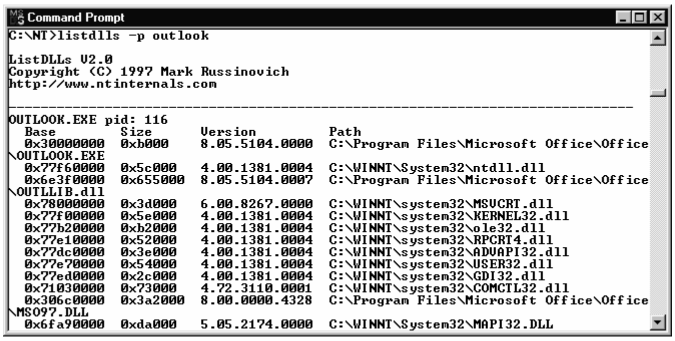
Unit OS5: Memory Management

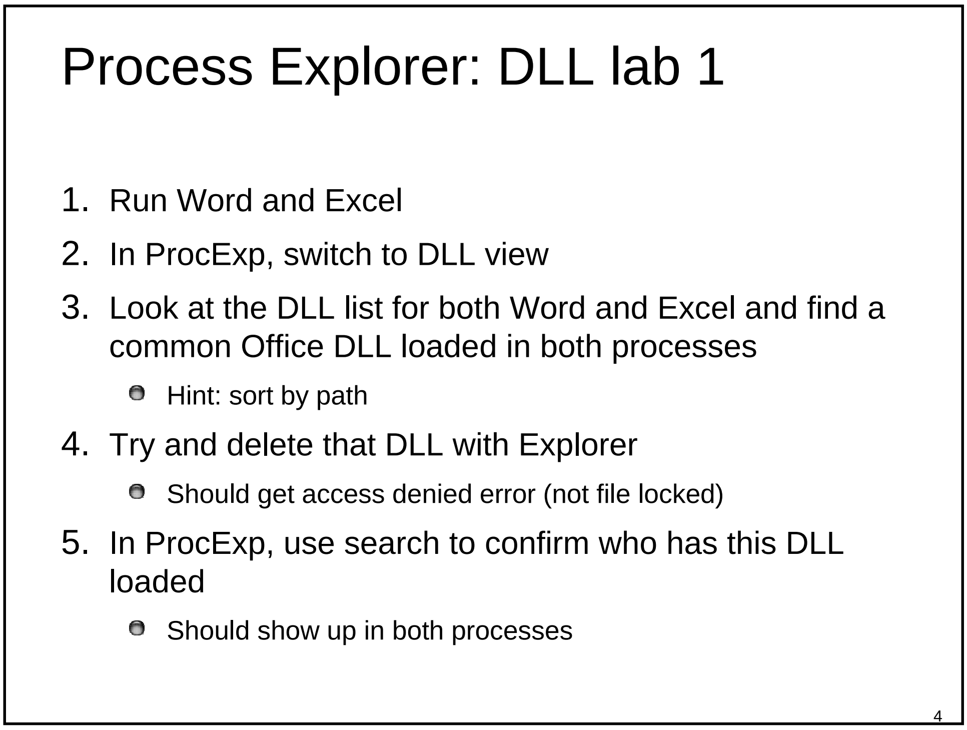
5.5. Demonstrations

DLL Usage

- To diagnose DLL conflicts, you need to know which DLLs were loaded and from where
  - Pviewer & pview & tlist lists the loaded DLLs, but not the path (e.g. type “tlist explorer”)
  - Dependency Walker can trace DLL loads
  - Process Explorer or listdlls from www.sysinternals.com lists full path

