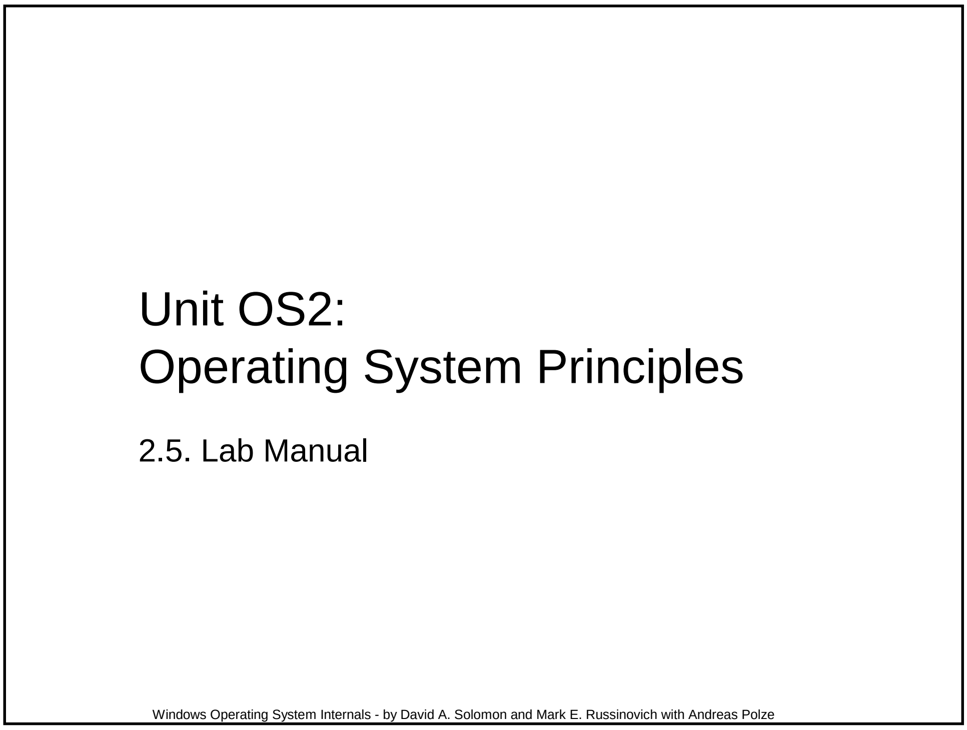
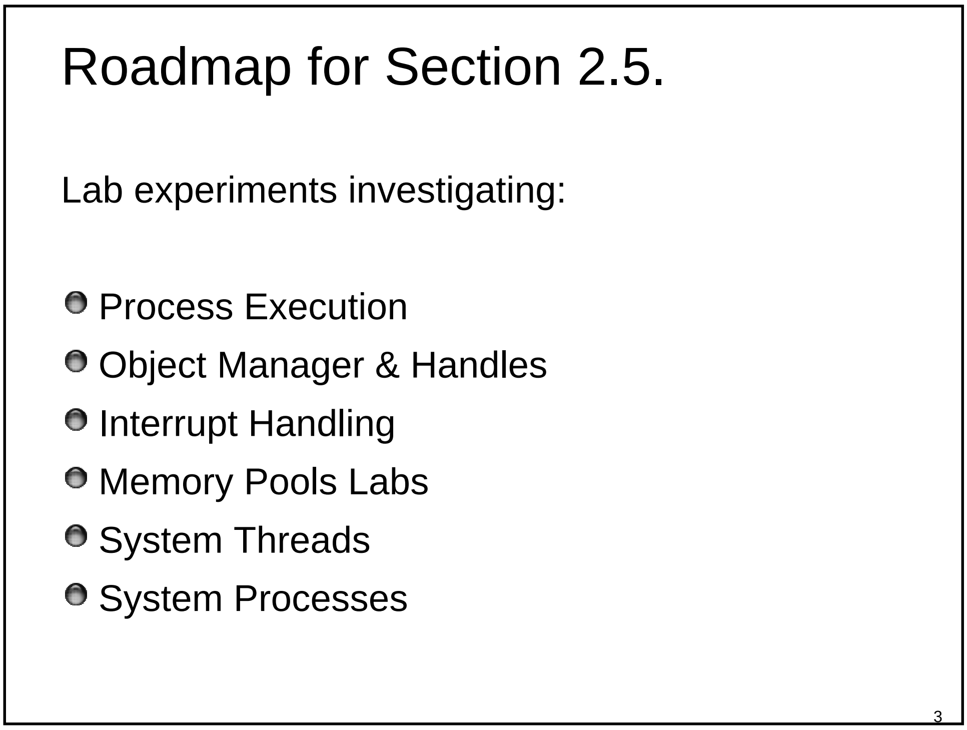


Unit OS2: Operating System Principles

2.5. Lab Manual

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

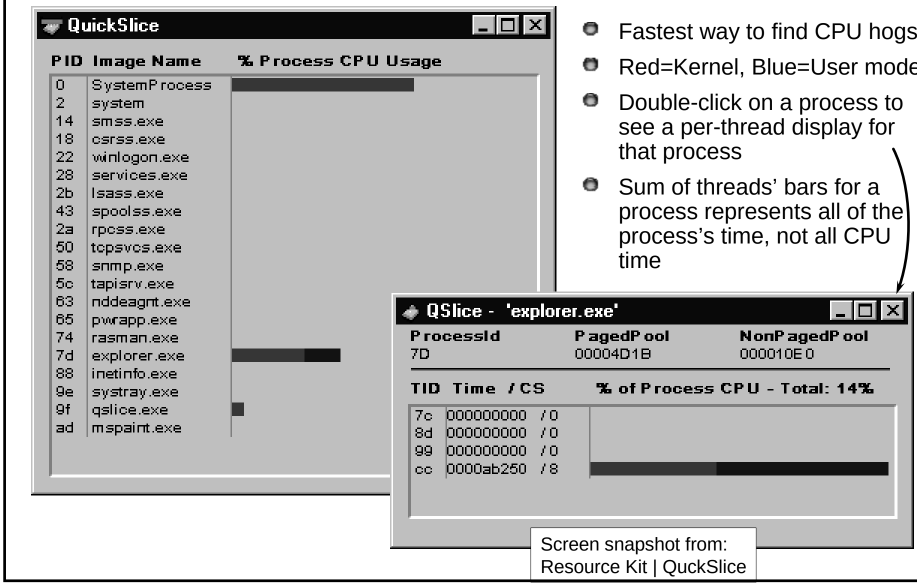


Roadmap for Section 2.5.

