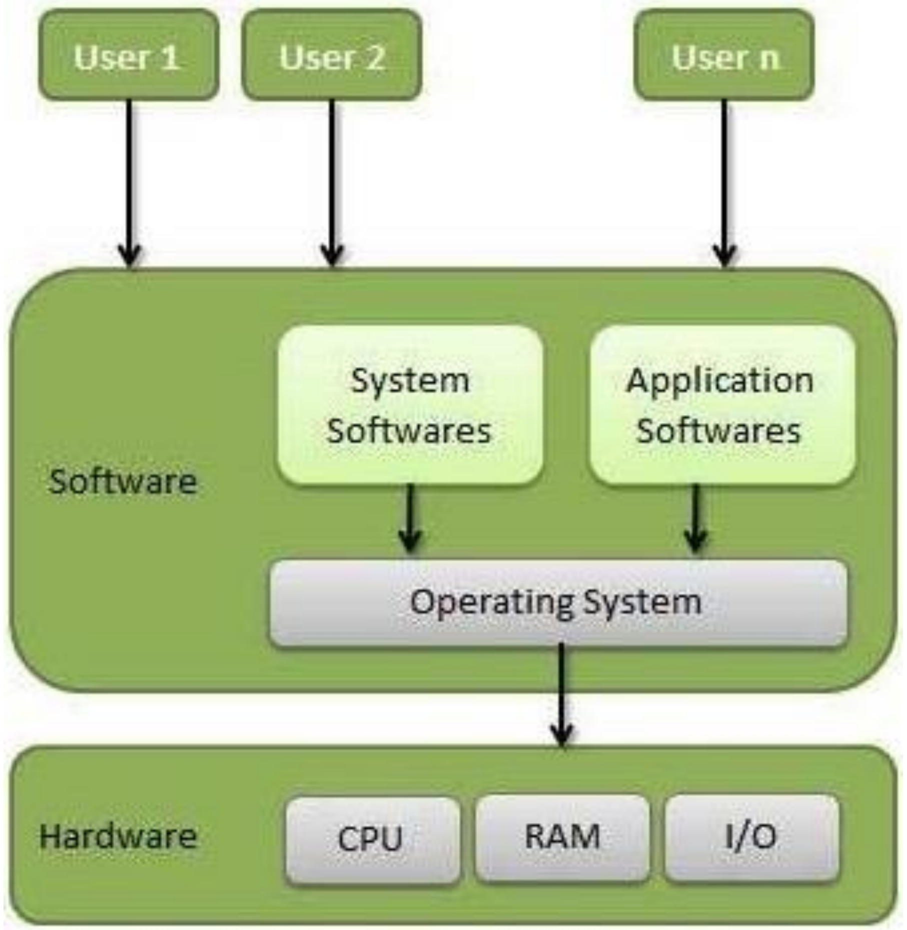
Operating Systems Concepts

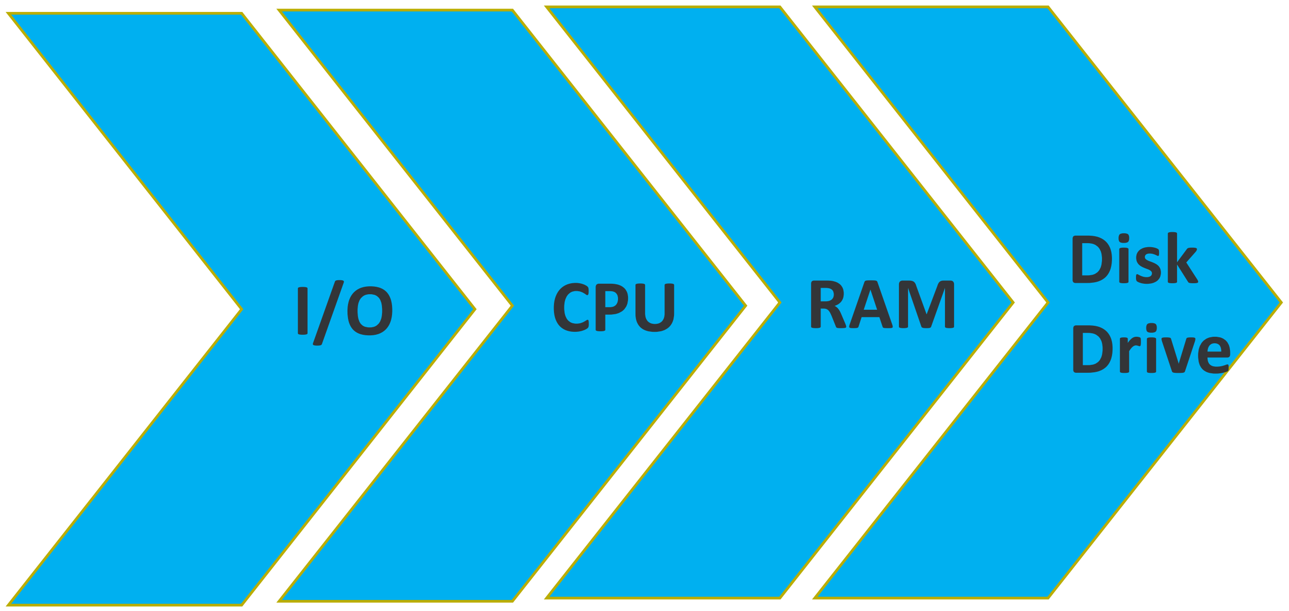
Some of important functions of an operating System

- The Kernel and Input/Output
- Processes
- The Filesystem
- Memory Management
- Virtual Machines



A Computer Model

- An operating system has to deal with the fact that a computer is made up of a CPU, random access memory (RAM), input/output (I/O) devices, and long-term storage.



OS Concepts

- **An operating system (OS) provides the interface between the users of a computer and that computer's hardware.**
  - ➢An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces.
  - ➢An operating system manages multiple users.
  - ➢An operating system manages multiple programs.

Multitasking

- Give each running program a “slice” of the CPU’s time.
- The CPU is running so fast that to any user it appears that the computer is running all the programs simultaneously.

Multitasking - example

- Let's consider a user working on a computer:
  - The user is writing an email in their email client, composing a message to a colleague.
  - At the same time, the user has a web browser open, where they are researching information for a project.
  - Additionally, the user has a music player running in the background, playing their favorite playlist.

