT.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\system32\WZCSAPI.dll
0x78ad0000 0x6e000 0x3 C:\WINDOWS\WinNSx\vb6_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_9417450B\comct132.dll
0x71b20000 0x43000 0x2 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcp.dll
0x71f60000 0x4000 0x1 C:\WINDOWS\system32\security.dll
0x76f60000 0x16000 0x1 C:\WINDOWS\system32\ntdsapi.dll
*****svchost.exe pid: 904
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService

Base      Size   LoadCount Path
----- -----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\svchost.exe
0x77f00000 0x9a000 0xffff C:\WINDOWS\system32\tdi.dll
0x77e80000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77d90000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c30000 0x5a000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x76cc0000 0x20000 0x1 C:\WINDOWS\system32\WLMARTA.dll
0x77ba0000 0x54000 0xe C:\WINDOWS\system32\msvcr7.dll
*****svchost.exe pid: 922
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs

Base      Size   LoadCount Path
----- -----
0x77c00000 0x44000 0x5 C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x5cf00000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x77160000 0x124000 0x2 C:\WINDOWS\system32\ole32.dll
0x74a40000 0x9000 0x1 C:\WINDOWS\system32\lmhsvc.dll
0x76c70000 0x17000 0x1 C:\WINDOWS\system32\iphlpapi.dll
0x71c60000 0x18000 0x5 C:\WINDOWS\system32\WS2_32.dll
0x71b10000 0x8000 0x5 C:\WINDOWS\system32\WS2HELP.dll
0x71b20000 0x43000 0x1 C:\WINDOWS\system32\mswsock.dll
0x76f30000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x76f90000 0x5000 0x1 C:\WINDOWS\system32\rasadhlp.dll
*****
```

```
C:\Windows\System32\cmd.exe
0x77c00000 0x44000 0x5 C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x5cf00000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x77160000 0x124000 0x2 C:\WINDOWS\system32\ole32.dll
0x74a40000 0x9000 0x1 C:\WINDOWS\system32\lmhsvc.dll
0x76c70000 0x17000 0x1 C:\WINDOWS\system32\iphlpapi.dll
0x71c60000 0x18000 0x5 C:\WINDOWS\system32\WS2_32.dll
0x71b10000 0x8000 0x5 C:\WINDOWS\system32\WS2HELP.dll
0x71b20000 0x43000 0x1 C:\WINDOWS\system32\mswsock.dll
0x76f30000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x76f90000 0x5000 0x1 C:\WINDOWS\system32\rasadhlp.dll
*****svchost.exe pid: 922
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs

Base      Size   LoadCount Path
----- -----
0x01000000 0x6000 0xffff C:\WINDOWS\System32\svchost.exe
0x77f40000 0x9a000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x40000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WLMARTA.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\system32\msvcr7.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c60000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLMAPI.dll
0x5cf00000 0x10000 0x8 C:\WINDOWS\system32\AMILIB.dll
0x77160000 0x124000 0x78 C:\WINDOWS\system32\ole32.dll
0x76d30000 0x17000 0x2 C:\WINDOWS\system32\vcrcv.dll
0x76e30000 0xb000 0x18 C:\WINDOWS\system32\rutil.dll
0x76cc0000 0x5000 0x3 C:\WINDOWS\system32\WMP.dll
0x76d10000 0x1c000 0x3 C:\WINDOWS\system32\DPNSVC.DLL
0x76ed0000 0x27000 0x11 C:\WINDOWS\system32\DNAPI.dll
0x71c60000 0x18000 0x4c C:\WINDOWS\system32\WS2_32.dll
0x71b10000 0x8000 0x32 C:\WINDOWS\system32\WS2HELP.dll
0x76c70000 0x17000 0x2 C:\WINDOWS\system32\iphlpapi.dll
0x76f50000 0x13000 0x2b C:\WINDOWS\system32\Secur32.dll
0x770e0000 0x7d000 0x45 C:\WINDOWS\system32\OLEAUT32.dll
0x761b0000 0x98000 0x26 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x1a C:\WINDOWS\system32\MSASN1.dll
0x76f60000 0x8000 0x8 C:\WINDOWS\system32\WTSAPI32.dll
0x76260000 0x10000 0x10 C:\WINDOWS\system32\WINSTA.dll
*****
```

```
tasklist /v | findstr cmd.exe
0x76a80000 0x18000 0x10 C:\WINDOWS\System32\ATL.DLL
0x753e0000 0x79000 0x3 C:\WINDOWS\System32\CRYPTUI.dll
0x76bb0000 0x2b000 0x8 C:\WINDOWS\System32\WINTRUST.dll
0x76c10000 0x28000 0x9 C:\WINDOWS\System32\WMSA.dll
0x76d30000 0x13000 0x8 C:\WINDOWS\System32\WMSAP1.dll
0x76c00000 0x17000 0x6 C:\WINDOWS\System32\WPAPI.dll
0x76df0000 0x12000 0x6 C:\WINDOWS\System32\ACTIVEDS.dll
0x76dc0000 0x26000 0x6 C:\WINDOWS\System32\adsldpc.dll
0x76eb0000 0x2d000 0x8 C:\WINDOWS\System32\credui.dll
0x77380000 0x7dd000 0xe C:\WINDOWS\System32\SHIEL32.dll
0x765a0000 0x10000 0xd C:\WINDOWS\System32\SETUPAPI.dll
0x76e90000 0x3b000 0x9 C:\WINDOWS\System32\RASAPI32.dll
0x76e40000 0x11000 0xd C:\WINDOWS\System32\rasman.dll
0x76ee0000 0x2e000 0xa C:\WINDOWS\System32\TAPI32.dll
0x76aa0000 0x2c000 0x9 C:\WINDOWS\System32\WINMM.dll
0x76750000 0x28000 0x3 C:\WINDOWS\System32\SCHEMELIB.dll
0x75970000 0x9ba000 0xffff C:\WINDOWS\System32\USERENV.dll
0x72430000 0x1c000 0x3 C:\WINDOWS\System32\WinCard.dll
0x76bc0000 0x90000 0x3 C:\WINDOWS\WinNsxs\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x76ad0000 0x6e000 0x9 C:\WINDOWS\WinNsxs\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\Comctl32.dll
0x74d40000 0x1d000 0x3 C:\WINDOWS\System32\RPCSHELL.dll
0x76b40000 0x21000 0x2 C:\WINDOWS\System32\RPCSVC.dll
0x76f90000 0x19000 0x3 C:\WINDOWS\System32\GLBLCK.dll
0x77700000 0x5000 0x1 C:\WINDOWS\System32\GOMRes.dll
0x77b90000 0x8000 0x7 C:\WINDOWS\System32\VERSION.dll
0x75820000 0x30000 0x1 C:\Windows\System32\schedsvc.dll
0x76c40000 0x14000 0x1 C:\Windows\System32\AUTHz.dll
0x71b20000 0x43000 0x8 C:\WINDOWS\System32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\whtcpip.dll
0x74d70000 0x5000 0x1 C:\WINDOWS\System32\MSIDLE.dll
0x74fc0000 0x23000 0x1 C:\Windows\System32\wksvc.dll
0x59ec0000 0xb000 0x1 C:\Windows\System32\wiaprt.dll
0x74ed0000 0x18000 0x1 C:\Windows\System32\svrsvc.dll
0x74ae0000 0x14000 0x3 C:\Windows\System32\browser.dll
0x74dc0000 0xf000 0x1 C:\Windows\System32\cryptsvc.dll
0x751c0000 0x3d000 0x1 C:\Windows\System32\certcli.dll
0x76b70000 0xb000 0x2 C:\Windows\System32\PSAPI.dll
0x5b890000 0x87000 0x2 C:\Windows\System32\VSSAPI.dll
0x76b10000 0x5000 0x2 C:\Windows\System32\vsfc.dll
0x76be0000 0x2a000 0x4 C:\Windows\System32\vsfc_os.dll
0x74f20000 0x10000 0x3 C:\Windows\System32\vservr.dll
0x76ad0000 0x3c000 0x4 C:\Windows\System32\ves.dll
0x74de0000 0xb000 0x1 C:\Windows\pchealth\helpctr\binaries\pchsvc.dll
0x73c70000 0x7000 0x1 C:\Windows\System32\seclogon.dll
```

