	<b>UNIVERSIDAD AUTÓNOMA "TOMÁS FRÍAS"</b> <b>CARRERA DE INGENIERÍA DE SISTEMAS</b>	
	<b>ESTUDIANTE:</b> Univ. Alex Adrián Méndez Moreira	
<b>MATERIA:</b> Arquitectura de computadoras (SIS-522)		
<b>DOCENTE:</b> Ing. Gustavo A. Puíta Choque	<b>CI:</b> 8612837	
<b>AUXILIAR:</b> Univ. Aldrin Roger Pérez Miranda	<b>PÁCTICA N° 3</b>	

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

Acceso:

La RAM permite tanto la lectura como la escritura de datos, lo que la hace útil para almacenar información temporalmente durante la ejecución de programas.

La ROM, por su parte, solo permite leer los datos, ya que está diseñada para almacenar información que no debe cambiar, como el firmware.

Volatilidad:

La RAM es volátil, lo que significa que los datos almacenados se pierden al apagar el sistema.

La ROM es no volátil, por lo que los datos permanecen intactos incluso cuando no hay energía.

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

Memoria Estática:

Pros: Ofrece mayor velocidad ya que no requiere actualizaciones periódicas de sus datos.

Contras: Es menos densa y más costosa en términos de fabricación, lo que la hace menos adecuada para grandes volúmenes de almacenamiento.

Memoria Dinámica:

Pros: Su mayor densidad y menor costo la hacen ideal para almacenamiento masivo.

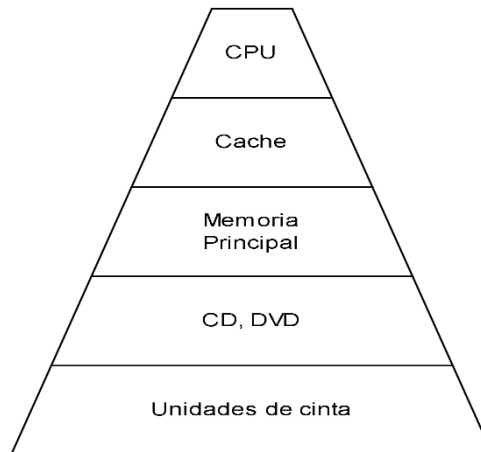
Contras: Necesita ser actualizada constantemente, lo que la hace más lenta en comparación con la memoria estática.

**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)**

La VRAM se utiliza en las tarjetas gráficas para gestionar eficientemente el almacenamiento de las imágenes que se muestran en la pantalla.

Su función principal es permitir que tanto el procesador gráfico (GPU) como el procesador principal (CPU) puedan acceder a la memoria de forma simultánea, mejorando el rendimiento en tareas relacionadas con gráficos y visualización.

**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)**



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

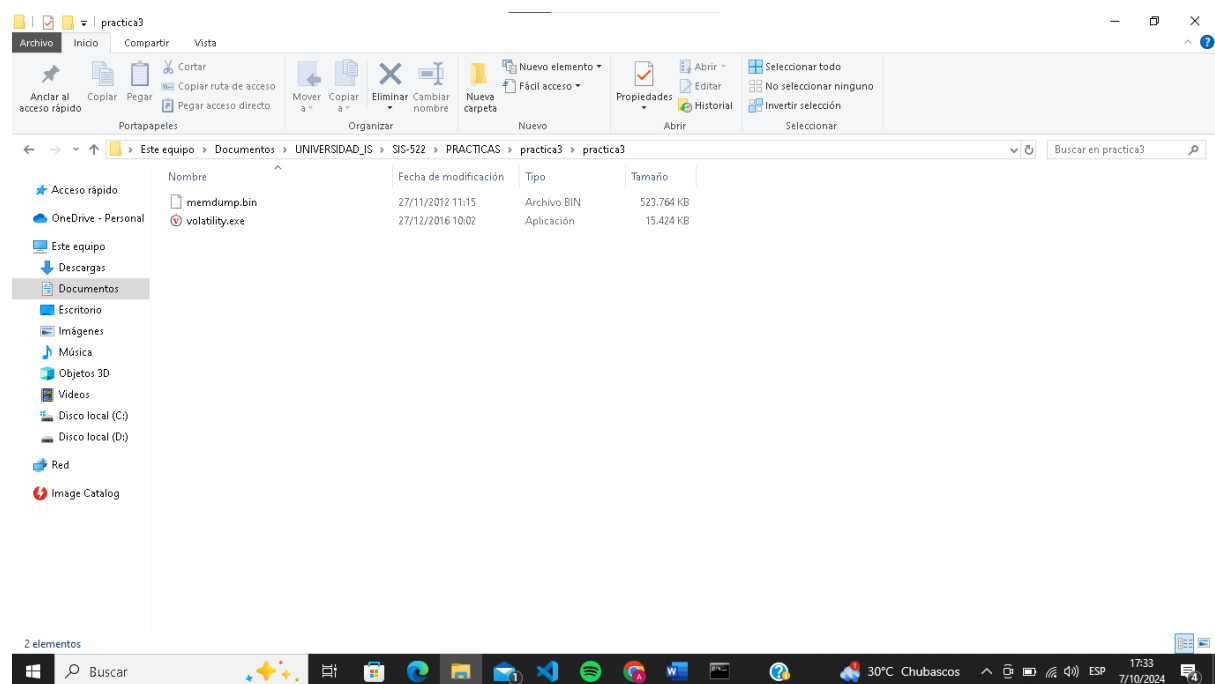
**Tamaño:** La caché L1 es la más pequeña, seguida de la L2, y la L3 es la más grande.

**Velocidad:** La caché L1 es la más rápida debido a su proximidad al núcleo del procesador. La L2 es más lenta que la L1, y la L3 es la más lenta de las tres.

**Proximidad al procesador:** La caché L1 está integrada directamente en el núcleo del procesador, la L2 suele estar cerca, pero fuera del núcleo, y la L3 se comparte entre varios núcleos y está más alejada en comparación con las otras dos.

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

**PASO 1**



## PASO 2

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>cd .\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
```

## PASO 3

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Usuario>cd .\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>ls
"ls" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>volatility imageinfo -f memdump.bin
"volatility" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>volatility imageinfo -f memdump.bin
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win2003SP8x86, Win2003SP1x86, Win2003SP2x86 (Instantiated with Win2003SP8x86)
                           AS Layer1 : IA32PagedMemory (Kernel AS)
                           AS Layer2 : FileAddressSpace (C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3\memdump.bin)
                           PAE type : No PAE
                           DTB : 0x39800L
                           KDBG : 0x805583d0L
      Number of Processors : 1
      Image Type (Service Pack) : 0
      KPCR for CPU 0 : 0xfffff000L
      KUSER_SHARED_DATA : 0xfffff000L
      Image date and time : 2012-11-27 02:01:57 UTC+0000
      Image local date and time : 2012-11-26 20:01:57 -0600

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
```

## PASO 4

```
C:\Windows\system32\cmd.exe
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffff000L
KUSER_SHARED_DATA : 0xfffff000L
Image date and time : 2012-11-27 02:01:57 UTC+0000
Image local date and time : 2012-11-26 20:01:57 -0600

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>volatility -f memdump.bin --profile=Win2003SP8x86 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
0x820c6020 smss.exe 372 4 3 17 ----- 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
0x8203fad0 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
0x81fd1f20 svchost.exe 804 488 9 133 0 0 2012-11-03 20:18:44 UTC+0000
0x81fd1f0 svchost.exe 904 488 5 78 0 0 2012-11-03 20:18:44 UTC+0000
0x81fd0908 svchost.exe 932 488 47 1092 0 0 2012-11-03 20:18:44 UTC+0000
0x81caf2d8 spoolsv.exe 1216 488 9 135 0 0 2012-11-03 20:19:12 UTC+0000
0x81cbad88 msdtc.exe 1240 488 15 160 0 0 2012-11-03 20:19:12 UTC+0000
0x81ca3d68 dfssvc.exe 1312 488 10 106 0 0 2012-11-03 20:19:12 UTC+0000
0x81c99020 svchost.exe 1404 488 2 60 0 0 2012-11-03 20:19:12 UTC+0000
0x81c82d88 lsmserv.exe 1436 488 11 276 0 0 2012-11-03 20:19:12 UTC+0000
0x81c80320 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
0x81c46208 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
0x81c4ad88 dns.exe 340 488 12 163 0 0 2012-11-03 21:41:26 UTC+0000
0x81bf9020 wlns.exe 756 488 19 214 0 0 2012-11-04 17:02:01 UTC+0000
0x81be0108 wuaucL.exe 1092 932 5 74 0 0 2012-11-04 18:57:32 UTC+0000
0x81b61b18 dlhst.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
0x81b0bb08 srvcung.exe 1496 488 3 87 0 0 2012-11-24 17:47:40 UTC+0000
0x81b0bf348 inetinfo.exe 308 488 25 515 0 0 2012-11-24 17:47:51 UTC+0000
0x81b71780 wmlprvse.exe 2116 740 7 208 0 0 2012-11-24 17:48:48 UTC+0000
0x81b6a4d8 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
0x81c25b68 mdd.exe 3468 2076 1 25 0 0 2012-11-27 02:01:56 UTC+0000

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
```

## PASO 5

```
C:\Windows\system32\cmd.exe
0x81b4b9d0 appmgr.exe 2992 488 4 102 0 0 2012-11-24 17:47:40 UTC+0000
0x81b0bb08 srvcung.exe 1496 488 3 87 0 0 2012-11-24 17:47:40 UTC+0000
0x81b0bf348 inetinfo.exe 308 488 25 515 0 0 2012-11-24 17:47:51 UTC+0000
0x81b71780 wmlprvse.exe 2116 740 7 208 0 0 2012-11-24 17:48:48 UTC+0000
0x81b6a4d8 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
0x81c25b68 mdd.exe 3468 2076 1 25 0 0 2012-11-27 02:01:56 UTC+0000

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>volatility -f memdump.bin --profile=Win2003SP8x86 pstree
Volatility Foundation Volatility Framework 2.6
Name PID PPID Thds Hnds Time
-----
0x822b07a8: System 4 0 52 842 1970-01-01 00:00:00 UTC+0000
.. 0x820c6020: smss.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
... 0x820496c8: 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
... 0x8203fad0: services.exe 488 444 21 422 2012-11-03 20:18:31 UTC+0000
... 0x81fd1f20: svchost.exe 804 488 9 133 2012-11-03 20:18:44 UTC+0000
... 0x81fd1f0: svchost.exe 904 488 5 78 2012-11-03 20:18:44 UTC+0000
... 0x81fd0908: svchost.exe 932 488 47 1092 2012-11-03 20:18:44 UTC+0000
... 0x81caf2d8: spoolsv.exe 1216 488 9 135 2012-11-03 20:19:12 UTC+0000
... 0x81cbad88: msdtc.exe 1240 488 15 160 2012-11-03 20:19:12 UTC+0000
... 0x81ca3d68: dfssvc.exe 1312 488 10 106 2012-11-03 20:19:12 UTC+0000
... 0x81c80320: ntfrs.exe 1452 488 19 282 2012-11-03 20:19:12 UTC+0000
... 0x81b4b9d0: appmgr.exe 2992 488 4 102 2012-11-24 17:47:40 UTC+0000
... 0x81b0bf348: inetinfo.exe 308 488 25 515 2012-11-24 17:47:51 UTC+0000
... 0x81caf2d8: spoolsv.exe 1216 488 9 135 2012-11-03 20:19:12 UTC+0000
... 0x81c46208: svchost.exe 1736 488 16 127 2012-11-03 20:19:27 UTC+0000
... 0x81c4ad88: dns.exe 340 488 12 163 2012-11-03 21:41:26 UTC+0000
... 0x81cbad88: msdtc.exe 1240 488 15 160 2012-11-03 20:19:12 UTC+0000
... 0x81fd0908: svchost.exe 932 488 47 1092 2012-11-03 20:18:44 UTC+0000
... 0x81be0108: wuaucL.exe 1092 932 5 74 2012-11-04 18:57:32 UTC+0000
... 0x81b61b18: dlhst.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
... 0x81b71780: wmlprvse.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
... 0x81bf9020: wlns.exe 756 488 19 214 2012-11-04 17:02:01 UTC+0000
... 0x81b6a4d8: POP3Svc.exe 2260 488 7 142 2012-11-24 17:55:08 UTC+0000
... 0x81c99020: svchost.exe 1404 488 2 60 2012-11-03 20:19:12 UTC+0000
... 0x81c4bd88: 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\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
```