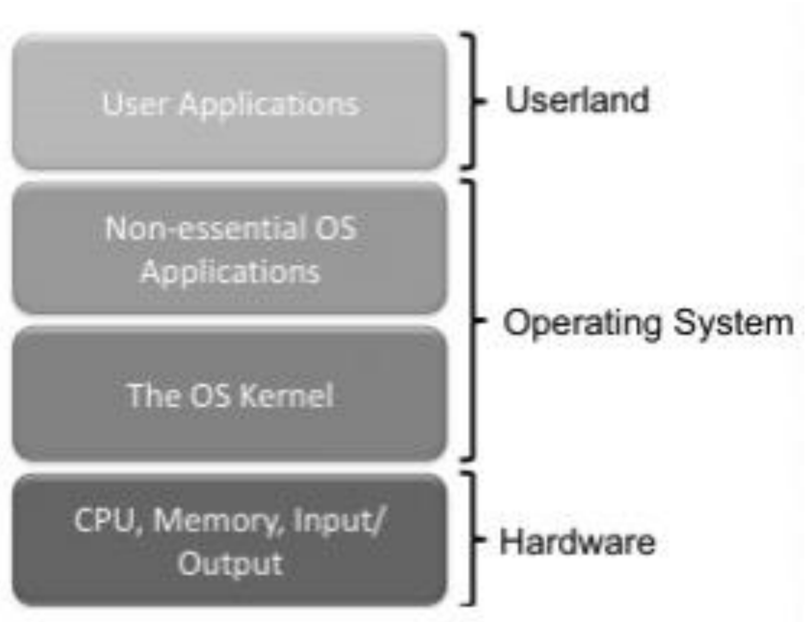
Multitasking - example

- In this scenario, the computer is multitasking:
    - The email client is running and handling the task of composing and sending an email to the colleague.
    - The web browser is also active, enabling the user to conduct research and browse the internet for relevant information.
    - Simultaneously, the music player is running as a background process, playing music for the user to enjoy while they work.

The computer's operating system manages multitasking by dividing the processor's time and resources efficiently among these different tasks.

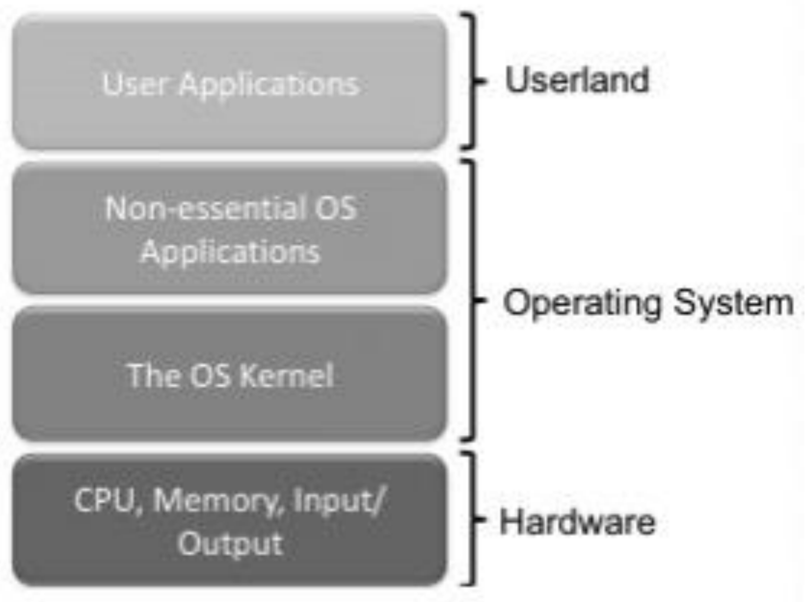
The Kernel and Input/Output

- **Kernel:** core component of the operating system.It handles the management of low-level hardware resources, including memory, processors, and input/output (I/O) devices, such as a keyboard, mouse, or video display.



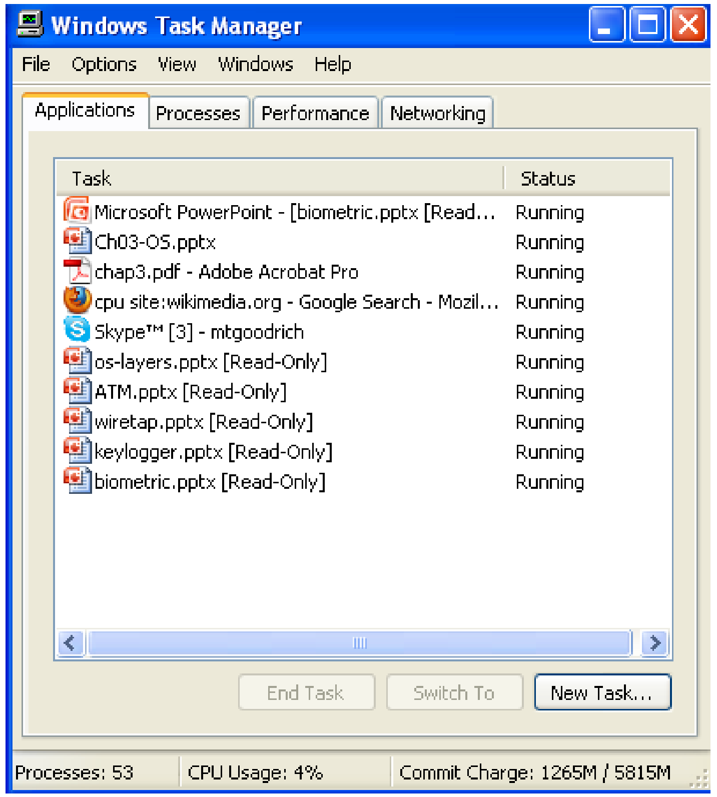
The Kernel and Input/Output

- Most operating systems define the tasks associated with the kernel in terms of a layer metaphor, with the hardware components, such as the CPU, memory, and input/output devices being on the bottom, and users and applications being on the top.



Processes

- A **process** is an instance of a program that is currently executing.
- The actual contents of all programs are initially stored in persistent storage, such as a hard drive.
- In order to be executed, a program must be loaded into random-access memory (RAM) and uniquely identified as a process.