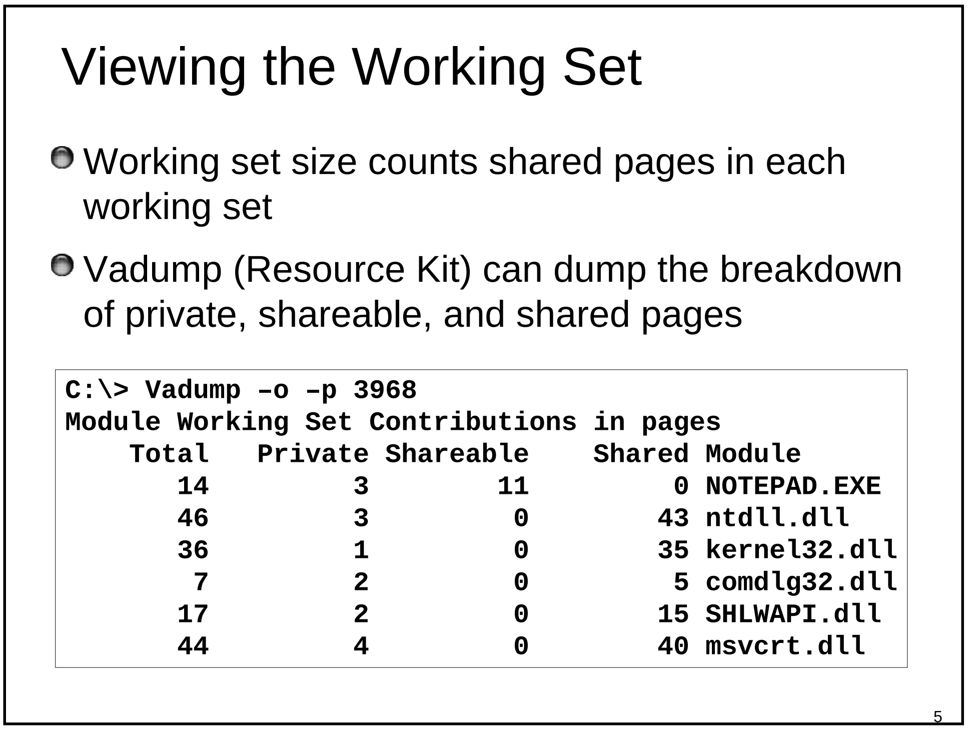


```
C:\NT>listdlls -p outlook

ListDLLs V2.0
Copyright (C) 1997 Mark Russinovich
http://www.ntinternals.com

-------------------------------------------------------------------------------
OUTLOOK.EXE pid: 116
  Base        Size      Version         Path
  0x30000000  0xb000    8.05.5104.0000  C:\Program Files\Microsoft Office\Office
\OUTLOOK.EXE
  0x77f60000  0x5c000   4.00.1381.0004  C:\WINNT\System32\ntdll.dll
  0x6e3f0000  0x655000  8.05.5104.0007  C:\Program Files\Microsoft Office\Office
\OUTLLIB.dll
  0x78000000  0x3d000   6.00.8267.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0004  C:\WINNT\system32\KERNEL32.dll
  0x77b20000  0xb2000   4.00.1381.0004  C:\WINNT\system32\ole32.dll
  0x77e10000  0x52000   4.00.1381.0004  C:\WINNT\system32\RPCRT4.dll
  0x77dc0000  0x3e000   4.00.1381.0004  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x54000   4.00.1381.0004  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0004  C:\WINNT\system32\GDI32.dll
  0x71030000  0x73000   4.72.3110.0001  C:\WINNT\system32\COMCTL32.dll
  0x306c0000  0x3a2000  8.00.0000.4328  C:\Program Files\Microsoft Office\Office
\MSO97.DLL
  0x6fa90000  0xda000   5.05.2174.0000  C:\WINNT\System32\MAPI32.DLL
```



Process Explorer: DLL lab 1

1. Run Word and Excel
2. In ProcExp, switch to DLL view
3. Look at the DLL list for both Word and Excel and find a common Office DLL loaded in both processes
   - Hint: sort by path
4. Try and delete that DLL with Explorer
   - Should get access denied error (not file locked)
5. In ProcExp, use search to confirm who has this DLL loaded
   - Should show up in both processes



