


PRÁCTICA N°3			
	<b>Materia:</b> Arquitectura de computadoras (SIS-522) – G1	<b>Estudiante:</b> Luis Adrian Rodriguez Flores	
	<b>Docente:</b> Ing. Gustavo A. Puita Choque	<b>CI:</b> 10477393	<b>RU:</b> 110115
	<b>Auxiliar:</b> Univ. Aldrin Roger Pérez Miranda	<b>Fecha de entrega:</b> 07/10/2024	

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

La RAM es una memoria volátil y de acceso aleatorio, mientras que la ROM es no volátil y de acceso secuencial.

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

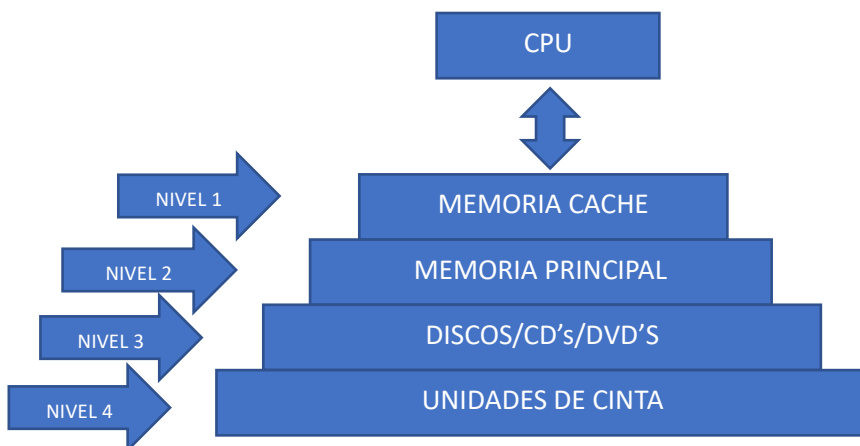
La SRAM: Es de alta velocidad de acceso, menor densidad y capacidad, mayor costo por bit.

La DRAM: Es de baja velocidad de acceso, mayor densidad y capacidad, menor costo por bit.

**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?**

La VRAM tiene una característica única: puede leer y escribir al mismo tiempo en diferentes ubicaciones de memoria. Esto permite que la información se refresque constantemente en el monitor mientras el sistema actualiza lo que se muestra en la pantalla. Es esencial para una experiencia visual fluida.

**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.**

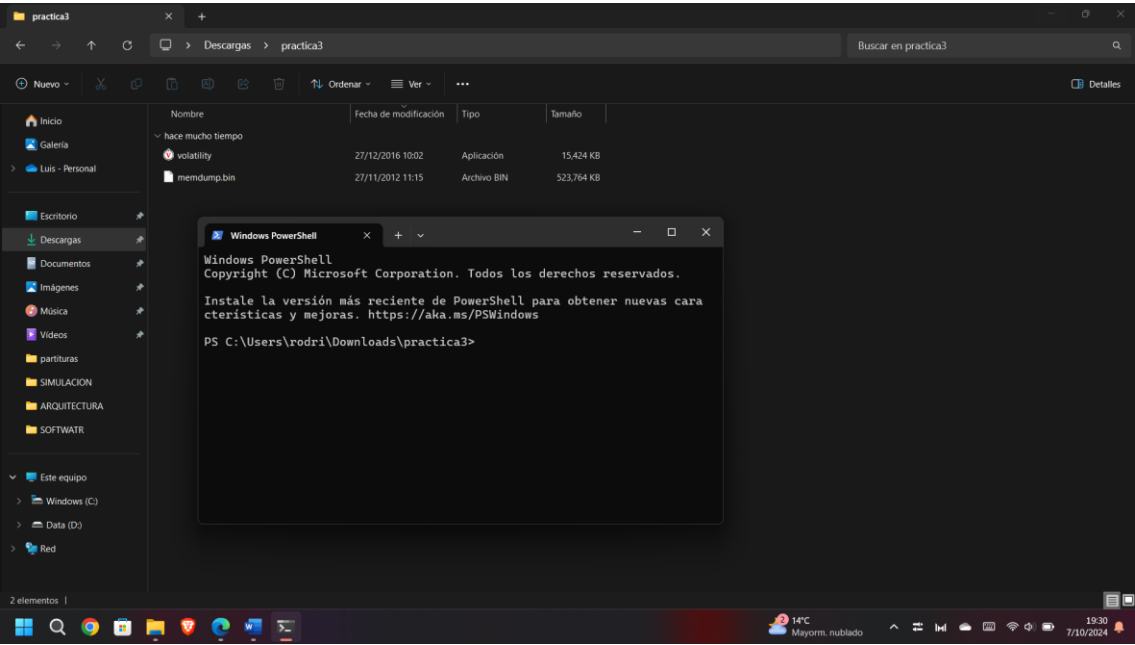


5. ¿Qué diferencias existen entre la memoria caché L1, L2 y L3 en términos de tamaño, velocidad y proximidad al procesador?

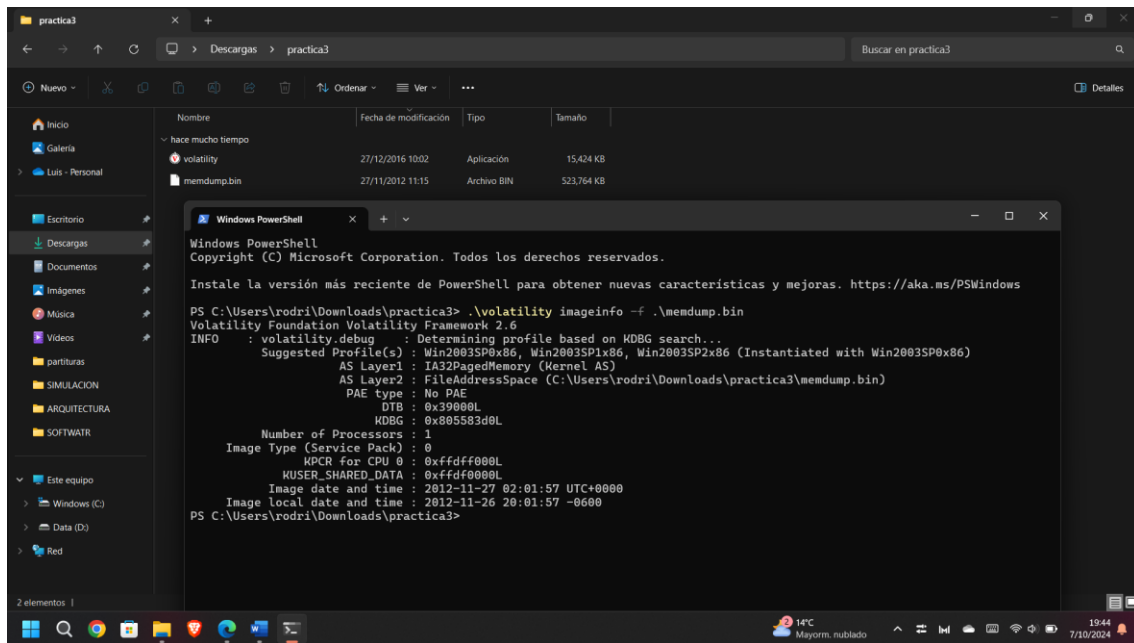
Característica	Memoria Caché L1	Memoria Caché L2	Memoria Caché L3
Tamaño	Pequeño	Mediano	Grande
Velocidad	Más rápida	Más lenta	Más lenta
Proximidad a laCPU	Más cercana	Cercana	Cercana

LABORATORIO:

