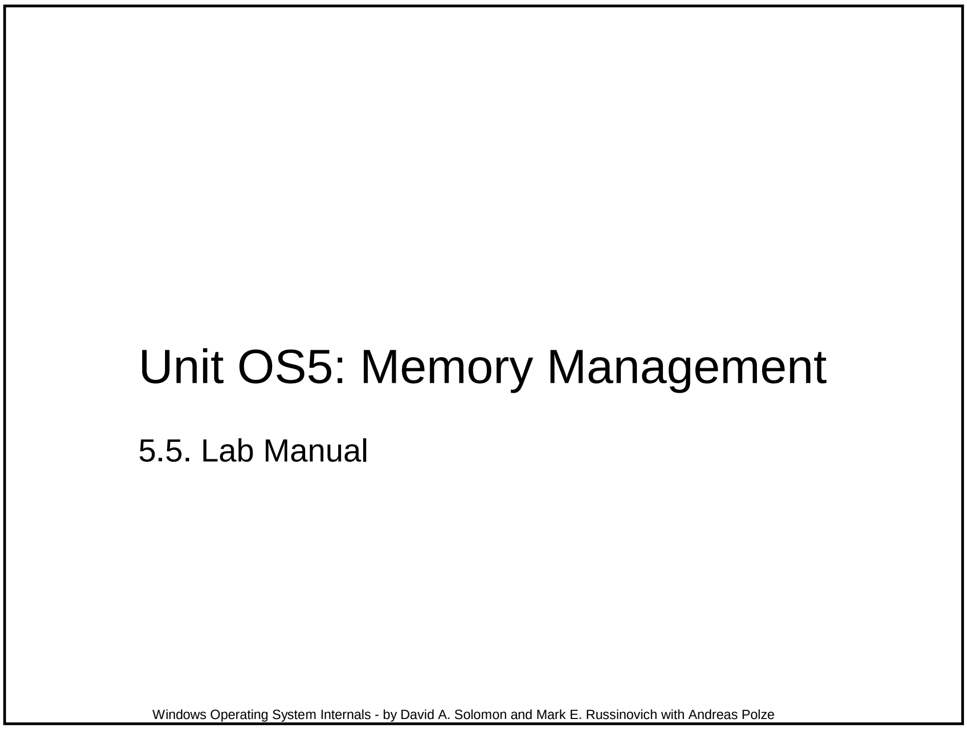
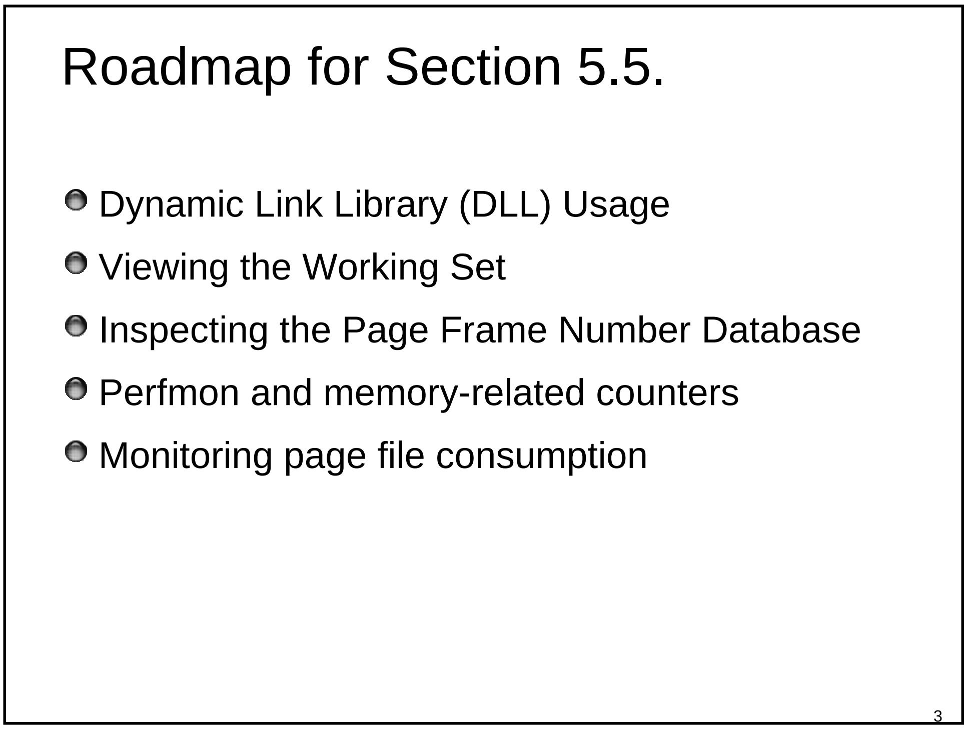