## PASO 6

```
C:\Windows\system32\cmd.exe
C:\Users\Usuario\Documents\UNIVERSIDAD_IDE\SIS-522\PRACTICAS\practica3>volatility -f memdump.bin --profile-Win2003SP8x86 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 0xf000 0xffff \SystemRoot\System32\smss.exe
0x77f40000 0xb000 0xffff 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:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ProfileControl=Off MaxRequestThreads=16

Base      Size  LoadCount Path
-----
0x4a680000 0x4000 0xffff \\?\C:\WINDOWS\system32\csrss.exe
0x77f40000 0xb000 0xffff C:\WINDOWS\system32\ntdll.dll
0x75a50000 0xb000 0xffff C:\WINDOWS\system32\CSRSRV.dll
0x75a60000 0xf000 0x3 C:\WINDOWS\system32\basesrv.dll
0x75a90000 0x4000 0x2 C:\WINDOWS\system32\winsrv.dll
0x77e40000 0xf000 0x10 C:\WINDOWS\system32\USER32.dll
0x77d00000 0x8f000 0x6 C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0x5 C:\WINDOWS\system32\GDI32.dll
0x75da0000 0xb000 0x1 C:\WINDOWS\system32\sxs.dll
0x77da0000 0x90000 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
-----
0x81000000 0x8b000 0xffff \\?\C:\WINDOWS\system32\winlogon.exe
0x77f40000 0xb000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x5000 0xffff C:\WINDOWS\system32\user32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x75970000 0xb000 0xffff C:\WINDOWS\system32\USERENV.dll
0x75810000 0x7000 0xffff C:\WINDOWS\system32\NDSAPI.dll
0x761b0000 0x90000 0xffff C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0xffff C:\WINDOWS\system32\WSASMI.dll
0x76f50000 0x13000 0xffff C:\WINDOWS\system32\Secur32.dll
0x76260000 0x10000 0xffff C:\WINDOWS\system32\NETAPI.dll
0x771c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x75800000 0x9000 0xffff C:\WINDOWS\system32\PROFMAP.dll
0x76b20000 0xf000 0xffff C:\WINDOWS\system32\REGAPI.dll
0x771c00000 0x18000 0xffff C:\WINDOWS\system32\WS2_32.dll
0x771bf0000 0x8000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x76b70000 0xb000 0xffff C:\WINDOWS\system32\PSAPI.dll
0x77090000 0x8000 0xffff C:\WINDOWS\system32\VERSION.dll
0x765a0000 0x108000 0xffff C:\WINDOWS\system32\SETUPAPI.dll
0x75840000 0x128000 0x2 C:\WINDOWS\system32\WSGIMA.dll
0x76b40000 0x21000 0x1 C:\WINDOWS\system32\SHSVCS.dll
0x77290000 0x49000 0x20 C:\WINDOWS\system32\SHLWAPI.dll
0x76b10000 0x5000 0x2 C:\WINDOWS\system32\sfcd.dll
0x76be0000 0x2a000 0x5 C:\WINDOWS\system32\sfcd_os.dll
0x76bb0000 0x2b000 0x5 C:\WINDOWS\system32\WINTRUST.dll
0x77160000 0x124000 0x2a C:\WINDOWS\system32\ole32.dll
0x76c10000 0x28000 0x5 C:\WINDOWS\system32\imagehlp.dll
0x70a40000 0xe000 0xa C:\WINDOWS\system32\Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.180.0_x-ww_8417458B\Comctl32.dll
0x72430000 0x1c000 0x7 C:\WINDOWS\system32\WINSCARD.DLL
0x76f00000 0x8000 0x7 C:\WINDOWS\system32\WTSAPI32.dll
0x75da0000 0xb000 0x1 C:\WINDOWS\system32\sxs.dll
0x77380000 0x7dd000 0xc C:\WINDOWS\system32\shell32.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\wssock32.dll
0x76cf0000 0x1f000 0x4 C:\WINDOWS\system32\iphlpapi.dll
0x74610000 0x5000 0x1 C:\WINDOWS\system32\icmp.dll
0x8ffdf0000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76cd0000 0x17000 0x1 C:\WINDOWS\system32\WPRAPI.dll
0x76df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEOS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adsldpc.dll
```

```
C:\Windows\system32\cmd.exe
0x74010000 0x5000 0x1 C:\WINDOWS\system32\icmp.dll
0x0ffdf000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76cd0000 0x17000 0x1 C:\WINDOWS\system32\WPAPI.dll
0x76df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEOS.dll
0x76dc0000 0x2b000 0x1 C:\WINDOWS\system32\adsldpc.dll
0x76f10000 0x2f000 0x10 C:\WINDOWS\system32\WLDAP32.dll
0x76b00000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x76a00000 0x18000 0x1 C:\WINDOWS\system32\ATL.dll
0x770e0000 0x7d000 0xc C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb000 0x1 C:\WINDOWS\system32\rtutils.dll
0x5ccf0000 0x10000 0x3 C:\WINDOWS\system32\SAMLIB.dll
0x71b20000 0x43000 0x4 C:\WINDOWS\system32\mswsock.dll
0x76f00000 0x5000 0x1 C:\WINDOWS\system32\irasadhlp.dll
0x71ca0000 0x5000 0x1 C:\WINDOWS\system32\Kerberos.dll
0x766e0000 0xe000 0x1 C:\WINDOWS\system32\cryptui.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x766f0000 0x16000 0x3 C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0x4 C:\WINDOWS\system32\DNSAPI.dll
0x76520000 0x1d000 0x2 C:\WINDOWS\system32\csddl.dll
0x75820000 0x1a000 0x6 C:\WINDOWS\system32\WinNotify.dll
0x76aa0000 0x2c000 0x7 C:\WINDOWS\system32\WINMM.dll
0x73070000 0x2b000 0x6 C:\WINDOWS\system32\WINSPOOL.DRV
0x71bd0000 0x11000 0x7 C:\WINDOWS\system32\WPR.dll
0x70bc0000 0x9000 0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.02.0.0_x-ww_BA69BA85\COMCTL32.dll
0x71b70000 0x33000 0x2 C:\WINDOWS\system32\UXTheme.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0xc000 0x1 C:\WINDOWS\system32\COMRes.dll
0x74cf0000 0x8000 0x1 C:\WINDOWS\system32\wbem\wbemprox.dll
0x750f0000 0x38000 0x2 C:\WINDOWS\system32\wbem\wbemcomn.dll
0x74ce0000 0xe000 0x1 C:\WINDOWS\system32\wbem\wbemsvcs.dll
0x75550000 0x71000 0x1 C:\WINDOWS\system32\wbem\fastprox.dll
0x708c0000 0x61000 0x1 C:\WINDOWS\system32\WSVCP60.dll
0x76c90000 0x2d000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x76540000 0x5000 0x1 C:\WINDOWS\system32\cscli.dll
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\ES.dll
0x76c00000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.dll
0x74fa0000 0x14000 0x1 C:\WINDOWS\system32\Cabinet.dll
0x73ca0000 0x12000 0xa C:\WINDOWS\system32\cryptnet.dll
0x722f0000 0x5000 0xa C:\WINDOWS\system32\SensAPI.dll
*****
services.exe pid: 400
Command line : C:\WINDOWS\system32\services.exe
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount  Path
-----
0x01000000 0x1b000 0xffff C:\WINDOWS\system32\services.exe
0x77f40000 0xb000 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 0x4d000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77000000 0x4f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x75070000 0xb000 0xffff C:\WINDOWS\system32\USERENV.dll
0x757a0000 0x52000 0xffff C:\WINDOWS\system32\SCESRV.dll
0x76c40000 0x14000 0xffff C:\WINDOWS\system32\AUTHZ.dll
0x71c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x75770000 0x21000 0xffff C:\WINDOWS\system32\umpnpmgr.dll
0x76260000 0x10000 0xffff C:\WINDOWS\system32\WINSTA.dll
0x5fb10000 0xc000 0xffff C:\WINDOWS\system32\WCOBAPI.dll
0x708c0000 0x61000 0xffff C:\WINDOWS\system32\WSVCP60.dll
0x76f50000 0x13000 0x6 C:\WINDOWS\system32\secur32.dll
0x75750000 0x12000 0x1 C:\WINDOWS\system32\eventlog.dll
0x71c00000 0x10000 0x7 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x8 C:\WINDOWS\system32\WS2HELP.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x76f00000 0x8000 0x1 C:\WINDOWS\system32\wtsapi32.dll
0x74190000 0x3000 0x1 C:\WINDOWS\system32\seccli.dll
0x765a0000 0x10000 0x2 C:\WINDOWS\system32\SETUPAPI.dll
0x74fa0000 0x14000 0x1 C:\WINDOWS\system32\Cabinet.dll
0x77160000 0x12d000 0x2 C:\WINDOWS\system32\ole32.dll
0x5ccf0000 0x10000 0x2 C:\WINDOWS\system32\SAMLIB.dll
0x69750000 0x10000 0x1 C:\WINDOWS\system32\ESSENT.dll
0x76c00000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.dll
0x76f10000 0x2f000 0x3 C:\WINDOWS\system32\WLDAP32.dll
0x71b20000 0x43000 0x2 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x766f0000 0x16000 0x1 C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x71ca0000 0x5000 0x1 C:\WINDOWS\system32\Kerberos.dll
0x766e0000 0xc000 0x1 C:\WINDOWS\system32\cryptui.dll
0x76190000 0x12000 0x1 C:\WINDOWS\system32\WSASN1.dll
*****
lsass.exe pid: 500
Command line : C:\WINDOWS\system32\lsass.exe
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount Path
-----
0x01000000 0x60000 0xfffff C:\WINDOWS\system32\lsass.exe
0x77f40000 0xb8000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d40000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x4d000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77b20000 0xc8000 0xfffff C:\WINDOWS\system32\SASRV.dll
0x77a00000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x779f0000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x774d0000 0x70000 0xfffff C:\WINDOWS\system32\SAMSRV.dll
0x776e0000 0xc8000 0xfffff C:\WINDOWS\system32\Crypt.dll
0x776d0000 0x27000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x771c0000 0x18000 0xfffff C:\WINDOWS\system32\WS2_32.dll
0x771b0000 0x80000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x77190000 0x12000 0xfffff C:\WINDOWS\system32\WSASN1.dll
0x771c40000 0x53000 0xfffff C:\WINDOWS\system32\NETAPI32.dll
0x5ccf0000 0x10000 0xfffff C:\WINDOWS\system32\SAMLIB.dll
0x77bd0000 0x11000 0xfffff C:\WINDOWS\system32\WPR.dll
0x776f0000 0x16000 0xfffff C:\WINDOWS\system32\NTDSAPI.dll
0x776f10000 0x2f000 0xfffff C:\WINDOWS\system32\WLDAP32.dll
0x774130000 0xe0000 0x1 C:\WINDOWS\system32\msprivs.dll
0x771ca0000 0x56000 0x6 C:\WINDOWS\system32\Kerberos.dll
0x776c90000 0x24000 0xf C:\WINDOWS\system32\msv1_0.dll
0x774250000 0x60000 0x8 C:\WINDOWS\system32\netlogon.dll
0x776710000 0x38000 0x8 C:\WINDOWS\system32\W32time.dll
0x780c0000 0x61000 0x8 C:\WINDOWS\system32\WSVCP60.dll
0x776cf0000 0x17000 0xa C:\WINDOWS\system32\lphlpapi.dll
0x775970000 0xb9000 0xfffff C:\WINDOWS\system32\USERENV.dll
0x776c40000 0x14000 0x17 C:\WINDOWS\system32\AUTHZ.dll
0x776750000 0x20000 0x7 C:\WINDOWS\system32\lschance.dll
0x771b0000 0x90000 0x1a C:\WINDOWS\system32\CRYPT32.dll
0x77410000 0x12000 0x3 C:\WINDOWS\system32\wdigest.dll
0x0ffdf0000 0x2d000 0x1 C:\WINDOWS\system32\rsenh.dll
0x776b70000 0xb0000 0x2 C:\WINDOWS\system32\PSAPI.DLL
0x7720e0000 0x19a000 0xa C:\WINDOWS\system32\NTDSA.dll
0x771d0000 0xb0000 0xe C:\WINDOWS\system32\NTDSFQ.dll
0x771b20000 0x42000 0xf C:\WINDOWS\system32\WSOCK32.dll
0x69750000 0x108000 0xc C:\WINDOWS\system32\ESSENT.dll
0x5f1d0000 0x80000 0x2 C:\WINDOWS\system32\ntdsmsg.dll
0x771e90000 0xf0000 0x2 C:\WINDOWS\system32\ntdsrsv.dll
0x771bb0000 0x90000 0x2 C:\WINDOWS\system32\WSOCK32.dll

C:\Windows\system32\cmd.exe
Base      Size      LoadCount Path
-----
0x771e90000 0xf0000 0x2 C:\WINDOWS\system32\ntdsrsv.dll
0x771bb0000 0x90000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x5b090000 0x87000 0x2 C:\WINDOWS\system32\VSAPI.DLL
0x776a0000 0x10000 0x3 C:\WINDOWS\system32\ATL.DLL
0x77160000 0x124000 0x12 C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0x9 C:\WINDOWS\system32\OLEAUT32.dll
0x63a80000 0x3a000 0x4 C:\WINDOWS\system32\KDCSVC.dll
0x5d9f0000 0x90000 0x1 C:\WINDOWS\system32\RASSFM.dll
0x77410000 0x20000 0x3 C:\WINDOWS\system32\SecC11.dll
0x7765a0000 0x108000 0x5 C:\WINDOWS\system32\SETUPAPI.dll
0x771ae0000 0x80000 0x1 C:\WINDOWS\system32\ushtcpip.dll
0x5deb0000 0x70000 0x1 C:\WINDOWS\system32\pwdssp.dll
0x771e0000 0x14000 0x1 C:\WINDOWS\system32\msapspc.dll
0x78080000 0x11000 0x1 C:\WINDOWS\system32\MSVCRT40.dll