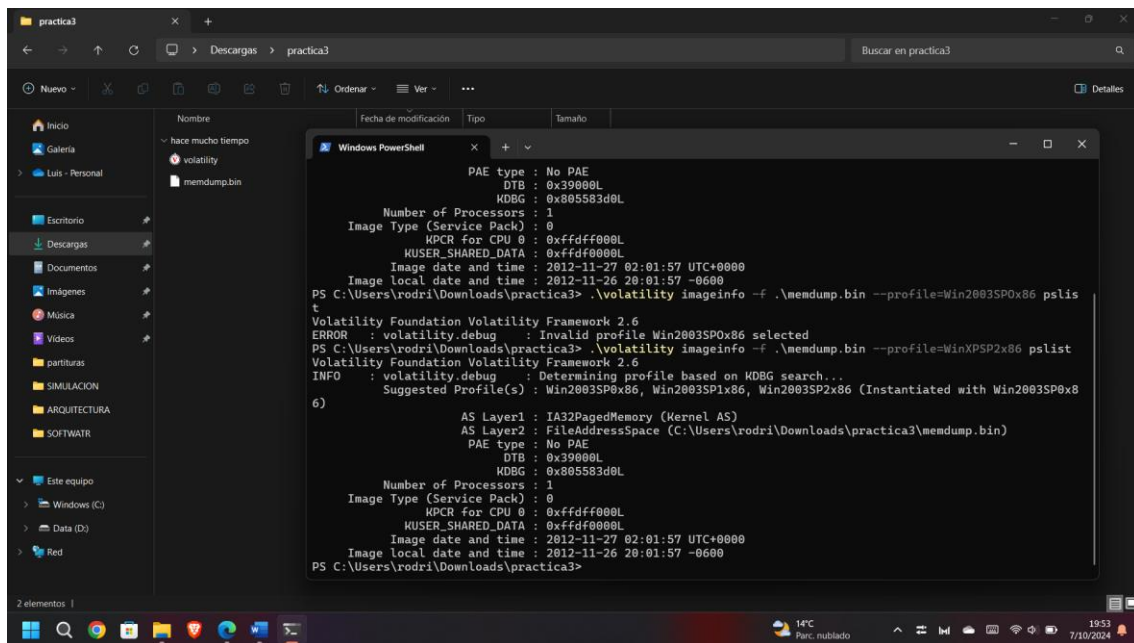
PASO 1



PASO 2



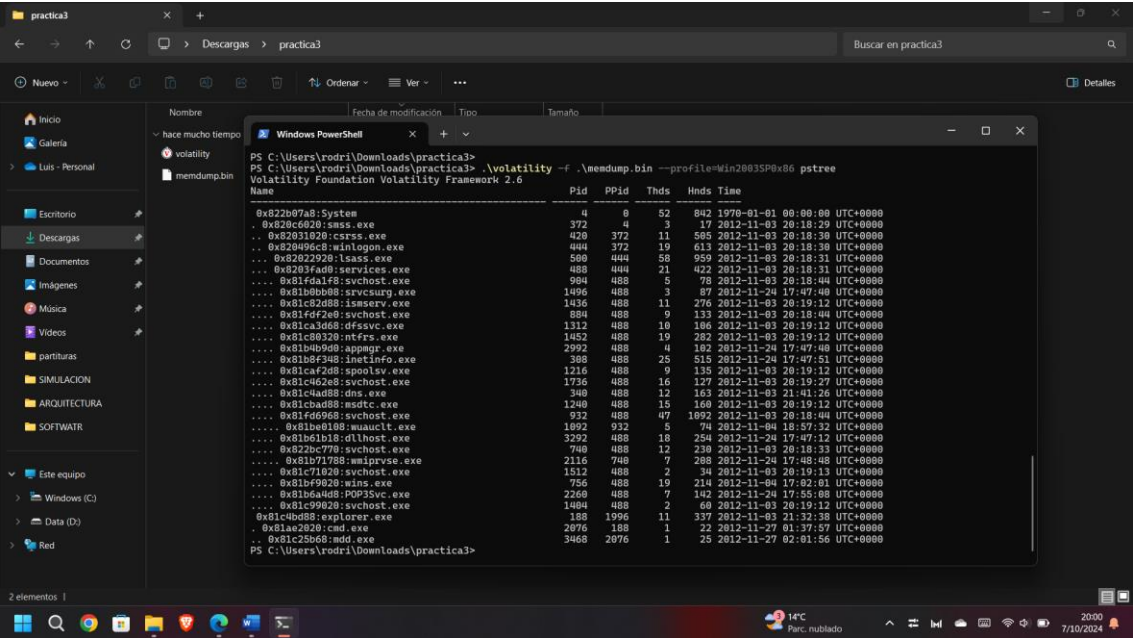
### PASO 3



### PASO 4

```
Windows PowerShell
KPCR for CPU 0 : 0xfffff000L
MUSER_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
PS C:\Users\rodri\Downloads\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 0 2012-11-03 20:18:29 UTC+0000
0x820c6020 smss.exe 372 4 3 17 0 0 2012-11-03 20:18:30 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
0x81fd2e0 svchost.exe 884 488 9 133 0 0 2012-11-03 20:18:44 UTC+0000
0x81fd1f8 svchost.exe 904 488 5 78 0 0 2012-11-03 20:18:44 UTC+0000
0x81fd6968 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
0x81cbad58 msdtc.exe 1240 488 15 160 0 0 2012-11-03 20:19:12 UTC+0000
0x81ca3d68 dfsvvc.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 ismserv.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
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
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 17:02:01 UTC+0000
0x81be0108 wuaucvt.exe 1092 932 5 74 0 0 2012-11-04 18:57:32 UTC+0000
0x81b6b1b8 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
0x81b6bb08 srvcsvr.exe 1496 488 3 87 0 0 2012-11-24 17:47:40 UTC+0000
0x81b8f348 inetinfo.exe 308 488 25 515 0 0 2012-11-24 17:47:51 UTC+0000
0x81b71788 wmiprvse.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
```

PASO 5



## PASO 6

[illegible]

```
Windows PowerShell
0x77290000 0x490000 0x29 C:\WINDOWS\system32\SHLWAPI.dll
0x76b10000 0x50000 0x2 C:\WINDOWS\system32\sfcdll.dll
0x76be0000 0x2a000 0x5 C:\WINDOWS\system32\sfcdll.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
0x76d00000 0x1c000 0xa C:\WINDOWS\system32\ole32.dll; Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\Comctl32.dll
0x77240000 0x1c000 0x7 C:\WINDOWS\system32\WINSCARD.DLL
0x76f00000 0x8000 0x7 C:\WINDOWS\system32\WTSAPI32.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\sxs.dll
0x77380000 0x7dd000 0xc C:\WINDOWS\system32\shell32.dll
0x771bb0000 0x9000 0x1 C:\WINDOWS\system32\wsock32.dll
0x76cf0000 0x17000 0x4 C:\WINDOWS\system32\iphlpapi.dll
0x74010000 0x5000 0x1 C:\WINDOWS\system32\icmp.dll
0x8ff00000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76f00000 0x17000 0x1 C:\WINDOWS\system32\MPRAPI.dll
0x76d00000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adslpdc.dll
0x76f10000 0x2f000 0x10 C:\WINDOWS\system32\WLDAP32.dll
0x76b80000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x76a80000 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
0x771b20000 0x38000 0x4 C:\WINDOWS\system32\mswsock.dll
0x76f60000 0x5000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x771ca0000 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x76e60000 0xc000 0x1 C:\WINDOWS\system32\cryptdll.dll
0x771ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x766f0000 0x16000 0x3 C:\WINDOWS\system32\WTSAPI.DLL
0x76ed0000 0x27000 0x4 C:\WINDOWS\system32\DNSAPI.dll
0x76520000 0x1d000 0x2 C:\WINDOWS\system32\csdcl.dll
0x75820000 0x1a000 0x6 C:\WINDOWS\system32\WNotify.dll
0x76aa0000 0x2c000 0x7 C:\WINDOWS\system32\WIMM.dll
0x77070000 0x26000 0x6 C:\WINDOWS\system32\WINSPOOL.DRV
0x771d0000 0x11000 0x7 C:\WINDOWS\system32\MPR.dll
0x770bc0000 0x9000 0x1 C:\WINDOWS\system32\Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_869BA05\COMCTL32.dll
0x771b70000 0x33000 0x2 C:\WINDOWS\system32\UxTheme.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.dll
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x774cf0000 0x8000 0x1 C:\WINDOWS\system32\wbem\wbemprox.dll
0x7750f0000 0x38000 0x2 C:\WINDOWS\system32\wbem\wbemcomn.dll
0x774ce0000 0xe000 0x1 C:\WINDOWS\system32\wbem\wbemsvc.dll
0x77550000 0x71000 0x1 C:\WINDOWS\system32\wbem\fastprox.dll
0x77090000 0x41000 0x1 C:\WINDOWS\system32\MSIcpg6.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\system32\msv1_0.dll
0x76540000 0x5000 0x1 C:\WINDOWS\system32\csui.dll
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\ES.DLL
0x76c60000 0x2000 0x1 C:\WINDOWS\system32\NTMARTA.DLL
0x774fa0000 0x14000 0x1 C:\WINDOWS\system32\Cabinet.dll
0x773ca0000 0x12000 0xa C:\WINDOWS\system32\cryptnet.dll
0x7722f0000 0x5000 0xa C:\WINDOWS\system32\SensApi.dll

*****
services.exe pid: 488
Command line : C:\WINDOWS\system32\services.exe

Base      Size      LoadCount  Path
-----
0x01000000 0x1b000 0xffff C:\WINDOWS\system32\services.exe
0x77f40000 0xba000 0xffff C:\WINDOWS\system32\ntdll.dll
0x77e40000 0xf4000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77ba0000 0x54000 0xffff C:\WINDOWS\system32\user32.dll
0x77d00000 0x40000 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 0xba000 0xffff C:\WINDOWS\system32\USERENV.dll
```

# Windows PowerShell

```

0x75970000 0xba000 0xffff C:\WINDOWS\system32\USERENV.dll
0x757a0000 0x52000 0xffff C:\WINDOWS\system32\SCESEVR.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\NCObjAPI.DLL
0x780c0000 0x61000 0xffff C:\WINDOWS\system32\MSVCP60.dll
0x76f50000 0x13000 0x6 C:\WINDOWS\system32\secur32.dll
0x75750000 0x12000 0x1 C:\WINDOWS\system32\eventlog.dll
0x71c00000 0x18000 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 0x30000 0x1 C:\WINDOWS\system32\scecli.dll
0x765a0000 0x100000 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
0x76c60000 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 0x56000 0x1 C:\WINDOWS\system32\kerberos.dll
0x766e0000 0xc000 0x1 C:\WINDOWS\system32\cryptdll.dll
0x76190000 0x12000 0x1 C:\WINDOWS\system32\MSASN1.dll
*****
lsass.exe pid: 500
Command line : C:\WINDOWS\system32\lsass.exe