Unit OS5: Memory Management

5.5. Lab Manual

Windows Operating System Internals - by David A. Solomon and Mark E. Russinovich with Andreas Polze

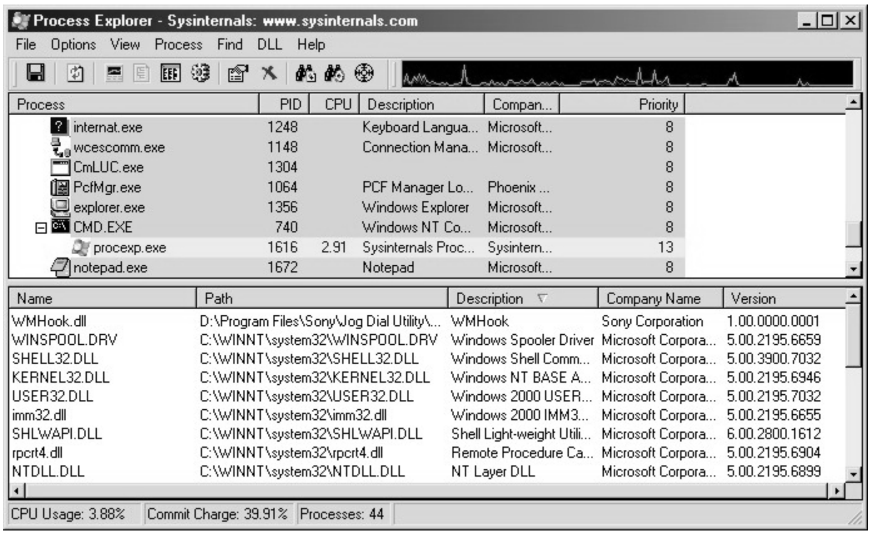


Roadmap for Section 5.5.

- Dynamic Link Library (DLL) Usage
- Viewing the Working Set
- Inspecting the Page Frame Number Database
- Perfmon and memory-related counters
- Monitoring page file consumption

3

Viewing DLLs and Memory Mapped Files



Process	PID	CPU	Description	Compan...	Priority
internat.exe	1248		Keyboard Langua...	Microsoft...	8
wcescomm.exe	1148		Connection Mana...	Microsoft...	8
CmLUC.exe	1304				8
PcfMgr.exe	1064		PCF Manager Lo...	Phoenix ...	8
explorer.exe	1356		Windows Explorer	Microsoft...	8
CMD.EXE	740		Windows NT Co...	Microsoft...	8
procexp.exe	1616	2.91	Sysinternals Proc...	Sysintern...	13
notepad.exe	1672		Notepad	Microsoft...	8

Name	Path	Description	Company Name	Version
WMHook.dll	D:\Program Files\Sony\Jog Dial Utility\...	WMHook	Sony Corporation	1.00.0000.0001
WINSPOOL.DRV	C:\WINNT\system32\WINSPOOL.DRV	Windows Spooler Driver	Microsoft Corpora...	5.00.2195.6659
SHELL32.DLL	C:\WINNT\system32\SHELL32.DLL	Windows Shell Comm...	Microsoft Corpora...	5.00.3900.7032
KERNEL32.DLL	C:\WINNT\system32\KERNEL32.DLL	Windows NT BASE A...	Microsoft Corpora...	5.00.2195.6946
USER32.DLL	C:\WINNT\system32\USER32.DLL	Windows 2000 USER...	Microsoft Corpora...	5.00.2195.7032
imm32.dll	C:\WINNT\system32\imm32.dll	Windows 2000 IMM3...	Microsoft Corpora...	5.00.2195.6655
SHLWAPI.DLL	C:\WINNT\system32\SHLWAPI.DLL	Shell Light-weight Utili...	Microsoft Corpora...	6.00.2800.1612
rpcrt4.dll	C:\WINNT\system32\rpcrt4.dll	Remote Procedure Ca...	Microsoft Corpora...	5.00.2195.6904
NTDLL.DLL	C:\WINNT\system32\NTDLL.DLL	NT Layer DLL	Microsoft Corpora...	5.00.2195.6899