```
tasklist /v | findstr spoolsv.exe
0x74d60000 0xb000 0x1 c:\windows\pchealth\helpctr\binaries\pchsvc.dll
0x73310000 0x7000 0x1 c:\windows\system32\seclogon.dll
0x76710000 0xc000 0x1 c:\windows\system32\sens.dll
0x76700000 0x38000 0x3 c:\windows\system32\w32time.dll
0x780c0000 0x51000 0x13 c:\windows\system32\MSVCP90.dll
0x58a50000 0x38000 0x1 c:\windows\system32\oleaut32.dll
0x74f40000 0x6000 0x1 c:\windows\system32\olecmn.dll
0x74e20000 0x32000 0x1 C:\WINDOWS\System32\wuaueng.dll
0x750c0000 0x28000 0x1 C:\WINDOWS\System32\MDPACK.dll
0x76ef0000 0x6e000 0x2 C:\WINDOWS\System32\WININET.dll
0x75da0000 0x9a000 0x1 C:\WINDOWS\System32\SSE.dll
0x755d0000 0x12c000 0x2 C:\WINDOWS\System32\msvscs.dll
0x500a0000 0x7000 0x1 C:\WINDOWS\System32\winrpcl.dll
0x76c00000 0x24000 0x1 C:\WINDOWS\WinNsxs\x86_Microsoft.Windows.WinHTTP_6595b64144ccf1df_5.1.0.0_x-ww_E0651936\winhttp.dll
0x752e0000 0x75000 0x1 C:\WINDOWS\System32\wbemcore.dll
0x75180000 0x3e000 0x4 C:\WINDOWS\System32\wbem\esscli.dll
0x750f0000 0x38000 0xf C:\WINDOWS\System32\wbem\wbemcomn.dll
0x75550000 0x71000 0x8 C:\WINDOWS\System32\wbem\FastProx.dll
0x74e00000 0x1b000 0x1 C:\WINDOWS\System32\wbem\wmutils.dll
0x75060000 0x2c000 0x1 C:\WINDOWS\System32\wbem\repdrvfs.dll
0x58b50000 0x68000 0x1 C:\WINDOWS\System32\wbem\mpvrsd.dll
0x5fb10000 0xccc00 0x2 C:\WINDOWS\System32\NCOBJAPI.dll
0x6f010000 0x14000 0x1 C:\WINDOWS\System32\wbem\wbem.dll
0x74c40000 0x9c000 0x1 C:\WINDOWS\System32\wbem\wbemsvc.dll
0x72510000 0x6000 0x1 C:\WINDOWS\System32\mlsap1.dll
0x76d90000 0x37000 0x1 C:\Windows\System32\netman.dll
0x73080000 0x9000 0x1 C:\Windows\System32\WZCSAPI.dll
0x75be0000 0x1b1000 0x2 C:\WINDOWS\System32\NETSHELL.dll
0x74de40000 0x11000 0x2 C:\WINDOWS\System32\CLUSAPI.dll
0x68440000 0x41000 0x1 C:\WINDOWS\System32\hntcfg.dll
0x753e0000 0xa3000 0x1 C:\WINDOWS\System32\RASDLG.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll
0x72060000 0x18000 0x2 C:\WINDOWS\System32\xactsrv.dll
0x5f8c0000 0x7000 0x3 C:\WINDOWS\System32\NETRAP.dll
0x722f0000 0x5000 0x1 C:\WINDOWS\System32\sensapi.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winmm.dll
0x75280000 0x43000 0x1 C:\WINDOWS\System32\wbem\wbemess.dll
0x5fa10000 0xd000 0x1 C:\WINDOWS\System32\wbem\ncprov.dll
0x73c80000 0x17000 0x1 C:\WINDOWS\System32\wbem\wbemcons.dll
```

```

C:\Windows\System32\cmd.exe
0x73c80000 0x17000 0x1 C:\WINDOWS\system32\wbem\wbemcons.dll
*****spoolsv.exe pid: 1216
Command line : C:\WINDOWS\system32\spoolsv.exe

Base Size LoadCount Path
0x01000000 0x10000 0xfffff C:\WINDOWS\system32\spoolsv.exe
0x77fa0000 0x9a000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77c80000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x6f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\system32\secur32.dll
0x74060000 0x16000 0x1 C:\WINDOWS\system32\SPOLSS.dll
0x71c80000 0x18000 0x3 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x2 C:\WINDOWS\system32\WS2HELP.dll
0x71c40000 0x53000 0x18 C:\WINDOWS\system32\NETAPI32.dll
0x76c70000 0x13000 0x1 C:\WINDOWS\system32\iphlpapi.dll
0x76f20000 0x55000 0x85 C:\WINDOWS\system32\win32k.dll
0x76f90000 0x55000 0x1 C:\WINDOWS\system32\win32kfull.dll
0x740a0000 0x4e000 0x4 C:\WINDOWS\system32\localspl.dll
0x771a0000 0x124000 0x19 C:\WINDOWS\system32\ole32.dll
0x77e90000 0x7d000 0x9 C:\WINDOWS\system32\OLEAUT32.dll
0x77b90000 0x8000 0x5 C:\WINDOWS\system32\VERSION.dll
0x76be0000 0x2a000 0x4 C:\WINDOWS\system32\sfc_os.dll
0x76bb0000 0x2b000 0x4 C:\WINDOWS\system32\WINTRUST.dll
0x761b0000 0x98000 0x9 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0xa C:\WINDOWS\system32\MSASN1.dll
0x76c10000 0x28000 0x4 C:\WINDOWS\system32\imagehlp.dll
0x75970000 0xba000 0x4 C:\WINDOWS\system32\USERENV.dll
0x73070000 0x26000 0x2 C:\WINDOWS\system32\winspool.drv
0x74020000 0xe000 0x1 C:\WINDOWS\system32\cnbjmon.dll
0x74060000 0x7900 0x1 C:\WINDOWS\system32\pjmon.dll
0x72460000 0xe000 0x1 C:\WINDOWS\system32\tcpmon.dll
0x72000000 0x7900 0x1 C:\WINDOWS\system32\mgmtapi.dll
0x71f20000 0x8000 0x1 C:\WINDOWS\system32\snmpapi.dll
0x71f10000 0x8000 0x1 C:\WINDOWS\system32\snmptrap.dll
0x72450000 0x8000 0x1 C:\WINDOWS\system32\usbmon.dll
0x71b20000 0x43000 0x5 C:\WINDOWS\system32\msvsock.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winnrn.dll

```

```

Seleccionar C:\Windows\System32\cmd.exe
0x57b60000 0x9000 0x1 C:\WINDOWS\System32\shgqs.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll
0x74030000 0x22000 0x1 C:\WINDOWS\System32\win32spl.dll
0x5f18c0000 0x7900 0x1 C:\WINDOWS\System32\NETTRAP.dll
0x740800000 0x15000 0x1 C:\WINDOWS\System32\lineprp.dll
0x740100000 0x7900 0x1 C:\WINDOWS\System32\lmp.dll
0x76f300000 0x16000 0x2 C:\WINDOWS\System32\MDPAPI.dll
0x71c00000 0x56000 0x1 C:\WINDOWS\System32\kerberos.dll
0x766d0000 0xc000 0x1 C:\WINDOWS\System32\crypt.dll
0x76df0000 0x32000 0x2 C:\WINDOWS\System32\ACTIVEDS.dll
0x76d60000 0x26000 0x5 C:\WINDOWS\System32\adlpr.dll
0x76b80000 0x2d000 0x3 C:\WINDOWS\System32\creduil.dll
0x77380000 0x7dd000 0x3 C:\WINDOWS\System32\SHELL32.dll
0x77290000 0x49000 0x5 C:\WINDOWS\System32\SHLWAPI.dll
0x76a80000 0x18000 0x2 C:\WINDOWS\System32\ATL.dll
0x76ad0000 0xe6000 0x2 C:\WINDOWS\x86_Microsoft.Windows.Common-Controls_6595b64144ccff1d_6.0.100.0_x-wi_84174508\comctl32.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\System32\CLBCatQ.dll
0x77010000 0x6c000 0x1 C:\WINDOWS\System32\COMRes.dll
0x712d0000 0x2d000 0x1 C:\WINDOWS\System32\adsldp.dll
0x75da0000 0x9a000 0x1 C:\WINDOWS\System32\LSKS.dll
*****msdtc.exe pid: 1248
Command line : C:\WINDOWS\system32\msdtc.exe

Base Size LoadCount Path
0x00400000 0x4000 0xfffff C:\WINDOWS\system32\msdtc.exe
0x77f40000 0x9a000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x77c80000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x6f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x61030000 0xf6000 0xfffff C:\WINDOWS\System32\MSDTCMT.dll
0x76ed0000 0x27000 0xfffff C:\WINDOWS\System32\DNSAPI.dll
0x71c00000 0x18000 0xfffff C:\WINDOWS\System32\WS2_32.dll
0x71bf0000 0x8000 0xfffff C:\WINDOWS\System32\WS2HELP.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\System32\Secur32.dll
0x780c0000 0x61000 0xfffff C:\WINDOWS\System32\MSVCP60.dll
0x61150000 0x71000 0xfffff C:\WINDOWS\System32\MSDTCPRTX.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\System32\OLEAUT32.dll

```