Lab experiments investigating:

- Process Execution
- Object Manager & Handles
- Interrupt Handling
- Memory Pools Labs
- System Threads
- System Processes

Thread Activity with QuickSlice



PID	Image Name	% Process CPU Usage
0	SystemProcess	
2	system	
14	smss.exe	
18	csrss.exe	
22	winlogon.exe	
28	services.exe	
2b	lsass.exe	
43	spoolss.exe	
2a	rpcss.exe	
50	tcpsvcs.exe	
58	snmp.exe	
5c	tapisrv.exe	
63	nddeagnt.exe	
65	pwrapp.exe	
74	rasman.exe	
7d	explorer.exe	
88	inetinfo.exe	
9e	systray.exe	
9f	qslice.exe	
ad	mspaint.exe	

ProcessId	PagedPool	NonPagedPool
7D	00004D1B	000010E0

TID	Time / CS	% of Process CPU - Total: 14%
7c	000000000 / 0	
8d	000000000 / 0	
99	000000000 / 0	
cc	0000ab250 / 8	

- Fastest way to find CPU hogs
- Red=Kernel, Blue=User mode
- Double-click on a process to see a per-thread display for that process
- Sum of threads' bars for a process represents all of the process's time, not all CPU time

Screen snapshot from:
Resource Kit | QuckSlice

Process Info with Task Manager

- Processes tab: List of processes
- Applications tab: List of top level visible windows

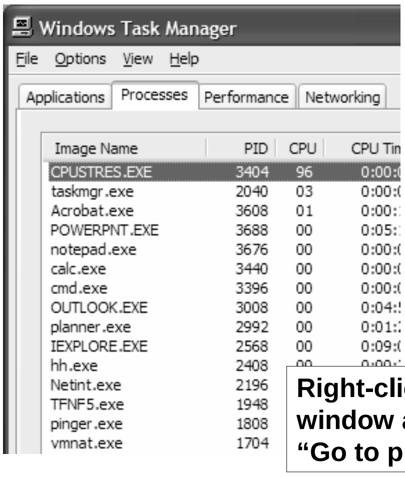
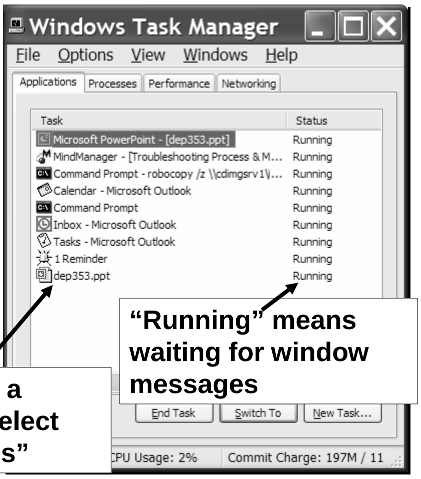


Image Name	PID	CPU	CPU Tin
CPUSTRES.EXE	3404	96	0:00:(
taskmgr.exe	2040	03	0:00:(
Acrobat.exe	3608	01	0:00::
POWERPNT.EXE	3688	00	0:05::
notepad.exe	3676	00	0:00:(
calc.exe	3440	00	0:00:(
cmd.exe	3396	00	0:00:(
OUTLOOK.EXE	3008	00	0:04:!
planner.exe	2992	00	0:01::
IEXPLORE.EXE	2568	00	0:09:(
hh.exe	2408	00	0:00::
Netint.exe	2196		
TFNF5.exe	1948		
pinger.exe	1808		
vmnat.exe	1704		



Task	Status
Microsoft PowerPoint - [dep353.ppt]	Running
MindManager - [Troubleshooting Process & M...	Running
Command Prompt - robocopy /z \\cdimgsrv1\j...	Running
Calendar - Microsoft Outlook	Running
Command Prompt	Running
Inbox - Microsoft Outlook	Running
Tasks - Microsoft Outlook	Running
1 Reminder	Running
dep353.ppt	Running

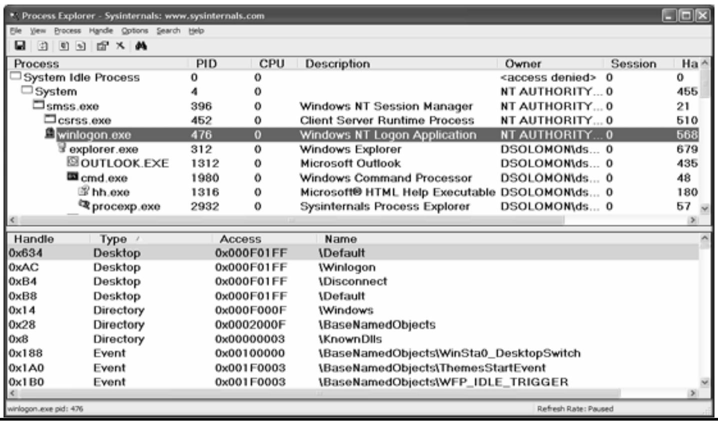
CPU Usage: 2%   Commit Charge: 197M / 11

Right-click on a window and select "Go to process"

"Running" means waiting for window messages

Process Details with Process Explorer

- "Super Task Manager"
  - Shows full image path, command line, environment variables, parent process, security access token, open handles, loaded DLLs & mapped files


Process Explorer - Sysinternals: www.sysinternals.com
File View Process Handle Options Search Help
winlogon.exe pid: 476
Refresh Rate: Paused

Process	PID	CPU	Description	Owner	Session	Ha
System Idle Process	0	0		<access denied>	0	0
System	4	0		NT AUTHORITY...	0	455
smss.exe	396	0	Windows NT Session Manager	NT AUTHORITY...	0	21
csrss.exe	452	0	Client Server Runtime Process	NT AUTHORITY...	0	510
winlogon.exe	476	0	Windows NT Logon Application	NT AUTHORITY...	0	568
explorer.exe	312	0	Windows Explorer	DSOLOMON\ds...	0	679
OUTLOOK.EXE	1312	0	Microsoft Outlook	DSOLOMON\ds...	0	435
cmd.exe	1980	0	Windows Command Processor	DSOLOMON\ds...	0	48
hh.exe	1316	0	Microsoft® HTML Help Executable	DSOLOMON\ds...	0	180
procexp.exe	2932	0	Sysinternals Process Explorer	DSOLOMON\ds...	0	57

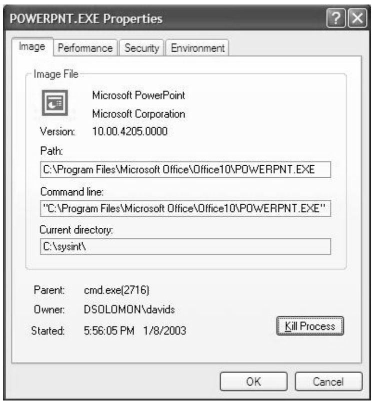
Handle	Type	Access	Name
0x634	Desktop	0x000F01FF	\Default
0xAC	Desktop	0x000F01FF	\Winlogon
0xB4	Desktop	0x000F01FF	\Disconnect
0xB8	Desktop	0x000F01FF	\Default
0x14	Directory	0x000F000F	\Windows
0x28	Directory	0x0002000F	\BaseNamedObjects
0x8	Directory	0x00000003	\KnownDlls
0x188	Event	0x00100000	\BaseNamedObjects\WinSta0_DesktopSwitch
0x1A0	Event	0x001F0003	\BaseNamedObjects\ThemesStartEvent
0x1B0	Event	0x001F0003	\BaseNamedObjects\WFP_IDLE_TRIGGER