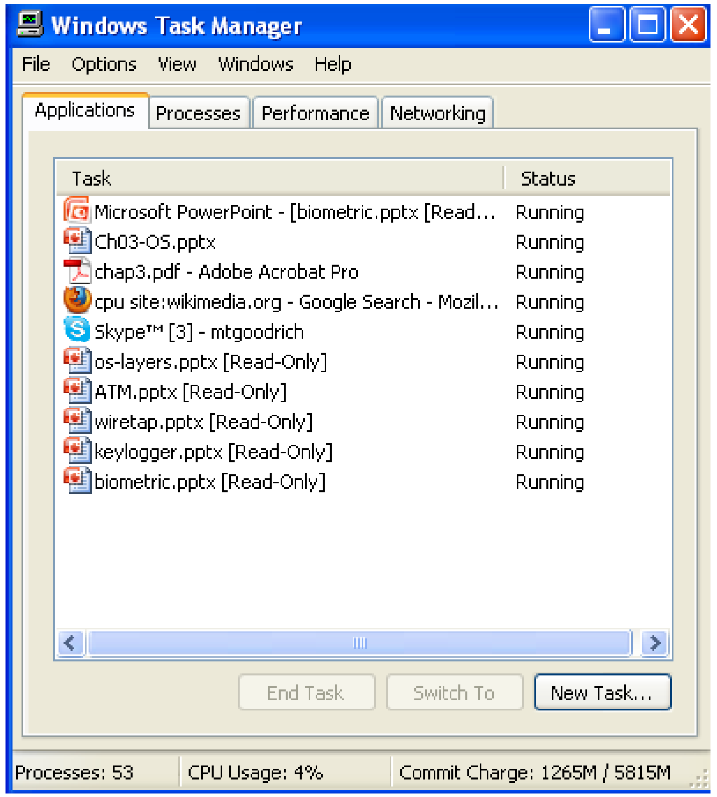

Windows Task Manager
File Options View Windows Help
Applications Processes Performance Networking
End Task
Switch To
New Task...

Task	Status
Microsoft PowerPoint - [biometric.pptx [Read...	Running
Ch03-OS.pptx	Running
chap3.pdf - Adobe Acrobat Pro	Running
cpu site:wikimedia.org - Google Search - Mozil...	Running
Skype™ [3] - mtgoodrich	Running
os-layers.pptx [Read-Only]	Running
ATM.pptx [Read-Only]	Running
wiretap.pptx [Read-Only]	Running
keylogger.pptx [Read-Only]	Running
biometric.pptx [Read-Only]	Running

Processes: 53 CPU Usage: 4% Commit Charge: 1265M / 5815M

Processes

- In this way, multiple copies of the same program can be run as different processes.
- For example, we can have multiple copies of MS Powerpoint open at the same time.


Windows Task Manager
File Options View Windows Help
Applications Processes Performance Networking
End Task Switch To New Task...

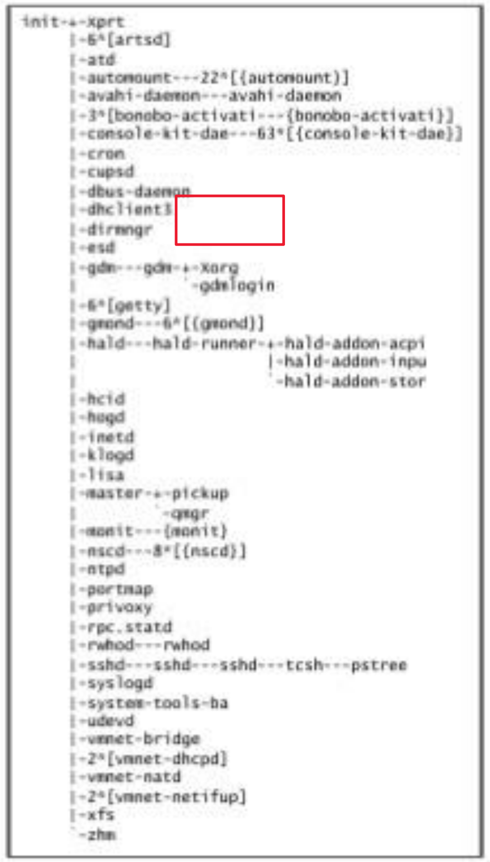
Task	Status
Microsoft PowerPoint - [biometric.pptx [Read...	Running
Ch03-OS.pptx	Running
chap3.pdf - Adobe Acrobat Pro	Running
cpu site:wikimedia.org - Google Search - Mozil...	Running
Skype™ [3] - mtgoodrich	Running
os-layers.pptx [Read-Only]	Running
ATM.pptx [Read-Only]	Running
wiretap.pptx [Read-Only]	Running
keylogger.pptx [Read-Only]	Running
biometric.pptx [Read-Only]	Running

Processes: 53 CPU Usage: 4% Commit Charge: 1265M / 5815M

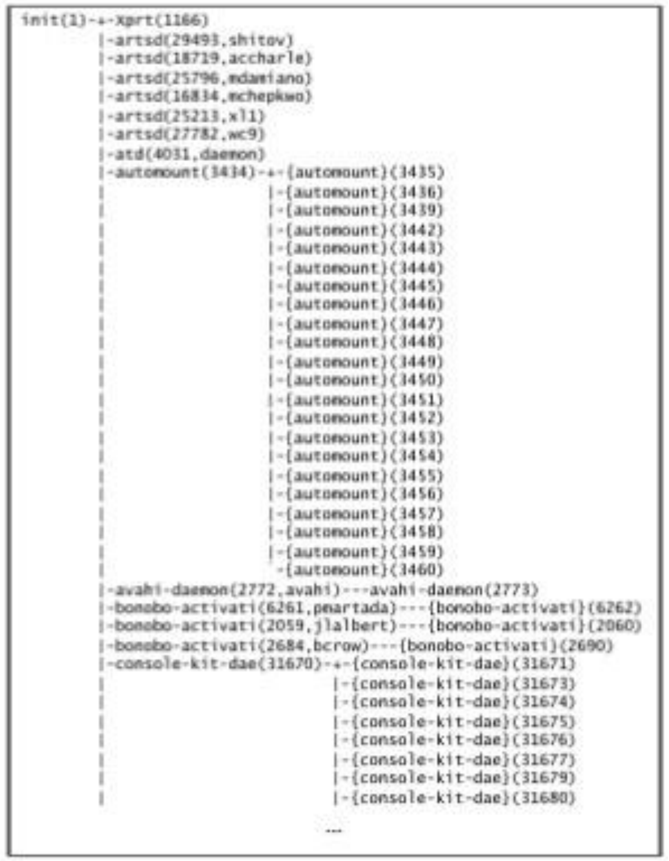
Processes

Process: the kernel defines the notion of a process , which is an instance of a program that is currently executing.