```

Base	Size	LoadCount	Path
0x01000000	0x6000	0xffff	C:\WINDOWS\system32\lsass.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
0x742c0000	0xc8000	0xffff	C:\WINDOWS\system32\LSASRV.dll
0x77ba0000	0x54000	0xffff	C:\WINDOWS\system32\msvcrt.dll
0x76f50000	0x13000	0xffff	C:\WINDOWS\system32\Secur32.dll
0x77d00000	0x8f000	0xffff	C:\WINDOWS\system32\USER32.dll
0x77c00000	0x44000	0xffff	C:\WINDOWS\system32\GDI32.dll
0x741d0000	0x76000	0xffff	C:\WINDOWS\system32\SAMSRV.dll
0x766e0000	0xc000	0xffff	C:\WINDOWS\system32\cryptdll.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
0x76190000	0x12000	0xffff	C:\WINDOWS\system32\MSASN1.dll
0x71c40000	0x53000	0xffff	C:\WINDOWS\system32\NETAPI32.dll
0x5ccf0000	0x10000	0xffff	C:\WINDOWS\system32\SAMLIB.dll
0x71bd0000	0x11000	0xffff	C:\WINDOWS\system32\MPR.dll
0x766f0000	0x16000	0xffff	C:\WINDOWS\system32\NTDSAPI.dll
0x76f10000	0x2f000	0xffff	C:\WINDOWS\system32\WLDAP32.dll
0x74130000	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
0x76710000	0x38000	0x8	C:\WINDOWS\system32\w32time.dll
0x780c0000	0x61000	0x8	C:\WINDOWS\system32\MSVCP60.dll
0x76cf0000	0x17000	0xa	C:\WINDOWS\system32\iphlpapi.dll
0x75970000	0xba000	0xffff	C:\WINDOWS\system32\USERENV.dll
0x76c40000	0x14000	0x17	C:\WINDOWS\system32\AUTHZ.dll
0x76750000	0x28000	0x7	C:\WINDOWS\system32\schannel.dll
0x761b0000	0x98000	0x1a	C:\WINDOWS\system32\CRYPT32.dll



```
Windows PowerShell
0x761b0000 0x98000 0x1a C:\WINDOWS\system32\CRYPT32.dll
0x74100000 0x12000 0x3 C:\WINDOWS\system32\wdigest.dll
0x0ff40000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb000 0x2 C:\WINDOWS\system32\PSAPI.dll
0x720e0000 0x19000 0xa C:\WINDOWS\system32\NTDSA.dll
0x71fd0000 0xb000 0xe C:\WINDOWS\system32\NTDSATQ.dll
0x71b20000 0x43000 0xf C:\WINDOWS\system32\WSMSOCK.dll
0x69750000 0x108000 0xc C:\WINDOWS\system32\ESENT.dll
0x5fd10000 0x89000 0x2 C:\WINDOWS\system32\ntdsmsg.dll
0x71e90000 0xf000 0x2 C:\WINDOWS\system32\ntdsbrv.dll
0x71bb0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x5b890000 0x87000 0x2 C:\WINDOWS\system32\VSSAPI.dll
0x76a80000 0x18000 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 0x9000 0x1 C:\WINDOWS\system32\RASSFM.dll
0x74190000 0x30000 0x3 C:\WINDOWS\system32\assec14.dll
0x765a0000 0x100000 0x5 C:\WINDOWS\system32\SETUPAPI.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\system32\wshtcpip.dll
0x5deb0000 0x7000 0x1 C:\WINDOWS\system32\pmdssp.dll
0x71e00000 0x14000 0x1 C:\WINDOWS\system32\msapsspc.dll
0x78080000 0x11000 0x1 C:\WINDOWS\system32\MSVCRT40.dll
0x720a0000 0x1f000 0x1 C:\WINDOWS\system32\NTDSKCC.dll
0x71f30000 0xa000 0x1 C:\WINDOWS\system32\W32TOPL.dll
0x74160000 0x2b000 0x1 C:\WINDOWS\system32\ipsecsvc.dll
0x74390000 0xc000 0x1 C:\WINDOWS\system32\oakley.dll
0x740f0000 0xc000 0x1 C:\WINDOWS\system32\WINIPSEC.dll
0x74120000 0x9000 0x1 C:\WINDOWS\system32\pstorvc.dll
0x74140000 0x17000 0x1 C:\WINDOWS\system32\psbase.dll
0x0ffa0000 0x20000 0x1 C:\WINDOWS\system32\dsenh.dll
0x58f40000 0x17000 0x1 C:\WINDOWS\system32\wbsecr1.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
0x77b90000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\es.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\system32\rasadhlp.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\system32\winrmr.dll
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\WTMARTA.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
0x76b80000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x77380000 0x7dd000 0x1 C:\WINDOWS\system32\SHELL32.dll
0x76e30000 0xb000 0x1 C:\WINDOWS\system32\rtutils.dll
0x70ad0000 0xe6000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x5a310000 0x7000 0x1 C:\WINDOWS\system32\w3ssl.dll
0x5b640000 0x15000 0x2 C:\WINDOWS\system32\strmfilt.dll
0x67150000 0xa000 0x2 C:\WINDOWS\system32\HTTPAPI.dll
*****
svchost.exe pid: 740
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\msvcrt.dll
0x71c00000 0x18000 0x6 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
```

```
Windows PowerShell
0x77c00000 0x44000 0x8 C:\WINDOWS\system32\GDI32.dll
0x76f50000 0x13000 0x2 c:\windows\system32\Secur32.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
0x770e0000 0x7d000 0x1 C:\WINDOWS\system32\OLEAUT32.dll
0x77160000 0x124000 0x3 C:\WINDOWS\system32\ole32.dll
0x77010000 0xc6000 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\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
0x76cf0000 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
0x766c0000 0xd000 0x1 c:\windows\system32\dnssrslvr.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
0x71c40000 0x53000 0x9 C:\WINDOWS\system32\NETAPI32.dll
0x76f10000 0x2f000 0x3 C:\WINDOWS\system32\WLDAP32.dll
0x76b00000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x77380000 0x7dd000 0x2 C:\WINDOWS\system32\SHELL32.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 0xb000 0x4 C:\WINDOWS\system32\rtutils.dll
0x5ccf0000 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
0x76f00000 0x8000 0x1 C:\WINDOWS\system32\WTSAPI32.dll
0x76260000 0x10000 0x2 C:\WINDOWS\system32\WINSTA.dll
0x69750000 0x108000 0x1 C:\WINDOWS\system32\ESENT.dll
0x730a0000 0x9000 0x1 C:\WINDOWS\system32\WZCSAPI.DLL
0x79ad0000 0xe6000 0x3 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\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: 904
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
```