The Process Explorer tool

1. Run Process Explorer & maximize window
2. Run Task Manager – click on Processes tab
3. Arrange windows so you can see both
4. Notice process tree vs flat list in Task Manager
   - If parent has exited, process is left justified
5. Sort on first column ("Process") and note tree view disappears
6. Sort Process column 2 more times and tree view returns
   - Can also Click on View->Show Process Tree or press CTRL+T to bring it back
7. Notice description and company name columns
8. Hover mouse over image name to see full path
9. Right click on a process and choose "Google"

Image Information

- Double click on Explorer.exe to bring up process properties
- Image tab:
  - Description, company name, version (from .EXE)
  - Full image path
  - Command line used to start process
  - Current directory
  - Parent process
  - User name
  - Start time



Microsoft PowerPoint
Microsoft Corporation
Version: 10.00.4205.0000

Path:
C:\Program Files\Microsoft Office\Office10\POWERPNT.EXE

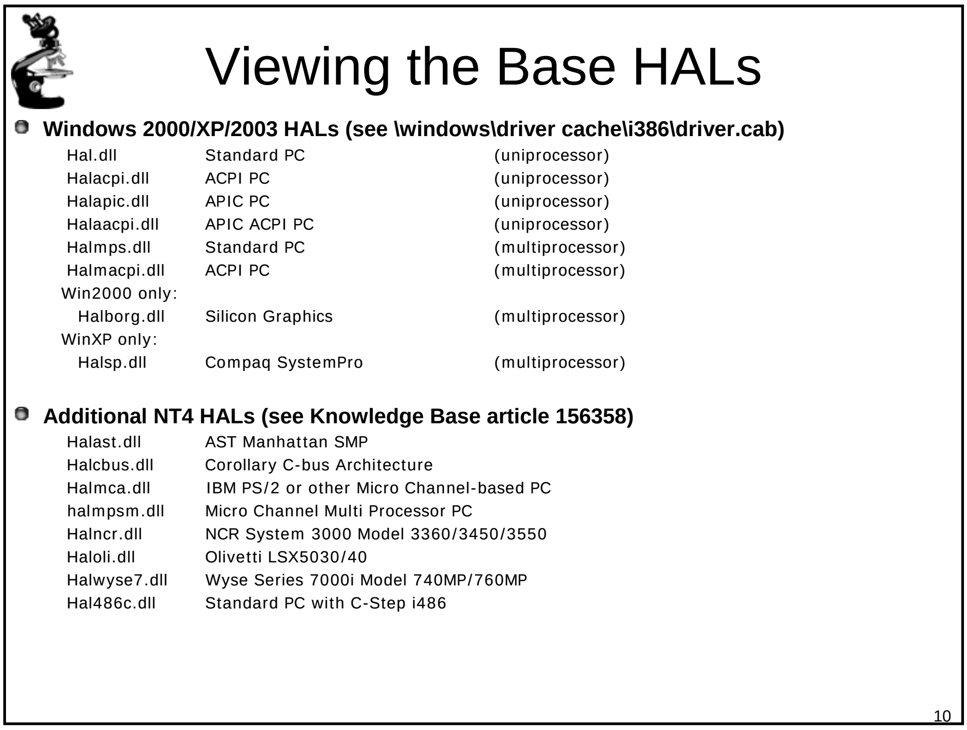
Command line:
"C:\Program Files\Microsoft Office\Office10\POWERPNT.EXE"

Current directory:
C:\sysint\

Parent: cmd.exe(2716)
Owner: DSOLOMON\davids
Started: 5:56:05 PM 1/8/2003

Viewing the Process Tree

1. Look at process hierarchy with TLIST /T
   - Start a Windows command prompt, then run Notepad from command prompt, then look at TLIST /T output
   - Exit the command prompt and notice “orphan” process with TLIST /T
2. Task Manager:
   - Applications tab: find the process that owns a window (right mouse click on window title)
   - Process tab: add a few additional columns: Virtual Memory size, Handle count, Thread count
     - Windows: add I/O counters; right click on a process & notice “end process tree” option



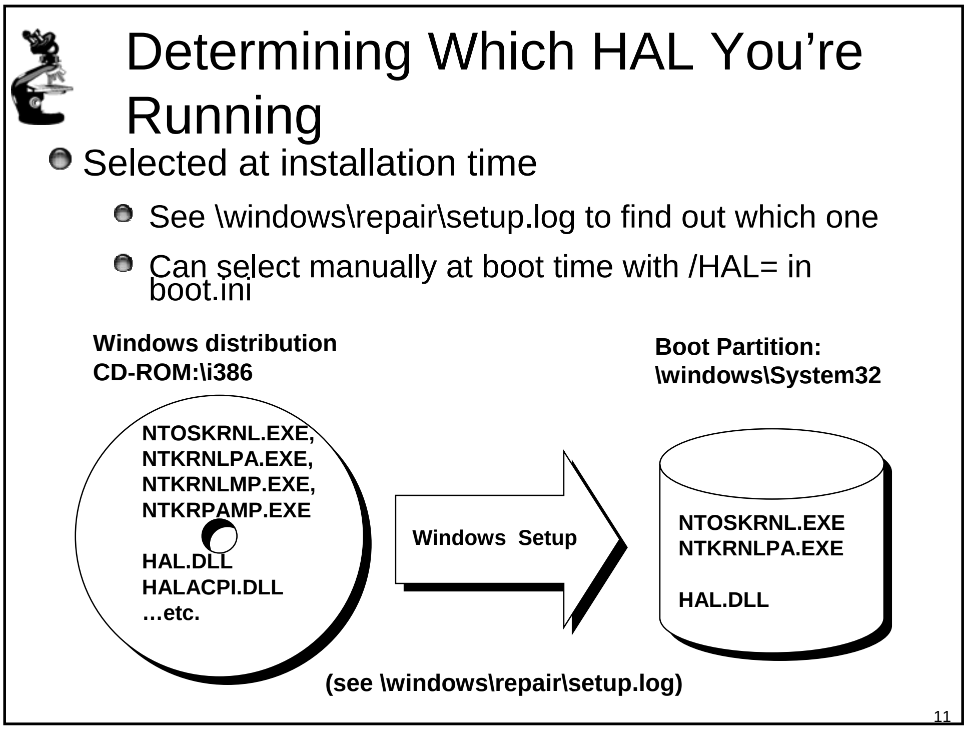
Viewing the Base HALs

- **Windows 2000/XP/2003 HALs (see \windows\driver cache\i386\driver.cab)**

Hal.dll	Standard PC	(uniprocessor)
Halacpi.dll	ACPI PC	(uniprocessor)
Halapic.dll	APIC PC	(uniprocessor)
Halaacpi.dll	APIC ACPI PC	(uniprocessor)
Halmps.dll	Standard PC	(multiprocessor)
Halmacpi.dll	ACPI PC	(multiprocessor)
Win2000 only:		
Halborg.dll	Silicon Graphics	(multiprocessor)
WinXP only:		
Halsp.dll	Compaq SystemPro	(multiprocessor)