```
□ Seleccionar C:\Windows\System32\cmd.exe
0x61150000 0x71000 0xfffff C:\WINDOWS\system32\MSDTCPRX.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x74f40000 0x18000 0xfffff C:\WINDOWS\system32\WTXCLU.DLL
0x77b90000 0x8000 0xfffff C:\WINDOWS\system32\VERSION.dll
0x71bb0000 0x9000 0xfffff C:\WINDOWS\system32\WSOCK32.dll
0x61100000 0x1a000 0xfffff C:\WINDOWS\system32\MSDTCLOG.dll
0x57b10000 0x6000 0xfffff C:\WINDOWS\system32\XOLEHLP.dll
0x71b20000 0x43000 0xfffff C:\WINDOWS\system32\MSWSOCK.DLL
0x76aa0000 0x2c000 0xfffff C:\WINDOWS\system32\WINMM.dll
0x74de0000 0x11000 0x2 C:\WINDOWS\system32\CLUSAPI.dll
0x74e40000 0x12000 0x1 C:\WINDOWS\system32\REUTILS.DLL
0x77080000 0x5a000 0x1 C:\WINDOWS\system32\MSDTCRENV.dll
0x72880000 0x6000 0x1 C:\WINDOWS\system32\WFC42U.DLL
0x77030000 0x6000 0x3 C:\WINDOWS\system32\COMRES.DLL
0x74f40000 0x1f000 0x1 C:\WINDOWS\system32\WTXOCI.dll
0x76f40000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WTMARTA.DLL
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
*****  
dfssvc.exe pid: 1312  
Command line : C:\WINDOWS\system32\dfssvc.exe  
  
Base Size LoadCount Path  
-----  
0x01000000 0x23000 0xfffff C:\WINDOWS\system32\dfssvc.exe  
0x77f40000 0x9a000 0xfffff C:\WINDOWS\system32\ntdll.dll  
0x77e40000 0x74000 0xfffff C:\WINDOWS\system32\kernel32.dll  
0x77b90000 0x54000 0xfffff C:\WINDOWS\system32\user32.dll  
0x77080000 0x30000 0xfffff C:\WINDOWS\system32\RPCRT4.dll  
0x77280000 0x49000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll  
0x77c60000 0x44000 0xfffff C:\WINDOWS\system32\ODI32.dll  
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll  
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll  
0x77380000 0x7dd000 0xfffff C:\WINDOWS\system32\SHIEL32.dll  
0x76f60000 0x32000 0xfffff C:\WINDOWS\system32\ACTIVEDS.dll  
0x76d60000 0x26000 0xfffff C:\WINDOWS\system32\adsldpc.dll  
0x76f10000 0x2f000 0xfffff C:\WINDOWS\system32\WLDAP32.dll  
0x76b80000 0x2d000 0xfffff C:\WINDOWS\system32\credui.dll  
0x76a80000 0x18000 0xfffff C:\WINDOWS\system32\ATL.dll  
0x77100000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll  
  
Windows Buscar Buscar Octopus Taskbar Icons 22:28 8/10/2024
```

```
□ Seleccionar C:\Windows\System32\cmd.exe
0x75d00000 0x10000 0xfffff C:\WINDOWS\system32\ATL.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x74d40000 0x11000 0xfffff C:\WINDOWS\system32\CLUSAPI.dll
0x74e40000 0x12000 0xfffff C:\WINDOWS\system32\REUTILS.dll
0x75970000 0x9a000 0xfffff C:\WINDOWS\system32\MSDTCRENV.dll
0x72880000 0x1f000 0xfffff C:\WINDOWS\system32\WFC42U.dll
0x76f60000 0x16000 0xfffff C:\WINDOWS\system32\WTSAPI.dll
0x76ed0000 0x27000 0xfffff C:\WINDOWS\system32\DNSSAPI.dll
0x71c60000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x71bb0000 0x9000 0xfffff C:\WINDOWS\system32\WSOCK32.dll
0x76ad0000 0xe6000 0x2 C:\WINDOWS\Win32\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-wv_8417450B\comctl32.dll
0x71b20000 0x43000 0x5 C:\WINDOWS\system32\mswsock.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\system32\rasadnlp.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x71c40000 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x766b0000 0xc000 0x1 C:\WINDOWS\system32\crypt.dll.dll
0x76720000 0x20000 0x1 C:\WINDOWS\system32\RPCS4.dll
0x76f70000 0x76000 0x1 C:\WINDOWS\system32\win32.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0x6c000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
0x712d0000 0x2d000 0x1 C:\WINDOWS\system32\adlplib.dll
0x75d40000 0x9a000 0x1 C:\WINDOWS\system32\SXS.dll
*****  
svchost.exe pid: 1404  
Command line : C:\WINDOWS\System32\svchost.exe -k WinErr  
  
Base Size LoadCount Path  
-----  
0x01000000 0x6000 0xfffff C:\WINDOWS\System32\svchost.exe
0x77f40000 0x9a000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0x74000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x30000 0xfffff C:\WINDOWS\system32\RPCS4.dll
0x77c50000 0x20000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x766b0000 0x20000 0x1 C:\WINDOWS\system32\WTMARTA.dll
0x77ha0000 0x54000 0x9 C:\WINDOWS\system32\mcvcrt.dll
0x77d00000 0x8f000 0x9 C:\WINDOWS\system32\USER32.dll
0x77c60000 0x44000 0x5 C:\WINDOWS\system32\ODI32.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\System32\SAMLIB.dll  
  
Windows Buscar Buscar Octopus Taskbar Icons 22:28 8/10/2024
```

```

[...] Seleccionar C:\Windows\System32\cmd.exe
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\wLDAP32.dll
0x5cf00000 0x16000 0x1 C:\WINDOWS\System32\SAM18.dll
0x77100000 0x124000 0x2 C:\WINDOWS\System32\ole32.dll
0x74d40000 0x9000 0x1 C:\WINDOWS\System32\ver32.dll
0x75970000 0x8000 0x1 C:\WINDOWS\System32\GDI32.dll
0x76200000 0x10000 0x1 C:\WINDOWS\System32\WINSTA.dll
0x71c40000 0x53000 0x2 C:\WINDOWS\System32\NETAPI32.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\System32\secur32.dll
*****lsmserv.exe pid: 1436
Command line : C:\WINDOWS\System32\lsmserv.exe

Base Size LoadCount Path
-----
0x01000000 0xc000 0xffff C:\WINDOWS\System32\lsmserv.exe
0x77f40000 0xba000 0xffff C:\WINDOWS\System32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\System32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\System32\msvcrt.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0x44000 0xffff C:\WINDOWS\System32\RPCRT4.dll
0x76f10000 0x2f000 0xffff C:\WINDOWS\System32\WLDAP32.dll
0x766e0000 0x9000 0xffff C:\WINDOWS\System32\CRYPT32.dll
0x5f1c0000 0x39000 0x1 C:\WINDOWS\System32\ntdllmsg.dll
0x71c00000 0x19000 0x16 C:\WINDOWS\System32\WS2_32.dll
0x71f10000 0x8000 0x14 C:\WINDOWS\System32\WS2HELP.dll
0x71b20000 0x43000 0x4 C:\WINDOWS\System32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wctcpip.dll
0x76f50000 0x13000 0x5 C:\WINDOWS\System32\SECUR32.dll
0x76ed0000 0x27000 0x4 C:\WINDOWS\System32\DNSAPI.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winrnm.dll
0x76fb0000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll
0x77d00000 0x2f000 0x7 C:\WINDOWS\System32\USER32.dll
0x77c00000 0x44000 0x5d C:\WINDOWS\System32\GDI32.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\System32\msv1_0.dll
0x63e00000 0x9000 0x1 C:\WINDOWS\System32\lsmip.dll
0x71f30000 0xa000 0x2 C:\WINDOWS\System32\WS2TOPL.dll
0x76b60000 0x16000 0x2 C:\WINDOWS\System32\NTDSAPI.dll
0x63e00000 0x10000 0x1 C:\WINDOWS\System32\ATL.dll
0x76a00000 0x18000 0x7 C:\WINDOWS\System32\OLEAUT32.dll
0x77160000 0x124000 0x14 C:\WINDOWS\System32\ole32.dll
0x77000000 0xd7000 0x10 C:\WINDOWS\System32\OLEAUT32.dll
0x76df0000 0x32000 0x3 C:\WINDOWS\System32\ACTIVEOS.dll

```