Viewing the Working Set

- Working set size counts shared pages in each working set
- Vadump (Resource Kit) can dump the breakdown of private, shareable, and shared pages

```
C:\> Vadump –o –p 3968
Module Working Set Contributions in pages
    Total   Private Shareable    Shared Module
       14         3        11         0 NOTEPAD.EXE
       46         3         0        43 ntdll.dll
       36         1         0        35 kernel32.dll
        7         2         0         5 comdlg32.dll
       17         2         0        15 SHLWAPI.dll
       44         4         0        40 msvcrt.dll
```

Process Memory Information

Task Manager Processes tab

① **“Mem Usage” = physical memory used by process (working set <u>size</u>, not working set limit)**

- ◆ **Note: shared pages are counted in each process**

② **“VM Size” = private (not shared) committed virtual space in processes == process’s paging file allocation**

③ **“Mem Usage” in status bar is <u>not</u> total of “Mem Usage” column (see later slide)**

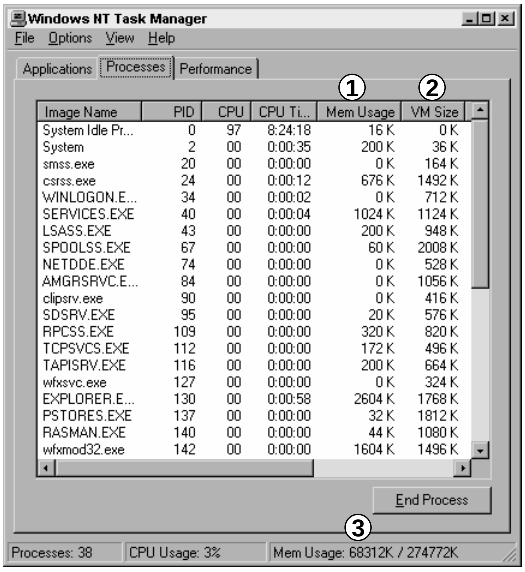


Image Name	PID	CPU	CPU Ti...	Mem Usage	VM Size
System Idle Pr...	0	97	8:24:18	16 K	0 K
System	2	00	0:00:35	200 K	36 K
smss.exe	20	00	0:00:00	0 K	164 K
csrss.exe	24	00	0:00:12	676 K	1492 K
WINLOGON.E...	34	00	0:00:02	0 K	712 K
SERVICES.EXE	40	00	0:00:04	1024 K	1124 K
LSASS.EXE	43	00	0:00:00	200 K	948 K
SPOOLSS.EXE	67	00	0:00:00	60 K	2008 K
NETDDE.EXE	74	00	0:00:00	0 K	528 K
AMGRSRVC.E...	84	00	0:00:00	0 K	1056 K
clipsrv.exe	90	00	0:00:00	0 K	416 K
SDSRV.EXE	95	00	0:00:00	20 K	576 K
RPCSS.EXE	109	00	0:00:00	320 K	820 K
TCPSVCS.EXE	112	00	0:00:00	172 K	496 K
TAPISRV.EXE	116	00	0:00:00	200 K	664 K
wfxsvc.exe	127	00	0:00:00	0 K	324 K
EXPLORER.E...	130	00	0:00:58	2604 K	1768 K
PSTORES.EXE	137	00	0:00:00	32 K	1812 K
RASMAN.EXE	140	00	0:00:00	44 K	1080 K
wfxmod32.exe	142	00	0:00:00	1604 K	1496 K