Windows PowerShell

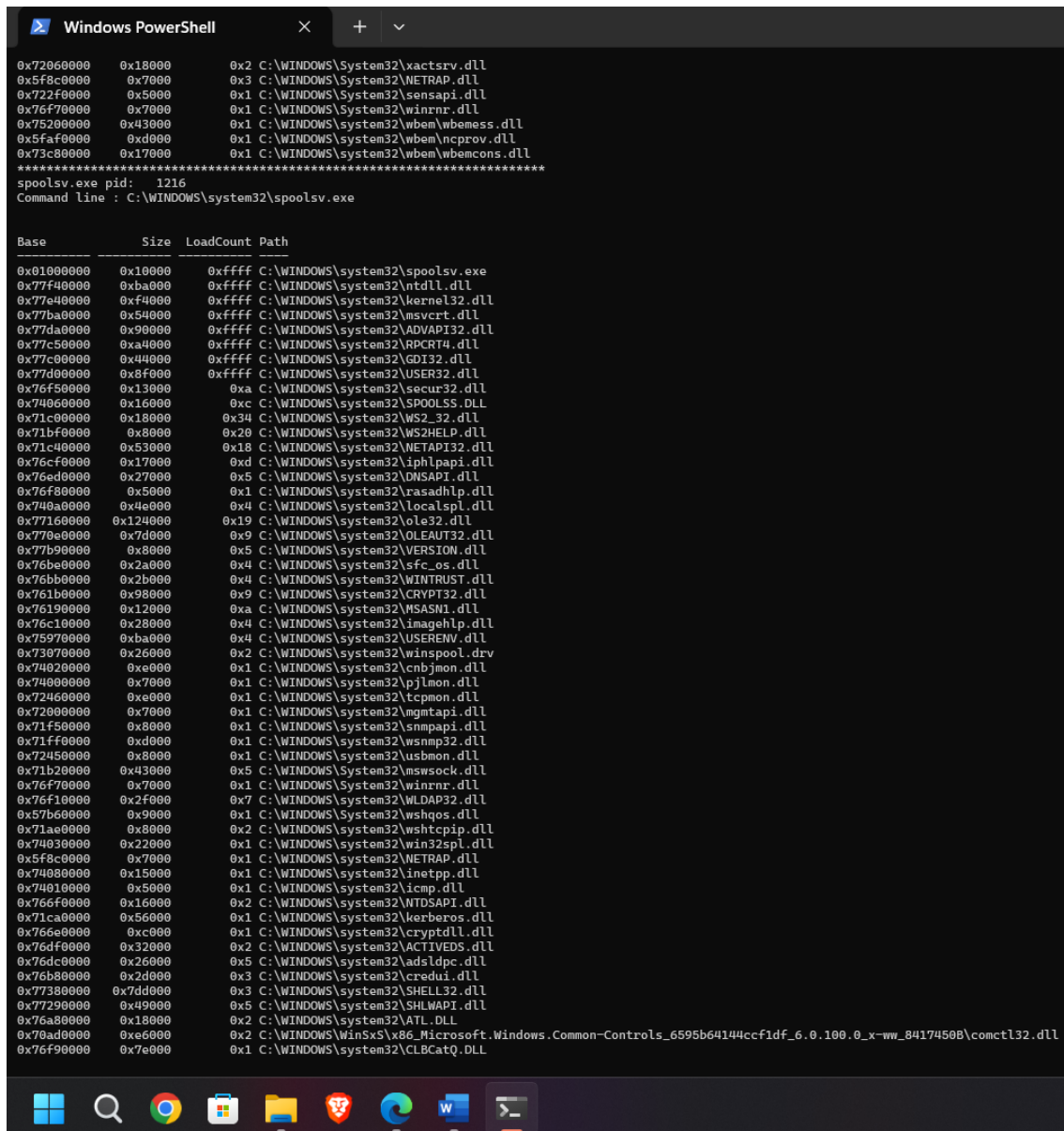


Base	Size	LoadCount	Path
0x01000000	0x6000	0xffff	C:\WINDOWS\system32\svchost.exe
0x77f40000	0xba000	0xffff	C:\WINDOWS\system32\ntdll.dll
0x77e40000	0xf4000	0xffff	C:\WINDOWS\system32\kernel32.dll
0x77da0000	0x90000	0xffff	C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x76c60000	0x20000	0x1	C:\WINDOWS\system32\NTMARTA.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	0x124000	0x2	C:\WINDOWS\system32\ole32.dll
0x74a40000	0x9000	0x1	c:\windows\system32\lmhsvc.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	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
0x76c60000	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
0x76f10000	0x2f000	0x1a	C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000	0x10000	0xe	C:\WINDOWS\System32\SAMLIB.dll
0x77160000	0x124000	0x78	C:\WINDOWS\system32\ole32.dll
0x76d30000	0x47000	0x2	c:\windows\system32\wzcsvc.dll
0x76e30000	0xb000	0x18	c:\windows\system32\rtutils.dll
0x76c00000	0x5000	0x3	c:\windows\system32\WMI.dll
0x76d10000	0x1c000	0x3	c:\windows\system32\DHCPSPVC.DLL
0x76ed0000	0x27000	0x11	c:\windows\system32\DNSAPI.dll
0x71c00000	0x18000	0x4c	c:\windows\system32\WS2_32.dll
0x71bf0000	0x8000	0x32	c:\windows\system32\WS2HELP.dll
0x76cf0000	0x17000	0xc	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
0x76f00000	0x8000	0x8	c:\windows\system32\WTSAPI32.dll
0x76260000	0x10000	0x10	c:\windows\system32\WINSTA.dll
0x71c40000	0x53000	0x5c	c:\windows\system32\NETAPI32.dll
0x77290000	0x49000	0x2c	C:\WINDOWS\system32\SHLWAPI.dll
0x69750000	0x108000	0x3	c:\windows\system32\ESSENT.dll
0x74d10000	0x29000	0x3	C:\WINDOWS\System32\rastls.dll
0x76a80000	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\MPRAPI.dll
0x76df0000	0x32000	0x6	C:\WINDOWS\System32\ACTIVEDS.dll
0x76dc0000	0x26000	0x6	C:\WINDOWS\System32\adsldpc.dll
0x76b80000	0x2d000	0x8	C:\WINDOWS\System32\credui.dll

```
Windows PowerShell
0x76b80000 0x2d000 0x8 C:\WINDOWS\System32\credui.dll
0x773d0000 0x7dd000 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\TAPI32.dll
0x76aa0000 0x2c000 0x9 C:\WINDOWS\System32\WINMM.dll
0x76750000 0x28000 0x3 C:\WINDOWS\System32\SCHANNEL.dll
0x75970000 0xba000 0xffff 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_8A69BA05\COMCTL32.dll
0x70ad0000 0xe6000 0x9 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\Comctl32.dll
0x74d00000 0x1d000 0x3 C:\WINDOWS\System32\raschap.dll
0x76b40000 0x21000 0x2 C:\Windows\System32\shsvcs.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\System32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\System32\COMRes.dll
0x77b90000 0x8000 0x7 C:\WINDOWS\system32\VERSION.dll
0x75020000 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\wshtcpip.dll
0x74d70000 0x5000 0x1 C:\WINDOWS\System32\MSIDLE.DLL
0x74fc0000 0x23000 0x1 C:\Windows\system32\wkssvc.dll
0x59ec0000 0xb000 0x1 C:\WINDOWS\System32\wiarpd.dll
0x74ed0000 0x18000 0x1 C:\Windows\system32\srsvcs.dll
0x74e00000 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\sfc.dll
0x76be0000 0x2a000 0x4 C:\Windows\system32\sfc_os.dll
0x74db0000 0xa000 0x1 C:\Windows\system32\dmserver.dll
0x76ad0000 0x3e000 0x4 C:\Windows\system32\es.dll
0x74d00000 0xb000 0x1 C:\Windows\pchealth\helpctr\binaries\pchsfc.dll
0x73c70000 0x7000 0x1 C:\Windows\system32\seclogon.dll
0x72310000 0xc000 0x1 C:\Windows\system32\sens.dll
0x76710000 0x38000 0x3 C:\Windows\system32\W32time.dll
0x780c0000 0xe1000 0x13 C:\Windows\system32\WSVCP60.dll
0x58af0000 0x25000 0x1 C:\Windows\system32\wbem\wmisvc.dll
0x74cd0000 0x6000 0x1 C:\Windows\system32\wuauerv.dll
0x74e20000 0x32000 0x1 C:\WINDOWS\System32\wuaueng.dll
0x750c0000 0x28000 0x1 C:\WINDOWS\System32\ADVAPI32.dll
0x760f0000 0x9e000 0x2 C:\WINDOWS\system32\WININET.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\System32\SXS.DLL
0x755d0000 0x12c000 0x2 C:\WINDOWS\System32\comsvcs.dll
0x590a0000 0x7000 0x1 C:\WINDOWS\System32\winsrpc.dll
0x76c90000 0x24000 0x1 C:\WINDOWS\System32\msv1_0.dll
0x70c60000 0x54000 0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.WinHTTP_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\esscli.dll
0x750f0000 0x38000 0xf C:\WINDOWS\system32\wbem\wbemcomn.dll
0x75550000 0x71000 0x8 C:\WINDOWS\system32\wbem\FastProx.dll
0x74600000 0x1b000 0x1 C:\WINDOWS\system32\wbem\wmiutils.dll
0x75060000 0x2c000 0x1 C:\WINDOWS\system32\wbem\repdrvfs.dll
0x58b50000 0x68000 0x1 C:\WINDOWS\system32\wbem\wmiprvse.dll
0x5fb10000 0xc000 0x2 C:\WINDOWS\system32\WCOBJAPI.DLL
0x0ff00000 0x2d000 0x1 C:\WINDOWS\System32\rsaenh.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\WZCAPI.DLL
0x75ba0000 0x1b1000 0x2 C:\WINDOWS\system32\WETSHL.dll
0x74de0000 0x11000 0x2 C:\WINDOWS\system32\CLUSAPI.dll
0x68400000 0x41000 0x1 C:\WINDOWS\system32\hnetcfg.dll
0x753e0000 0xa3000 0x1 C:\WINDOWS\System32\RASDLG.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll
0x72060000 0x18000 0x2 C:\WINDOWS\System32\ractsrv.dll
```



## Windows PowerShell



```
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x712d0000 0x2d000 0x1 C:\WINDOWS\system32\adsldp.dll
0x75da0000 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL
```

\*\*\*\*\*

```
msdtc.exe pid: 1240
Command line : C:\WINDOWS\system32\msdtc.exe
```

Base	Size	LoadCount	Path
0x00400000	0x4000	0xffff	C:\WINDOWS\system32\msdtc.exe
0x77f40000	0xba000	0xffff	C:\WINDOWS\system32\ntdll.dll
0x77e40000	0xf4000	0xffff	C:\WINDOWS\system32\kernel32.dll
0x77160000	0x124000	0xffff	C:\WINDOWS\system32\ole32.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
0x77da0000	0x90000	0xffff	C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x61030000	0xf6000	0xffff	C:\WINDOWS\system32\MSDTCM.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
0x76f50000	0x13000	0xffff	C:\WINDOWS\system32\Secur32.dll
0x780c0000	0x61000	0xffff	C:\WINDOWS\system32\MSVCP60.dll
0x61150000	0x71000	0xffff	C:\WINDOWS\system32\MSDTCPRX.dll
0x770e0000	0x7d000	0xffff	C:\WINDOWS\system32\OLEAUT32.dll
0x71c40000	0x53000	0xffff	C:\WINDOWS\system32\NETAPI32.dll
0x74f40000	0x18000	0xffff	C:\WINDOWS\system32\MTXCLU.DLL
0x77b90000	0x8000	0xffff	C:\WINDOWS\system32\VERSION.dll
0x71bb0000	0x9000	0xffff	C:\WINDOWS\system32\WSOCK32.dll
0x611d0000	0x1a000	0xffff	C:\WINDOWS\system32\MSDTCLOG.dll
0x57b10000	0x6000	0xffff	C:\WINDOWS\system32\XOLEHLP.dll
0x71b20000	0x43000	0xffff	C:\WINDOWS\system32\MSWSOCK.DLL
0x76aa0000	0x2c000	0xffff	C:\WINDOWS\system32\WINMM.dll
0x74de0000	0x11000	0x2	C:\WINDOWS\system32\CLUSAPI.DLL
0x74ef0000	0x12000	0x1	C:\WINDOWS\system32\RESUTILS.DLL
0x75970000	0xba000	0x1	C:\WINDOWS\system32\USERENV.dll
0x72880000	0xf4000	0x1	C:\WINDOWS\system32\MFC42u.DLL
0x77010000	0xc6000	0x3	C:\WINDOWS\system32\COMRES.DLL
0x74f10000	0x1f000	0x1	C:\WINDOWS\system32\MTXOCI.DLL
0x76f90000	0x7e000	0x1	C:\WINDOWS\system32\CLBCatQ.DLL
0x76c60000	0x20000	0x1	C:\WINDOWS\system32\NTMARTA.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	0xffff	C:\WINDOWS\system32\Dfssvc.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	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x77290000	0x49000	0xffff	C:\WINDOWS\system32\SHLWAPI.dll
0x77c00000	0x44000	0xffff	C:\WINDOWS\system32\GDI32.dll
0x77d00000	0x8f000	0xffff	C:\WINDOWS\system32\USER32.dll
0x71c40000	0x53000	0xffff	C:\WINDOWS\system32\NETAPI32.dll
0x77380000	0x7dd000	0xffff	C:\WINDOWS\system32\SHELL32.dll
0x76df0000	0x32000	0xffff	C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000	0x26000	0xffff	C:\WINDOWS\system32\adsldpc.dll
0x76f10000	0x2f000	0xffff	C:\WINDOWS\system32\WLDAP32.dll
0x76b80000	0x2d000	0xffff	C:\WINDOWS\system32\credui.dll



Windows PowerShell

0x76b800000x2d0000xffffC:\WINDOWS\system32\credui.dll

0x76a800000x180000xffffC:\WINDOWS\system32\ATL.DLL

0x771600000x1240000xffffC:\WINDOWS\system32\ole32.dll

0x770e00000x7d0000xffffC:\WINDOWS\system32\OLEAUT32.dll

0x74de00000x110000xffffC:\WINDOWS\system32\CLUSAPI.dll

0x74ef00000x120000xffffC:\WINDOWS\system32\RESUTILS.dll

0x759700000xba0000xffffC:\WINDOWS\system32\USERENV.dll

0x728800000xf40000xffffC:\WINDOWS\system32\MFC42u.DLL

0x766f00000x160000xffffC:\WINDOWS\system32\NTDSAPI.dll

0x76ed00000x270000xffffC:\WINDOWS\system32\DNSAPI.dll

0x71c900000x180000xffffC:\WINDOWS\system32\WS2\_32.dll

0x71bf00000x80000xffffC:\WINDOWS\system32\WS2HELP.dll

0x76f500000x130000xffffC:\WINDOWS\system32\Secur32.dll

0x71bb00000x90000xffffC:\WINDOWS\system32\WSOCK32.dll

0x76ad00000xe60000x2C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.100.0\_x-ww\_8417450B\comctl32.dll