```

[...] Seleccionar C:\Windows\System32\cmd.exe
0x77000000 0x7d000 0x10 C:\WINDOWS\system32\OLEAUT32.dll
0x76df0000 0x32000 0x3 C:\WINDOWS\System32\ACTIVEOS.dll
0x76dc0000 0x26000 0x5 C:\WINDOWS\System32\admidpc.dll
0x76b30000 0x2d000 0x5 C:\WINDOWS\System32\credui.dll
0x77380000 0x7dd000 0x5 C:\WINDOWS\System32\SHELL32.dll
0x77290000 0x49000 0x4 F C:\WINDOWS\System32\ole32.dll
0x76010000 0x7000 0x6 C:\WINDOWS\Win32\v86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x74010000 0x5000 0x1 C:\WINDOWS\Win32\v86_ICMP.DLL
0x76c70000 0x17000 0x3 C:\WINDOWS\System32\iphlpapi.dll
0x76f00000 0x76000 0x1 C:\WINDOWS\System32\CLBCatQ.dll
0x77010000 0x6000 0x1 C:\WINDOWS\System32\COMRes.dll
0x77b90000 0x8000 0x3 C:\WINDOWS\System32\VERSION.dll
0x71300000 0x47000 0x1 C:\WINDOWS\System32\linetrv\adsis.dll
0x72880000 0x4f000 0x2 C:\WINDOWS\System32\MFC42u.dll
0x64760000 0x24000 0x2 C:\WINDOWS\System32\IisRTL.dll
0x64760000 0x37000 0x1 C:\WINDOWS\System32\linetrv\iisui.dll
0x76bc0000 0x90000 0x2 C:\WINDOWS\Win32\v86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x71bd0000 0x11000 0x1 C:\WINDOWS\System32\MPR.dll
0x761b0000 0x98000 0x3 C:\WINDOWS\System32\COMCTL32.dll
0x76190000 0x12000 0x2 C:\WINDOWS\System32\MSASN1.dll
0x71430000 0x16000 0x1 C:\WINDOWS\System32\ADMPROX.DLL
0x0fffd0000 0x2d000 0x1 C:\WINDOWS\System32\rsenh.dll
0x76b50000 0xb000 0x1 C:\WINDOWS\System32\PSAPI.dll
0x75950000 0x7000 0x1 C:\WINDOWS\System32\ole32.dll
0x5c150000 0x6000 0x1 C:\WINDOWS\System32\linetrv\smtpadm.dll
0x5c140000 0x6000 0x1 C:\WINDOWS\System32\SMTPAPI.dll
0x69530000 0xc000 0x2 C:\WINDOWS\System32\olextrace.dll
0x5b780000 0x6000 0x2 C:\WINDOWS\System32\STATXH.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\System32\WSOCK32.dll
0x5c87f0000 0x35000 0x1 C:\WINDOWS\System32\linetrv\seo.dll
0x5cf40000 0x6000 0x1 C:\WINDOWS\System32\RNWH.dll
0x6f350000 0x1f6000 0x1 C:\WINDOWS\System32\cdosys.dll
0x760f0000 0x9e000 0x1 C:\WINDOWS\System32\WININET.dll
0x75fc0000 0x89000 0x1 C:\WINDOWS\System32\urlmon.dll
0x74ba0000 0x97000 0x1 C:\WINDOWS\System32\INETCOMM.dll
0x74b70000 0x20000 0x1 C:\WINDOWS\System32\MSOERT2.dll
0x64430000 0xe000 0x1 C:\WINDOWS\System32\inetres.dll

```

ntfrs.exe pid: 1452

Command line : C:\WINDOWS\system32\ntfrs.exe

```

[...] Seleccionar C:\Windows\System32\cmd.exe
0x64430000 0xe000 0x1 C:\WINDOWS\system32\inetres.dll
***** ntfrs.exe pid: 1452
Command line : C:\WINDOWS\system32\ntfrs.exe

Base Size LoadCount Path
----- -----
0x01000000 0xc3000 0xfffff C:\WINDOWS\system32\ntfrs.exe
0x77fa0000 0xb4000 0xfffff *PCC
0x77e00000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x00000000 0x0 0x0
0x00000000 0x8219a100 0x303c
0x4e4e4e4e 0x4e4e4e4e 0x4e4e
***** svchost.exe pid: 1512
Command line : C:\WINDOWS\system32\svchost.exe -k regsvc

Base Size LoadCount Path
----- -----
0x01000000 0x6000 0xfffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xb4000 0xfffff C:\WINDOWS\System32\ntdll.dll
0x77e00000 0xf4000 0xfffff C:\WINDOWS\System32\kernel32.dll
0x77da0000 0x80000 0xfffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\System32\RPCRT4.dll
0x74a20000 0x12000 0x1 c:\windows\system32\regsvc.dll
0x77ba0000 0x54000 0x1 C:\WINDOWS\system32\msvcr32.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\system32\secur32.dll
***** svchost.exe pid: 1736
Command line : C:\WINDOWS\System32\svchost.exe -k termsvc

Base Size LoadCount Path
----- -----
0x01000000 0x6000 0xfffff C:\WINDOWS\System32\svchost.exe
0x77f40000 0xb4000 0xfffff C:\WINDOWS\System32\ntdll.dll
0x77e00000 0xf4000 0xfffff C:\WINDOWS\System32\kernel32.dll
0x77d00000 0x80000 0xfffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\System32\RPCRT4.dll
0x76c80000 0x20000 0x1 C:\WINDOWS\System32\WLMARTA.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\System32\msvcr32.dll
***** explorer.exe pid: 188
Command line : C:\WINDOWS\Explorer.EXE

Base Size LoadCount Path
----- -----
0x01000000 0xff000 0xfffff C:\WINDOWS\Explorer.EXE
0x77f40000 0xb4000 0xfffff C:\WINDOWS\System32\ntdll.dll
0x77e00000 0xf4000 0xfffff C:\WINDOWS\System32\kernel32.dll
0x77b40000 0x54000 0xfffff C:\WINDOWS\System32\msvcr32.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\System32\RPCRT4.dll
0x77c60000 0x44000 0xfffff C:\WINDOWS\System32\GDI32.dll
0x773c0000 0x20000 0x1 C:\WINDOWS\System32\OLEAUT32.dll
0x770e0000 0xd7000 0x3 C:\WINDOWS\System32\OLEAUT32.dll
0x76c40000 0x14000 0x1 C:\WINDOWS\System32\AUXTHZ.dll
0x74f60000 0x1d000 0x1 C:\WINDOWS\System32\msnslsap1.dll
0x76df0000 0x32000 0x1 C:\WINDOWS\System32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\System32\adsldpc.dll
0x71c40000 0x53000 0x3 C:\WINDOWS\System32\NETAPI32.dll
0x76bb0000 0x2d000 0x1 C:\WINDOWS\System32\credui.dll
0x77380000 0x7dd000 0x1 C:\WINDOWS\System32\SHELL32.dll
0x77290000 0x49000 0x3 C:\WINDOWS\System32\SHLWAPI.dll
0x76a80000 0x18000 0x1 C:\WINDOWS\System32\ATL.dll
0x761b0000 0x39800 0x1 C:\WINDOWS\System32\CRYPT32.dll
0x76200000 0x12000 0x1 C:\WINDOWS\System32\CRYPTUI.dll
0x76a00000 0x20000 0x2 C:\WINDOWS\Win32_V86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-wv_84174508\comctl32.dll
0x76b20000 0xf000 0x1 C:\WINDOWS\System32\RPCAPI.dll
0x0ff40000 0x2d000 0x1 C:\WINDOWS\System32\vrcaenh.dll
0x76b50000 0xb4000 0x1 C:\WINDOWS\System32\PSAPI.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\System32\VERSION.dll
0x75970000 0xba000 0xfffff C:\WINDOWS\System32\USERENV.dll

```