CPU Usage: 3.88% Commit Charge: 39.91% Processes: 44

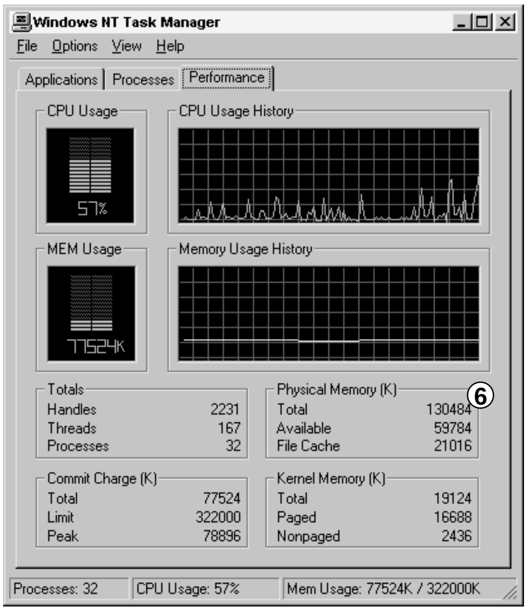
Prefetch Lab

- Lab
  - Run Filemon – set filter as Notepad.exe
  - Make a temporary directory somewhere (e.g. \temp)
  - Run “Notepad \temp\x.y”
  - Exit Notepad
  - Run Notepad again
  - In Filemon log, find creation of .PF file after first run, then use of new .PF in 2nd run

Memory Management Information

Task Manager Performance tab

- ⑥ “Available” = sum of free, standby, and zero page lists (physical)
- Majority are likely standby pages
- Windows 2000/XP/Server 2003: count of shareable pages on standby, modified, and modified nowrite list are included in what was “File Cache” in NT4
  - New name is “System Cache”