0x720a0000 0x1f000 0x1 C:\WINDOWS\system32\NTDSKCC.dll
0x771f30000 0xa0000 0x1 C:\WINDOWS\system32\W32TOPL.dll
0x77410000 0x20000 0x1 C:\WINDOWS\system32\lpsvc.dll
0x77420000 0xc0000 0x1 C:\WINDOWS\system32\lschance.dll
0x7740f0000 0xc0000 0x1 C:\WINDOWS\system32\WINIPSEC.DLL
0x774120000 0x00000 0x1 C:\WINDOWS\system32\pstorevc.dll
0x774140000 0x17000 0x1 C:\WINDOWS\system32\psbase.dll
0x0ffa0000 0x22000 0x1 C:\WINDOWS\system32\dsenh.dll
0x58f40000 0x17000 0x1 C:\WINDOWS\system32\wlsctrl.dll
0x77290000 0x49000 0x6 C:\WINDOWS\system32\SHLWAPI.dll
0x776f90000 0x70000 0x1 C:\WINDOWS\system32\ClbcatQ.DLL
0x77010000 0x60000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x2 C:\WINDOWS\system32\VERSION.dll
0x776ad0000 0x3e000 0x1 C:\WINDOWS\system32\res.dll
0x776f0000 0x50000 0x1 C:\WINDOWS\system32\rsadhlp.dll
0x776f70000 0x70000 0x1 C:\WINDOWS\system32\winnr.dll
0x776c0000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x776cd0000 0x17000 0x1 C:\WINDOWS\system32\WPRAPI.dll
0x776df0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVE05.dll
0x776dc0000 0x26000 0x1 C:\WINDOWS\system32\wddlpcc.dll
0x776b0000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x77300000 0x7dd000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x776e0000 0xb0000 0x1 C:\WINDOWS\system32\rtutils.dll
0x770ad0000 0xe0000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x5a310000 0x70000 0x1 C:\WINDOWS\system32\w3ssl.dll
0x5b640000 0x15000 0x2 C:\WINDOWS\system32\strmfilt.dll
0x67150000 0xa0000 0x2 C:\WINDOWS\system32\HTTPAPI.dll

*****
svchost.exe pid: 740
command line: C:\WINDOWS\system32\svchost -k rpcss
```

```
C:\Windows\system32\cmd.exe

Base             Size      LoadCount Path
-----
0x01000000      0x6000      0xffff C:\WINDOWS\system32\svchost.exe
0x77f40000      0xb000      0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000      0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77d40000      0x90000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000      0xa4000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77500000      0x48000     0x1 C:\WINDOWS\system32\RPCSS.dll
0x77ba0000      0x54000     0xf C:\WINDOWS\system32\msvcrt.dll
0x71c00000      0x18000     0x0 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000      0x8000      0x9 C:\WINDOWS\system32\WS2HELP.dll
0x77d00000      0x8f000     0xa C:\WINDOWS\system32\USER32.dll
0x77c00000      0x44000     0x8 C:\WINDOWS\system32\GDI32.dll
0x77f50000      0x13000     0x2 C:\WINDOWS\system32\Secur32.dll
0x77b20000      0x43000     0x3 C:\WINDOWS\system32\mswsock.dll
0x71ae0000      0x8000      0x1 C:\WINDOWS\system32\wshtcpip.dll
0x76f90000      0x7e000     0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x770e0000      0x7d000     0x1 C:\WINDOWS\system32\OLEAUT32.dll
0x77160000      0x124000    0x3 C:\WINDOWS\system32\ole32.dll
0x77010000      0xc0000     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      0xb000      0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000      0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77d40000      0x90000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000      0xa4000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x76d10000      0x1c000     0x3 C:\WINDOWS\system32\dhcpcsvc.dll
0x77ba0000      0x54000     0x11b7 C:\WINDOWS\system32\msvcrt.dll
0x76ed0000      0x27000     0x5 C:\WINDOWS\system32\DNSAPI.dll
0x71c00000      0x18000     0x8ce C:\WINDOWS\system32\WS2_32.dll
0x71bf0000      0x8000      0x8c7 C:\WINDOWS\system32\WS2HELP.dll
0x77c6f0000      0x17000     0x8c2 C:\WINDOWS\system32\iphlpapi.dll
0x77d00000      0x8f000     0x11af C:\WINDOWS\system32\USER32.dll
0x77c00000      0x44000     0x8da C:\WINDOWS\system32\GDI32.dll
0x76f50000      0x13000     0x7 C:\WINDOWS\system32\Secur32.dll
0x776c0000      0xd000      0x1 C:\WINDOWS\system32\dnsrslvr.dll
0x776d0000      0x37000     0x1 C:\WINDOWS\system32\netman.dll
0x776d0000      0x37000     0x1 C:\WINDOWS\system32\netman.dll
```

```
C:\Windows\system32\cmd.exe

0x76ed0000      0x27000     0x5 C:\WINDOWS\system32\DNSAPI.dll
0x71c00000      0x18000     0x8ce C:\WINDOWS\system32\WS2_32.dll
0x71bf0000      0x8000      0x8c7 C:\WINDOWS\system32\WS2HELP.dll
0x77c6f0000      0x17000     0x8c2 C:\WINDOWS\system32\iphlpapi.dll
0x77d00000      0x8f000     0x11af C:\WINDOWS\system32\USER32.dll
0x77c00000      0x44000     0x8da C:\WINDOWS\system32\GDI32.dll
0x76f50000      0x13000     0x7 C:\WINDOWS\system32\Secur32.dll
0x776c0000      0xd000      0x1 C:\WINDOWS\system32\dnsrslvr.dll
0x776d0000      0x37000     0x1 C:\WINDOWS\system32\netman.dll
0x776d0000      0x37000     0x1 C:\WINDOWS\system32\WPRAP1.dll
0x776df0000      0x32000     0x1 C:\WINDOWS\system32\ACTIVE05.dll
0x776dc0000      0x26000     0x1 C:\WINDOWS\system32\adsldpc.dll
0x771c40000      0x53000     0x9 C:\WINDOWS\system32\NETAPI32.dll
0x76f10000      0x2f000     0x3 C:\WINDOWS\system32\WLDAP32.dll
0x76b80000      0x2d000     0x1 C:\WINDOWS\system32\credui.dll
0x77380000      0x7dd000    0x2 C:\WINDOWS\system32\SHL32.dll
0x77290000      0x49000     0x7 C:\WINDOWS\system32\SHLAPI.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
0x776e30000      0xb000      0x4 C:\WINDOWS\system32\rtutils.dll
0x5ccf0000      0x10000     0x1 C:\WINDOWS\system32\SAMLIB.dll
0x765a0000      0x10000     0x1 C:\WINDOWS\system32\SETUPAPI.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
0x76a80000      0x2c000     0x2 C:\WINDOWS\system32\WINMM.dll
0x761b0000      0x90000     0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000      0x12000     0x2 C:\WINDOWS\system32\WSASN1.dll
0x76d30000      0x47000     0x1 C:\WINDOWS\system32\WZCSvc.DLL
0x76cc0000      0x5000      0x1 C:\WINDOWS\system32\WMI.dll
0x76f00000      0x8000      0x1 C:\WINDOWS\system32\WTSAPI32.dll
0x76260000      0x18000     0x2 C:\WINDOWS\system32\WINSTA.dll
0x69f50000      0x10000     0x1 C:\WINDOWS\system32\GSENT.dll
0x730a0000      0x9000      0x1 C:\WINDOWS\system32\WZCSAPI.DLL
0x70a40000      0xe000      0x3 C:\WINDOWS\WinSxS\x86_Microsoft_Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x71b20000      0x43000     0x2 C:\WINDOWS\system32\mswsock.dll
0x71ae0000      0x8000      0x1 C:\WINDOWS\system32\wshtcpip.dll
0x71f00000      0x4000      0x1 C:\WINDOWS\system32\security.dll
0x766f0000      0x16000     0x1 C:\WINDOWS\system32\ntdsapi.dll
*****
svchost.exe pid: 884
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
```



```
C:\Windows\system32\cmd.exe

Base      Size      LoadCount Path
-----
0x01000000 0x60000 0xfffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d40000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WIMMART.A.DLL
0x77ba0000 0x54000 0xe C:\WINDOWS\system32\msvcrt.dll
0x77d00000 0x8f000 0x7 C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0x5 C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x77160000 0x12000 0xe C:\WINDOWS\system32\SAMLIB.dll
0x74400000 0x90000 0x1 C:\Windows\system32\lmsvc.dll
0x76cf0000 0x17000 0x1 C:\Windows\system32\iphlpapi.dll
0x71c00000 0x18000 0x5 C:\Windows\system32\WS2_32.dll
0x71bf0000 0x8000 0x5 C:\Windows\system32\WS2HELP.dll
0x71b20000 0x43000 0x1 C:\WINDOWS\system32\mswsock.dll
0x76ed0000 0x27000 0x1 C:\WINDOWS\system32\DNSAPI.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\system32\rasadhlp.dll
*****
svchost.exe pid: 932
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs

Base      Size      LoadCount Path
-----
0x01000000 0x60000 0xfffff C:\WINDOWS\System32\svchost.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77d40000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WIMMART.A.DLL
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x1a C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0xe C:\WINDOWS\system32\SAMLIB.dll
0x77160000 0x12000 0x70 C:\WINDOWS\system32\GDI32.dll
0x76d30000 0x47000 0x2 C:\Windows\system32\wzcsvc.dll
0x76e30000 0xb0000 0x18 C:\Windows\system32\ntutils.dll
0x76cc0000 0x5000 0x3 C:\Windows\system32\WMI.dll
0x76d10000 0x1c000 0x3 C:\Windows\system32\DHCPSPVC.DLL
```

```
C:\Windows\system32\cmd.exe

0x77290000 0x49000 0x2c C:\WINDOWS\system32\SHLWAPI.dll
0x69750000 0x100000 0x3 C:\Windows\system32\NENET.dll
0x74d10000 0x29000 0x3 C:\WINDOWS\system32\Nastls.dll
0x76a00000 0x18000 0x10 C:\WINDOWS\system32\ATL.DLL
0x75360000 0x79000 0x3 C:\WINDOWS\system32\CRYPTUI.dll
0x76bb0000 0x2b000 0xc C:\WINDOWS\system32\WINTRUST.dll
0x76c10000 0x28000 0x9 C:\WINDOWS\system32\imagehlp.dll
0x766f0000 0x16000 0xc C:\WINDOWS\system32\NTDSAPI.dll
0x76cd0000 0x17000 0x6 C:\WINDOWS\system32\WPRAPI.dll
0x76df0000 0x32000 0x6 C:\WINDOWS\system32\ACTIVE05.dll
0x76dc0000 0x20000 0x6 C:\WINDOWS\system32\adsldpc.dll
0x76b00000 0x2d000 0x8 C:\WINDOWS\system32\credui.dll
0x77380000 0x7d000 0xe C:\WINDOWS\system32\SHELL32.dll
0x765a0000 0x100000 0xd C:\WINDOWS\system32\SETUPAPI.dll
0x76e90000 0x3b000 0x9 C:\WINDOWS\system32\RASAPI32.dll
0x76e40000 0x11000 0xd C:\WINDOWS\system32\rasman.dll
0x76e60000 0x2e000 0xa C:\WINDOWS\system32\TAPI2.dll
0x76a10000 0x2c000 0x9 C:\WINDOWS\system32\WIMMART.A.DLL
0x76750000 0x28000 0x3 C:\WINDOWS\system32\SCHANNEL.dll
0x75970000 0xb0000 0xfffff C:\WINDOWS\system32\USERENV.dll
0x72430000 0x1c000 0x3 C:\WINDOWS\system32\WinSCard.dll
0x70bc0000 0x90000 0x3 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA85\COMCTL32.dll
0x70ad0000 0xe0000 0x9 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\Comctl32.dll
0x74d00000 0x1d000 0x3 C:\WINDOWS\system32\raschap.dll
0x70b40000 0x21000 0x2 C:\Windows\system32\shsvcs.dll
0x76f90000 0x70000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b00000 0x80000 0x7 C:\WINDOWS\system32\VERSION.dll
0x75020000 0x30000 0x1 C:\Windows\system32\svcschedv.dll
0x76c40000 0x14000 0x1 C:\Windows\system32\AUTHZ.dll
0x71b20000 0x43000 0x8 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x80000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x74d70000 0x5000 0x1 C:\WINDOWS\system32\WSIDLE.DLL
0x74fc0000 0x23000 0x1 C:\Windows\system32\Wlsvc.dll
0x59ec0000 0xb0000 0x1 C:\WINDOWS\system32\wiarp.dll
0x74ed0000 0x18000 0x1 C:\Windows\system32\svrsvc.dll
0x74e00000 0x14000 0x3 C:\Windows\system32\browser.dll
0x74dc0000 0xf000 0x1 C:\Windows\system32\cryptsp.dll
0x751c0000 0x3d000 0x1 C:\Windows\system32\certcli.dll
0x76b70000 0xb0000 0x2 C:\Windows\system32\PSAPI.DLL
0x5b890000 0x87000 0x2 C:\Windows\system32\VSSAPI.DLL
0x70b10000 0x5000 0x2 C:\Windows\system32\svcs.dll
0x76be0000 0x20000 0x4 C:\Windows\system32\svcs.dll
0x74db0000 0xa000 0x1 C:\Windows\system32\dsrver.dll
```

```
C:\Windows\system32\cmd.exe
0x76d0000 0x3e000 0x4 c:\Windows\system32\es.dll
0x74d0000 0xb0000 0x1 c:\Windows\pchealth\helpctr\binaries\pchsvc.dll
0x73c70000 0x7000 0x1 c:\Windows\system32\seclogon.dll