```
Seleccionar C:\Windows\System32\cmd.exe
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77c60000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77d20000 0x49000 0xfffff C:\WINDOWS\system32\SHELL32.dll
0x77d40000 0x7e000 0xfffff C:\WINDOWS\system32\OLE32.dll
0x77d60000 0x124000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x77d80000 0x7d000 0xfffff C:\WINDOWS\system32\BROWSEU.dll
0x77e00000 0x106000 0xfffff C:\WINDOWS\system32\SHDOCVW.dll
0x76920000 0x157000 0xfffff C:\WINDOWS\system32\UXTheme.dll
0x71b70000 0x33000 0xfffff C:\WINDOWS\system32\UXTheme.dll
0x76ad0000 0x6e000 0x3ff C:\WINDOWS\Win32\x86_Microsoft.Windows.Common-Controls_6595b64144ccfd6_0.0.100.0_x-ww_8417450B\comctl32.dll
0x75e90000 0x22000 0x2 C:\WINDOWS\system32\appHelp.dll
0x76f00000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x7 C:\WINDOWS\system32\VERSION.dll
0x76540000 0x50000 0x2 C:\WINDOWS\system32\cscui.dll
0x76520000 0x1d000 0x2 C:\WINDOWS\system32\CSIDL.dll
0x5aff0000 0x5d000 0x1 C:\WINDOWS\system32\thmeui.dll
0x76f50000 0x13000 0x4 C:\WINDOWS\system32\SeCur32.dll
0x76280000 0x5000 0x1 C:\WINDOWS\system32\MSIMG32.dll
0x75970000 0xb4000 0x3 C:\WINDOWS\system32\USERENV.dll
0x768e0000 0x8000 0x1 C:\WINDOWS\system32\WIN32.dll
0x768f0000 0x7e000 0x4 C:\WINDOWS\system32\Win32.dll
0x71b10000 0x53000 0x1a C:\WINDOWS\system32\NETAPI32.dll
0x75c40000 0x10000 0x4 C:\WINDOWS\system32\SAMLIB.dll
0x765a0000 0x10000 0xd C:\WINDOWS\system32\SETUPAPI.dll
0x75b70000 0x1b1000 0x1 C:\WINDOWS\system32\NETSHELL.dll
0x76b80000 0x2d000 0x4 C:\WINDOWS\system32\credui.dll
0x71c60000 0x18000 0x8 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x7 C:\WINDOWS\system32\WS2HELP.dll
0x76cf0000 0x17000 0x1 C:\WINDOWS\system32\iphlpapi.dll
0x74de0000 0x11000 0x1 C:\WINDOWS\system32\CLUSAPI.dll
0x76260000 0x10000 0x3 C:\WINDOWS\system32\WINSTA.dll
0x74920000 0x44000 0x1 C:\WINDOWS\system32\webcheck.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x748f0000 0x21000 0x2 C:\WINDOWS\system32\stObject.dll
0x748e0000 0xa000 0x2 C:\WINDOWS\system32\BatchMeter.dll
0x748c0000 0x7000 0x4 C:\WINDOWS\system32\POWERPROF.dll
0x76f80000 0x8000 0x2 C:\WINDOWS\system32\WTSAPI32.dll
0x74970000 0x58000 0x2 C:\WINDOWS\system32\WTSAPI.dll
0x72320000 0x20000 0x3 C:\WINDOWS\system32\MTNSPOOL.DRV
0x76df0000 0x32000 0x3 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x5 C:\WINDOWS\system32\adsldpc.dll
0x76f10000 0x2f000 0x4 C:\WINDOWS\system32\WLDAPI32.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x76dc0000 0x26000 0x5 C:\WINDOWS\system32\adsldpc.dll
0x76f10000 0x2f000 0x4 C:\WINDOWS\system32\WLDAPI32.dll
0x76a80000 0x18000 0x3 C:\WINDOWS\system32\AT.dll
0x748d0000 0x8000 0x2 C:\WINDOWS\system32\CFGMR32.dll
0x71bd0000 0x11000 0x5 C:\WINDOWS\system32\MPR.dll
0x76aa0000 0x7e000 0x4 C:\WINDOWS\system32\INET.dll
0x72700000 0x7000 0x4 C:\WINDOWS\system32\DRP.dll
0x5f120000 0x6000 0x1 C:\WINDOWS\system32\ntlanman.dll
0x5f180000 0x16000 0x2 C:\WINDOWS\system32\NETUI0.dll
0x5f8e0000 0x31000 0x1 C:\WINDOWS\system32\NETUI1.dll
0x75ea0000 0x9000 0x1 C:\WINDOWS\system32\davctrl.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\LSA.dll
0x760f0000 0x9e000 0x1 C:\WINDOWS\system32\WININET.dll
0x761b0000 0x98000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x3 C:\WINDOWS\system32\MSASN1.dll
0x76050000 0x95000 0x1 C:\WINDOWS\system32\shdoclc.dll
0x75fc0000 0x89000 0x2 C:\WINDOWS\system32\urlmon.dll
0x76e90000 0x3b000 0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e40000 0x11000 0x2 C:\WINDOWS\system32\rasman.dll
0x76e00000 0x2e000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76e30000 0xb0000 0x4 C:\WINDOWS\system32\rtutils.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\system32\WZCSPAPI.dll
0x76c00000 0x17000 0x1 C:\WINDOWS\system32\MPRAPI.dll
0x77110000 0x8000 0x1 C:\WINDOWS\system32\WS2SOCK.dll
0x72400000 0x12000 0x1 C:\WINDOWS\system32\WS2SDS.dll
0x72470000 0x1a000 0x2 C:\WINDOWS\system32\wmdocs.dll
0x71530000 0x1f000 0x1 C:\WINDOWS\system32\aclui.dll
0x76cc0000 0x20000 0x1 C:\WINDOWS\system32\WMTARTA.dll
*****dns.exe pid: 340
Command line : C:\WINDOWS\system32\dns.exe

Base           Size  LoadCount Path
-----
0x01000000 0x8d000 0xfffff C:\WINDOWS\System32\dns.exe
0x77f40000 0xba000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcr7.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x44000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x71c60000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x71c40000 0x53000 0xfffff C:\WINDOWS\System32\NETAPI32.dll
0x76f10000 0x2f000 0xfffff C:\WINDOWS\System32\LDAP32.dll
0x76e00000 0x27000 0xfffff C:\WINDOWS\System32\DNAPI.dll
0x76f60000 0x10000 0xfffff C:\WINDOWS\System32\TDSN32.dll
0x77f50000 0x12000 0xfffff C:\WINDOWS\System32\SHLWAPI.dll
0x76c70000 0x24000 0xfffff C:\WINDOWS\System32\iphlpapi.dll
0x76c40000 0x17000 0xfffff C:\WINDOWS\System32\WPRAPI.dll
0x76d40000 0x32000 0xfffff C:\WINDOWS\System32\ACTIVEDS.dll
0x76dc0000 0x26000 0xfffff C:\WINDOWS\System32\adlpr.dll
0x76b80000 0x2d000 0xfffff C:\WINDOWS\System32\credui.dll
0x77380000 0x7dd000 0xfffff C:\WINDOWS\System32\SHELL32.dll
0x76a80000 0x18000 0xfffff C:\WINDOWS\System32\ATL.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\System32\ole32.dll
0x77080000 0x7d000 0xfffff C:\WINDOWS\System32\OLEAUT32.dll
0x76e30000 0xb000 0xfffff C:\WINDOWS\System32\rutil.dll
0x5ccf0000 0x10000 0xfffff C:\WINDOWS\System32\SAMLIB.dll
0x765a0000 0x10000 0xfffff C:\WINDOWS\System32\SETUPAPI.dll
0x76ad0000 0xe6000 0x3 C:\Windows\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x76d80000 0x37000 0x1 C:\WINDOWS\System32\netman.dll
0x76e90000 0x3b000 0x2 C:\WINDOWS\System32\RASAPI32.dll
0x76e40000 0x11000 0x2 C:\WINDOWS\System32\RPCRT4.dll
0x76d90000 0x2000 0x2 C:\WINDOWS\System32\YAP32.dll
0x76aa0000 0x2c000 0x2 C:\WINDOWS\System32\WTNW32.dll
0x76b10000 0x89000 0x3 C:\WINDOWS\System32\CRYPT32.dll
0x76190000 0x12000 0x3 C:\WINDOWS\System32\WSASN1.dll
0x76d30000 0x47000 0x1 C:\WINDOWS\System32\WZCSvc.dll
0x76c60000 0x5000 0x1 C:\WINDOWS\System32\WZP.dll
0x76d10000 0x1c000 0x1 C:\WINDOWS\System32\DPNSVC.dll
0x76f00000 0x8000 0x1 C:\WINDOWS\System32\WTSAPI32.dll
0x76260000 0x10000 0x2 C:\WINDOWS\System32\WINSTA.dll
0x69750000 0x108000 0x1 C:\WINDOWS\System32\ESSENT.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\System32\WZCSAPI.dll
0x71b20000 0x3000 0x3 C:\WINDOWS\System32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll
0x71ca0000 0x56000 0x1 C:\WINDOWS\System32\kerberos.dll
0x76e60000 0xc000 0x1 C:\WINDOWS\System32\crypt.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\System32\msv1_0.dll
0x74010000 0x5000 0x1 C:\WINDOWS\System32\ICMP.DLL
0x77f60000 0x4000 0x1 C:\WINDOWS\System32\security.dll
*****  
wins.exe pid: 756  
Command line : C:\WINDOWS\System32\wins.exe
```

```
Seleccionar C:\Windows\System32\cmd.exe
Command line : C:\WINDOWS\System32\wins.exe