0x71b200000x430000x5C:\WINDOWS\system32\mswsock.dll

0x76f800000x50000x1C:\WINDOWS\system32\psapi.dll

0x71ae00000x80000x1C:\WINDOWS\System32\wshtcpip.dll

0x71ca00000x560000x1C:\WINDOWS\system32\kerberos.dll

0x766e00000xc90000x1C:\WINDOWS\system32\cryptdll.dll

0x761900000x120000x1C:\WINDOWS\system32\MSASN1.dll

0x76f700000x70000x1C:\WINDOWS\System32\winrnr.dll

0x76f900000x7e0000x1C:\WINDOWS\system32\CLBCatQ.DLL

0x770100000xc60000x1C:\WINDOWS\system32\COMRes.dll

0x77b900000x80000x1C:\WINDOWS\system32\VERSION.dll

0x712d00000x2d0000x1C:\WINDOWS\system32\adsldp.dll

0x75da00000xba0000x1C:\WINDOWS\system32\SXS.DLL

\*\*\*\*\*

svchost.exe pid: 1404

Command line : C:\WINDOWS\System32\svchost.exe -k WinErr

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
0x76c60000	0x20000	0x1	C:\WINDOWS\System32\NTHART4.DLL
0x77ba0000	0x54000	0x9	C:\WINDOWS\system32\msvcrt.dll
0x77d00000	0x8f000	0x9	C:\WINDOWS\system32\USER32.dll
0x77c00000	0x4000	0x5	C:\WINDOWS\system32\GDI32.dll
0x76f10000	0x2f000	0x1	C:\WINDOWS\system32\WLDAP32.dll
0x5cfc0000	0x10000	0x1	C:\WINDOWS\System32\SAHLB.dll
0x77160000	0x124000	0x2	C:\WINDOWS\system32\ole32.dll
0x74da0000	0x9000	0x1	c:\windows\system32\ersvc.dll
0x75970000	0xba000	0x1	C:\WINDOWS\system32\USERENV.dll
0x76260000	0x10000	0x1	c:\windows\system32\WINSTA.dll
0x71c40000	0x53000	0x2	c:\windows\system32\NETAPI32.dll
0x76f50000	0x13000	0x1	C:\WINDOWS\System32\secur32.dll

\*\*\*\*\*

ismserv.exe pid: 1436

Command line : C:\WINDOWS\System32\ismserv.exe

Base	Size	LoadCount	Path
0x01000000	0xc000	0xffff	C:\WINDOWS\System32\ismserv.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	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x76f10000	0x2f000	0xffff	C:\WINDOWS\system32\WLDAP32.dll
0x71c40000	0x53000	0xffff	C:\WINDOWS\System32\NETAPI32.dll
0x766e0000	0xc000	0xffff	C:\WINDOWS\System32\cryptdll.dll
0x5fd0000	0x89000	0x1	C:\WINDOWS\System32\ntdsmsg.dll



```
Windows PowerShell
>

0x5f1d0000 0x80000 0x1 C:\WINDOWS\System32\ntdsmsg.dll
0x71c00000 0x18000 0x16 C:\WINDOWS\system32\WS2_32.DLL
0x71bf0000 0x8000 0x14 C:\WINDOWS\System32\WS2HELP.dll
0x71b20000 0x43000 0x4 C:\WINDOWS\system32\wssock.dll
0x71ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll
0x76f50000 0x13000 0x5 C:\WINDOWS\system32\SECUR32.DLL
0x76ed0000 0x27000 0x4 C:\WINDOWS\System32\DNSAPI.dll
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winmr.dll
0x76f80000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll
0x77d00000 0x8f000 0x7e C:\WINDOWS\system32\USER32.DLL
0x77c00000 0x40000 0x5d C:\WINDOWS\system32\GDI32.dll
0x76c00000 0x24000 0x1 C:\WINDOWS\system32\user1_0.dll
0x63e80000 0x9000 0x1 C:\WINDOWS\System32\ismip.dll
0x71f30000 0xa000 0x2 C:\WINDOWS\System32\W32TQIP.dll
0x766f0000 0x16000 0x2 C:\WINDOWS\System32\NTDSAPI.dll
0x63e50000 0x11000 0x1 C:\WINDOWS\System32\ismsmtp.dll
0x76a80000 0x18000 0x7 C:\WINDOWS\System32\ATL.DLL
0x77160000 0x124000 0x1c C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0x10 C:\WINDOWS\system32\OLEAUT32.dll
0x76df0000 0x32000 0x3 C:\WINDOWS\System32\ACTIVEDS.dll
0x76dc0000 0x26000 0x5 C:\WINDOWS\System32\adslpc.dll
0x76db0000 0x2d000 0x4 C:\WINDOWS\System32\credui.dll
0x77d00000 0x7d000 0x5 C:\WINDOWS\system32\SHELL32.dll
0x77729000 0x49000 0xf C:\WINDOWS\system32\SHLWAPI.dll
0x70ad0000 0xe6000 0x6 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x74010000 0x5900 0x1 C:\WINDOWS\system32\TCMP.DLL
0x76cf0000 0x17000 0x3 C:\WINDOWS\System32\iphlpapi.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\System32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\System32\COMRes.dll
0x77b90000 0x8000 0x3 C:\WINDOWS\system32\VERSION.dll
0x71300000 0x47000 0x1 C:\WINDOWS\system32\inetrv\adsiis.dll
0x72800000 0xf4000 0x2 C:\WINDOWS\system32\HFC42u.DLL
0x647b0000 0x24000 0x2 C:\WINDOWS\system32\IisRTL.DLL
0x64760000 0x37000 0x1 C:\WINDOWS\system32\inetrv\iisui.dll
0x70bc0000 0x9000 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 0x98000 0x3 C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0x2 C:\WINDOWS\system32\MSASN1.dll
0x71430000 0x10000 0x1 C:\WINDOWS\System32\ADMINPROX.DLL
0x0ffd0000 0x2d000 0x1 C:\WINDOWS\System32\rsaenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\System32\PSAPI.DLL
0x75da0000 0xba000 0x1 C:\WINDOWS\System32\SXS.DLL
0x5c150000 0x2e000 0x1 C:\WINDOWS\system32\inetrv\smtpadm.dll
0x5c140000 0x6000 0x1 C:\WINDOWS\system32\SMTPAPI.dll
0x6930000 0x900 0x2 C:\WINDOWS\system32\exttrace.dll
0x5b7c0000 0x6000 0x2 C:\WINDOWS\system32\STAXMEX.dll
0x71bb0000 0x9000 0x1 C:\WINDOWS\system32\WSOCK32.dll
0x5c870000 0x35000 0x1 C:\WINDOWS\system32\inetrv\seo.dll
0x5cdf0000 0x6000 0x1 C:\WINDOWS\system32\RMH.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 0x2000 0x1 C:\WINDOWS\system32\HSOERT2.dll
0x64430000 0xe000 0x1 C:\WINDOWS\system32\inetres.dll
*****
ntfrs.exe pid: 1452
Command Line : C:\WINDOWS\system32\ntfrs.exe

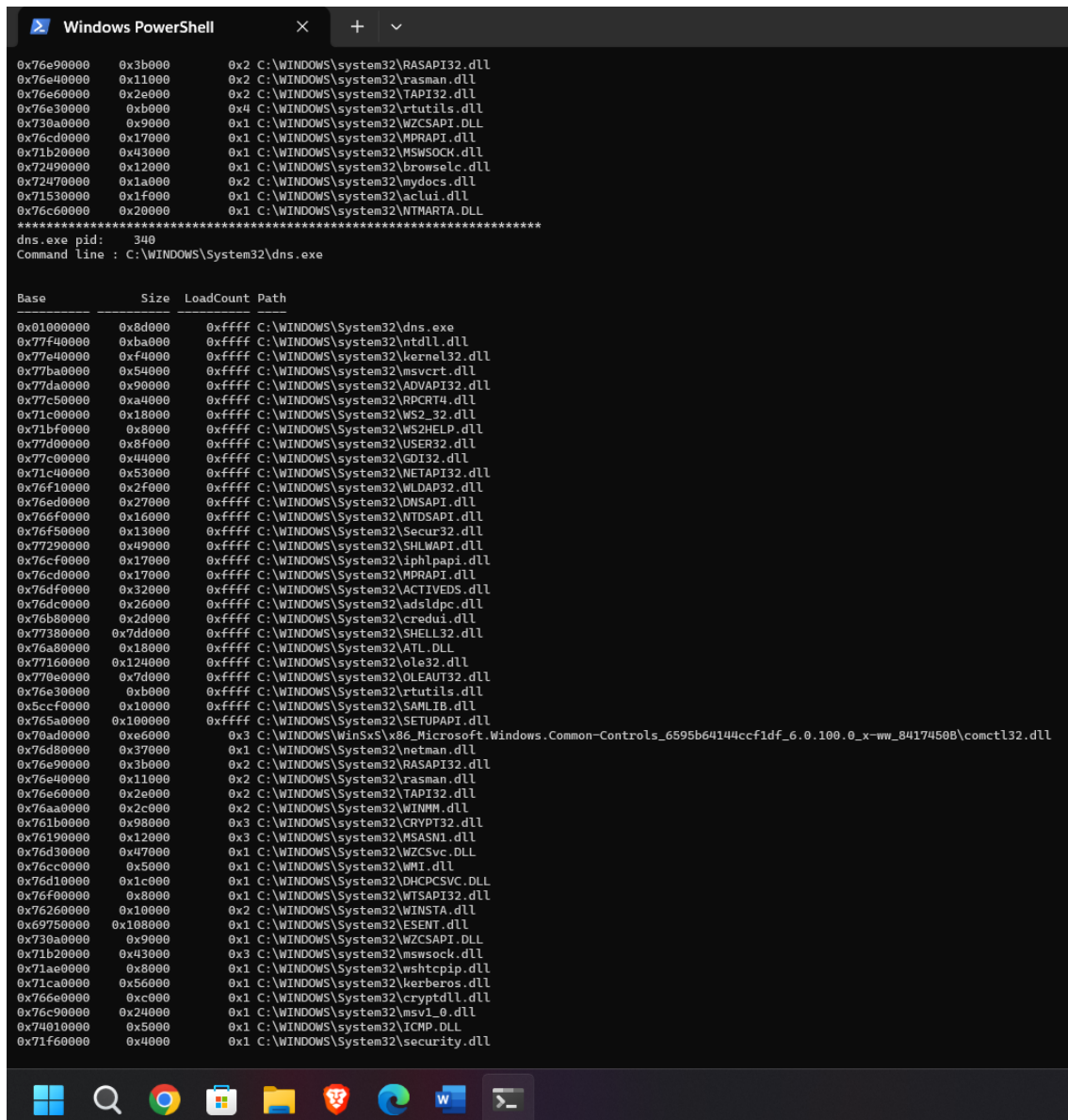
Base Size LoadCount Path
-----
0x01000000 0xc3000 0xffff C:\WINDOWS\system32\ntfrs.exe
0x77f40000 0xba000 0xffff DCC
0x00000000 0x0 0x0 C:\WINDOWS\system32\kernel32.dll
```