- **Additional NT4 HALs (see Knowledge Base article 156358)**

Halast.dll	AST Manhattan SMP
Halcbus.dll	Corollary C-bus Architecture
Halmca.dll	IBM PS/2 or other Micro Channel-based PC
halmpsm.dll	Micro Channel Multi Processor PC
Halncr.dll	NCR System 3000 Model 3360/3450/3550
Haloli.dll	Olivetti LSX5030/40
Halwyse7.dll	Wyse Series 7000i Model 740MP/760MP
Hal486c.dll	Standard PC with C-Step i486



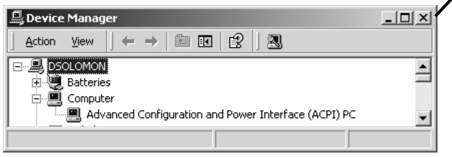
Determining Which HAL You're Running

- Selected at installation time
  - See \windows\repair\setup.log to find out which one
  - Can select manually at boot time with /HAL= in boot.ini

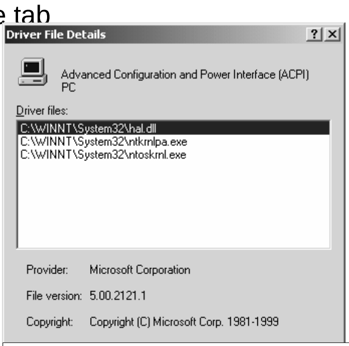
(see \windows\repair\setup.log)

Determine the HAL

- Can also see by viewing the “device drivers” for the Computer
  - Go to Control Panel->System – Hardware tab
  - Click on “Device Manager”
  - Click on “Computer”
  - Right click/Properties on “driver” for PC



DSOLOMON
Batteries
Computer
Advanced Configuration and Power Interface (ACPI) PC



Advanced Configuration and Power Interface (ACPI) PC

Driver files:
C:\WINNT\System32\hal.dll
C:\WINNT\System32\ntkrnlpa.exe
C:\WINNT\System32\ntoskrnl.exe

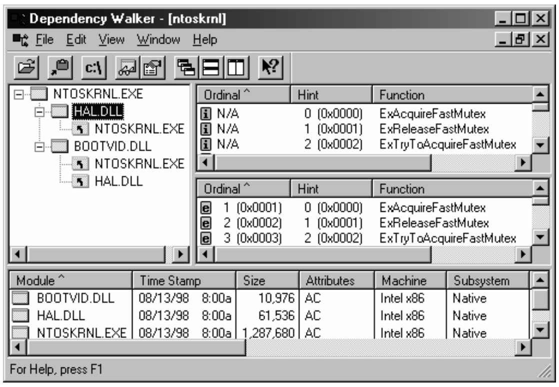
Provider: Microsoft Corporation
File version: 5.00.2121.1
Copyright: Copyright (C) Microsoft Corp. 1981-1999

Screen snapshot from:
Control Panel | System | Hardware | Device Manager | Computer properties | Driver Details

Examining NTOSKRNL & HAL Image Dependencies

- **Tool: Dependency Walker (Depends.Exe in Resource Kit & Platform SDK)**
  - **Allows viewing of image->DLL relationships, imports, and exports**

- NTOSKRNL.EXE
  - Executive and Kernel
- HAL.DLL
  - Hardware Abstraction Layer - interface to hardware platform
- BOOTVID.DLL
  - Boot video driver
  - Added in Win2000
- KDCOM.DLL
  - Kernel debugger communication code



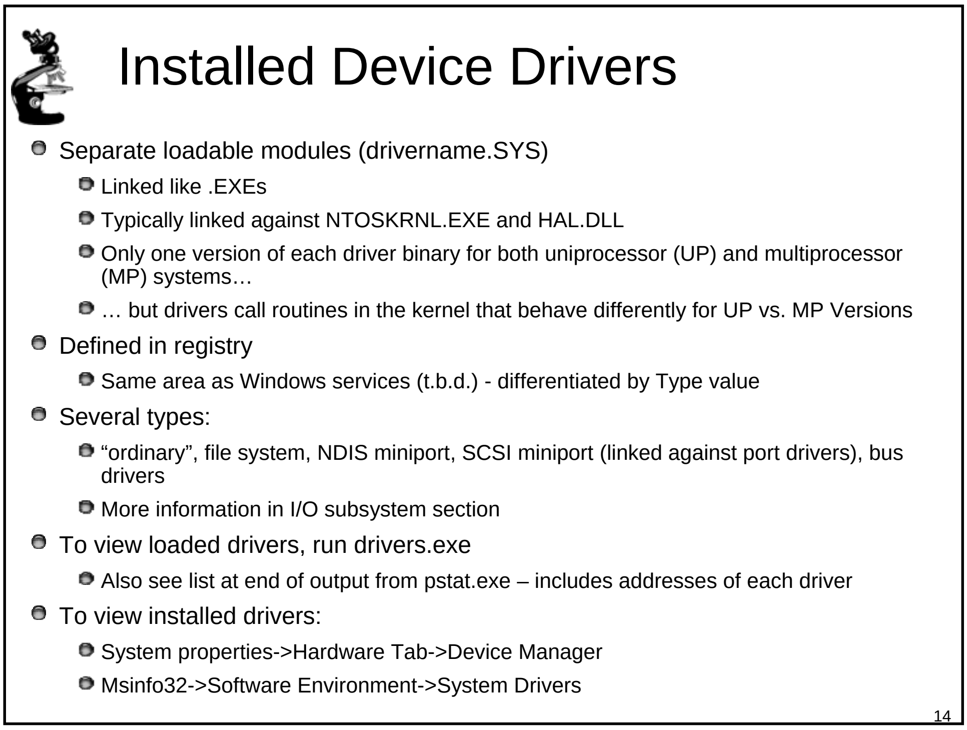
```
NTOSKRNL.EXE
  HAL.DLL
    NTOSKRNL.EXE
  BOOTVID.DLL
    NTOSKRNL.EXE
    HAL.DLL
```

Ordinal ^	Hint	Function
N/A	0 (0x0000)	ExAcquireFastMutex
N/A	1 (0x0001)	ExReleaseFastMutex
N/A	2 (0x0002)	ExTryToAcquireFastMutex

Ordinal ^	Hint	Function
1 (0x0001)	0 (0x0000)	ExAcquireFastMutex
2 (0x0002)	1 (0x0001)	ExReleaseFastMutex
3 (0x0003)	2 (0x0002)	ExTryToAcquireFastMutex