The **Process IDs:** Each process running on a given computer is identified by a unique nonnegative integer, called the process ID (PID).



```
init-+-xprt
     |-6*[artsd]
     |-atd
     |-automount---22*[{automount}]
     |-avahi-daemon---avahi-daemon
     |-3*[bonobo-activati---{bonobo-activati}]
     |-console-kit-dae---63*[{console-kit-dae}]
     |-cron
     |-cupsd
     |-dbus-daemon
     |-dhclient3
     |-dirmngr
     |-esd
     |-gdm---gdm-+-Xorg
     |           `-gdmlogin
     |-6*[getty]
     |-gmond---6*[{gmond}]
     |-hald---hald-runner-+-hald-addon-acpi
     |                    |-hald-addon-inpu
     |                    `-hald-addon-stor
     |-hcid
     |-hogd
     |-inetd
     |-klogd
     |-lisa
     |-master-+-pickup
     |        `-qmgr
     |-monit---{monit}
     |-nscd---8*[{nscd}]
     |-ntpd
     |-portmap
     |-privoxy
     |-rpc.statd
     |-rwhod---rwhod
     |-sshd---sshd---sshd---tcsh---pstree
     |-syslogd
     |-system-tools-ba
     |-udevd
     |-vmnet-bridge
     |-2*[vmnet-dhcpd]
     |-vmnet-natd
     |-2*[vmnet-netifup]
     |-xfs
     `-zhm
```



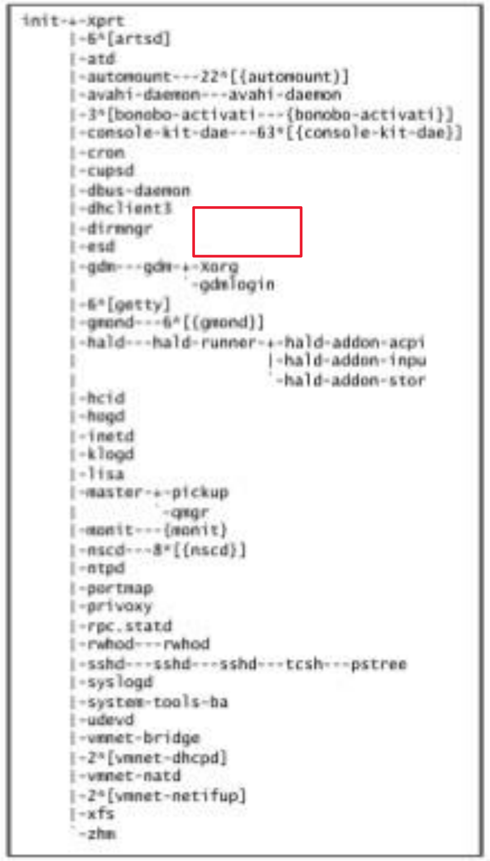
```
init(1)-+-Xprt(1166)
        |-artsd(29493,shitov)
        |-artsd(18719,accharle)
        |-artsd(25796,mdamiano)
        |-artsd(16834,mchepkwo)
        |-artsd(25213,x11)
        |-artsd(27782,wc9)
        |-atd(4031,daemon)
        |-automount(3434)-+-{automount}(3435)
        |                 |-{automount}(3436)
        |                 |-{automount}(3439)
        |                 |-{automount}(3442)
        |                 |-{automount}(3443)
        |                 |-{automount}(3444)
        |                 |-{automount}(3445)
        |                 |-{automount}(3446)
        |                 |-{automount}(3447)
        |                 |-{automount}(3448)
        |                 |-{automount}(3449)
        |                 |-{automount}(3450)
        |                 |-{automount}(3451)
        |                 |-{automount}(3452)
        |                 |-{automount}(3453)
        |                 |-{automount}(3454)
        |                 |-{automount}(3455)
        |                 |-{automount}(3456)
        |                 |-{automount}(3457)
        |                 |-{automount}(3458)
        |                 |-{automount}(3459)
        |                 `-{automount}(3460)
        |-avahi-daemon(2772,avahi)---avahi-daemon(2773)
        |-bonobo-activati(6261,pmartada)---{bonobo-activati}(6262)
        |-bonobo-activati(2059,jlalbert)---{bonobo-activati}(2060)
        |-bonobo-activati(2684,bcrow)---{bonobo-activati}(2690)
        |-console-kit-dae(31670)-+-{console-kit-dae}(31671)
        |                        |-{console-kit-dae}(31673)
        |                        |-{console-kit-dae}(31674)
        |                        |-{console-kit-dae}(31675)
        |                        |-{console-kit-dae}(31676)
        |                        |-{console-kit-dae}(31677)
        |                        |-{console-kit-dae}(31679)
        |                        |-{console-kit-dae}(31680)
                                ...
```

Process tree for a Linux system

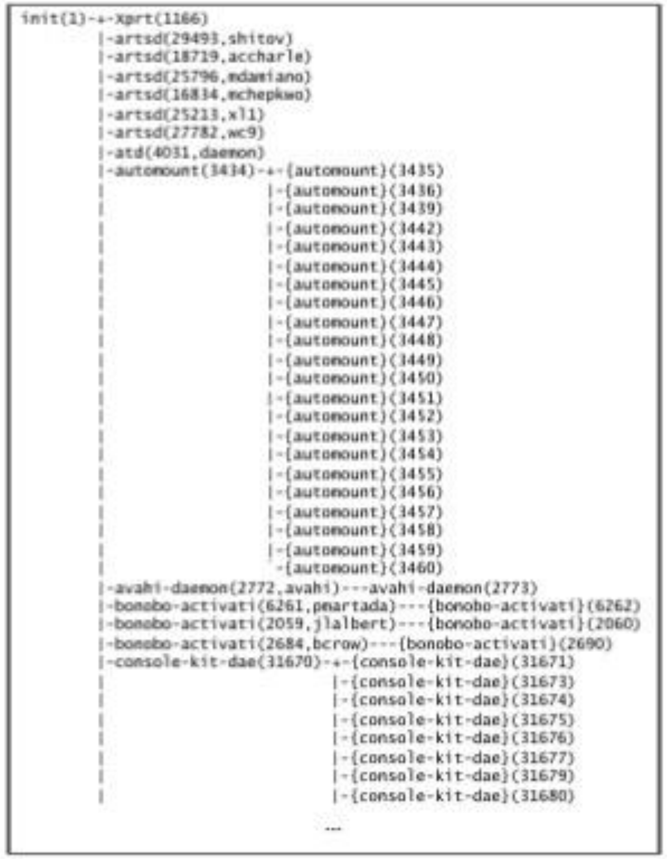
Processes

IPC: operating systems usually include mechanisms to facilitate inter-process communication (IPC).