-----  
Base Size LoadCount Path  
-----  
0x0100000000 0x27000 0xfffff C:\WINDOWS\System32\wins.exe  
0x77f40000 0xb4000 0xfffff C:\WINDOWS\System32\ntdll.dll  
0x77c40000 0xF4000 0xfffff C:\WINDOWS\System32\kernel32.dll  
0x77ba0000 0x54000 0xfffff C:\WINDOWS\System32\msvcrtd.dll  
0x77da0000 0x80000 0xfffff C:\WINDOWS\System32\ADVAPI32.dll  
0x77c40000 0x4000 0xfffff C:\WINDOWS\System32\RPCRT4.dll  
0x71c40000 0x53000 0xfffff C:\WINDOWS\System32\NETAPI32.dll  
0x77d00000 0x8f000 0xfffff C:\WINDOWS\System32\USER32.dll  
0x77c80000 0x44000 0xfffff C:\WINDOWS\System32\GDI32.dll  
0x71c80000 0x18000 0xfffff C:\WINDOWS\System32\WS2_32.dll  
0x71bf0000 0x8000 0xfffff C:\WINDOWS\System32\WS2HELP.dll  
0x77160000 0x124000 0xfffff C:\WINDOWS\System32\ole32.dll  
0x5b890000 0x87000 0xfffff C:\WINDOWS\System32\VSSAPI.dll  
0x76a80000 0x18000 0xfffff C:\WINDOWS\System32\ATL.dll  
0x770e0000 0x7d000 0xfffff C:\WINDOWS\System32\OLEAUT32.dll  
0x71b20000 0x43000 0x5 C:\WINDOWS\System32\mswsock.dll  
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll  
0x76ed0000 0x27000 0x2 C:\WINDOWS\System32\DNSAPI.dll  
0x76f00000 0x5000 0x1 C:\WINDOWS\System32\EMGU32.dll  
0x76f10000 0x2f000 0x1 C:\WINDOWS\System32\LDAP32.dll  
0x76f30000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll  
0x69750000 0x108000 0x1 C:\WINDOWS\System32\escent.dll  
0x5ccf0000 0x10000 0x1 C:\WINDOWS\System32\SAMLIB.dll  
0x76f90000 0x7e000 0x1 C:\WINDOWS\System32\CLBCatQ.dll  
0x77010000 0x6c000 0x1 C:\WINDOWS\System32\COMRes.dll  
0x77b50000 0x8000 0x2 C:\WINDOWS\System32\VERSION.dll  
0x76ad0000 0x3e000 0x1 C:\WINDOWS\System32\es.dll  
0x76f50000 0x13000 0x3 C:\WINDOWS\System32\securn32.dll  
0x76c90000 0x24000 0x1 C:\WINDOWS\System32\msv1_0.dll
*****  
wuauclt.exe pid: 1092  
Command line : "C:\WINDOWS\System32\wuauclt.exe"

-----  
Base Size LoadCount Path  
-----  
0x0100000000 0x26000 0xfffff C:\WINDOWS\system32\wuauclt.exe  
0x77f40000 0xb4000 0xfffff C:\WINDOWS\System32\ntdll.dll  
0x77e40000 0x74000 0xfffff C:\WINDOWS\System32\kernel32.dll
```

```
Selezionare C:\Windows\System32\cmd.exe
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x40000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77290000 0x49000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x77070000 0x30000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x75fc0000 0x80000 0xfffff C:\WINDOWS\system32\VERSION.dll
0x77b90000 0x80000 0xfffff C:\WINDOWS\Win32x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\COMCTL32.dll
0x76f00000 0x80000 0xfffff C:\WINDOWS\system32\WTSAPI32.dll
0x76260000 0x10000 0xfffff C:\WINDOWS\system32\WIN32A.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x750c0000 0x28000 0xfffff C:\WINDOWS\system32\ADVAPI.dll
0x74c40000 0x68000 0x1 C:\WINDOWS\system32\RPCHED20.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0x6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL
*****
dllhost.exe pid: 3292
Command line : C:\WINDOWS\system32\dllhost.exe /ProcessId:{02D4B3F1-FD8B-11D1-960D-00805FC79235}

Base ----- Size LoadCount Path
-----
0x01000000 0x4000 0xfffff C:\WINDOWS\system32\dllhost.exe
0x77f40000 0xb3000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e00000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ha0000 0x54000 0xfffff C:\WINDOWS\system32\msvcr7.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x3f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x76f90000 0x7e000 0x8 C:\WINDOWS\system32\CLBCatQ.DLL
0x770e0000 0xd000 0x1 C:\WINDOWS\system32\OLEAUT32.dll
0x77010000 0x6000 0x8 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x13 C:\WINDOWS\system32\VERSION.dll
0x755d0000 0x12c000 0x8 C:\WINDOWS\system32\COMSVCS.dll
0x74f10000 0x1f000 0x1 C:\WINDOWS\system32\mtxoc1.dll
0x0fffd0000 0x2d000 0x1 C:\WINDOWS\system32\rsenh.dll
0x76b70000 0xb0000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x76590000 0x1d000 0x1 C:\WINDOWS\system32\RPCSVC.dll
0x76ad0000 0x20000 0x2 C:\WINDOWS\system32\LES.DLL
0x75d10000 0x8ca000 0x1 C:\WINDOWS\system32\SXS.DLL
0x57b10000 0x6000 0x1 C:\WINDOWS\system32\XOLEHELP.dll
*****
```

```
Selezionare C:\Windows\System32\cmd.exe
0x71bb0000 0x9000 0x4 C:\WINDOWS\system32\WSOCK32.dll
0x71c00000 0x18000 0x8 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x9 C:\WINDOWS\system32\WS2HELP.dll
0x74de0000 0x11000 0x2 C:\WINDOWS\system32\CLUSAPI.dll
0x74ef0000 0x12000 0x1 C:\WINDOWS\system32\RESULTS.dll
0x75970000 0xba000 0x1 C:\WINDOWS\system32\USERENV.dll
0x72880000 0xf4000 0x1 C:\WINDOWS\system32\WFC42u.dll
0x76f50000 0x13000 0x2 C:\WINDOWS\system32\secur32.dll
0x71b20000 0x43000 0x2 C:\WINDOWS\system32\mswsock.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\RPCAPI.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\system32\winrnr.dll
0x76f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x76f60000 0x5000 0x1 C:\WINDOWS\system32\rasdhlp.dll
0x6fb00000 0x47000 0x1 C:\WINDOWS\system32\catdrv.dll
0x6f6f0000 0xa000 0x1 C:\WINDOWS\system32\catdrvps.dll
0x6f6e0000 0x3000 0x2 C:\WINDOWS\system32\catcavx.dll
0x6f5f0000 0x05000 0x2 C:\WINDOWS\system32\catcvut.dll
0x61e50000 0x9000 0x2 C:\WINDOWS\system32\WfcSubs.dll
0x75c50000 0x28000 0x1 C:\WINDOWS\system32\WMTARTA.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
*****
appmgr.exe pid: 2992
Command line : C:\WINDOWS\system32\serverappliance\appmgr.exe

Base ----- Size LoadCount Path
-----
0x01000000 0x23000 0xfffff C:\WINDOWS\system32\serverappliance\appmgr.exe
0x77fa0000 0xba000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e00000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77b50000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x780c0000 0x61000 0xfffff C:\WINDOWS\system32\RPCSVC.dll
0x77c90000 0x60000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x5d000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x5d000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0xd000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb0000 0x1 C:\WINDOWS\system32\rtutils.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x1 C:\WINDOWS\system32\VERSION.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL
0x74ce0000 0xe000 0x1 C:\WINDOWS\system32\wbemsvc.dll
*****
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x71c00000 0x18000 0x4 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x2 C:\WINDOWS\system32\WS2HELP.dll
0x76f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x71c40000 0x53000 0x2 C:\WINDOWS\system32\NETAPI32.dll
0x76f10000 0x10000 0x2 C:\WINDOWS\system32\Secur32.dll
0x00020000 0xf000 0x1 C:\WINDOWS\system32\ServerAppliance\taskctx.dll
0x75180000 0x3e000 0x1 C:\WINDOWS\system32\wbem\lesscli.dll
*****
srvcsvr.exe pid: 1496
Command line : C:\WINDOWS\system32\serverappliance\srvcsvr.exe

Base Size LoadCount Path
-----
0x01000000 0x13000 0xfffff C:\WINDOWS\system32\serverappliance\srvcsvr.exe
0x77f40000 0x9ba000 0x1 C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x780c0000 0x61000 0xfffff C:\WINDOWS\system32\MSVCP90.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI4.dll
0x77c50000 0x44000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\SEH.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\OLE32.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x76b70000 0xb000 0xfffff C:\WINDOWS\system32\PSAPI.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
0x75da0000 0x9ba000 0x1 C:\WINDOWS\system32\SHELL.dll
0x76e30000 0xb000 0x3 C:\WINDOWS\system32\rutilts.dll
0x00610000 0xf000 0x1 C:\WINDOWS\system32\serverappliance\linitsrc.dll
0x00620000 0xf000 0x1 C:\WINDOWS\system32\ServerAppliance\taskctx.dll
0x00630000 0x15000 0x1 C:\WINDOWS\system32\ServerAppliance\appsrvc.dll
0x74cf0000 0x8000 0x1 C:\WINDOWS\system32\wbem\wbemprox.dll
0x750f0000 0x38000 0x2 C:\WINDOWS\system32\wbem\wbemcomm.dll
0x71c00000 0x18000 0x3 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x2 C:\WINDOWS\system32\WS2HELP.dll
0x74ce0000 0xe000 0x1 C:\WINDOWS\system32\wbem\wbemsvc.dll
0x75550000 0x8f000 0x1 C:\WINDOWS\system32\wbem\fastprox.dll
0x767d0000 0x16000 0x1 C:\WINDOWS\system32\WS2SAPI.dll
0x76ed0000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x77c40000 0x53000 0x1 C:\WINDOWS\system32\NETAPI32.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x71c40000 0x53000 0x1 C:\WINDOWS\system32\NETAPI32.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\system32\Secur32.dll
*****
inetinfo.exe pid: 388
Command line : c:\WINDOWS\system32\inetsrv\inetinfo.exe