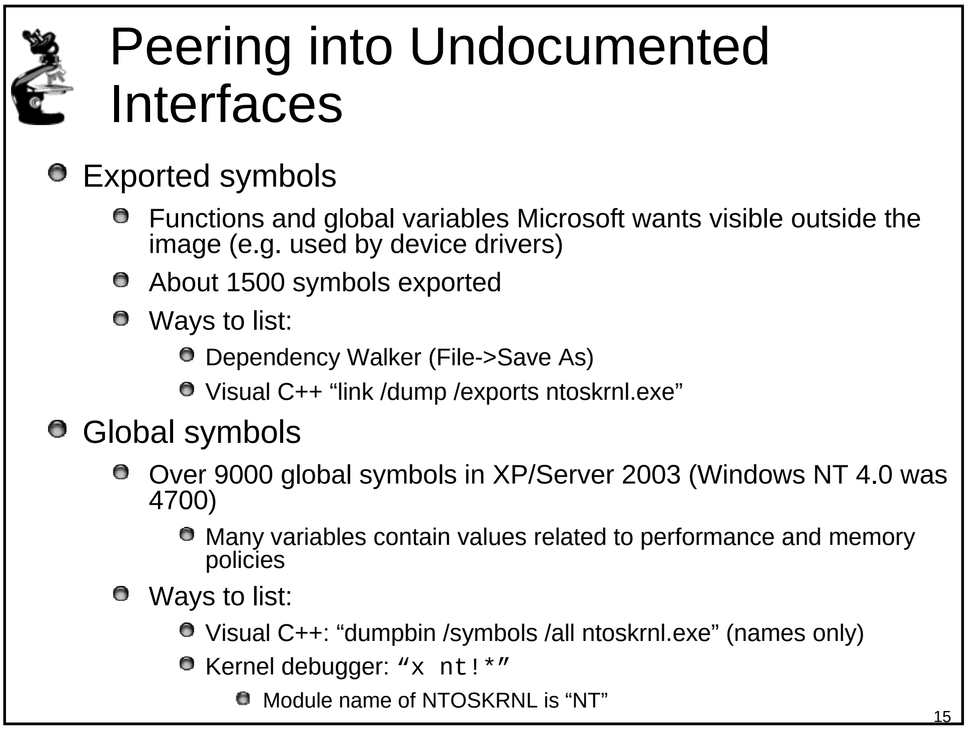
Module ^	Time Stamp	Size	Attributes	Machine	Subsystem
BOOTVID.DLL	08/13/98 8:00a	10,976	AC	Intel x86	Native
HAL.DLL	08/13/98 8:00a	61,536	AC	Intel x86	Native
NTOSKRNL.EXE	08/13/98 8:00a	1,287,680	AC	Intel x86	Native

For Help, press F1



Installed Device Drivers

- Separate loadable modules (drivername.SYS)
  - Linked like .EXEs
  - Typically linked against NTOSKRNL.EXE and HAL.DLL
  - Only one version of each driver binary for both uniprocessor (UP) and multiprocessor (MP) systems…
  - … but drivers call routines in the kernel that behave differently for UP vs. MP Versions
- Defined in registry
  - Same area as Windows services (t.b.d.) - differentiated by Type value
- Several types:
  - “ordinary”, file system, NDIS miniport, SCSI miniport (linked against port drivers), bus drivers
  - More information in I/O subsystem section
- To view loaded drivers, run drivers.exe
  - Also see list at end of output from pstat.exe – includes addresses of each driver
- To view installed drivers:
  - System properties->Hardware Tab->Device Manager
  - Msinfo32->Software Environment->System Drivers



Peering into Undocumented Interfaces

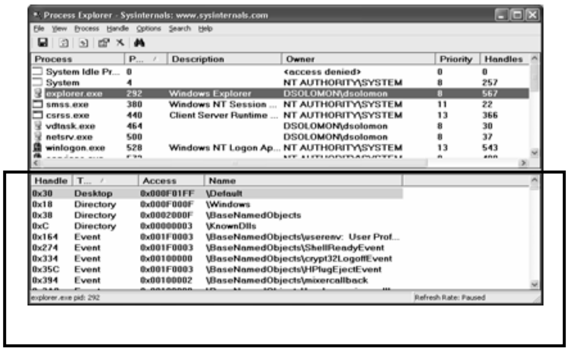
- Exported symbols
  - Functions and global variables Microsoft wants visible outside the image (e.g. used by device drivers)
  - About 1500 symbols exported
  - Ways to list:
    - Dependency Walker (File->Save As)
    - Visual C++ “link /dump /exports ntoskrnl.exe”
- Global symbols
  - Over 9000 global symbols in XP/Server 2003 (Windows NT 4.0 was 4700)
    - Many variables contain values related to performance and memory policies
  - Ways to list:
    - Visual C++: “dumpbin /symbols /all ntoskrnl.exe” (names only)
    - Kernel debugger: `“x nt!*”`
      - Module name of NTOSKRNL is “NT”

Image Subsystem Type

- Look at subsystem startup information in registry
- Using EXETYPE, look at subsystem types for:
  - \windows\system32\notepad.exe, cmd.exe, csrss.exe

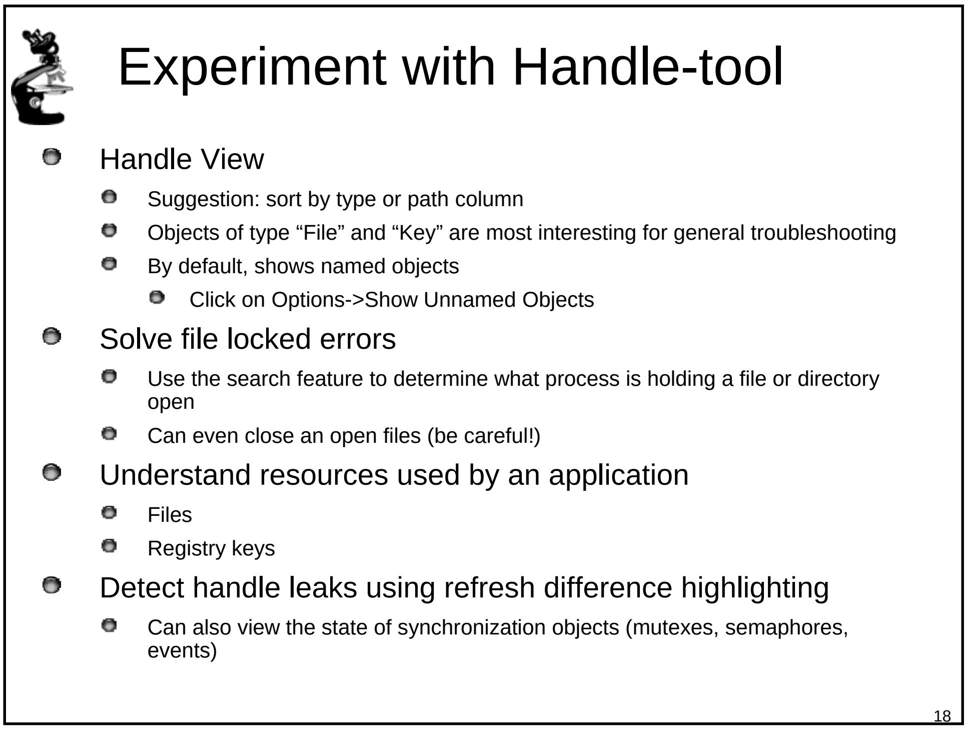
Viewing Open Handles

- Process Explorer (GUI version) or handle (character cell version) from www.sysinternals.com
  - Uses a device driver to walk handle table, so doesn't need Global Flag set


Process Explorer - Sysinternals: www.sysinternals.com
File View Process Handle Options Search Help