0x72310000 0xc000 0x1 c:\Windows\system32\sens.dll
0x7170000 0x30000 0x3 c:\Windows\system32\W32time.dll
0x709c0000 0x61000 0x13 c:\Windows\system32\WSVCP60.dll
0x58af0000 0x25000 0x1 c:\Windows\system32\wbem\wmisvc.dll
0x74cd0000 0x6000 0x1 c:\Windows\system32\wuaueng.dll
0x74e20000 0x32000 0x1 c:\Windows\system32\wuaueng.dll
0x750c0000 0x20000 0x1 c:\Windows\system32\ADVAPI32.dll
0x760f0000 0x9e000 0x2 c:\Windows\system32\WININET.dll
0x75da0000 0xb000 0x1 c:\Windows\system32\SXS.dll
0x755d0000 0x12c000 0x2 c:\Windows\system32\comsvcs.dll
0x750a0000 0x7000 0x1 c:\Windows\system32\winspvc.dll
0x76c90000 0x24000 0x1 c:\Windows\system32\msv1_0.dll
0x70c0000 0x54000 0x1 c:\Windows\WinSxS\x86_Microsoft.Windows.Common-Internet_6595b64144ccf1df_5.1.0.0_x-ww_E0651936\winhttp.dll
0x752e0000 0x75000 0x1 c:\Windows\system32\wbem\wbemcore.dll
0x75180000 0x3e000 0x4 c:\Windows\system32\wbem\wbemesscli.dll
0x750f0000 0x38000 0xf c:\Windows\system32\wbem\wbemcomn.dll
0x75550000 0x71000 0x8 c:\Windows\system32\wbem\FastProx.dll
0x74e60000 0x1b000 0x1 c:\Windows\system32\wbem\wmutils.dll
0x75060000 0x2c000 0x1 c:\Windows\system32\wbem\repdrvfs.dll
0x60050000 0x60000 0x1 c:\Windows\system32\wbem\wmiprvse.dll
0x5fb10000 0xc000 0x2 c:\Windows\system32\WCOBJAPI.dll
0x0ff0000 0x2d000 0x1 c:\Windows\system32\rsasenh.dll
0x74ce0000 0xe000 0x1 c:\Windows\system32\wbem\wbemsvc.dll
0x72510000 0x6000 0x1 c:\Windows\system32\ntlsapi.dll
0x76d80000 0x37000 0x1 c:\Windows\system32\Netman.dll
0x730a0000 0x9000 0x1 c:\Windows\system32\WZCSCAPI.dll
0x75be0000 0x1b1000 0x2 c:\Windows\system32\NETSHELL.dll
0x74de0000 0x11000 0x2 c:\Windows\system32\CLUSAPI.dll
0x6040000 0x41000 0x1 c:\Windows\system32\hnetcfg.dll
0x753e0000 0xa3000 0x1 c:\Windows\system32\RASD16.dll
0x76f0000 0x5000 0x1 c:\Windows\system32\rsasdhlp.dll
0x72060000 0x18000 0x2 c:\Windows\system32\actserv.dll
0x5f8c0000 0x7000 0x3 c:\Windows\system32\NETRAP.dll
0x722f0000 0x5000 0x1 c:\Windows\system32\sensapi.dll
0x76f70000 0x7000 0x1 c:\Windows\system32\WinInet.dll
0x7520000 0x43000 0x1 c:\Windows\system32\wbem\wbemess.dll
0x5fa0000 0x3d000 0x1 c:\Windows\system32\wbem\ncprov.dll
0x73c0000 0x17000 0x1 c:\Windows\system32\wbem\wbemcons.dll
*****
spoolsv.exe pid: 1216
Command line : c:\Windows\system32\spoolsv.exe
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount  Path
-----
0x01000000 0x10000 0xfffff C:\Windows\system32\spoolsv.exe
0x77f40000 0xb0000 0xfffff C:\Windows\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\Windows\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\Windows\system32\msvcrt.dll
0x77da0000 0x90000 0xfffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0x4d000 0xfffff C:\Windows\system32\RPCRT4.dll
0x77e0000 0x24000 0xfffff C:\Windows\system32\GDI32.dll
0x77f0000 0x0f000 0xfffff C:\Windows\system32\USER32.dll
0x76f50000 0x13000 0xa C:\Windows\system32\secur32.dll
0x74060000 0x16000 0xc C:\Windows\system32\SPoolSS.DLL
0x71c0000 0x18000 0x34 C:\Windows\system32\WS2_32.dll
0x71bf0000 0x8000 0x20 C:\Windows\system32\WS2HELP.dll
0x71c40000 0x53000 0x18 C:\Windows\system32\NETAPI32.dll
0x76cf0000 0x17000 0xd C:\Windows\system32\iphlpapi.dll
0x76ed0000 0x27000 0x5 C:\Windows\system32\ADVAPI32.dll
0x76f0000 0x5000 0x1 c:\Windows\system32\rsasdhlp.dll
0x740a0000 0x4e000 0x4 C:\Windows\system32\localapi.dll
0x77160000 0x124000 0x10 C:\Windows\system32\ole32.dll
0x770e0000 0x7d000 0x9 C:\Windows\system32\OLEAUT32.dll
0x77b90000 0x8000 0x5 C:\Windows\system32\VERSION.dll
0x76be0000 0x2a000 0x4 C:\Windows\system32\sfcs.dll
0x76bb0000 0x2b000 0x4 C:\Windows\system32\WINTRUST.dll
0x761b0000 0x09000 0x9 C:\Windows\system32\CRYPT32.dll
0x76190000 0x12000 0xa C:\Windows\system32\WSASAPI.dll
0x76c10000 0x28000 0x4 C:\Windows\system32\imagehlp.dll
0x75070000 0x3ba000 0x4 C:\Windows\system32\USERENV.dll
0x73070000 0x26000 0x2 C:\Windows\system32\winpool_drv
0x74020000 0xe000 0x1 c:\Windows\system32\cnbjmon.dll
0x74000000 0x7000 0x1 c:\Windows\system32\pjlmon.dll
0x72460000 0xe000 0x1 c:\Windows\system32\vcpcmon.dll
0x72000000 0x7000 0x1 c:\Windows\system32\mgmtapi.dll
0x71f50000 0x0000 0x1 c:\Windows\system32\snmpapi.dll
0x71ff0000 0x4000 0x1 c:\Windows\system32\wsnmp32.dll
0x72450000 0x8000 0x1 c:\Windows\system32\usbmon.dll
0x71b20000 0x43000 0x5 C:\Windows\system32\mswsock.dll
0x76f70000 0x7000 0x1 c:\Windows\system32\WinInet.dll
0x76f10000 0x2f000 0x7 C:\Windows\system32\WLDAP32.dll
0x57b60000 0x9000 0x1 c:\Windows\system32\wsqhqs.dll
0x71ae0000 0x8000 0x2 c:\Windows\system32\wshtcpip.dll
0x74030000 0x22000 0x1 c:\Windows\system32\Win32spl.dll
0x5f8c0000 0x7000 0x1 c:\Windows\system32\NETRAP.dll
0x74080000 0x15000 0x1 c:\Windows\system32\inetpp.dll
```

```
C:\Windows\system32\cmd.exe
0x740a0000 0x4e0000 0x4 C:\Windows\system32\localspl.dll
0x77160000 0x1240000 0x19 C:\Windows\system32\ole32.dll
0x770e0000 0x7d0000 0x9 C:\Windows\system32\OLEAUT32.dll
0x77b90000 0x80000 0x5 C:\Windows\system32\VERSION.dll
0x76be0000 0x2a0000 0x4 C:\Windows\system32\sfcd.dll
0x76bb0000 0x2b0000 0x4 C:\Windows\system32\WINTLUST.dll
0x761b0000 0x90000 0x0 C:\Windows\system32\CRVPT32.dll
0x76190000 0x120000 0xa C:\Windows\system32\WSASN1.dll
0x76c10000 0x280000 0x4 C:\Windows\system32\imagehlp.dll
0x75970000 0xb0000 0x4 C:\Windows\system32\USERENV.dll
0x73070000 0x260000 0x2 C:\Windows\system32\winspool.drv
0x74020000 0xe0000 0x1 C:\Windows\system32\cnbjmon.dll
0x74000000 0x70000 0x1 C:\Windows\system32\pjmon.dll
0x72460000 0xe0000 0x1 C:\Windows\system32\fcmon.dll
0x72000000 0x70000 0x1 C:\Windows\system32\mgmap1.dll
0x71f50000 0x80000 0x1 C:\Windows\system32\snmpapi.dll
0x71ff0000 0xd0000 0x1 C:\Windows\system32\wsnmp32.dll
0x72450000 0x80000 0x1 C:\Windows\system32\usbmon.dll
0x71b20000 0x430000 0x5 C:\Windows\system32\mswsock.dll
0x76f70000 0x70000 0x1 C:\Windows\system32\winhnr.dll
0x76f10000 0x2f0000 0x7 C:\Windows\system32\WLDAP32.dll
0x57b60000 0x90000 0x1 C:\Windows\system32\wsnqos.dll
0x71ae0000 0x0000 0x2 C:\Windows\system32\wshtcpip.dll
0x74030000 0x220000 0x1 C:\Windows\system32\win32spl.dll
0x5f8c0000 0x70000 0x1 C:\Windows\system32\NETRAP.dll
0x74000000 0x150000 0x1 C:\Windows\system32\inetpp.dll
0x74010000 0x50000 0x1 C:\Windows\system32\icmp.dll
0x766f0000 0x160000 0x2 C:\Windows\system32\NTDSAPI.dll
0x71ca0000 0x50000 0x1 C:\Windows\system32\kerberos.dll
0x766e0000 0xc0000 0x1 C:\Windows\system32\cryptdll.dll
0x76df0000 0x320000 0x2 C:\Windows\system32\ACTIVEDES.dll
0x76dc0000 0x260000 0x5 C:\Windows\system32\adsldpc.dll
0x76b00000 0x2d0000 0x3 C:\Windows\system32\credui.dll
0x77300000 0x7d0000 0x3 C:\Windows\system32\SHELL32.dll
0x77290000 0x40000 0x5 C:\Windows\system32\SHLWAPI.dll
0x76a00000 0x180000 0x2 C:\Windows\system32\ATL.DLL
0x70ad0000 0xe0000 0x2 C:\Windows\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x76f90000 0x7e0000 0x1 C:\Windows\system32\CLBCatQ.DLL
0x77010000 0xc0000 0x1 C:\Windows\system32\COMRES.dll
0x71c00000 0x2d0000 0x1 C:\Windows\system32\adsldp.dll
0x75da0000 0xb0000 0x1 C:\Windows\system32\SXS.DLL
*****
msdtc.exe pid: 1240
Command line : C:\Windows\system32\msdtc.exe

C:\Windows\system32\cmd.exe
Base      Size      LoadCount Path
-----
0x00400000 0x40000 0xffff C:\Windows\system32\msdtc.exe
0x77f40000 0xb0000 0xffff C:\Windows\system32\ntdll.dll
0x77e40000 0xf40000 0xffff C:\Windows\system32\kernel32.dll
0x77160000 0x1240000 0xffff C:\Windows\system32\ole32.dll
0x77ba0000 0x540000 0xffff C:\Windows\system32\msvcrt.dll
0x77e00000 0x440000 0xffff C:\Windows\system32\GDI32.dll
0x77d00000 0x0f0000 0xffff C:\Windows\system32\USER32.dll
0x77da0000 0x90000 0xffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0xa40000 0xffff C:\Windows\system32\RPCRT4.dll
0x61030000 0xf0000 0xffff C:\Windows\system32\WSDOTCTM.dll
0x76ed0000 0x270000 0xffff C:\Windows\system32\DNSAPI.dll
0x71c00000 0x180000 0xffff C:\Windows\system32\WS2_32.dll
0x71bf0000 0x80000 0xffff C:\Windows\system32\WS2HELP.dll
0x76f50000 0x130000 0xffff C:\Windows\system32\Secur32.dll
0x760c0000 0x610000 0xffff C:\Windows\system32\WSVCP60.dll
0x61150000 0x710000 0xffff C:\Windows\system32\WSDOTCPRX.dll
0x770e0000 0x7d0000 0xffff C:\Windows\system32\OLEAUT32.dll
0x71c40000 0x530000 0xffff C:\Windows\system32\NETAPI32.dll
0x74f40000 0x180000 0xffff C:\Windows\system32\WTXCLU.DLL
0x77b90000 0x80000 0xffff C:\Windows\system32\VERSION.dll
0x71bb0000 0x90000 0xffff C:\Windows\system32\WSOCK32.dll
0x611d0000 0x1a0000 0xffff C:\Windows\system32\WSDOTCLOG.dll
0x70100000 0x0000 0xffff C:\Windows\system32\XOLEHLP.dll
0x71b20000 0x430000 0xffff C:\Windows\system32\WSWSOCK.DLL
0x76aa0000 0x2c0000 0xffff C:\Windows\system32\WINMM.dll
0x74de0000 0x110000 0x2 C:\Windows\system32\CLUSAPI.DLL
0x74ef0000 0x120000 0x1 C:\Windows\system32\RESUTILS.DLL
0x75970000 0xb0000 0x1 C:\Windows\system32\USERENV.dll
0x72800000 0xf40000 0x1 C:\Windows\system32\WFC42u.DLL
0x77010000 0xc0000 0x3 C:\Windows\system32\COMRES.DLL
0x74f10000 0x1f0000 0x1 C:\Windows\system32\Wtxoc.dll
0x76f90000 0x7e0000 0x1 C:\Windows\system32\CLBCatQ.DLL
0x76c60000 0x2d0000 0x1 C:\Windows\system32\WIMARTA.DLL
0x76f10000 0x2f0000 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
-----
0x00400000 0x40000 0xffff C:\Windows\system32\msdtc.exe
0x77f40000 0xb0000 0xffff C:\Windows\system32\ntdll.dll
0x77e40000 0xf40000 0xffff C:\Windows\system32\kernel32.dll
0x77160000 0x1240000 0xffff C:\Windows\system32\ole32.dll
0x77ba0000 0x540000 0xffff C:\Windows\system32\msvcrt.dll
0x77e00000 0x440000 0xffff C:\Windows\system32\GDI32.dll
0x77d00000 0x0f0000 0xffff C:\Windows\system32\USER32.dll
0x77da0000 0x90000 0xffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0xa40000 0xffff C:\Windows\system32\RPCRT4.dll
0x61030000 0xf0000 0xffff C:\Windows\system32\WSDOTCTM.dll
0x76ed0000 0x270000 0xffff C:\Windows\system32\DNSAPI.dll
0x71c00000 0x180000 0xffff C:\Windows\system32\WS2_32.dll
0x71bf0000 0x80000 0xffff C:\Windows\system32\WS2HELP.dll
0x76f50000 0x130000 0xffff C:\Windows\system32\Secur32.dll
0x760c0000 0x610000 0xffff C:\Windows\system32\WSVCP60.dll
0x61150000 0x710000 0xffff C:\Windows\system32\WSDOTCPRX.dll
0x770e0000 0x7d0000 0xffff C:\Windows\system32\OLEAUT32.dll
0x71c40000 0x530000 0xffff C:\Windows\system32\NETAPI32.dll
0x74f40000 0x180000 0xffff C:\Windows\system32\WTXCLU.DLL
0x77b90000 0x80000 0xffff C:\Windows\system32\VERSION.dll
0x71bb0000 0x90000 0xffff C:\Windows\system32\WSOCK32.dll
0x611d0000 0x1a0000 0xffff C:\Windows\system32\WSDOTCLOG.dll
0x70100000 0x0000 0xffff C:\Windows\system32\XOLEHLP.dll
0x71b20000 0x430000 0xffff C:\Windows\system32\WSWSOCK.DLL
0x76aa0000 0x2c0000 0xffff C:\Windows\system32\WINMM.dll
0x74de0000 0x110000 0x2 C:\Windows\system32\CLUSAPI.DLL
0x74ef0000 0x120000 0x1 C:\Windows\system32\RESUTILS.DLL
0x75970000 0xb0000 0x1 C:\Windows\system32\USERENV.dll