Signal: unixbased systems incorporate signals , which are essentially notifications sent from one process to another.



```
init-+-xprt
     |-6*[artsd]
     |-atd
     |-automount---22*[{automount}]
     |-avahi-daemon---avahi-daemon
     |-3*[bonobo-activati---{bonobo-activati}]
     |-console-kit-dae---63*[{console-kit-dae}]
     |-cron
     |-cupsd
     |-dbus-daemon
     |-dhclient3
     |-dirmngr
     |-esd
     |-gdm---gdm-+-Xorg
     |           `-gdmlogin
     |-6*[getty]
     |-gmond---6*[{gmond}]
     |-hald---hald-runner-+-hald-addon-acpi
     |                    |-hald-addon-inpu
     |                    `-hald-addon-stor
     |-hcid
     |-hogd
     |-inetd
     |-klogd
     |-lisa
     |-master-+-pickup
     |        `-qmgr
     |-monit---{monit}
     |-nscd---8*[{nscd}]
     |-ntpd
     |-portmap
     |-privoxy
     |-rpc.statd
     |-rwhod---rwhod
     |-sshd---sshd---sshd---tcsh---pstree
     |-syslogd
     |-system-tools-ba
     |-udevd
     |-vmnet-bridge
     |-2*[vmnet-dhcpd]
     |-vmnet-natd
     |-2*[vmnet-netifup]
     |-xfs
     `-zhm
```

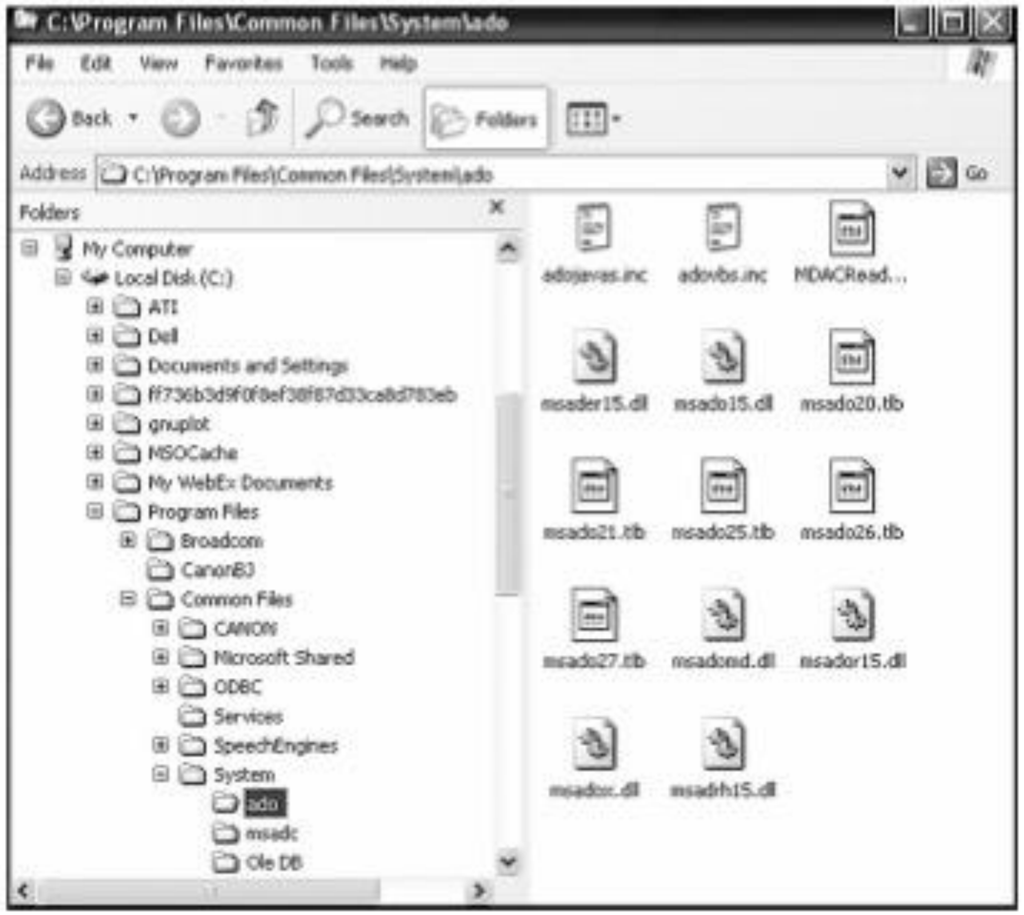


```
init(1)-+-Xprt(1166)
        |-artsd(29493,shitov)
        |-artsd(18719,accharle)
        |-artsd(25796,mdamiano)
        |-artsd(16834,mchepkwo)
        |-artsd(25213,x11)
        |-artsd(27782,wc9)
        |-atd(4031,daemon)
        |-automount(3434)-+-{automount}(3435)
        |                 |-{automount}(3436)
        |                 |-{automount}(3439)
        |                 |-{automount}(3442)
        |                 |-{automount}(3443)
        |                 |-{automount}(3444)
        |                 |-{automount}(3445)
        |                 |-{automount}(3446)
        |                 |-{automount}(3447)
        |                 |-{automount}(3448)
        |                 |-{automount}(3449)
        |                 |-{automount}(3450)
        |                 |-{automount}(3451)
        |                 |-{automount}(3452)
        |                 |-{automount}(3453)
        |                 |-{automount}(3454)
        |                 |-{automount}(3455)
        |                 |-{automount}(3456)
        |                 |-{automount}(3457)
        |                 |-{automount}(3458)
        |                 |-{automount}(3459)
        |                 `-{automount}(3460)
        |-avahi-daemon(2772,avahi)---avahi-daemon(2773)
        |-bonobo-activati(6261,pmartada)---{bonobo-activati}(6262)
        |-bonobo-activati(2059,jlalbert)---{bonobo-activati}(2060)
        |-bonobo-activati(2684,bcrow)---{bonobo-activati}(2690)
        |-console-kit-dae(31670)-+-{console-kit-dae}(31671)
        |                        |-{console-kit-dae}(31673)
        |                        |-{console-kit-dae}(31674)
        |                        |-{console-kit-dae}(31675)
        |                        |-{console-kit-dae}(31676)
        |                        |-{console-kit-dae}(31677)
        |                        |-{console-kit-dae}(31679)
        |                        |-{console-kit-dae}(31680)
                                ...
```