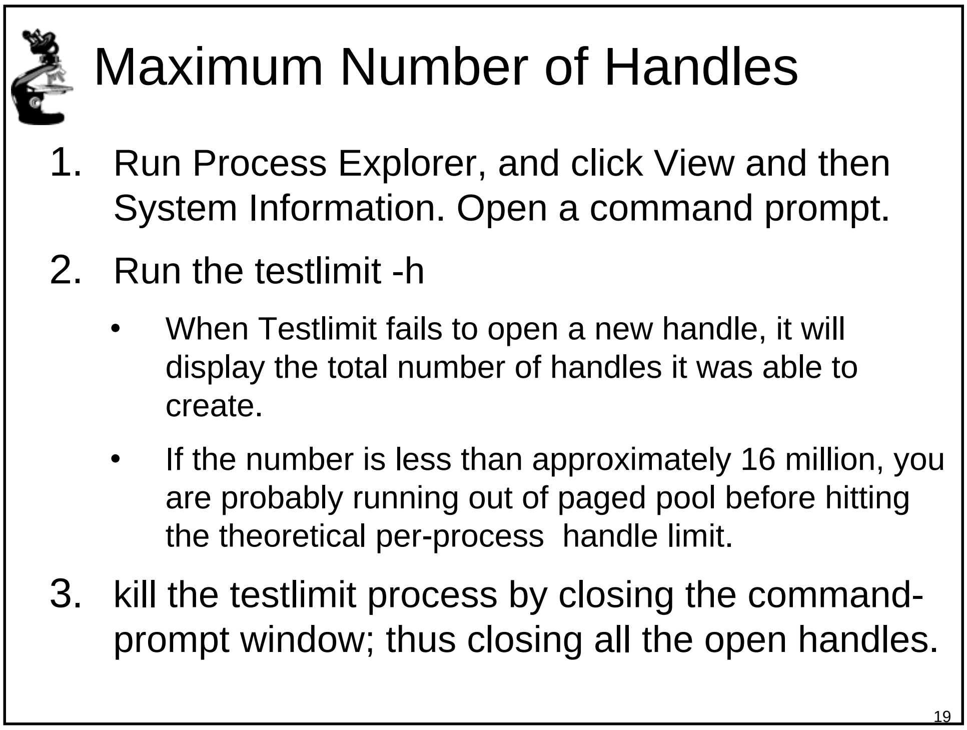
Process	P...	Description	Owner	Priority	Handles
System Idle Pr...	0		<access denied>	0	0
System	4		NT AUTHORITY\SYSTEM	8	257
explorer.exe	292	Windows Explorer	DSOLOMON\dsolomon	8	567
smss.exe	380	Windows NT Session ...	NT AUTHORITY\SYSTEM	11	22
csrss.exe	440	Client Server Runtime ...	NT AUTHORITY\SYSTEM	13	366
vdtask.exe	464		DSOLOMON\dsolomon	8	30
netsrv.exe	500		DSOLOMON\dsolomon	8	37
winlogon.exe	528	Windows NT Logon Ap...	NT AUTHORITY\SYSTEM	13	543

Handle	T...	Access	Name
0x30	Desktop	0x000F01FF	\Default
0x18	Directory	0x000F000F	\Windows
0x38	Directory	0x0002000F	\BaseNamedObjects
0xC	Directory	0x00000003	\KnownDlls
0x164	Event	0x001F0003	\BaseNamedObjects\userenv: User Prof...
0x274	Event	0x001F0003	\BaseNamedObjects\ShellReadyEvent
0x334	Event	0x00100000	\BaseNamedObjects\crypt32LogoffEvent
0x35C	Event	0x001F0003	\BaseNamedObjects\HPlugEjectEvent
0x394	Event	0x00100002	\BaseNamedObjects\mixercallback



Experiment with Handle-tool

- Handle View
  - Suggestion: sort by type or path column
  - Objects of type “File” and “Key” are most interesting for general troubleshooting
  - By default, shows named objects
    - Click on Options->Show Unnamed Objects
- Solve file locked errors
  - Use the search feature to determine what process is holding a file or directory open
  - Can even close an open files (be careful!)
- Understand resources used by an application
  - Files
  - Registry keys
- Detect handle leaks using refresh difference highlighting
  - Can also view the state of synchronization objects (mutexes, semaphores, events)



Maximum Number of Handles

1. Run Process Explorer, and click View and then System Information. Open a command prompt.
2. Run the testlimit -h
   - When Testlimit fails to open a new handle, it will display the total number of handles it was able to create.
   - If the number is less than approximately 16 million, you are probably running out of paged pool before hitting the theoretical per-process handle limit.
3. kill the testlimit process by closing the command-prompt window; thus closing all the open handles.

Viewing Open Handles with Kernel Debugger

- If looking at a dump, use !handle in Kernel Debugger (see help for options)

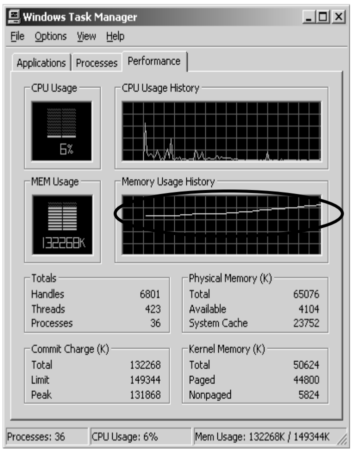
```
lkd> !handle 0 f 9e8 file

processor number 0
Searching for Process with Cid == 9e8
Searching for handles of type file

PROCESS 82ce72d0  SessionId: 0  Cid: 09e8    Peb: 7ffdf000  ParentCid: 06ec

   DirBase: 06602000  ObjectTable: e1c879c8  HandleCount: 430.
   Image: POWERPNT.EXE
...

0280: Object: 82c5e230  GrantedAccess: 00120089

Object: 82c5e230  Type: (82fdde70) File
   ObjectHeader: 82c5e218

      HandleCount: 1  PointerCount: 1

      Directory Object: 00000000  Name:
            \slides\ntint\new\4-systemarchitecture.ppt {HarddiskVolume1}
```

Troubleshooting a Pool Leak

- Run NotMyFault and select "Leak Pool"

  (available from http://www.sysinternals.com/files/notmyfault.zip)

  - Allocates paged pool buffers and doesn't free them
  - Stops leaking when you select "Stop Leaking"