Base Size LoadCount Path
-----
0x01000000 0x6000 0xfffff C:\WINDOWS\system32\inetsrv\inetinfo.exe
0x77f40000 0x9ba000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0x4f000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrtd.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x64700000 0x31000 0xfffff C:\WINDOWS\system32\linetsrv\IISUTIL.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x5d760000 0x5000 0x2 C:\WINDOWS\system32\linetsrv\rpcref.dll
0x647b0000 0x24000 0x11 C:\WINDOWS\system32\IisRtL.dll
0x71c40000 0x18000 0x3d C:\WINDOWS\system32\WS2_32.dll
0x71430000 0x10000 0x3 C:\WINDOWS\system32\ADMPROX.dll
0x649c0000 0x8000 0x1 C:\WINDOWS\system32\linetsrv\iisadmin.dll
0x5b890000 0x37000 0x1 C:\WINDOWS\system32\VSSAPI.dll
0x76a80000 0x18000 0x8 C:\WINDOWS\system32\ATL.dll
0x770e0000 0x7d000 0x15 C:\WINDOWS\system32\OLEAUT32.dll
0x71c40000 0x53000 0x15 C:\WINDOWS\system32\NETAPI32.dll
0x6e0b0000 0xf000 0x1 C:\WINDOWS\system32\linetsrv\COADMIN.dll
0x71430000 0x10000 0x2 C:\WINDOWS\system32\ADMPROX.dll
0x648b0000 0x13d000 0x2 C:\WINDOWS\system32\linetsrv\IISCFG.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.dll
0x76f10000 0x2f000 0x7 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0x6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll
0x620a0000 0x39000 0x1 C:\WINDOWS\system32\linetsrv\metadata.dll
0x77290000 0x49000 0xa C:\WINDOWS\system32\SHLNAPI.dll
0x0ff00000 0x2d000 0x1 C:\WINDOWS\system32\raenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x77380000 0x7dd000 0x5 C:\WINDOWS\system32\SHL32.dll
0x768a0000 0xe6000 0x3 C:\WINDOWS\Win32\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x77380000 0x7dd000 0x5 C:\WINDOWS\system32\SHELL32.dll
0x76ad0000 0xe6000 0x3 C:\WINDOWS\Win32\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x761b0000 0x98000 0x4 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x4 C:\WINDOWS\system32\SECUR32.dll
0x50000000 0x10000 0x4 C:\WINDOWS\system32\RPCRT4.dll
0x71ff0000 0x4000 0x3 C:\WINDOWS\system32\Security.dll
0x76f50000 0x13000 0x1a C:\WINDOWS\system32\SECUR32.dll
0x64830000 0x10000 0x2 C:\WINDOWS\system32\TSMAP.dll
0x5a120000 0x10000 0x2 C:\WINDOWS\system32\inetrv\wamreg.dll
0x6f750000 0x78000 0x1 C:\WINDOWS\system32\inetrv\SMTPSVC.dll
0x643e0000 0x3e000 0x1 C:\WINDOWS\system32\inetrv\INFOCOMM.dll
0x61ec0000 0xf000 0x4 C:\WINDOWS\system32\inetrv\ISATQ.dll
0x01490000 0x3a000 0x1 C:\WINDOWS\system32\ODBC32.dll
0x76bc0000 0x90000 0x2 C:\WINDOWS\Win32\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x762b0000 0x47000 0x2 C:\WINDOWS\system32\comdig32.dll
0x71bb0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x76ed0000 0x27000 0x6 C:\WINDOWS\system32\DNSSAPI.dll
0x00ff0000 0xe000 0x4 C:\WINDOWS\system32\FCACHDLL.dll
0x5cf00000 0x6000 0x7 C:\WINDOWS\system32\RWNH.dll
0x69530000 0xc000 0x8 C:\WINDOWS\system32\exstrace.dll
0x5d700000 0x6000 0xb C:\WINDOWS\system32\STAXMEM.dll
0x766f0000 0x16000 0x2 C:\WINDOWS\system32\NTDSAPI.dll
0x01000000 0x10000 0x3 C:\WINDOWS\system32\RPCRT4.dll
0x76750000 0x20000 0x2 C:\WINDOWS\system32\svchannel.dll
0x75970000 0x6b000 0x2 C:\WINDOWS\system32\USERENV.dll
0x62da0000 0x7000 0x1 C:\WINDOWS\system32\inetrv\lonsint.dll
0x71b20000 0x43000 0x6 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\w32tcpip.dll
0x76bb0000 0x2b000 0x1 C:\WINDOWS\system32\wintrust.dll
0x76c10000 0x28000 0x1 C:\WINDOWS\system32\imagehelp.dll
0x63eb0000 0x7000 0x1 C:\WINDOWS\system32\linetrv\viscomlog.dll
0x76c70000 0x17000 0x5 C:\WINDOWS\system32\iphlpapi.dll
0x5c870000 0x35000 0x1 C:\WINDOWS\system32\linetrv\seo.dll
0x76d80000 0x37000 0x1 C:\WINDOWS\system32\netman.dll
0x76cd0000 0x17000 0x1 C:\WINDOWS\system32\MPRAPI.dll
0x76df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adsldpc.dll
0x76b30000 0xd2000 0x1 C:\WINDOWS\system32\credui.dll
0x76e30000 0xb000 0x4 C:\WINDOWS\system32\rvtutils.dll
0x76550000 0x10000 0x1 C:\WINDOWS\system32\RPCAPI.dll
0x767f0000 0x10000 0x2 C:\WINDOWS\system32\MSASN1.dll
0x76ca0000 0x11000 0x2 C:\WINDOWS\system32\rasman.dll
0x76e40000 0x2e000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76aa0000 0x2c000 0x2 C:\WINDOWS\system32\WIMWW.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x76ee0000 0x2e000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76aa0000 0x2c000 0x2 C:\WINDOWS\system32\WIMWW.dll
0x76d30000 0x47000 0x1 C:\WINDOWS\system32\WZCSV.dll
0x76cc0000 0x5000 0x1 C:\WINDOWS\system32\WZPVC.dll
0x76d10000 0x1c000 0x1 C:\WINDOWS\system32\WZPCSV.dll
0x76f00000 0x10000 0x1 C:\WINDOWS\system32\WZPCSV32.dll
0x76760000 0x10000 0x2 C:\WINDOWS\system32\WIMINST.dll
0x60755000 0x0f0000 0x1 C:\WINDOWS\system32\ESSENT.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\system32\WZCSAPI.dll
0x02180000 0x79000 0x1 C:\WINDOWS\system32\linetrv\aqeuee.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\system32\rasdhlp.dll
0x71ca0000 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x766e0000 0xccc00 0x1 C:\WINDOWS\system32\cryptdll.dll
0x02460000 0xd000 0x1 C:\WINDOWS\system32\linetrv\ntfsdrv.dll
0x5e6e0000 0xb000 0x1 C:\WINDOWS\system32\POP3server\P3Store.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winnrn.dll
*****
wmiprvse.exe pid: 2116
Command line : C:\WINDOWS\system32\wbem\wmiprvse.exe

Base Size LoadCount Path
-----.
0x01000000 0x35000 0xfffff C:\WINDOWS\system32\wbem\wmiprvse.exe
0x77f40000 0x9b000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e00000 0x4f000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcr7.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x44000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c70000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x75f0f000 0x38000 0xfffff C:\WINDOWS\system32\wbem\wbemcomm.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x75550000 0x71000 0xfffff C:\WINDOWS\system32\wbem\FastProx.dll
0x780c0000 0x61000 0xfffff C:\WINDOWS\system32\MSVCP60.dll
0x766f0000 0x16000 0xfffff C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0xfffff C:\WINDOWS\system32\DNSSAPI.dll
0x71c00000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71b70000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x76f50000 0x2f000 0xfffff C:\WINDOWS\system32\WLDAP32.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x5fb10000 0xcc000 0xfffff C:\WINDOWS\system32\WCobjAPI.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x5fb10000 0xc000 0xfffff C:\WINDOWS\system32\NCODjAPI.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0x6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x770b0000 0x5000 0x1 C:\WINDOWS\system32\VERSION.dll
0x74ef0000 0xe000 0x1 C:\WINDOWS\system32\Wbem\wbemsvc.dll
0x72f40000 0x1b000 0x1 C:\WINDOWS\system32\Wbem\wutil.dll
0x72f40000 0x26000 0x1 C:\WINDOWS\system32\Wbem\wmpprov.dll
0x76cc0000 0x5000 0x1 C:\WINDOWS\system32\WMI.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WTMARBT.dll
0x5cf00000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x76c40000 0x14000 0x1 C:\WINDOWS\system32\authz.dll
0x75180000 0x3e000 0x1 C:\WINDOWS\system32\wbem\esscli.dll
0x5f180000 0x3b000 0x1 C:\WINDOWS\system32\wbem\ntevt.dll
0x5e020000 0x27000 0x1 C:\WINDOWS\system32\wbem\PROVTHRD.dll
0x60020000 0x10000 0x1 C:\WINDOWS\system32\msvcr7.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x006e0000 0x15000 0x1 C:\WINDOWS\system32\ServerAppliance\saevfltr.dll
0x76e30000 0xb000 0x1 C:\WINDOWS\system32\rvtutils.dll
0x00c00000 0x15000 0x1 C:\WINDOWS\system32\ServerAppliance\appsvcs.dll
0x71b20000 0x43000 0x4 C:\WINDOWS\system32\mswsock.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\system32\rasadmin.dll
0x77c50000 0x56000 0x1 C:\WINDOWS\system32\kernetc.dll
0x71c40000 0x56000 0x1 C:\WINDOWS\system32\crypt.dll
0x766c0000 0xc000 0x1 C:\WINDOWS\system32\crypt.dll
0x76190000 0x12000 0x1 C:\WINDOWS\system32\WSASN1.dll
*****  
POP3SVC.exe pid: 2260  
Command line : c:\windows\system32\pop3server\pop3svc.exe  
  