0x72800000 0xf40000 0x1 C:\Windows\system32\WFC42u.DLL
0x77010000 0xc0000 0x3 C:\Windows\system32\COMRES.DLL
0x74f10000 0x1f0000 0x1 C:\Windows\system32\Wtxoc.dll
0x76f90000 0x7e0000 0x1 C:\Windows\system32\CLBCatQ.DLL
0x76c60000 0x2d0000 0x1 C:\Windows\system32\WIMARTA.DLL
0x76f10000 0x2f0000 0x1 C:\Windows\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\Windows\system32\SAMLIB.dll
*****
```



```
C:\Windows\system32\cmd.exe
0x766f0000 0x10000 0x2 C:\WINDOWS\system32\WTSAPI.dll
0x63e50000 0x11000 0x1 C:\WINDOWS\system32\ismstmp.dll
0x76a80000 0x10000 0x7 C:\WINDOWS\system32\ATL.DLL
0x77160000 0x124000 0x1c C:\WINDOWS\system32\ole32.dll
0x779e0000 0x7d000 0x10 C:\WINDOWS\system32\OLEAUT32.dll
0x766f0000 0x3d000 0x3 C:\WINDOWS\system32\ACTIVEPRO.dll
0x76dc0000 0x2e000 0x5 C:\WINDOWS\system32\adsldpc.dll
0x76b80000 0x2d000 0x4 C:\WINDOWS\system32\credui.dll
0x77380000 0x7dd000 0x5 C:\WINDOWS\system32\SHELL32.dll
0x77290000 0x49000 0xf C:\WINDOWS\system32\SHLWAPI.dll
0x78ad0000 0xe0000 0x6 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x74010000 0x5000 0x1 C:\WINDOWS\system32\ICMP.DLL
0x76cf0000 0x17000 0x3 C:\WINDOWS\system32\iphlpapi.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\olecatq.dll
0x77010000 0xc0000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x3 C:\WINDOWS\system32\VERSION.dll
0x71300000 0x47000 0x1 C:\WINDOWS\system32\inetrvvdsiis.dll
0x72800000 0xf4000 0x2 C:\WINDOWS\system32\WFC42u.DLL
0x647b0000 0x24000 0x2 C:\WINDOWS\system32\IisRTL.DLL
0x64760000 0x37000 0x1 C:\WINDOWS\system32\inetrvvlsui.dll
0x79bc0000 0x90000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x71bd0000 0x11000 0x1 C:\WINDOWS\system32\MPR.dll
0x761b0000 0x09000 0x3 C:\WINDOWS\system32\RCVRPT2.dll
0x76190000 0x12000 0x2 C:\WINDOWS\system32\WSASN1.dll
0x71430000 0x10000 0x1 C:\WINDOWS\system32\ADVAPI32.dll
0x0ff00000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.DLL
0x75da0000 0xb000 0x1 C:\WINDOWS\system32\SXS.DLL
0x5c150000 0x2e000 0x1 C:\WINDOWS\system32\inetrvvsmtpdm.dll
0x5c140000 0xb000 0x1 C:\WINDOWS\system32\SMTPAPI.dll
0x69300000 0x0000 0x2 C:\WINDOWS\system32\extracat.dll
0x5b7e0000 0x0000 0x2 C:\WINDOWS\system32\STAXMEM.dll
0x71bb0000 0x0000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x5c070000 0x35000 0x1 C:\WINDOWS\system32\inetrvvseo.dll
0x5cfd0000 0x0000 0x1 C:\WINDOWS\system32\RAWNH.dll
0x6f350000 0x1f000 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\WSOERT2.dll
0x64430000 0xe000 0x1 C:\WINDOWS\system32\inetres.dll
*****
ntfrs.exe pid: 1452
Command line : C:\WINDOWS\system32\ntfrs.exe
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount Path
-----
0x01000000 0xc3000 0xfffff C:\WINDOWS\system32\ntfrs.exe
0x77f40000 0xb0000 0xfffff *pCQ
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x00000000 0x0 0x0
0x00000000 0x8219a100 0x303c
0x00000000 0x04e4e4e 0x04e4e
*****
svchost.exe pid: 1512
Command line : C:\WINDOWS\system32\svchost.exe -k regsvr

Base      Size      LoadCount Path
-----
0x01000000 0xb0000 0xfffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x00000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77a20000 0x12000 0x1 C:\WINDOWS\system32\regsvr.dll
0x77ba0000 0x54000 0x1 C:\WINDOWS\system32\msvcrt.dll
0x76f50000 0x13000 0x1 C:\WINDOWS\system32\securl.dll
*****
svchost.exe pid: 1736
Command line : C:\WINDOWS\system32\svchost.exe -k termsrvs

Base      Size      LoadCount Path
-----
0x01000000 0xb0000 0xfffff C:\WINDOWS\system32\svchost.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x00000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WIMARTA.DLL
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x76f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\GAMLI0.dll
0x77160000 0x12000 0x0 C:\WINDOWS\system32\ole32.dll
0x75130000 0x4000 0x1 C:\WINDOWS\system32\termsrv.dll
```

```
C:\Windows\system32\cmd.exe

Base      Size      LoadCount Path
-----
0x01000000 0x0000 0xffff C:\WINDOWS\System32\svchost.exe
0x77f40000 0xb000 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
0x776c0000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x77ba0000 0x54000 0xffff C:\WINDOWS\system32\msvcrt.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x77160000 0x124000 0x6 C:\WINDOWS\system32\ole32.dll
0x75130000 0x40000 0x1 C:\Windows\system32\termsrv.dll
0x74d90000 0x0000 0x1 C:\Windows\system32\ICAAPI.dll
0x76f50000 0x13000 0x3 C:\Windows\system32\Secur32.dll
0x71c00000 0x18000 0x1 C:\Windows\system32\WS2_32.dll
0x71bf0000 0x8000 0x1 C:\Windows\system32\WS2HELP.dll
0x770e0000 0x7d000 0x3 C:\WINDOWS\system32\OLEAUT32.dll
0x77640000 0x14000 0x1 C:\Windows\system32\AUTHZ.dll
0x74f60000 0x1d000 0x1 C:\Windows\system32\NtLsaapi.dll
0x76df0000 0x32000 0x1 C:\Windows\system32\ACTIVEOS.dll
0x76dc0000 0x26000 0x1 C:\Windows\system32\adsldpc.dll
0x71c40000 0x53000 0x3 C:\Windows\system32\NETAPI32.dll
0x76b80000 0x2d000 0x1 C:\Windows\system32\credui.dll
0x77380000 0x7d000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x77290000 0x49000 0x3 C:\WINDOWS\system32\SHLWAPI.dll
0x776a0000 0x19000 0x1 C:\Windows\system32\ATL.dll
0x761b0000 0x0000 0x1 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x1 C:\WINDOWS\system32\WSASN1.dll
0x79a00000 0xe0000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x76b20000 0xf000 0x1 C:\WINDOWS\system32\REGAPI.dll
0x0ffd0000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.dll
0x77b90000 0x8000 0x1 C:\WINDOWS\system32\VERSION.dll
0x75970000 0xb000 0xffff C:\WINDOWS\system32\USERENV.dll
*****
explorer.exe pid: 100
command line : C:\WINDOWS\Explorer.EXE
```

```
C:\Windows\system32\cmd.exe

Base      Size      LoadCount Path
-----
0x01000000 0xffff00 0xffff C:\WINDOWS\Explorer.EXE
0x77f40000 0xb000 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 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x776c0000 0x20000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77290000 0x49000 0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x77380000 0x7d000 0xffff C:\WINDOWS\system32\SHELL32.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x75eb0000 0x106000 0xffff C:\WINDOWS\system32\BROWSEUI.dll
0x76920000 0x157000 0xffff C:\WINDOWS\system32\SHDOCVW.dll
0x71b70000 0x33000 0xffff C:\WINDOWS\system32\UXTheme.dll
0x76a00000 0xe0000 0x3f C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x7 C:\WINDOWS\system32\VERSION.dll
0x76540000 0x5000 0x2 C:\WINDOWS\system32\cscui.dll
0x76520000 0x1d000 0x2 C:\WINDOWS\system32\CSCDLL.dll
0x5aff0000 0x6d000 0x1 C:\WINDOWS\system32\Themeui.dll
0x76f50000 0x13000 0x4 C:\WINDOWS\system32\Secur32.dll
0x76200000 0x5000 0x1 C:\WINDOWS\system32\WSIM32.dll
0x75970000 0xb000 0x3 C:\WINDOWS\system32\USERENV.dll
0x760e0000 0x8000 0x1 C:\WINDOWS\system32\LINKINFO.dll
0x768f0000 0x24000 0x4 C:\WINDOWS\system32\ntshrui.dll
0x71c40000 0x53000 0x1a C:\WINDOWS\system32\NETAPI32.dll
0x5ccf0000 0x10000 0x4 C:\WINDOWS\system32\SHELL32.dll
0x765a0000 0x100000 0xd C:\WINDOWS\system32\SETUPAPI.dll
0x76b00000 0x1b1000 0x1 C:\WINDOWS\system32\NETSHELL.dll
0x76b80000 0x2d000 0x4 C:\WINDOWS\system32\credui.dll
0x71c00000 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
0x74ef0000 0x21000 0x2 C:\WINDOWS\system32\stobject.dll
0x748e0000 0xa000 0x2 C:\WINDOWS\system32\BstMeter.dll
```

```
C:\Windows\system32\cmd.exe
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\BatMeter.dll
0x748c0000 0x7000 0x4 C:\WINDOWS\system32\POWRPROF.dll
0x76f00000 0x8000 0x2 C:\WINDOWS\system32\WTSAPI32.dll
0x74970000 0x80000 0x2 C:\WINDOWS\system32\printui.dll
0x73070000 0x20000 0x3 C:\WINDOWS\system32\WINSPOOL.DRV
0x76df0000 0x32000 0x3 C:\WINDOWS\system32\ACTIVE05.dll
0x76dc0000 0x20000 0x5 C:\WINDOWS\system32\adsldpc.dll
0x76f10000 0x2f000 0x4 C:\WINDOWS\system32\WLDAP32.dll
0x76a00000 0x18000 0x3 C:\WINDOWS\system32\ATL.dll
0x748d0000 0x8000 0x2 C:\WINDOWS\system32\CFGM32.dll
0x71bd0000 0x11000 0x5 C:\WINDOWS\system32\WPR.dll
0x76aa0000 0x2c000 0x4 C:\WINDOWS\system32\WINMM.dll
0x75e90000 0x7000 0x1 C:\WINDOWS\system32\drprov.dll
0x5f120000 0xe000 0x1 C:\WINDOWS\system32\ntlanman.dll
0x5f6a0000 0x10000 0x2 C:\WINDOWS\system32\NETUI08.dll
0x5f6e0000 0x31000 0x1 C:\WINDOWS\system32\NETUI1.dll
0x75ea0000 0x9000 0x1 C:\WINDOWS\system32\davclnt.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL
0x760f0000 0x90000 0x1 C:\WINDOWS\system32\WININET.dll
0x761b0000 0x90000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x3 C:\WINDOWS\system32\WSASN1.dll
0x76050000 0x95000 0x1 C:\WINDOWS\system32\shdoclc.dll
0x75fc0000 0x80000 0x2 C:\WINDOWS\system32\urImon.dll
0x76e90000 0x30000 0x2 C:\WINDOWS\system32\RASAPI32.dll
0x76e40000 0x11000 0x2 C:\WINDOWS\system32\Nasman.dll
0x76e60000 0x20000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76e30000 0xb000 0x4 C:\WINDOWS\system32\ntutils.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\system32\WZC3API.DLL
0x76cd0000 0x17000 0x1 C:\WINDOWS\system32\WPRAPI.dll
0x71b20000 0x43000 0x1 C:\WINDOWS\system32\WSWSOCK.dll
0x72490000 0x12000 0x1 C:\WINDOWS\system32\browserc.dll
0x72470000 0x1000 0x2 C:\WINDOWS\system32\Wydcs.dll
0x71530000 0x1f000 0x1 C:\WINDOWS\system32\aclui.dll
0x76c00000 0x20000 0x1 C:\WINDOWS\system32\WIMMART.A.DLL
*****
dns.exe pid: 340
Command line : C:\WINDOWS\System32\dns.exe
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount  Path
-----
0x01000000 0x8d000 0xfffff C:\WINDOWS\System32\dns.exe
0x77f40000 0xb000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x44000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x71c00000 0x21000 0xfffff C:\WINDOWS\system32\Wsock32.dll
0x71bf0000 0x9000 0xfffff C:\WINDOWS\system32\WS2HELP.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x71c40000 0x53000 0xfffff C:\WINDOWS\System32\NETAPI32.dll
0x76f10000 0x2f000 0xfffff C:\WINDOWS\system32\WLDAP32.dll
0x76ed0000 0x27000 0xfffff C:\WINDOWS\system32\DNSAPI.dll
0x766f0000 0x10000 0xfffff C:\WINDOWS\System32\NTDSAPI.dll
0x76f50000 0x13000 0xfffff C:\WINDOWS\system32\Secur32.dll
0x77200000 0x40000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x76cf0000 0x17000 0xfffff C:\WINDOWS\system32\iphlpapi.dll
0x76cd0000 0x17000 0xfffff C:\WINDOWS\system32\WPRAPI.dll
0x76df0000 0x32000 0xfffff C:\WINDOWS\System32\ACTIVE05.dll
0x76dc0000 0x20000 0xfffff C:\WINDOWS\System32\adsldpc.dll
0x76b80000 0x2d000 0xfffff C:\WINDOWS\System32\credui.dll
0x77380000 0x7d000 0xfffff C:\WINDOWS\system32\SHELL32.dll
0x76a00000 0x18000 0xfffff C:\WINDOWS\System32\ATL.dll
0x77160000 0x124000 0xfffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb000 0xfffff C:\WINDOWS\System32\ntutils.dll
0x5ccf0000 0x10000 0xfffff C:\WINDOWS\System32\SAHMLIB.dll
0x765a0000 0x100000 0xfffff C:\WINDOWS\System32\SETUPAPI.dll
0x70ad0000 0xe000 0x3 C:\WINDOWS\WinSxS\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\Nasman.dll