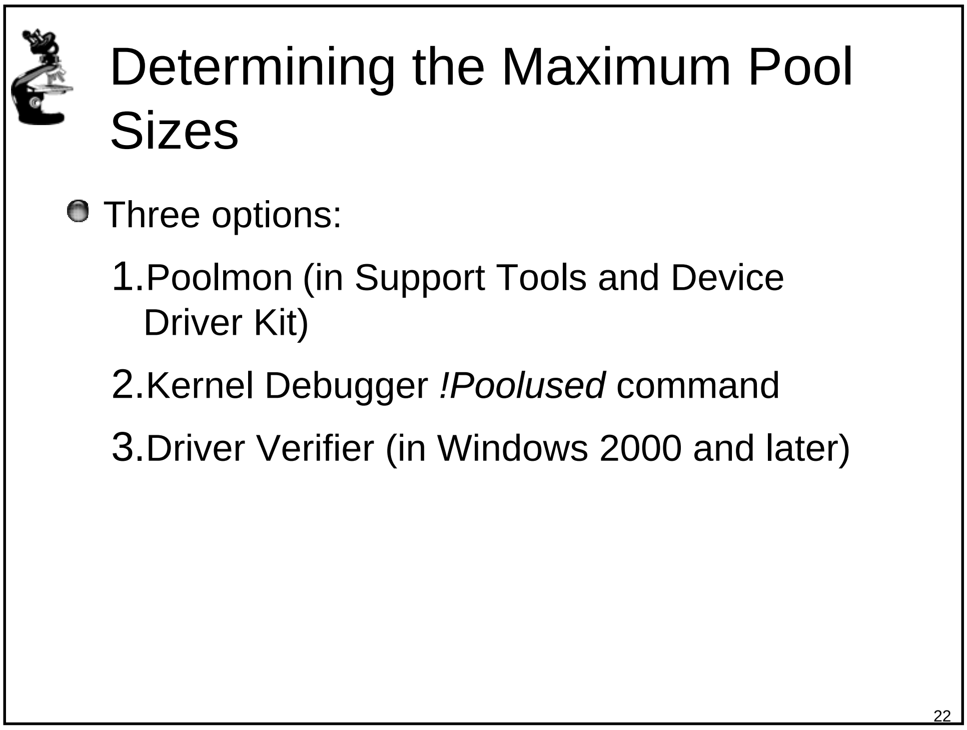
Totals
Handles 6801
Threads 423
Processes 36

Physical Memory (K)
Total 65076
Available 4104
System Cache 23752

Commit Charge (K)
Total 132268
Limit 149344
Peak 131868

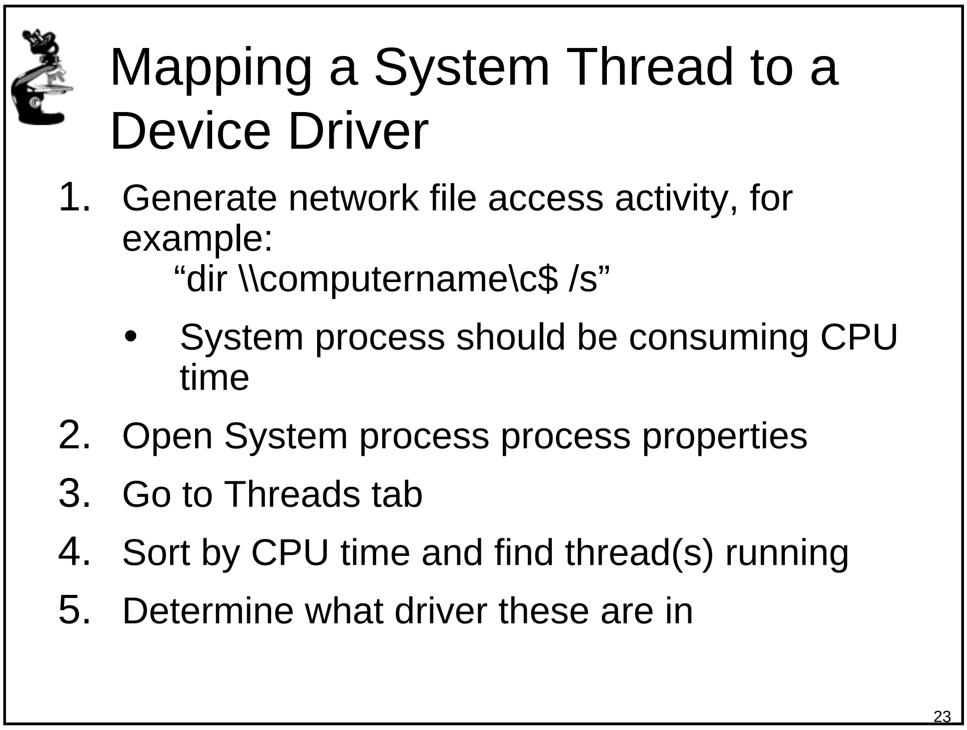
Kernel Memory (K)
Total 50624
Paged 44800
Nonpaged 5824

Processes: 36 | CPU Usage: 6% | Mem Usage: 132268K / 149344K



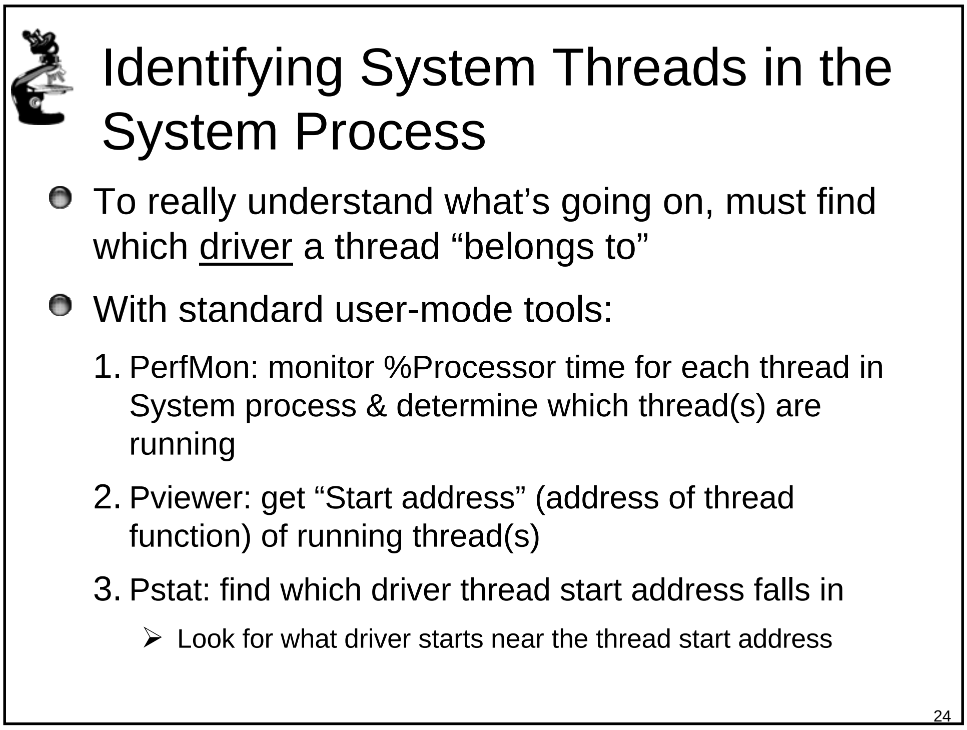
Determining the Maximum Pool Sizes

- Three options:
  1. Poolmon (in Support Tools and Device Driver Kit)
  2. Kernel Debugger *!Poolused* command
  3. Driver Verifier (in Windows 2000 and later)