Processes: 38 | CPU Usage: 3% | Mem Usage: 68312K / 274772K

Screen snapshot from:
Task Manager | Processes tab

6

Process Memory Information

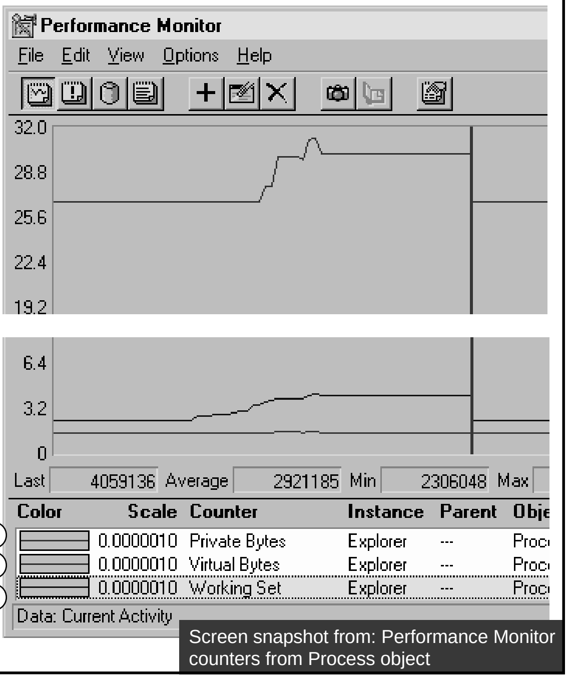
PerfMon - Process Object

⑦ “Virtual Bytes” = committed + reserved virtual space, including shared pages

① “Working Set” = working set size (not limit) (physical)

② “Private Bytes” = private virtual space (same as “VM Size” from Task Manager Processes list)

- Also: In Threads object, look for threads in Transition state - evidence of swapping (usually caused by severe memory pressure)



Last 4059136 Average 2921185 Min 2306048 Max

Color	Scale	Counter	Instance	Parent	Obje
▭	0.0000010	Private Bytes	Explorer	---	Proc
▭	0.0000010	Virtual Bytes	Explorer	---	Proc
▭	0.0000010	Working Set	Explorer	---	Proc

Data: Current Activity

Screen snapshot from: Performance Monitor counters from Process object

Memory Management Information

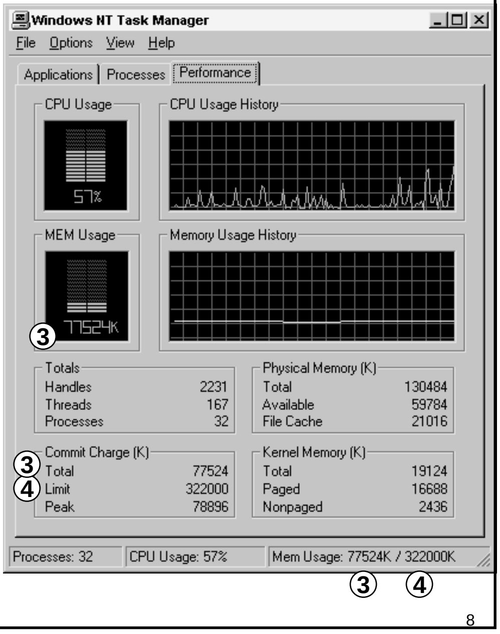
Task Manager
Performance tab

③ Total committed private virtual memory (total of “VM Size” in process tab + Kernel Memory Paged)

- not all of this space has actually been used in the paging files; it is “how much would be used if it was all paged out”
- “Commit charge limit” = sum of physical memory available for processes + current total size of paging file(s)

④ does not reflect true maximum page file sizes (expansion)

- when “total” reaches “limit”, further VirtualAlloc attempts by any process will fail



Totals
Handles 2231
Threads 167
Processes 32

Physical Memory (K)
Total 130484
Available 59784
File Cache 21016

Commit Charge (K)
Total 77524
Limit 322000
Peak 78896

Kernel Memory (K)
Total 19124
Paged 16688
Nonpaged 2436

Processes: 32 | CPU Usage: 57% | Mem Usage: 77524K / 322000K

③ ④

8