0x76e60000 0x20000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76a00000 0x2c000 0x2 C:\WINDOWS\system32\WINMM.dll
0x761b0000 0x90000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x3 C:\WINDOWS\system32\WSASN1.dll
0x76d30000 0x47000 0x1 C:\WINDOWS\System32\WZC3Svc.DLL
0x76cc0000 0x5000 0x1 C:\WINDOWS\system32\WMI.dll
0x76d10000 0x1c000 0x1 C:\WINDOWS\System32\DHCP32Svc.DLL
0x76f00000 0xb000 0x1 C:\WINDOWS\System32\WTSAPI32.dll
0x76c00000 0x10000 0x2 C:\WINDOWS\system32\WINSTA.dll
0x69750000 0x10000 0x1 C:\WINDOWS\System32\ESSENT.dll
```



```
C:\Windows\system32\cmd.exe
0x76e40000 0x11000 0x2 C:\WINDOWS\system32\krasman.dll
0x76e60000 0x2e000 0x2 C:\WINDOWS\system32\TAPI32.dll
0x76aa0000 0x2c000 0x2 C:\WINDOWS\system32\WINMM.dll
0x761b0000 0x90000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x3 C:\WINDOWS\system32\MSASNI.dll
0x76d30000 0x71000 0x1 C:\WINDOWS\system32\WZCSVC.DLL
0x76cc0000 0x50000 0x1 C:\WINDOWS\system32\WMI.dll
0x76d10000 0x1c000 0x1 C:\WINDOWS\system32\DHCPSPVC.DLL
0x76f00000 0x80000 0x1 C:\WINDOWS\system32\WTSAPI32.dll
0x76260000 0x10000 0x2 C:\WINDOWS\system32\WINSTA.dll
0x69750000 0x100000 0x1 C:\WINDOWS\system32\VESENT.dll
0x730a0000 0x90000 0x1 C:\WINDOWS\system32\WZCSAPI.DLL
0x71b20000 0x43000 0x3 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x80000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x71ca0000 0x50000 0x1 C:\WINDOWS\system32\kerberos.dll
0x766e0000 0xc000 0x1 C:\WINDOWS\system32\crypt.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x74010000 0x5000 0x1 C:\WINDOWS\system32\ICMP.DLL
0x71f00000 0x4000 0x1 C:\WINDOWS\system32\security.dll
*****
wins.exe pid: 756
Command line : C:\WINDOWS\system32\wins.exe

Base      Size      LoadCount Path
-----
0x01000000 0x27000 0xffff C:\WINDOWS\system32\wins.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 0x4a000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x771c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x771c00000 0x18000 0xffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x80000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x5b090000 0x87000 0xffff C:\WINDOWS\system32\VSAPI.DLL
0x76a00000 0x10000 0xffff C:\WINDOWS\system32\ATL.DLL
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x71b20000 0x43000 0x5 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x80000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x76f70000 0x71000 0x1 C:\WINDOWS\system32\Winmm.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x76f00000 0x50000 0x1 C:\WINDOWS\system32\krasman.dll
0x69750000 0x100000 0x1 C:\WINDOWS\system32\vevent.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc0000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x2 C:\WINDOWS\system32\VERSION.dll
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\res.dll
0x76f50000 0x13000 0x3 C:\WINDOWS\system32\Secur32.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
*****
wins.exe pid: 756
Command line : C:\WINDOWS\system32\wins.exe
```

```
C:\Windows\system32\cmd.exe
0x71bf0000 0x80000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x5b090000 0x87000 0xffff C:\WINDOWS\system32\VSAPI.DLL
0x76a00000 0x10000 0xffff C:\WINDOWS\system32\ATL.DLL
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x71b20000 0x43000 0x5 C:\WINDOWS\system32\mswsock.dll
0x71ae0000 0x80000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x76f70000 0x71000 0x1 C:\WINDOWS\system32\Winmm.dll
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll
0x76f00000 0x50000 0x1 C:\WINDOWS\system32\krasman.dll
0x69750000 0x100000 0x1 C:\WINDOWS\system32\vevent.dll
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAMLIB.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc0000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x2 C:\WINDOWS\system32\VERSION.dll
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\res.dll
0x76f50000 0x13000 0x3 C:\WINDOWS\system32\Secur32.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
-----
0x01000000 0x26000 0xffff C:\WINDOWS\system32\wuauclt.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
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77300000 0x7dd000 0xffff C:\WINDOWS\system32\SHELL32.dll
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0x4a000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77290000 0x49000 0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x75fc0000 0x89000 0xffff C:\WINDOWS\system32\urlmon.dll
0x77b90000 0x80000 0xffff C:\WINDOWS\system32\VERSION.dll
0x76ad0000 0x3e000 0xffff C:\WINDOWS\system32\Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.1808_x-ww_8417450B\COMCTL32.dll
0x76f00000 0x50000 0xffff C:\WINDOWS\system32\WTSAPI32.dll
0x76d30000 0x71000 0xffff C:\WINDOWS\system32\WZCSVC.dll
0x771c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
*****
wuauclt.exe pid: 1092
Command line : "C:\WINDOWS\system32\wuauclt.exe"
```



```
C:\Windows\system32\cmd.exe
0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77290000 0x49000 0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x75fc0000 0x89000 0xffff C:\WINDOWS\system32\urlmon.dll
0x77b90000 0x93000 0xffff C:\WINDOWS\system32\VERSION.dll
0x76da0000 0xe8000 0xffff C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450b\COMCTL32.dll
0x76f00000 0x80000 0xffff C:\WINDOWS\system32\WTSAPI32.dll
0x76260000 0x18000 0xffff C:\WINDOWS\system32\WINSTA.dll
0x71c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x750c0000 0x28000 0xffff C:\WINDOWS\system32\ADVPACK.dll
0x74c40000 0x68000 0x1 C:\WINDOWS\system32\RICHED20.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x75da0000 0xb9000 0x1 C:\WINDOWS\system32\SXS.DLL
*****
dllhost.exe pid: 3292
Command line : C:\WINDOWS\system32\dllhost.exe /ProcessId:{0204B3F1-FD88-11D1-9600-008005FC79235}

Base      Size  LoadCount Path
-----
0x01000000 0x4000 0xffff C:\WINDOWS\system32\dllhost.exe
0x77f40000 0xb9000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\system32\msvcrt.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x77c00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\USER32.dll
0x77da0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x76f90000 0x7e000 0x0 C:\WINDOWS\system32\CLBCatQ.DLL
0x770e0000 0x7d000 0x1e C:\WINDOWS\system32\OLEAUT32.dll
0x77010000 0xc6000 0x0 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x93000 0x13 C:\WINDOWS\system32\VERSION.dll
0x755d0000 0x12c000 0x6 C:\WINDOWS\system32\COMSVCS.DLL
0x74f10000 0x1f000 0x1 C:\WINDOWS\system32\mtxoc1.dll
0x0ffdb000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb9000 0x1 C:\WINDOWS\system32\PSAPI.DLL
0x59c60000 0x1d000 0x1 C:\WINDOWS\system32\txflog.dll
0x76ad0000 0x3e000 0x2 C:\WINDOWS\system32\IES.DLL
0x75da0000 0xb9000 0x1 C:\WINDOWS\system32\SXS.DLL
0x57b10000 0x60000 0x1 C:\WINDOWS\system32\XOLEHLP.dll
0x61150000 0x71000 0x2 C:\WINDOWS\system32\WSDOTCPRX.dll

Windows taskbar and system tray area showing search bar, taskbar icons, and system clock (17:45, 7/10/2024).
```

```
C:\Windows\system32\cmd.exe
0x77010000 0xc6000 0x0 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x93000 0x13 C:\WINDOWS\system32\VERSION.dll
0x755d0000 0x12c000 0x6 C:\WINDOWS\system32\COMSVCS.DLL
0x74f10000 0x1f000 0x1 C:\WINDOWS\system32\mtxoc1.dll
0x0ffdb000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb9000 0x1 C:\WINDOWS\system32\PSAPI.DLL
0x59c60000 0x1d000 0x1 C:\WINDOWS\system32\txflog.dll
0x76ad0000 0x3e000 0x2 C:\WINDOWS\system32\IES.DLL
0x75da0000 0xb9000 0x1 C:\WINDOWS\system32\SXS.DLL
0x57b10000 0x60000 0x1 C:\WINDOWS\system32\XOLEHLP.dll
0x61150000 0x71000 0x2 C:\WINDOWS\system32\WSDOTCPRX.dll
0x71c40000 0x53000 0x2 C:\WINDOWS\system32\NETAPI32.dll
0x780c0000 0x61000 0x2 C:\WINDOWS\system32\WSVCP60.dll
0x74f40000 0x18000 0x2 C:\WINDOWS\system32\MTXCLU.DLL
0x71bb0000 0x99000 0x4 C:\WINDOWS\system32\WSOCK32.dll
0x71c00000 0x18000 0xc C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x80000 0x9 C:\WINDOWS\system32\WS2HELP.dll
0x74de0000 0x11000 0x2 C:\WINDOWS\system32\CLUSAPI.DLL
0x74ef0000 0x12000 0x1 C:\WINDOWS\system32\RESUTILS.DLL
0x75070000 0xb9000 0x1 C:\WINDOWS\system32\USERENV.dll
0x72800000 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\DNSAPI.dll
0x76f70000 0x70000 0x1 C:\WINDOWS\system32\WinInet.dll
0x76f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x76f00000 0x50000 0x1 C:\WINDOWS\system32\rsasdhlp.dll
0x6f600000 0x47000 0x1 C:\WINDOWS\system32\catsrv.dll
0x6f670000 0xa0000 0x1 C:\WINDOWS\system32\catsrvps.dll
0x6ed00000 0x1b000 0x2 C:\WINDOWS\system32\lbcatex.dll
0x6f5d0000 0x95000 0x2 C:\WINDOWS\system32\catsrvut.dll
0x61e50000 0x90000 0x2 C:\WINDOWS\system32\WfcSubs.dll
0x76c60000 0x28000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x5ccf0000 0x10000 0x1 C:\WINDOWS\system32\SAHLIB.dll
*****
appmgr.exe pid: 2902
Command line : C:\WINDOWS\system32\serverappliance\appmgr.exe

Base      Size  LoadCount Path
-----
0x01000000 0x22000 0xffff C:\WINDOWS\system32\serverappliance\appmgr.exe
0x77f40000 0xb9000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll

Windows taskbar and system tray area showing search bar, taskbar icons, and system clock (17:46, 7/10/2024).
```

```
C:\Windows\system32\cmd.exe
0x1000000 0x13000 0xffff C:\Windows\system32\serverappliance\srvcsvcs.exe
0x77f40000 0xb4000 0xffff C:\Windows\system32\ntdll.dll
0x77e40000 0xb4000 0xffff C:\Windows\system32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\Windows\system32\msvcrt.dll
0x780c0000 0x61000 0xffff C:\Windows\system32\WSVCP60.dll
0x77da0000 0x90000 0xffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0x4a000 0xffff C:\Windows\system32\RPCRT4.dll
0x77d00000 0x8f000 0xffff C:\Windows\system32\USER32.dll
0x77c00000 0x44000 0xffff C:\Windows\system32\GDI32.dll
0x77160000 0x124000 0xffff C:\Windows\system32\ole32.dll
0x770e0000 0x7d000 0xffff C:\Windows\system32\OLEAUT32.dll
0x76b70000 0xb0000 0xffff C:\Windows\system32\PSAPI.DLL
0x76f90000 0x7e000 0x1 C:\Windows\system32\ClbCatQ.DLL
0x77610000 0xc0000 0x1 C:\Windows\system32\COMRes.dll
0x77090000 0xb0000 0x1 C:\Windows\system32\VERSION.dll
0x75da0000 0xb4000 0x1 C:\Windows\system32\SXS.dll
0x76e30000 0xb0000 0x3 C:\Windows\system32\rtutils.dll
0x00610000 0xf000 0x1 C:\Windows\system32\serverappliance\initrvc.dll
0x00620000 0xf000 0x1 C:\Windows\system32\serverappliance\taskctx.dll
0x00630000 0x15000 0x1 C:\Windows\system32\serverappliance\appsrvcs.dll
0x74cf0000 0x80000 0x1 C:\Windows\system32\wbem\wbemprox.dll
0x756f0000 0x38000 0x2 C:\Windows\system32\wbem\wbemcomn.dll
0x71c00000 0x19000 0x3 C:\Windows\system32\W52_32.dll
0x71bf0000 0x80000 0x2 C:\Windows\system32\W52HELP.dll
0x74ce0000 0xe0000 0x1 C:\Windows\system32\wbem\wbemsvcs.dll
0x75550000 0x71000 0x1 C:\Windows\system32\wbem\fastprox.dll
0x766f0000 0x16000 0x1 C:\Windows\system32\NTDSAPI.dll