Mapping a System Thread to a Device Driver

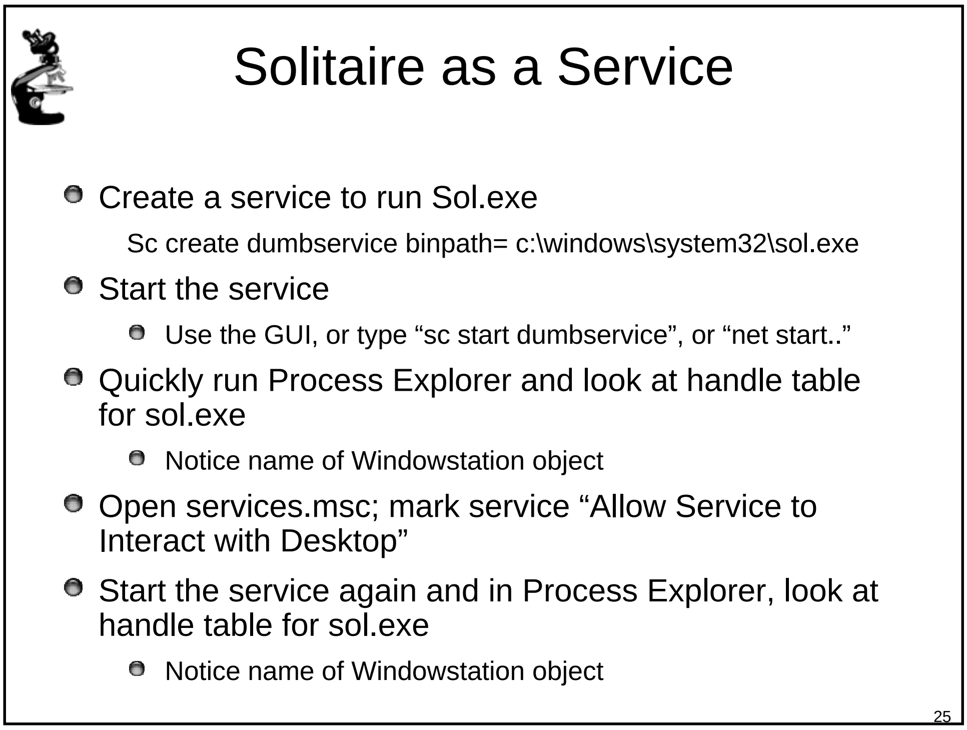
1. Generate network file access activity, for example:
   “dir \\computername\c$ /s”
   - System process should be consuming CPU time
2. Open System process process properties
3. Go to Threads tab
4. Sort by CPU time and find thread(s) running
5. Determine what driver these are in



Identifying System Threads in the System Process

- To really understand what’s going on, must find which driver a thread “belongs to”
- With standard user-mode tools:
  1. PerfMon: monitor %Processor time for each thread in System process & determine which thread(s) are running
  2. Pviewer: get “Start address” (address of thread function) of running thread(s)
  3. Pstat: find which driver thread start address falls in
     - ➢ Look for what driver starts near the thread start address

24



Solitaire as a Service

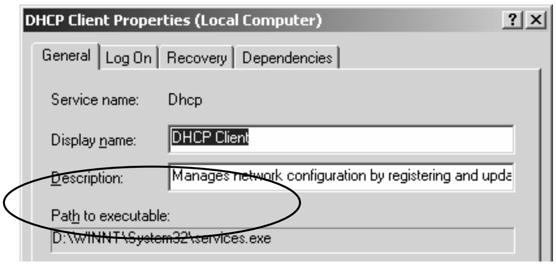
- Create a service to run Sol.exe

  Sc create dumbservice binpath= c:\windows\system32\sol.exe
- Start the service
  - Use the GUI, or type “sc start dumbservice”, or “net start..”
- Quickly run Process Explorer and look at handle table for sol.exe
  - Notice name of Windowstation object
- Open services.msc; mark service “Allow Service to Interact with Desktop”
- Start the service again and in Process Explorer, look at handle table for sol.exe
  - Notice name of Windowstation object

25

Listing Installed Services

- Not always a 1-to-1 mapping
  - Some service processes contain more than one service
    - Conserves virtual memory, reduces boot time
  - This is up to the developer of the service
- Service properties displayed through Control Panel (services.msc) show name of .EXE
  - But not which process the services is running in



DHCP Client Properties (Local Computer)

Service name: Dhcp

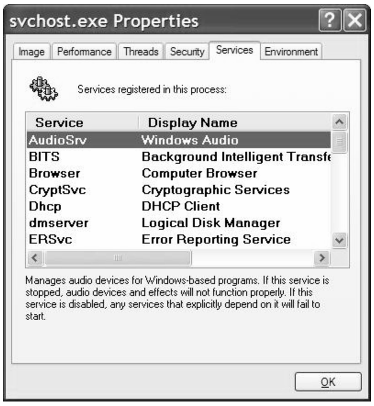
Display name: DHCP Client

Description: Manages network configuration by registering and upda

Path to executable:
D:\WINNT\System32\services.exe

Viewing Service Details Inside Service Processes

- Tlist /S (Debugging Tools) or Tasklist /svc (XP/2003) list internal name of services inside service processes
- Process Explorer shows more: external display name and description



svchost.exe Properties

Services registered in this process:

Service	Display Name
AudioSrv	Windows Audio
BITS	Background Intelligent Transfe
Browser	Computer Browser
CryptSvc	Cryptographic Services
Dhcp	DHCP Client
dmserver	Logical Disk Manager
ERSvc	Error Reporting Service

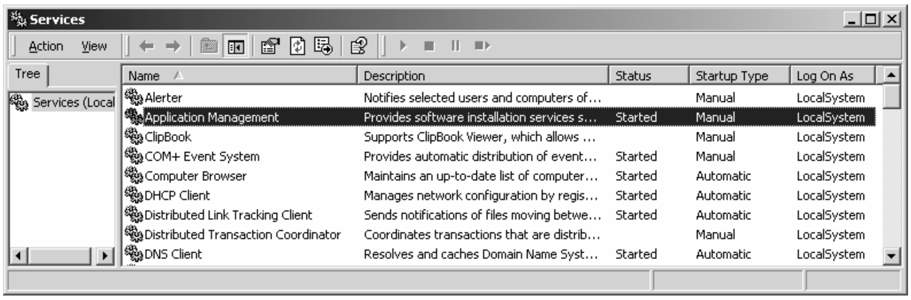
Manages audio devices for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Viewing Services Running Inside Processes

1. Open a command prompt
2. Type “tasklist /svc”
3. Find the Svchost.exe process with the most services inside it
4. In Process Explorer, double click on that Svchost.exe process
5. Click on Services tab
6. Notice extra details about each service displayed by Process Explorer

Service Configuration & Control Tools

- To view & control services:
  - Control Panel->Administrative Tools->Services



Name	Description	Status	Startup Type	Log On As
Alerter	Notifies selected users and computers of…		Manual	LocalSystem
Application Management	Provides software installation services s…	Started	Manual	LocalSystem
ClipBook	Supports ClipBook Viewer, which allows …		Manual	LocalSystem
COM+ Event System	Provides automatic distribution of event…	Started	Manual	LocalSystem
Computer Browser	Maintains an up-to-date list of computer…	Started	Automatic	LocalSystem
DHCP Client	Manages network configuration by regis…	Started	Automatic	LocalSystem
Distributed Link Tracking Client	Sends notifications of files moving betwe…	Started	Automatic	LocalSystem
Distributed Transaction Coordinator	Coordinates transactions that are distrib…		Manual	LocalSystem
DNS Client	Resolves and caches Domain Name Syst…	Started	Automatic	LocalSystem

- No option to add/remove – done at install/uninstall time