CPU Usage: 57%

MEM Usage: 77524K

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

Screen snapshot from:
Task Manager | Performance tab

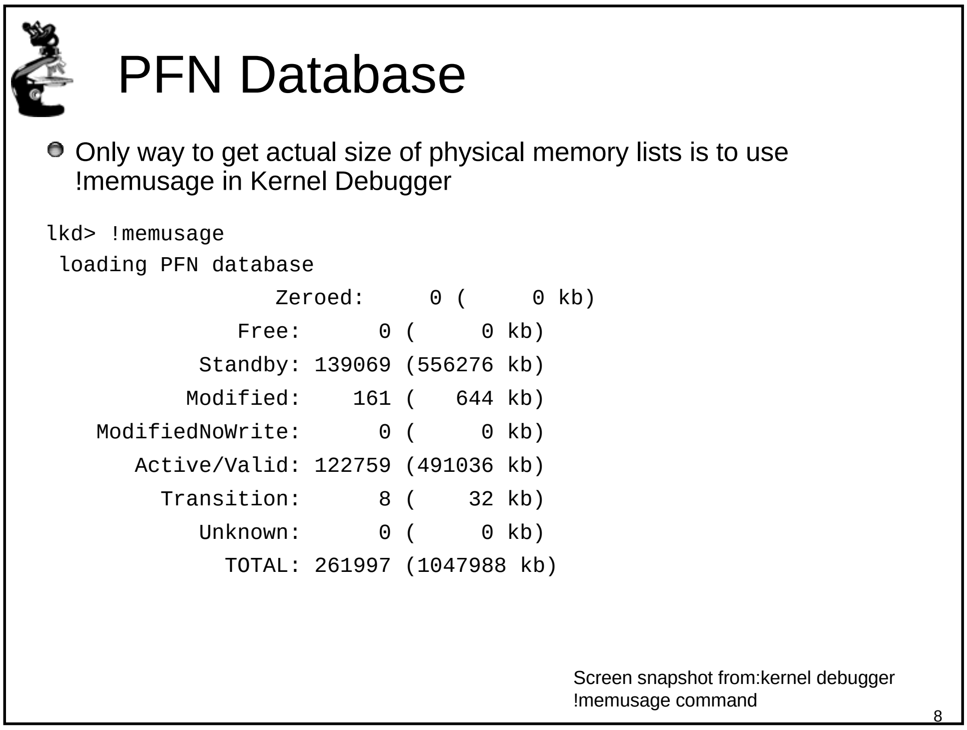
PFN Database

- PFN = Page Frame Number
  = Physical Page Number
- PFN Database keeps track of the state of each physical page
  - An array of structures, one element per physical page
  - Maintains reference and share counts for pages in working sets
  - Structure elements implement forward and backward links for free, modified, standby, zero, and bad page lists
  - Does not reflect memory not managed by NT (e.g. adapter ram)

```
kd> !pte ff709348
!pte ff709348
FF709348  - PDE at C0300FF4    PTE at C03FDC24
          contains 00410063  contains 0049E063
          pfn 00410 DA--KWV  pfn 0049E DA--KWV
kd> !pfn 410
!pfn 410
    PFN address FFBCC180
    flink       00000000  blink / share count 000000B0  pteaddress C0300FF4
    reference count 0001                                 color 0
    restore pte 00000000  containing page        00030  Active
```

Screen snapshot from: kernel debugger !pte command
use resulting displayed PFN on !pfn command

7

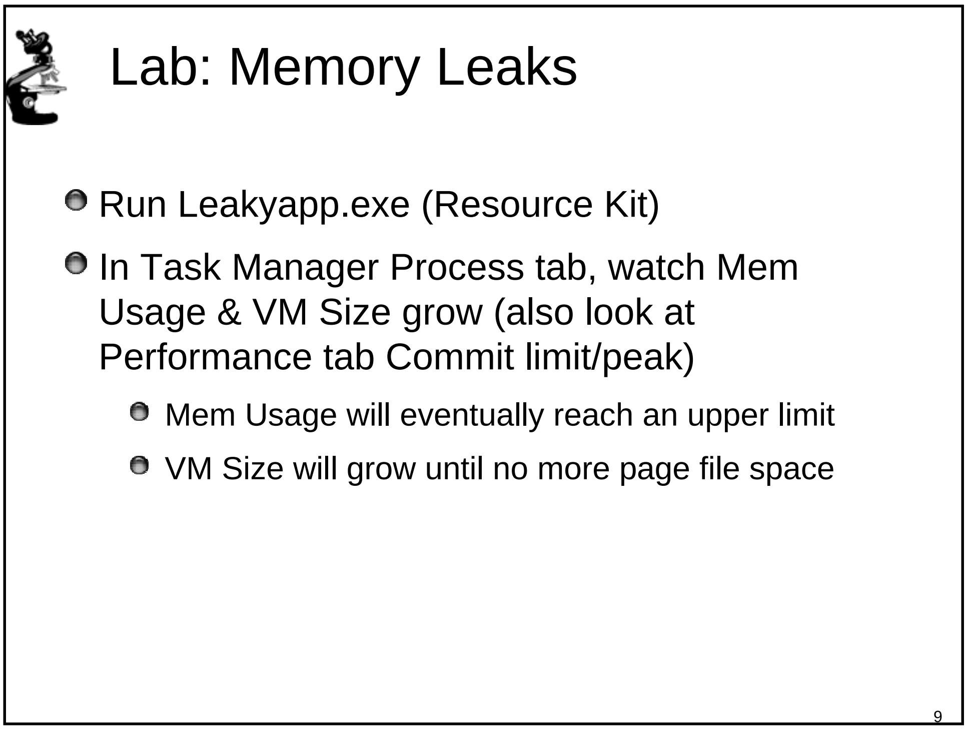


PFN Database

- Only way to get actual size of physical memory lists is to use !memusage in Kernel Debugger

```
lkd> !memusage
 loading PFN database
                 Zeroed:      0 (      0 kb)
                  Free:      0 (      0 kb)
               Standby: 139069 (556276 kb)
              Modified:    161 (    644 kb)
       ModifiedNoWrite:      0 (      0 kb)
          Active/Valid: 122759 (491036 kb)
            Transition:      8 (     32 kb)
               Unknown:      0 (      0 kb)
                 TOTAL: 261997 (1047988 kb)
```