Windows PowerShell

Base	Size	LoadCount	Path
0x01000000	0xfff000	0xffff	C:\WINDOWS\Explorer.EXE
0x77f40000	0xba0000	0xffff	C:\WINDOWS\system32\ntdll.dll
0x77c40000	0xf40000	0xffff	C:\WINDOWS\system32\kernel32.dll
0x77ba0000	0x500000	0xffff	C:\WINDOWS\system32\user32.dll
0x77da0000	0x900000	0xffff	C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000	0xa40000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x77c00000	0x440000	0xffff	C:\WINDOWS\system32\GDI32.dll
0x77d00000	0x8f0000	0xffff	C:\WINDOWS\system32\USER32.dll
0x77290000	0x490000	0xffff	C:\WINDOWS\system32\SHLWAPI.dll
0x77380000	0x7dd000	0xffff	C:\WINDOWS\system32\SHELL32.dll
0x77160000	0x124000	0xffff	C:\WINDOWS\system32\ole32.dll
0x770e0000	0x7d0000	0xffff	C:\WINDOWS\system32\OLEAUT32.dll
0x75eb0000	0x106000	0xffff	C:\WINDOWS\system32\BROWSEUI.dll
0x76920000	0x157000	0xffff	C:\WINDOWS\system32\SHDOCVW.dll
0x71b70000	0x330000	0xffff	C:\WINDOWS\system32\UxTheme.dll
0x70ad0000	0xe60000	0x3f	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8417450B\comctl32.dll
0x75e60000	0x220000	0x2	C:\WINDOWS\system32\apphelp.dll
0x76f90000	0x7e0000	0x1	C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000	0xc60000	0x1	C:\WINDOWS\system32\COMRes.dll
0x77b90000	0x800000	0x7	C:\WINDOWS\system32\VERSION.dll
0x76540000	0x500000	0x2	C:\WINDOWS\system32\csrss.dll
0x76520000	0x1d0000	0x2	C:\WINDOWS\system32\CSCDLL.dll
0x5aff0000	0x6d0000	0x1	C:\WINDOWS\system32\themeui.dll
0x76f50000	0x130000	0x4	C:\WINDOWS\system32\Secur32.dll
0x76280000	0x500000	0x1	C:\WINDOWS\system32\MSIMG32.dll
0x75970000	0xba0000	0x3	C:\WINDOWS\system32\USERENV.dll
0x768e0000	0x800000	0x1	C:\WINDOWS\system32\LINKINFO.dll
0x768f0000	0x240000	0x4	C:\WINDOWS\system32\ntshrui.dll
0x71c40000	0x530000	0x1a	C:\WINDOWS\system32\NETAPI32.dll
0x5ccf0000	0x100000	0x4	C:\WINDOWS\system32\SAMLIB.dll
0x765a0000	0x1000000	0xd	C:\WINDOWS\system32\SETUPAPI.dll
0x75be0000	0x1b1000	0x1	C:\WINDOWS\system32\NETSHELL.dll
0x76b80000	0x2d0000	0x4	C:\WINDOWS\system32\credui.dll
0x71c90000	0x180000	0x8	C:\WINDOWS\system32\WS2_32.dll
0x71bf0000	0x800000	0x7	C:\WINDOWS\system32\WS2HELP.dll
0x76cf0000	0x170000	0x1	C:\WINDOWS\system32\iphlpapi.dll
0x79de0000	0x110000	0x1	C:\WINDOWS\system32\CLUSAPI.dll
0x76260000	0x100000	0x3	C:\WINDOWS\system32\WINSTA.dll
0x74920000	0x440000	0x1	C:\WINDOWS\system32\webcheck.dll
0x71bb0000	0x900000	0x1	C:\WINDOWS\system32\WSOCK32.dll
0x748f0000	0x210000	0x2	C:\WINDOWS\system32\stobject.dll
0x748e0000	0xa00000	0x2	C:\WINDOWS\system32\BatMeter.dll
0x748c0000	0x700000	0x4	C:\WINDOWS\system32\POWERPROF.dll
0x76f00000	0x800000	0x2	C:\WINDOWS\system32\WTSAPI32.dll
0x74970000	0x880000	0x2	C:\WINDOWS\system32\printui.dll
0x73070000	0x260000	0x3	C:\WINDOWS\system32\WINSPOOL.DRV
0x76df0000	0x320000	0x3	C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000	0x260000	0x5	C:\WINDOWS\system32\adsldpc.dll
0x76f10000	0x2f0000	0x4	C:\WINDOWS\system32\WLDPAP32.dll
0x76a80000	0x180000	0x3	C:\WINDOWS\system32\ATL.DLL
0x748d0000	0x800000	0x2	C:\WINDOWS\system32\CFGHGR32.dll
0x71bd0000	0x110000	0x5	C:\WINDOWS\system32\HPR.dll
0x76ea0000	0x2c0000	0x4	C:\WINDOWS\system32\WINMM.dll
0x75e90000	0x700000	0x1	C:\WINDOWS\system32\drprov.dll
0x5f120000	0xe00000	0x1	C:\WINDOWS\system32\ntlanman.dll
0x5f8a0000	0x160000	0x2	C:\WINDOWS\system32\NETUI0.dll
0x5f860000	0x310000	0x1	C:\WINDOWS\system32\NETUI1.dll
0x75ea0000	0x900000	0x1	C:\WINDOWS\system32\davclnt.dll
0x75da0000	0xba0000	0x1	C:\WINDOWS\system32\SXS.DLL
0x760f0000	0x9e0000	0x1	C:\WINDOWS\system32\WININET.dll
0x761b0000	0x980000	0x3	C:\WINDOWS\system32\CRYPT32.dll
0x76190000	0x120000	0x3	C:\WINDOWS\system32\MSASN1.dll
0x76050000	0x950000	0x1	C:\WINDOWS\system32\shdoclc.dll
0x75fc0000	0x890000	0x2	C:\WINDOWS\system32\urlmon.dll
0x76e90000	0x3b0000	0x2	C:\WINDOWS\system32\RASAPI32.dll



Windows PowerShell

\*\*\*\*\*  
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 0xa4000 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  
0x71c00000 0x18000 0xffff C:\WINDOWS\System32\WS2\_32.dll  
0x71bf0000 0x8000 0xffff C:\WINDOWS\System32\WS2HELP.dll  
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll  
0x5b890000 0x87000 0xffff C:\WINDOWS\System32\VSSAPI.DLL  
0x76a80000 0x18000 0xffff C:\WINDOWS\System32\ATL.DLL  
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll  
0x71b20000 0x43000 0x5 C:\WINDOWS\system32\mswsock.dll  
0x771ae0000 0x8000 0x1 C:\WINDOWS\System32\wshtcpip.dll  
0x76ed0000 0x27000 0x2 C:\WINDOWS\System32\DNSAPI.dll  
0x76f70000 0x7000 0x1 C:\WINDOWS\System32\winrnr.dll  
0x76f10000 0x2f000 0x1 C:\WINDOWS\system32\WLDAP32.dll  
0x76f80000 0x5000 0x1 C:\WINDOWS\System32\rasadhlp.dll  
0x69750000 0x108000 0x1 C:\WINDOWS\System32\esent.dll  
0x6cfc0000 0x10000 0x1 C:\WINDOWS\System32\SHLWAPI.dll  
0x76f90000 0x7e000 0x1 C:\WINDOWS\System32\CLBCatQ.DLL  
0x77010000 0xc6000 0x1 C:\WINDOWS\System32\COMRes.dll  
0x77b90000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll  
0x76ad0000 0x3e000 0x1 C:\WINDOWS\system32\es.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  
0x77380000 0x7dd000 0xffff C:\WINDOWS\system32\SHLWAPI.dll  
0x77da0000 0x90000 0xffff C:\WINDOWS\system32\ADVAPI32.dll  
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 0x8000 0xffff C:\WINDOWS\system32\VERSION.dll  
0x77ad0000 0xe6000 0xffff C:\WINDOWS\WinSxS\x86\_Microsoft.Windows.Common-Controls\_6595b64144ccf1df\_6.0.100.0\_x-ww\_84174508\COMCTL32.dll  
0x76f00000 0x8000 0xffff C:\WINDOWS\system32\WTSAPI32.dll  
0x76260000 0x10000 0xffff C:\WINDOWS\system32\WINSTA.dll  
0x771c40000 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 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL  
\*\*\*\*\*  
dlhhost.exe pid: 3292