Process tree for a Linux system

The Filesystem

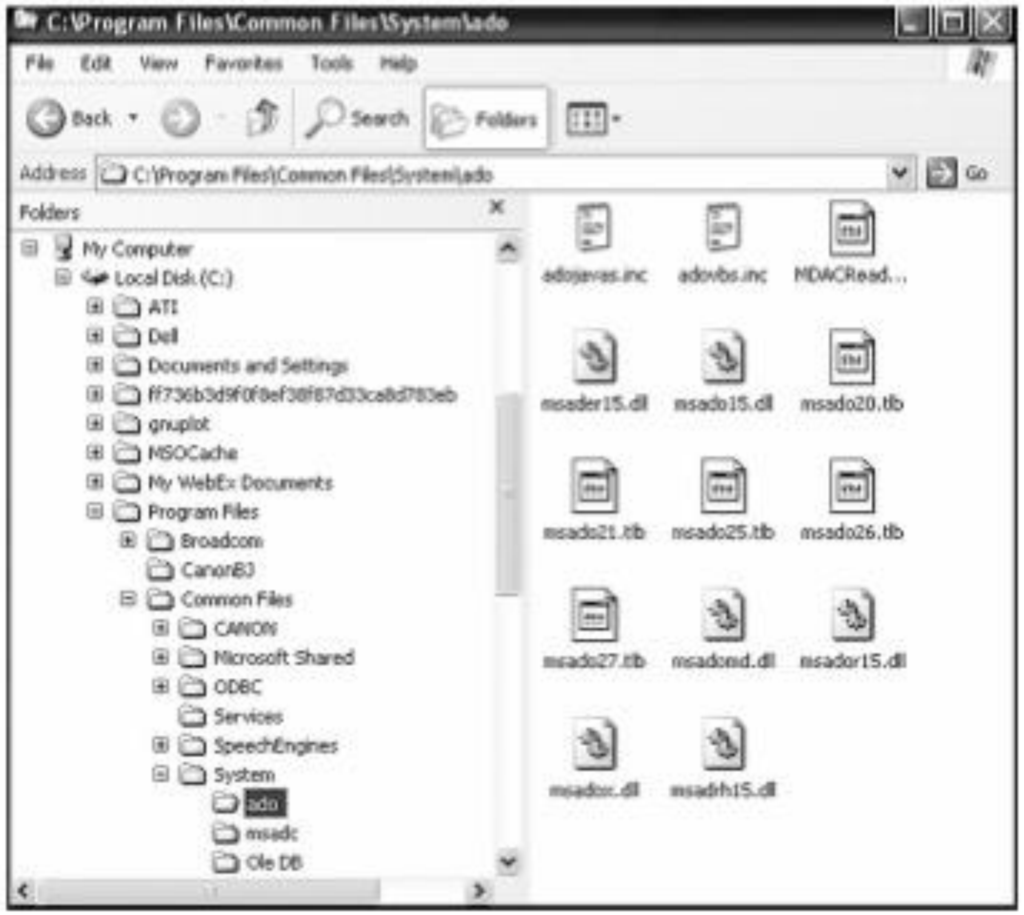
- A **filesystem** is an abstraction of how the external, nonvolatile memory of the computer is organized.
- Operating systems typically organize files hierarchically into folders, also called directories.



A filesystem as a tree

The Filesystem

- Each folder may contain files and/or subfolders.
- Thus, a volume, or drive, consists of a collection of nested folders that form a tree.
- The topmost folder is the root of this tree and is also called the root folder.