0x76ed0000 0x27000 0x1 C:\Windows\system32\DNSAPI.dll
0x76f10000 0x2f000 0x1 C:\Windows\system32\WLDAP32.dll
0x71c40000 0x53000 0x1 C:\Windows\system32\NETAPI32.dll
0x76f50000 0xa4000 0x1 C:\Windows\system32\Secur32.dll
*****
inetinfo.exe pid: 300
Command line : C:\Windows\system32\inetrv\inetinfo.exe

Base      Size  LoadCount Path
-----
0x01000000 0x0000 0xffff C:\Windows\system32\inetrv\inetinfo.exe
0x77f40000 0xb4000 0xffff C:\Windows\system32\ntdll.dll
0x77e40000 0xb4000 0xffff C:\Windows\system32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\Windows\system32\msvcrt.dll
0x77da0000 0x90000 0xffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0x4a000 0xffff C:\Windows\system32\RPCRT4.dll
```

```
C:\Windows\system32\cmd.exe
0x766f0000 0x16000 0x2 C:\Windows\system32\NTDSAPI.dll
0x015e0000 0x17000 0x1 C:\Windows\system32\odbcint.dll
0x76750000 0x28000 0x2 C:\Windows\system32\schannel.dll
0x75970000 0xb4000 0x2 C:\Windows\system32\USERENV.dll
0x62da0000 0x7000 0x1 C:\Windows\system32\inetrv\lonsint.dll
0x71b20000 0x43000 0x6 C:\Windows\system32\mswsock.dll
0x71ae0000 0x80000 0x1 C:\Windows\system32\wshtcpip.dll
0x76bb0000 0x2b000 0x1 C:\Windows\system32\wintrust.dll
0x76c10000 0x20000 0x1 C:\Windows\system32\imagehlp.dll
0x63eb0000 0x70000 0x1 C:\Windows\system32\inetrv\iscomlog.dll
0x76cf0000 0x17000 0x5 C:\Windows\system32\iphlpapi.dll
0x5c870000 0x35000 0x1 C:\Windows\system32\inetrv\vsoc.dll
0x76d80000 0x37000 0x1 C:\Windows\system32\netman.dll
0x76cd0000 0x17000 0x1 C:\Windows\system32\WPRAPI.dll
0x76df0000 0x32000 0x1 C:\Windows\system32\ACTIVEEO.dll
0x76dc0000 0x26000 0x1 C:\Windows\system32\adsldpc.dll
0x76db0000 0x2d000 0x1 C:\Windows\system32\credui.dll
0x76e30000 0xb0000 0x0 C:\Windows\system32\rtutils.dll
0x765a0000 0x100000 0x1 C:\Windows\system32\SETUPAPI.dll
0x76e90000 0x3b000 0x2 C:\Windows\system32\NTDSAPI32.dll
0x76e40000 0x11000 0x2 C:\Windows\system32\irasman.dll
0x76e60000 0x2e000 0x2 C:\Windows\system32\TAPI32.dll
0x76aa0000 0x2c000 0x2 C:\Windows\system32\WINMM.dll
0x76d30000 0x47000 0x1 C:\Windows\system32\WZCsvc.dll
0x76cc0000 0x5000 0x1 C:\Windows\system32\WMI.dll
0x76d10000 0x1c000 0x1 C:\Windows\system32\DHCPsvc.dll
0x76f00000 0x80000 0x1 C:\Windows\system32\WTSAPI32.dll
0x76260000 0x18000 0x2 C:\Windows\system32\WINSTA.dll
0x69750000 0x100000 0x1 C:\Windows\system32\IESENT.dll
0x730a0000 0x9000 0x1 C:\Windows\system32\WZCAPI.DLL
0x02180000 0x79000 0x1 C:\Windows\system32\inetrv\vaqueue.dll
0x76f80000 0x5000 0x1 C:\Windows\system32\irasadhlp.dll
0x71ca0000 0x50000 0x1 C:\Windows\system32\kerberos.dll
0x76de0000 0x0000 0x1 C:\Windows\system32\cryptui.dll
0x02460000 0x0000 0x1 C:\Windows\system32\inetrv\ntfsdrv.dll
0x5e6c0000 0xb000 0x1 C:\Windows\system32\POP3Server\VP3Store.dll
0x76f70000 0x7000 0x1 C:\Windows\system32\winrnr.dll
*****
wmiprvse.exe pid: 2116
Command line : C:\Windows\system32\wbem\wmiprvse.exe

Base      Size  LoadCount Path
-----
0x01000000 0x0000 0xffff C:\Windows\system32\wmiprvse.exe
0x77f40000 0xb4000 0xffff C:\Windows\system32\ntdll.dll
0x77e40000 0xb4000 0xffff C:\Windows\system32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\Windows\system32\msvcrt.dll
0x77da0000 0x90000 0xffff C:\Windows\system32\ADVAPI32.dll
0x77c50000 0x4a000 0xffff C:\Windows\system32\RPCRT4.dll
```

```
C:\Windows\system32\cmd.exe

Base      Size      LoadCount Path
-----
0x01000000 0x35000 0xffff C:\WINDOWS\system32\wbem\wmiprvse.exe
0x77f40000 0xb8000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x54000 0xffff C:\WINDOWS\system32\user32.dll
0x77c00000 0x8f000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77e00000 0x44000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x750f0000 0x38000 0xffff C:\WINDOWS\system32\wbem\wbemcomn.dll
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x77550000 0x71000 0xffff C:\WINDOWS\system32\wbem\FastProx.dll
0x780c0000 0x61000 0xffff C:\WINDOWS\system32\WSVCP60.dll
0x766f0000 0x16000 0xffff C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0xffff C:\WINDOWS\system32\DNSAPI.dll
0x71c00000 0x18000 0xffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x76f10000 0x2f000 0xffff C:\WINDOWS\system32\WLDAP32.dll
0x71c40000 0x53000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x76f50000 0x13000 0xffff C:\WINDOWS\system32\Secur32.dll
0x5fb10000 0x4000 0xffff C:\WINDOWS\system32\NCOBJAPI.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
0x74ce0000 0xe000 0x1 C:\WINDOWS\system32\wbem\wbemsvr.dll
0x74e60000 0x1b000 0x1 C:\WINDOWS\system32\wbem\wbemutils.dll
0x72fa0000 0x26000 0x1 C:\WINDOWS\system32\wbem\wmiprov.dll
0x76cc0000 0x5000 0x1 C:\WINDOWS\system32\WMI.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\NTKARTA.DLL
0x5cf00000 0x18000 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 0x2f000 0x1 C:\WINDOWS\system32\wbem\PROVTHRD.dll
0x60020000 0x18000 0x1 C:\WINDOWS\system32\msvcrt.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x76e30000 0x15000 0x1 C:\WINDOWS\system32\ServerAppliance\saevfltr.dll
0x76e30000 0x9000 0x1 C:\WINDOWS\system32\ntutils.dll
0x80c00000 0x15000 0x1 C:\WINDOWS\system32\ServerAppliance\appsrvcs.dll
0x71b20000 0x43000 0x4 C:\WINDOWS\system32\mswsock.dll
0x76f00000 0x5000 0x1 C:\WINDOWS\system32\rsasdhlp.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
```

```
C:\Windows\system32\cmd.exe
*****
POP3Svc.exe pid: 2260
Command line : c:\Windows\system32\pop3server\pop3svc.exe

Base      Size      LoadCount Path
-----
0x01000000 0xb8000 0xffff C:\WINDOWS\system32\pop3server\pop3svc.exe
0x77f40000 0xb8000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x54000 0xffff C:\WINDOWS\system32\user32.dll
0x77c00000 0x8f000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77d00000 0x8f000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77e00000 0x44000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f00000 0x44000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x77550000 0x71000 0xffff C:\WINDOWS\system32\wbem\FastProx.dll
0x780c0000 0x61000 0xffff C:\WINDOWS\system32\WSVCP60.dll
0x766f0000 0x16000 0xffff C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0xffff C:\WINDOWS\system32\DNSAPI.dll
0x71c00000 0x18000 0xffff C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0xffff C:\WINDOWS\system32\WS2HELP.dll
0x71b20000 0x43000 0xffff C:\WINDOWS\system32\WSOCK32.dll
0x76f50000 0x13000 0xffff C:\WINDOWS\system32\Secur32.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
0x5e0e0000 0xf1000 0x1 C:\WINDOWS\system32\pop3server\Pop3Auth.dll
0x76df0000 0x32000 0x3 C:\WINDOWS\system32\ACTIVEDES.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\NTDSAPI.dll
0x76e00000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
0x79ad0000 0xe000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.180.0_x-ww_8A17450B\comctl32.dll
0x76e90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x5e6d0000 0x19000 0x1 C:\WINDOWS\system32\pop3server\Pop3Admin.dll
0x780c0000 0x61000 0x1 C:\WINDOWS\system32\WSVCP60.dll
0x71300000 0x47000 0x1 C:\WINDOWS\system32\inetstrv\ads11s.dll
0x72880000 0xf4000 0x2 C:\WINDOWS\system32\WFC42u.DLL
0x64760000 0x24000 0x2 C:\WINDOWS\system32\IisRTL.dll
0x64760000 0x7000 0x1 C:\WINDOWS\system32\inetstrv\isui.dll
0x70bc0000 0x9000 0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.02.0.0_x-ww_8A69BA85\COMCTL32.dll
```

```
C:\Windows\system32\cmd.exe
0x5c150000 0x2e000 0x1 C:\WINDOWS\system32\inetresv\smtpadm.dll
0x5c140000 0x60000 0x1 C:\WINDOWS\system32\SMTPAPI.dll
0x69530000 0xc0000 0x1 C:\WINDOWS\system32\vxstrace.dll
0x5b7e0000 0x60000 0x1 C:\WINDOWS\system32\STAXMEM.dll
0x71bb0000 0x90000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x71ae0000 0x80000 0x1 C:\WINDOWS\system32\wshtcpip.dll
*****
cmd.exe pid: 2076
Command line : "C:\WINDOWS\system32\cmd.exe"

Base      Size      LoadCount Path
-----
0x44d00000 0x60000 0xfffff C:\WINDOWS\system32\cmd.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.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
0x71bd0000 0x11000 0xfffff C:\WINDOWS\system32\WPR.dll
*****
mdd.exe pid: 3460
Command line : mdd.exe -o dc-memdump.bin

Base      Size      LoadCount Path
-----
0x00400000 0x19000 0xfffff C:\ITShare\mdd.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
0x77380000 0x7d000 0xfffff C:\WINDOWS\system32\SHELL32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\GDI32.dll
0x77d00000 0x8f000 0xfffff C:\WINDOWS\system32\USER32.dll
0x77c00000 0x44000 0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x70a00000 0xe0000 0x1 C:\WINDOWS\system32\Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x0ff00000 0x2d000 0x1 C:\WINDOWS\system32\Vsaaenh.dll
0x76700000 0xb0000 0x1 C:\WINDOWS\system32\PSAPI.DLL

C:\Users\Usuario\Documents\UNIVERSIDAD_IS\SIS-522\PRACTICAS\practica3\practica3>
```

```
C:\Windows\system32\cmd.exe
Base      Size      LoadCount Path
-----
0x00000000 0x20000 0xfffff C:\WINDOWS\system32\serverappliance\apmgr.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x780c0000 0x61000 0xfffff C:\WINDOWS\system32\WSVCP60.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
0x77160000 0x12000 0xfffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xfffff C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb0000 0x1 C:\WINDOWS\system32\ntutils.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc0000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x80000 0x1 C:\WINDOWS\system32\VERSION.dll
0x75da0000 0xb0000 0x1 C:\WINDOWS\system32\SXS.DLL
0x74ce0000 0xe0000 0x1 C:\WINDOWS\system32\wbem\wbemsvcs.dll
0x75500000 0x71000 0x2 C:\WINDOWS\system32\wbem\fastprox.dll
0x750f0000 0x30000 0x3 C:\WINDOWS\system32\wbem\wbemcomn.dll
0x766f0000 0x10000 0x2 C:\WINDOWS\system32\WTDOSAPI.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\WDSAPI.dll
0x71c00000 0x10000 0x4 C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x80000 0x2 C:\WINDOWS\system32\WS2HELP.dll
0x76f10000 0x2f000 0x2 C:\WINDOWS\system32\WLDAP32.dll
0x71c40000 0x53000 0x2 C:\WINDOWS\system32\NETAPI32.dll
0x76f50000 0x13000 0x2 C:\WINDOWS\system32\Secur32.dll
0x00020000 0xf0000 0x1 C:\WINDOWS\system32\serverappliance\taskctx.dll
0x75100000 0x30000 0x1 C:\WINDOWS\system32\wbem\esscli.dll
*****
srvcung.exe pid: 1496
Command line : C:\WINDOWS\system32\serverappliance\srvcung.exe

Base      Size      LoadCount Path
-----
0x01000000 0x13000 0xfffff C:\WINDOWS\system32\serverappliance\srvcung.exe
0x77f40000 0xb0000 0xfffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xfffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xfffff C:\WINDOWS\system32\msvcrt.dll
0x770c0000 0x61000 0xfffff C:\WINDOWS\system32\WSVCP60.dll
0x77da0000 0x90000 0xfffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa4000 0xfffff C:\WINDOWS\system32\RPCRT4.dll
```