Windows PowerShell

+

▼

dllhost.exe pid: 3292

Command line : C:\WINDOWS\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}

Base	Size	LoadCount	Path
0x01000000	0x4000	0xffff	C:\WINDOWS\system32\dllhost.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
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	0x90000	0xffff	C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x76f90000	0x7e000	0x8	C:\WINDOWS\system32\CLBCatQ.DLL
0x770e0000	0x7d000	0x1e	C:\WINDOWS\system32\OLEAUT32.dll
0x77010000	0xc6000	0x8	C:\WINDOWS\system32\COMRes.dll
0x77b90000	0x8000	0x13	C:\WINDOWS\system32\VERSION.dll
0x755d0000	0x12c000	0x6	C:\WINDOWS\system32\COMSVCS.DLL
0x74f10000	0x1f000	0x1	C:\WINDOWS\system32\mtxoci.dll
0x0ffdf0000	0x2d000	0x1	C:\WINDOWS\system32\rsaenh.dll
0x76b70000	0xb000	0x1	C:\WINDOWS\system32\PSAPI.DLL
0x5ac60000	0x1d000	0x1	C:\WINDOWS\system32\txflog.dll
0x76ad0000	0x3e000	0x2	C:\WINDOWS\system32\ES.DLL
0x75da0000	0xba000	0x1	C:\WINDOWS\system32\SXS.DLL
0x57b10000	0x6000	0x1	C:\WINDOWS\system32\XOLEHLP.dll
0x61150000	0x71000	0x2	C:\WINDOWS\system32\MSDTCPRX.dll
0x71c40000	0x53000	0x2	C:\WINDOWS\system32\NETAPI32.dll
0x780c0000	0x61000	0x2	C:\WINDOWS\system32\MSVCP60.dll
0x74f40000	0x18000	0x2	C:\WINDOWS\system32\MTXCLU.DLL
0x71bb0000	0x9000	0x4	C:\WINDOWS\system32\WSOCK32.dll
0x71c00000	0x18000	0xc	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\RESUTILS.DLL
0x75970000	0xba000	0x1	C:\WINDOWS\system32\USERENV.dll
0x72880000	0xf4000	0x1	C:\WINDOWS\system32\MFC42u.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	0x7000	0x1	C:\WINDOWS\System32\winnr.dll
0x76f10000	0x2f000	0x2	C:\WINDOWS\system32\WLDP32.dll
0x76f80000	0x5000	0x1	C:\WINDOWS\system32\rasadhlp.dll
0x6f680000	0x47000	0x1	C:\WINDOWS\system32\catsrv.dll
0x6f670000	0xa000	0x1	C:\WINDOWS\system32\catsrvps.dll
0x6ed00000	0x1b000	0x2	C:\WINDOWS\system32\clbcatex.dll
0x6f5d0000	0x95000	0x2	C:\WINDOWS\system32\catsrvut.dll
0x61e50000	0x9000	0x2	C:\WINDOWS\system32\MfcSubs.dll
0x76c60000	0x20000	0x1	C:\WINDOWS\system32\NTMARTA.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	0xffff	C:\WINDOWS\system32\serverappliance\appmgr.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
0x780c0000	0x61000	0xffff	C:\WINDOWS\system32\MSVCP60.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
0x77160000	0x124000	0xffff	C:\WINDOWS\system32\ole32.dll

# Windows PowerShell

```

0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x770e0000 0x7d000 0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x76e30000 0xb000 0x1 C:\WINDOWS\system32\rtutils.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 0xba000 0x1 C:\WINDOWS\system32\SXS.DLL
0x74ce0000 0xe000 0x1 C:\WINDOWS\system32\wbem\wbemsvc.dll
0x75550000 0x71000 0x2 C:\WINDOWS\system32\wbem\fastprox.dll
0x750f0000 0x38000 0x3 C:\WINDOWS\system32\wbem\wbemcomn.dll
0x766f0000 0x16000 0x2 C:\WINDOWS\system32\NTDSAPI.dll
0x76ed0000 0x27000 0x2 C:\WINDOWS\system32\DNSAPI.dll
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
0x76f50000 0x13000 0x2 C:\WINDOWS\system32\Secur32.dll
0x00820000 0xf000 0x1 C:\WINDOWS\system32\ServerAppliance\taskctx.dll
0x75180000 0x3e000 0x1 C:\WINDOWS\system32\wbem\esscli.dll

```

\*\*\*\*\*

svcsurg.exe pid: 1496

Command line : C:\WINDOWS\system32\serverappliance\svcsurg.exe

Base	Size	LoadCount	Path
0x01000000	0x13000	0xffff	C:\WINDOWS\system32\serverappliance\svcsurg.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
0x780c0000	0x61000	0xffff	C:\WINDOWS\system32\MSVCP60.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
0x77160000	0x124000	0xffff	C:\WINDOWS\system32\ole32.dll
0x770e0000	0x7d000	0xffff	C:\WINDOWS\system32\OLEAUT32.dll
0x76b70000	0xb000	0xffff	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	0xba000	0x1	C:\WINDOWS\system32\SXS.DLL
0x76e30000	0xb000	0x3	C:\WINDOWS\system32\rtutils.dll
0x00610000	0xf000	0x1	C:\WINDOWS\system32\serverappliance\initsrv.dll
0x00620000	0xf000	0x1	C:\WINDOWS\system32\ServerAppliance\taskctx.dll
0x00630000	0x15000	0x1	C:\WINDOWS\system32\ServerAppliance\appsrvcs.dll
0x74cf0000	0x8000	0x1	C:\WINDOWS\system32\wbem\wbemprox.dll
0x750f0000	0x38000	0x2	C:\WINDOWS\system32\wbem\wbemcomn.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	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	0x13000	0x1	C:\WINDOWS\system32\Secur32.dll

\*\*\*\*\*

inetinfo.exe pid: 308

Command line : C:\WINDOWS\system32\inetsrv\inetinfo.exe

Base	Size	LoadCount	Path
0x01000000	0x6000	0xffff	C:\WINDOWS\system32\inetsrv\inetinfo.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





```
Windows PowerShell
0x77ba0000 0x540000 0xffff C:\WINDOWS\system32\msvcrt.dll
0x77da0000 0x900000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77c50000 0xa40000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77d00000 0x8f0000 0xffff C:\WINDOWS\system32\USER32.dll
0x77e00000 0x440000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77f00000 0x310000 0xffff C:\WINDOWS\system32\inetrv\IISUTIL.dll
0x77160000 0x124000 0xffff C:\WINDOWS\system32\ole32.dll
0x5d760000 0x5000 0x2 C:\WINDOWS\system32\inetrv\rpcrref.dll
0x647b0000 0x24000 0x11 C:\WINDOWS\system32\IISRTL.dll
0x71c00000 0x18000 0x3d C:\WINDOWS\system32\WS2_32.dll
0x71bf0000 0x8000 0x33 C:\WINDOWS\system32\WS2HELP.dll
0x649f0000 0x8000 0x1 C:\WINDOWS\system32\inetrv\iisadmin.dll
0x5b900000 0x87000 0x1 C:\WINDOWS\system32\VSAPI.DLL
0x76a00000 0x18000 0x8 C:\WINDOWS\system32\ATL.DLL
0x770c0000 0x7d000 0x15 C:\WINDOWS\system32\OLEAUT32.dll
0x71c40000 0x53000 0xf C:\WINDOWS\system32\METAPI32.dll
0x5e0b0000 0xf000 0x1 C:\WINDOWS\system32\inetrv\COADMIN.dll
0x71430000 0x10000 0x2 C:\WINDOWS\system32\ADMINPROX.dll
0x648b0000 0x13d000 0x2 C:\WINDOWS\system32\inetrv\IISCFG.DLL
0x76c60000 0x20000 0x1 C:\WINDOWS\system32\MTWARTA.DLL
0x76f10000 0x2f000 0x7 C:\WINDOWS\system32\WLDAP32.dll
0x5ccf0000 0x10000 0x4 C:\WINDOWS\system32\SAMLIB.dll
0x76f90000 0x7e000 0x1 C:\WINDOWS\system32\CLBCatQ.DLL
0x77010000 0xc6000 0x1 C:\WINDOWS\system32\COMRes.dll
0x77b90000 0x8000 0x2 C:\WINDOWS\system32\VERSION.dll
0x620a0000 0x39000 0x1 C:\WINDOWS\system32\inetrv\metadatas.dll
0x77290000 0x49000 0xa C:\WINDOWS\system32\SHLWAPI.dll
0x0ff00000 0x2d000 0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000 0xb000 0x1 C:\WINDOWS\system32\PSAPI.DLL
0x77380000 0x7dd000 0x5 C:\WINDOWS\system32\SHELL32.dll
0x70ad0000 0xe6000 0x3 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x761b0000 0x98000 0xc C:\WINDOWS\system32\CRYPT32.dll
0x76190000 0x12000 0xe C:\WINDOWS\system32\MSASN1.dll
0x5b530000 0xd000 0x1 C:\WINDOWS\system32\inetrv\svcxext.dll
0x71f60000 0x4000 0x3 C:\WINDOWS\system32\Security.dll
0x76f90000 0x13000 0x1a C:\WINDOWS\system32\SECUR32.DLL
0x64830000 0x10000 0x1 C:\WINDOWS\system32\IISMAP.dll
0x5a120000 0x10000 0x2 C:\WINDOWS\system32\inetrv\Wamreg.dll
0x6b750000 0x78000 0x1 C:\WINDOWS\system32\inetrv\SMTPSVC.dll
0x643e0000 0x3e000 0x1 C:\WINDOWS\system32\inetrv\INFOCOMM.dll
0x63ec0000 0xf000 0x4 C:\WINDOWS\system32\inetrv\ISATQ.dll
0x01490000 0x3a000 0x1 C:\WINDOWS\system32\ODBC32.dll
0x70bc0000 0x90000 0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x762b0000 0x47000 0x1 C:\WINDOWS\system32\condlg32.dll
0x71bb0000 0x9000 0x2 C:\WINDOWS\system32\WSOCK32.dll
0x76ed0000 0x27000 0x6 C:\WINDOWS\system32\DNSAPI.dll
0x00ff0000 0xe000 0x4 C:\WINDOWS\system32\FCACHDLL.dll
0x5cfd0000 0x6000 0x7 C:\WINDOWS\system32\RWMMH.dll
0x69530000 0xc000 0x8 C:\WINDOWS\system32\exstrace.dll
0x5b7e0000 0x6000 0xb C:\WINDOWS\system32\STAXMEM.dll
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 0xba000 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\wshtcpip.dll
0x76bb0000 0x2b000 0x1 C:\WINDOWS\system32\wintrust.dll
0x76c10000 0x28000 0x1 C:\WINDOWS\system32\imagehlp.dll
0x63eb0000 0x7000 0x1 C:\WINDOWS\system32\inetrv\iscomlog.dll
0x76cf0000 0x17000 0x5 C:\WINDOWS\system32\iphlpapi.dll
0x5c870000 0x35000 0x1 C:\WINDOWS\system32\inetrv\seo.dll
0x76d00000 0x27000 0x1 C:\WINDOWS\system32\netman.dll
0x76cd0000 0x17000 0x1 C:\WINDOWS\system32\WPRAPI.dll
0x764f0000 0x32000 0x1 C:\WINDOWS\system32\ACTIVEDS.dll
0x76dc0000 0x26000 0x1 C:\WINDOWS\system32\adsldpe.dll
0x76b80000 0x2d000 0x1 C:\WINDOWS\system32\credui.dll
0x76e30000 0xb000 0x4 C:\WINDOWS\system32\rtutils.dll
```