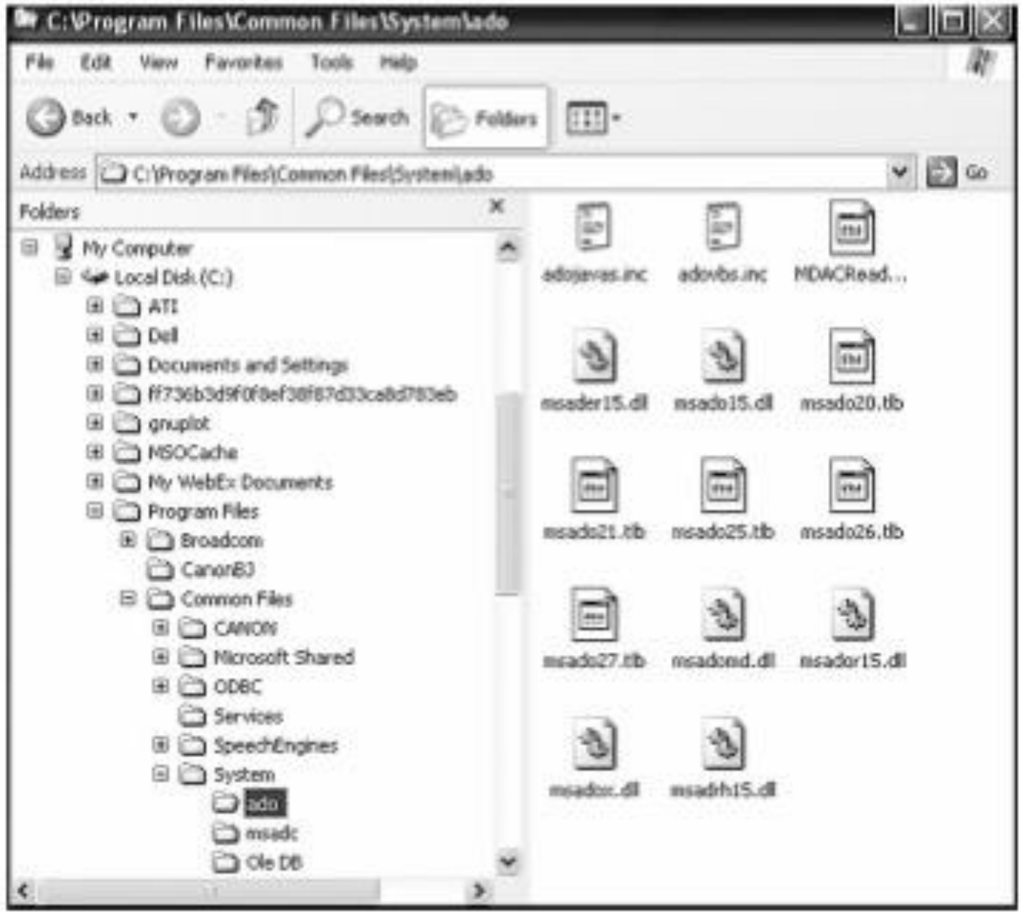


A filesystem as a tree

The Filesystem

Filesystem: filesystem is another key component of an operating system. It is an abstraction of how the external, nonvolatile memory of the computer is organized.

File Access Control: determine which uses can access which resources.

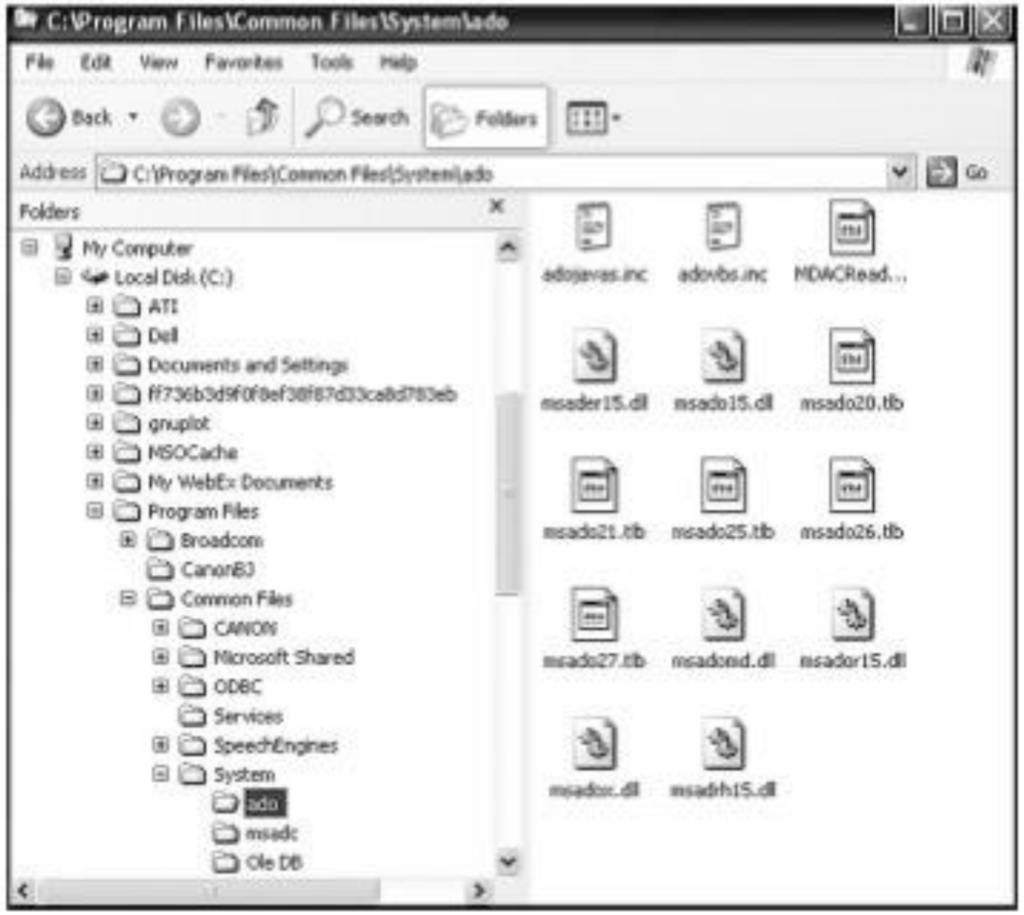


A filesystem as a tree

The Filesystem

File Permissions: file permissions are checked by the operating system to determine if a file is readable, writable, or executable by a user or group of users.

Unix File Permissions: the read, write, and execute bits are implemented in binary.



A filesystem as a tree

Memory Management

Memory Management: is another service that OS provides. Memory management refers to management of Primary Memory or Main Memory.

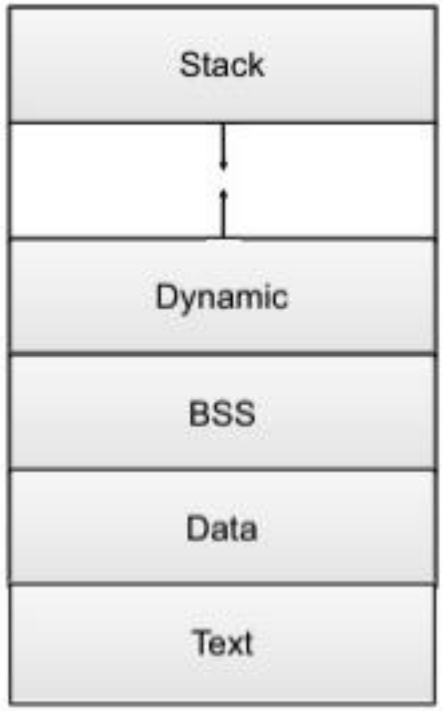
Text: machine code of the program

Data: static program variables (prior execution)

BSS: block started by symbol, contains static variables that are uninitialized

Heap: dynamic segment, stores data such as objects written in C++ or Java, during the execution.

Stack: houses a stack data structure.



The Unix memory model

Memory Management - example

Let's consider a simple program running on a computer:

- The program requires memory to store variables, data structures, and code instructions during its execution.
- When the program is launched, the operating system allocates a portion of the computer's memory to it.
- As the program executes, it creates and modifies variables, stores data, and executes instructions.
- The program may dynamically allocate memory for data structures, such as arrays or linked lists, as needed during runtime.
- Once the program finishes its execution, it releases the memory it was using back to the operating system for reuse.