Base Size LoadCount Path  
-----  
0x01000000 0xb000 0xfffff C:\WINDOWS\system32\POP3Server\pop3svc.exe
0x77f40000 0xb000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kerne32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcr7.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x44000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77d60000 0x10000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77710000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\OLE32.dll
0x77080000 0xd7000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x77c80000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
```

```
Seleccionar C:\Windows\System32\cmd.exe
0x77000000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x71c00000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x71b70000 0x8000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x71b20000 0x43000 0xfffff C:\WINDOWS\system32\MSWSOCK.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CRYPT32.dll
0x77b30000 0x8000 0x1 C:\WINDOWS\system32\CRYPTSP.dll
0x5e0e0000 0xf000 0x1 C:\WINDOWS\system32\POP3Server\Pop3Auth.dll
0x76d40000 0x32000 0x3 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x4 C:\WINDOWS\system32\adsldpc.dll
0x71c40000 0x53000 0xb C:\WINDOWS\system32\NETAPI32.dll
0x76f10000 0x2f000 0x4 C:\WINDOWS\system32\WLDAP32.dll
0x76b80000 0x2d000 0x3 C:\WINDOWS\system32\credui.dll
0x77380000 0x7dd000 0x4 C:\WINDOWS\system32\SHELL32.dll
0x77290000 0x49000 0x7 C:\WINDOWS\system32\SHLWAPI.dll
0x76a80000 0x18000 0x4 C:\WINDOWS\system32\ATL.dll
0x766f0000 0x16000 0x1 C:\WINDOWS\system32\WTSAPI.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\DNNSAPI.dll
0x76ad0000 0x6e000 0x2 C:\WINDOWS\Win32\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x5e600000 0x19000 0x1 C:\WINDOWS\system32\POP3Server\P3Admin.dll
0x780c0000 0x51000 0x1 C:\WINDOWS\system32\MSVCP90.dll
0x71f10000 0x41000 0x1 C:\WINDOWS\system32\CRYPT32.dll
0x72380000 0x74000 0x2 C:\WINDOWS\system32\WFC420.dll
0x647b0000 0x24000 0x2 C:\WINDOWS\system32\ListRTL.dll
0x64760000 0x37000 0x1 C:\WINDOWS\system32\linetrv\lisisui.dll
0x78bc0000 0x37000 0x1 C:\WINDOWS\Win32\x86.Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x71bd0000 0x11000 0x1 C:\WINDOWS\system32\VPR.dll
0x761b0000 0x08000 0x2 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x1 C:\WINDOWS\system32\WSASN1.dll
0x71430000 0x10000 0x1 C:\WINDOWS\system32\ADMWPDX.dll
0x0ffd0000 0x2d000 0x1 C:\WINDOWS\system32\rsraenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\SX.dll
0x5c150000 0x2e000 0x1 C:\WINDOWS\system32\linetrv\smtpadm.dll
0x5c140000 0x6000 0x1 C:\WINDOWS\system32\SMTPAPI.dll
0x69530000 0xc000 0x1 C:\WINDOWS\system32\extstrace.dll
0x5b7e0000 0x6000 0x1 C:\WINDOWS\system32\STAHMEM.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
*****  
cmd.exe pid: 2870  
Command line : "C:\WINDOWS\system32\cmd.exe"
```

```

[+] Seleccionar C:\Windows\System32\cmd.exe
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\wSOCK32.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll
*****
cmd.exe pid: 2976
Command line : "C:\WINDOWS\system32\cmd.exe"

Base Size LoadCount Path
-----
0x44d00000 0x50000 0xffff C:\WINDOWS\system32\cmd.exe
0x77f40000 0xa000 0xffff C:\WINDOWS\System32\ntdll.dll
0x77e00000 0xf4000 0xffff C:\WINDOWS\System32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\System32\msvcrt.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0x40000 0xffff C:\WINDOWS\System32\RPCRT4.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\System32\USER32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\System32\GDI32.dll
0x71bd0000 0x11000 0xffff C:\WINDOWS\System32\MPR.dll
*****
mdd.exe pid: 3468
Command line : mdd.exe -o dc-memdump.bin

Base Size LoadCount Path
-----
0x00400000 0x19000 0xffff C:\ITShare\mdd.exe
0x77f40000 0xa000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e00000 0xf4000 0xffff C:\WINDOWS\System32\kernel32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\System32\ADVAPI32.dll
0x77c50000 0x40000 0xffff C:\WINDOWS\System32\RPCRT4.dll
0x77380000 0x7dd000 0xffff C:\WINDOWS\System32\SHELL32.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\System32\msvcrt.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\System32\GDI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\System32\USER32.dll
0x77290000 0x49000 0xffff C:\WINDOWS\System32\SHLWAPI.dll
0x70ad0000 0x86000 0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x0fd00000 0x2d000 0x1 C:\WINDOWS\System32\rsenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\System32\PSAPI.dll

C:\Users\Marxs\Desktop\Nueva carpeta (2)\practica3>

```

## Preguntas de verificación del laboratorio

¿Qué hora inicia el proceso explorer.exe?

R.- A las 21:32

0x81c462e8 svchost.exe	1736	488	16	127	0	0	2012-11-03	20:19:27 UTC+0000
0x81c4bd88 explorer.exe	188	1996	11	337	0	0	2012-11-03	21:32:38 UTC+0000
0x81c4ad28 dvc.exe	240	488	12	162	0	0	2012-11-03	21:41:26 UTC+0000

¿Qué hora inicia el proceso svchost.exe?

R.- a las 20:18:33

0x8031ad00 services.exe	488	444	21	422	0	0	2012-11-03	20:18:31 UTC+0000
0x80222920 lsass.exe	500	444	58	959	0	0	2012-11-03	20:18:31 UTC+0000
0x822bc770 svchost.exe	740	488	12	230	0	0	2012-11-03	20:18:33 UTC+0000
0x81fdf2e0 svchost.exe	884	488	9	133	0	0	2012-11-03	20:18:44 UTC+0000

¿Cuál es el nombre del proceso PID: 420?

R.- csrss.exe

¿Cuál es el nombre del proceso PID: 932?

R.- svchost.exe

## PARTE PRÁCTICA (50 pts)

1) Determina cuántos bits en total puede almacenar una memoria

RAM de 128K x 4 (5 pts)

R.-  $128 \times 4 = 512 \times 1000 = 512000$  bits

2) ¿Cuántos bits puede almacenar una memoria de 10G x 16?

R.-  $10 \times 16 = 160 \times 1000^3 = 1600000000000 = 160G$

3) Cuantas localidades de memoria se puede direccionar con 32 líneas de dirección.

R.-  $2^{32}=4.294.967.296$  localidades

4) ¿Cuántas localidades de memoria se pueden direccionar con 1024 líneas de dirección?

R.-  $2^{1024}= 1,797693134862315907729305190789 \times 10^{308}$

5) ¿Cuántas localidades de memoria se pueden direccionar con 64 líneas de dirección?

R.-  $2^{64}=18.446.744.073.709.551.616$

6) Cuantas líneas de dirección se necesitan para una memoria ROM de 512M x 8.

R.-  $n=\ln(512)/\ln(2)=9$  líneas de dirección

7) ¿Cuántas líneas de dirección se necesitan para una memoria ROM de 128M x 128?

R.-  $n=\ln(128)/\ln(2)=7$  líneas de dirección

8) ¿Cuántos bits en total puede almacenar una memoria RAM 128M x 4, de él resultado gigabytes?

R.- 0.0625 GB

9) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en teras?

R.- 0.004096 terabit

10) ¿Cuántos bits en total puede almacenar una memoria RAM 64M x 64, de él resultado en terabytes?

R.- 0.000488 terabytes