## Preguntas de verificación del laboratorio

¿Qué hora inicia el proceso explorer.exe?

2012-11-03 21:32:38 UTC+0000

¿Qué hora inicia el proceso svchost.exe?

2012-11-03 20:18:33 UTC+0000

¿Cuál es el nombre del proceso PID: 420?

0x82031020 csrss.exe

¿Cuál es el nombre del proceso PID: 932?

### PARTE PRÁCTICA (50 pts)

- 1) Determina cuántos bits en total puede almacenar una memoria RAM de 128k x 4 (5 pts)

$$128 * 2^{10} * 4 = 524288 \text{ bits.}$$

- 2) ¿Cuántos bits puede almacenar una memoria de 10g x 16? (5 pts)

$$10 * 2^{30} * 16 = 171798691840 \text{ bits.}$$

- 3) ¿Cuántas localidades de memoria se puede direccionar con 32 líneas de dirección? (5 pts)

$$2^{32} = 4294967296 \text{ localidades.}$$

- 4) ¿Cuántas localidades de memoria se pueden direccionar con 1024 líneas de dirección? (5 pts)

$$2^{1024} = 1,7976931349 \times 10^{308} \text{ localidades.}$$

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

$$2^{64} = 1,8446744074 \times 10^{19} \text{ localidades.}$$

- 6) ¿Cuántas líneas de dirección se necesitan para una memoria ROM de 512m x 8? (5 pts)

$$n = (\ln (512 * 2^{20})) / (\ln (2)) = 29 \text{ líneas.}$$

- 7) ¿Cuántas líneas de dirección se necesitan para una memoria ROM de 128m x 128? (5 pts)

$$n = (\ln (128 * 2^{20})) / (\ln (2)) = 27 \text{ líneas.}$$

- 8) ¿Cuántos bits en total puede almacenar una memoria RAM 128m x 4?, de él resultado gigabytes (5 pts)

$$128 * 2^{20} * 4 = 536870912 / (8 * 2^{30}) = 0,0625 \text{ gigabytes.}$$

- 9) ¿Cuántos bits en total puede almacenar una memoria RAM 64m x 64?, de él resultado en teras (5 pts)

$$64 * 2^{20} * 64 = 4294967296 / (8 * 2^{40}) = 0,00048828125 \text{ terabytes.}$$

- 10) ¿Cuántos bits en total puede almacenar una memoria RAM 64m x 64?, de él resultado en terabytes (5 pts)

$$64 * 2^{20} * 64 = 4294967296 / (8 * 2^{40}) = 0,00048828125 \text{ terabytes.}$$