# Windows PowerShell

```
0x76e30000      0xb000      0x4 C:\WINDOWS\system32\rtutils.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
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      0x8000      0x1 C:\WINDOWS\system32\WTSAPI32.dll
0x76260000      0x10000      0x2 C:\WINDOWS\system32\WINSTA.dll
0x69750000      0x108000      0x1 C:\WINDOWS\system32\ESNT.dll
0x730a0000      0x9000      0x1 C:\WINDOWS\system32\WZCSAPI.DLL
0x02180000      0x79000      0x1 C:\WINDOWS\system32\inetrv\aqueue.dll
0x76f80000      0x5000      0x1 C:\WINDOWS\system32\rasadhlp.dll
0x71ca0000      0x56000      0x1 C:\WINDOWS\system32\kerberos.dll
0x766e0000      0xc000      0x1 C:\WINDOWS\system32\cryptdll.dll
0x02460000      0xd000      0x1 C:\WINDOWS\system32\inetrv\ntfsdrv.dll
0x5e6c0000      0xb000      0x1 C:\WINDOWS\system32\POP3Server\p3Store.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	0x35000	0xffff	C:\WINDOWS\system32\wbem\wmiprvse.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	0xa4000	0xffff	C:\WINDOWS\system32\RPCRT4.dll
0x77d00000	0x8f000	0xffff	C:\WINDOWS\system32\USER32.dll
0x77c00000	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
0x75550000	0x71000	0xffff	C:\WINDOWS\system32\wbem\FastProx.dll
0x780c0000	0x61000	0xffff	C:\WINDOWS\system32\MSVCP60.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	0xc000	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\wbemsvc.dll
0x74e60000	0x1b000	0x1	C:\WINDOWS\system32\wbem\wmiutils.dll
0x72fa0000	0x26000	0x1	C:\WINDOWS\system32\wbem\wmiprov.dll
0x76cc0000	0x5000	0x1	C:\WINDOWS\system32\WMI.dll
0x76c60000	0x20000	0x1	C:\WINDOWS\system32\NTMARTA.DLL
0x5ccf0000	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	0x2f000	0x1	C:\WINDOWS\system32\wbem\PROVTHRD.dll
0x60020000	0x10000	0x1	C:\WINDOWS\system32\msvcirt.dll
0x71bb0000	0x9000	0x1	C:\WINDOWS\system32\WSOCK32.dll
0x006e0000	0x15000	0x1	C:\WINDOWS\system32\ServerAppliance\saevfltr.dll
0x76e30000	0xb000	0x1	C:\WINDOWS\system32\rtutils.dll
0x00c80000	0x15000	0x1	C:\WINDOWS\system32\ServerAppliance\appsrvcs.dll
0x71b20000	0x43000	0x4	C:\WINDOWS\system32\mswsock.dll
0x76f80000	0x5000	0x1	C:\WINDOWS\system32\rasadhlp.dll



Windows PowerShell

0x76f800000x50000x1C:\WINDOWS\system32\rasadhlp.dll

0x71ae00000x80000x1C:\WINDOWS\system32\wshtcpip.dll

0x71ca00000x560000x1C:\WINDOWS\system32\kerberos.dll

0x766e00000xc0000x1C:\WINDOWS\system32\cryptdll.dll

0x761900000x120000x1C:\WINDOWS\system32\MSASN1.dll

\*\*\*\*\*

POP3Svc.exe pid: 2260

Command line : c:\windows\system32\pop3server\pop3svc.exe

Base	Size	LoadCount	Path
0x81000000	0xb000	0xffff	C:\WINDOWS\system32\POP3Server\pop3svc.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	0xa4000	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
0x71c00000	0x18000	0xffff	C:\WINDOWS\system32\WS2_32.dll
0x71bf0000	0x8000	0xffff	C:\WINDOWS\system32\WS2HELP.dll
0x71b20000	0x43000	0xffff	C:\WINDOWS\system32\MSWSOCK.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	0xf000	0x1	C:\WINDOWS\system32\POP3Server\Pop3Auth.dll
0x76df0000	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\DNSAPI.dll
0x78ad0000	0xe6000	0x2	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_8A17450B\comctl32.dll
0x76c90000	0x24000	0x1	C:\WINDOWS\system32\msv1_0.dll
0x5e6d0000	0x19000	0x1	C:\WINDOWS\system32\POP3Server\P3Admin.dll
0x780c0000	0x61000	0x1	C:\WINDOWS\system32\MSVCP60.dll
0x71300000	0x47000	0x1	C:\WINDOWS\system32\inetsrv\adsis.dll
0x72800000	0xf4000	0x2	C:\WINDOWS\system32\WFC42u.DLL
0x647b0000	0x2d000	0x2	C:\WINDOWS\system32\IISRTL.dll
0x64760000	0x37000	0x1	C:\WINDOWS\system32\inetsrv\iisui.dll
0x70b00000	0x90000	0x1	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_5.82.0.0_x-ww_8A69BA05\COMCTL32.dll
0x71bd0000	0x11000	0x1	C:\WINDOWS\system32\WPR.dll
0x761b0000	0x98000	0x2	C:\WINDOWS\system32\CRYPT32.dll
0x76190000	0x12000	0x1	C:\WINDOWS\system32\MSASN1.dll
0x71430000	0x10000	0x1	C:\WINDOWS\system32\ADMPROX.DLL
0x08fd0000	0x2d000	0x1	C:\WINDOWS\system32\rsaenh.dll
0x76b70000	0xb000	0x1	C:\WINDOWS\system32\PSAPI.DLL
0x75da0000	0xba000	0x1	C:\WINDOWS\system32\SXS.DLL
0x5c150000	0x2e000	0x1	C:\WINDOWS\system32\inetsrv\smtpadm.dll
0x5c140000	0x6000	0x1	C:\WINDOWS\system32\SMTPAPI.dll
0x69530000	0xc000	0x1	C:\WINDOWS\system32\extracex.dll
0x5b7e0000	0x6000	0x1	C:\WINDOWS\system32\STAXMEM.dll
0x71bb0000	0x9000	0x1	C:\WINDOWS\system32\WSOCK32.dll
0x71ae0000	0x8000	0x1	C:\WINDOWS\system32\wshtcpip.dll

\*\*\*\*\*

cmd.exe pid: 2076

Command line : "C:\WINDOWS\system32\cmd.exe"

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

```
Base          Size      LoadCount Path
-----
0x4ad00000    0x60000    0xfffff C:\WINDOWS\system32\cmd.exe
0x77f40000    0xba000    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\MPR.dll
*****
mdd.exe pid: 3468
Command line : mdd.exe -o dc-memdump.bin

Base          Size      LoadCount Path
-----
0x00400000    0x19000    0xfffff C:\ITShare\mdd.exe
0x77f40000    0xba000    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
0x77290000    0x49000    0xfffff C:\WINDOWS\system32\SHLWAPI.dll
0x70ad0000    0xc6000    0x1 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.100.0_x-ww_84174508\comctl32.dll
0x0ff40000    0x2d000    0x1 C:\WINDOWS\system32\rsaenh.dll
0x76b70000    0xb000    0x1 C:\WINDOWS\system32\PSAPI.DLL
PS C:\Users\rodri\Downloads\practica3>
```

**Preguntas de verificación del laboratorio**

- ¿Qué hora inicia el proceso explorer.exe?: 21:32:38
- ¿Qué hora inicia el proceso svchost.exe?: 20:19:12
- ¿Cuál es el nombre del proceso PID: 420?: CSRSS.EXE
- ¿Cuál es el nombre del proceso PID: 932?: SVCHOST.EXE

**PARTE PRÁCTICA**

PARTE PRACTICA: Se trabajara con 1000

1) Almacenar Bits:  $128K \times 4 \Rightarrow 128000 \times 4 = 512000 \text{ Bits}$

2) Almacenar Bits:  $10G \times 16 \Rightarrow 10 \cdot 1000^3 \times 16 = 160000000000 \text{ Bits}$

3) Localidades con 32 líneas de dirección:  $2^{32} = 4294967296 \times 10^9$   
Localidades de memoria almacenadas

4) Localidades con 1024:  $2^{1024} = 17976931349 \times 10^{308}$   
Localidades de memoria almacenadas

5) Cuantas localidades de memoria se pueden direccionar con 64 líneas de direccionar:  $2^{64} = 18446744073709551616$  localidades

6) Cuantas líneas de dirección se necesita para una memoria ROM de  $512M \times 8$ :  $\frac{\ln(512 \cdot 1000^2)}{\ln(2)} = 29$  líneas

7) Cuantas líneas de dirección se necesitan para una memoria ROM de  $128M \times 128$ :  $\frac{\ln(128 \cdot 1000^2)}{\ln(2)} = 27$  líneas

8) Cuantos bits en total puede almacenar una memoria RAM  $128M \times 4$ , de el resultado en gigabytes:  $128 \cdot 1000^2 \times 4 = 512000000 \text{ Bits}$   
De bits a Bytes:  $\frac{512000000}{8} = 64000000$

De Bytes a gigabytes:  $\frac{64000000}{1000^3} = 0,064 \text{ gigabytes}$

9) Cuantos bits en total puede almacenar una memoria RAM  $64M \times 64$  de el resultado en teras:  $64 \cdot 1000^2 \times 64 = 4096000000 \text{ Bits}$

Bits a Bytes:  $\frac{4096000000}{8} = 512000000$  | Bytes a Teras:

$\frac{512000000}{1000^4} = 0,000512 \text{ Teras}$



Tema:

Fecha:

Nº:

TOP

10) Cuantos Bits en total puede almacenar una memoria RAM 64M x 64  
de el resultado en TeraBytes

$$64 \cdot 1000^2 \times 64 = 4096\,000\,000$$

$$\text{Bits a Bytes: } \frac{4096\,000\,000}{8} = 512\,000\,000 \text{ Bytes}$$

$$\text{Bytes a Terabyte: } \frac{512\,000\,000}{1000^4} = 0,000512 \text{ Terabytes}$$