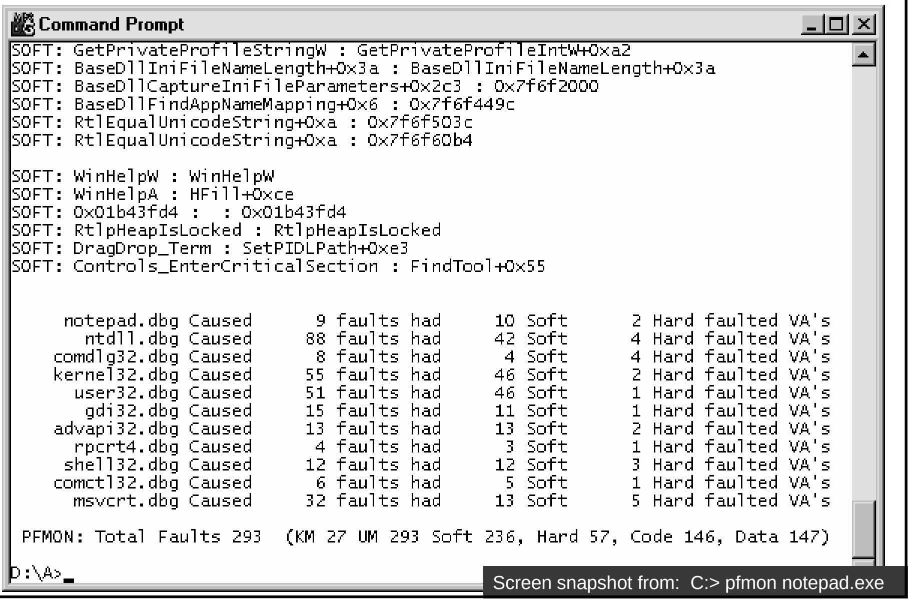
Screen snapshot from:kernel debugger
!memusage command



Lab: Memory Leaks

- Run Leakyapp.exe (Resource Kit)
- In Task Manager Process tab, watch Mem Usage & VM Size grow (also look at Performance tab Commit limit/peak)
  - Mem Usage will eventually reach an upper limit
  - VM Size will grow until no more page file space

Page Fault Monitor (pfmon)



```
SOFT: GetPrivateProfileStringW : GetPrivateProfileIntW+0xa2
SOFT: BaseDllIniFileNameLength+0x3a : BaseDllIniFileNameLength+0x3a
SOFT: BaseDllCaptureIniFileParameters+0x2c3 : 0x7f6f2000
SOFT: BaseDllFindAppNameMapping+0x6 : 0x7f6f449c
SOFT: RtlEqualUnicodeString+0xa : 0x7f6f503c
SOFT: RtlEqualUnicodeString+0xa : 0x7f6f60b4

SOFT: WinHelpW : WinHelpW
SOFT: WinHelpA : HFill+0xce
SOFT: 0x01b43fd4 :  : 0x01b43fd4
SOFT: RtlpHeapIsLocked : RtlpHeapIsLocked
SOFT: DragDrop_Term : SetPIDLPath+0xe3
SOFT: Controls_EnterCriticalSection : FindTool+0x55


     notepad.dbg Caused      9 faults had     10 Soft      2 Hard faulted VA's
       ntdll.dbg Caused     88 faults had     42 Soft      4 Hard faulted VA's
    comdlg32.dbg Caused      8 faults had      4 Soft      4 Hard faulted VA's
    kernel32.dbg Caused     55 faults had     46 Soft      2 Hard faulted VA's
      user32.dbg Caused     51 faults had     46 Soft      1 Hard faulted VA's
       gdi32.dbg Caused     15 faults had     11 Soft      1 Hard faulted VA's
    advapi32.dbg Caused     13 faults had     13 Soft      2 Hard faulted VA's
      rpcrt4.dbg Caused      4 faults had      3 Soft      1 Hard faulted VA's
     shell32.dbg Caused     12 faults had     12 Soft      3 Hard faulted VA's
    comctl32.dbg Caused      6 faults had      5 Soft      1 Hard faulted VA's
      msvcrt.dbg Caused     32 faults had     13 Soft      5 Hard faulted VA's

 PFMON: Total Faults 293  (KM 27 UM 293 Soft 236, Hard 57, Code 146, Data 147)

D:\A>_
```

Screen snapshot from: C:> pfmon notepad.exe