Memory Management - example

Memory management involves several essential tasks, such as:

- **Memory Allocation:** The operating system must allocate memory to programs when they are executed. It must ensure that each program gets the required memory space without interfering with other programs or the operating system itself.

- **Memory Deallocation:** When a program completes its execution or no longer needs specific memory, the allocated memory should be released and made available for other processes.

- **Memory Protection:** The operating system must protect memory regions assigned to different processes, preventing one process from accessing or modifying the memory space of another process. This is crucial for security and stability.

- **Memory Swapping:** In systems with limited physical memory (RAM), memory swapping may occur, where parts of a program that are not currently in use are temporarily stored in the slower secondary storage (like the hard disk) to free up RAM for other processes.

Virtual Machines

Virtual machines (VMs) are software computers that provide the same functionality as physical computers.

Unlike emulators, VMs have direct access to the host CPU disks and RAM, so they run fast and efficient (compared to emulators).

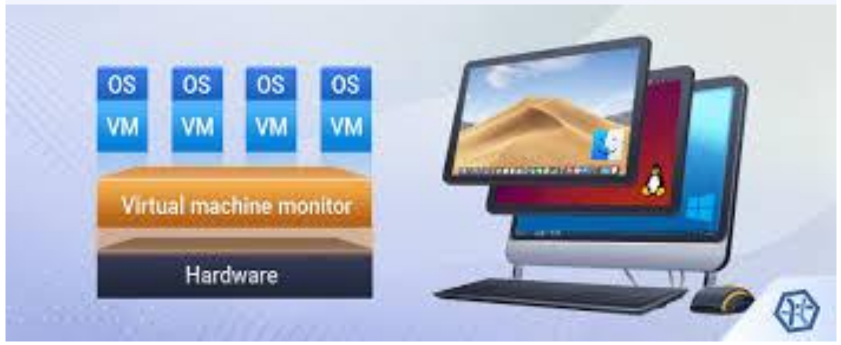
Advantages:

Many VMs in a single host – hardware cost is shared.

Portable – VM can be shut down and moved to another host and then started up again (sometimes automatically).

Secure – VM–Host interface acts as a sandbox. Prevents malware from getting out of VM.

Convenient – Easy to manage VM backups, ideal for remote access / monitoring. Great for security research.



Virtual Machines

Disadvantages

- Hosting may be in another (or unknown) legal jurisdiction.
- CIA issues.
- Infected VMs may be able to escape the VM "sandbox" and infect other VMs and the host. (see BluePill)
  - ➢ http://en.wikipedia.org/wiki/Blue_Pill_%28software%29
- Malware detection in the VM can be thwarted if malware detects that it is in a VM or sandbox (and stays inactive).
- Hiberfile, pagefile, .vmem and .vmdk files are susceptible to physical access attacks.
- Hosting company can access inside of VM through VMI extensions.
  - ➢ https://www.researchgate.net/publication/270081646_CloudSec_A_Security_Monitoring_Appliance_For_Virtual_Machines_In_The_IaaS_Cloud_Model

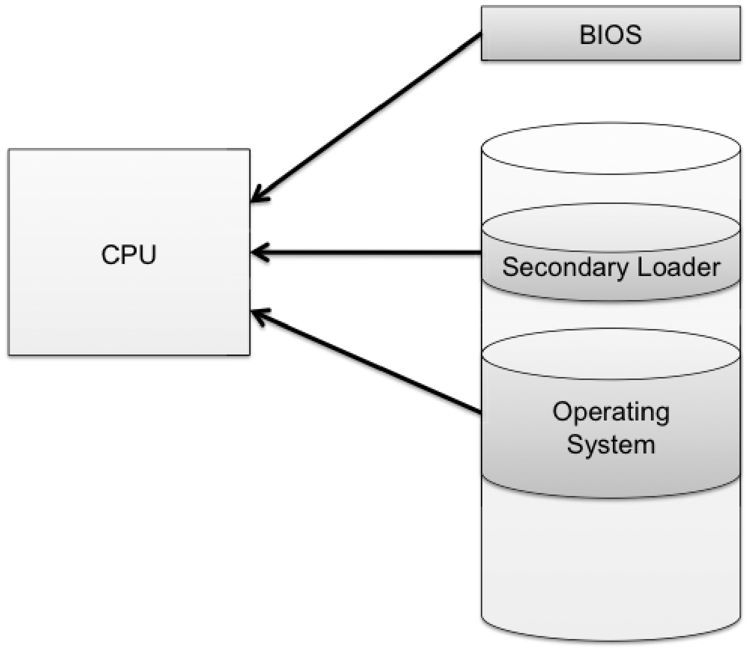
Two Types of Virtual Machines
Process virtual machines (platform-independent environment)
System virtual machines (Support the sharing of a host computer's physical resources)

The Boot Sequence

- The action of loading an operating system into memory from a powered-off state is known as booting or bootstrapping.

- When a computer is turned on, it first executes code stored in a firmware component known as the BIOS (basic input/output system).

- On modern systems, the BIOS loads into memory the second-stage boot loader, which handles loading the rest of the operating system into memory and then passes control of execution to the operating system.



BIOS Passwords

- A malicious user could potentially seize execution of a computer at several points in the boot process.

- To prevent an attacker from initiating the first stages of booting, many computers feature a BIOS password that does not allow a second-stage boot loader to be executed without proper authentication.

Hibernation

- Modern machines have the ability to go into a powered-off state known as hibernation.
- While going into hibernation, the OS stores the contents of machine's memory into a hibernation file (such as hiberfil.sys) on disk so the computer can be quickly restored later.
- But… without additional security precautions, hibernation exposes a machine to potentially invasive forensic investigation.

1. User closes a laptop computer, putting it into hibernation.

2. Attacker copies the hiberfil.sys file to discover any unencrypted passwords that were stored in memory when the computer was put into hibernation.

Hibernation - example

Let's consider a laptop user working on a project:

- The user is working on a document, editing and making changes.
- Suddenly, they realize that they need to attend an urgent meeting in a different location, and the laptop's battery is running low.
- Instead of shutting down the laptop and losing all their work progress, the user decides to hibernate the computer.
- They initiate the hibernation process through the operating system's power options or by closing the laptop lid (if configured to hibernate in such cases).
- The computer saves the current state, including all open applications, documents, and running processes, to the hard disk in a special file called the hibernation file.
- The laptop powers off completely, conserving the remaining battery power.

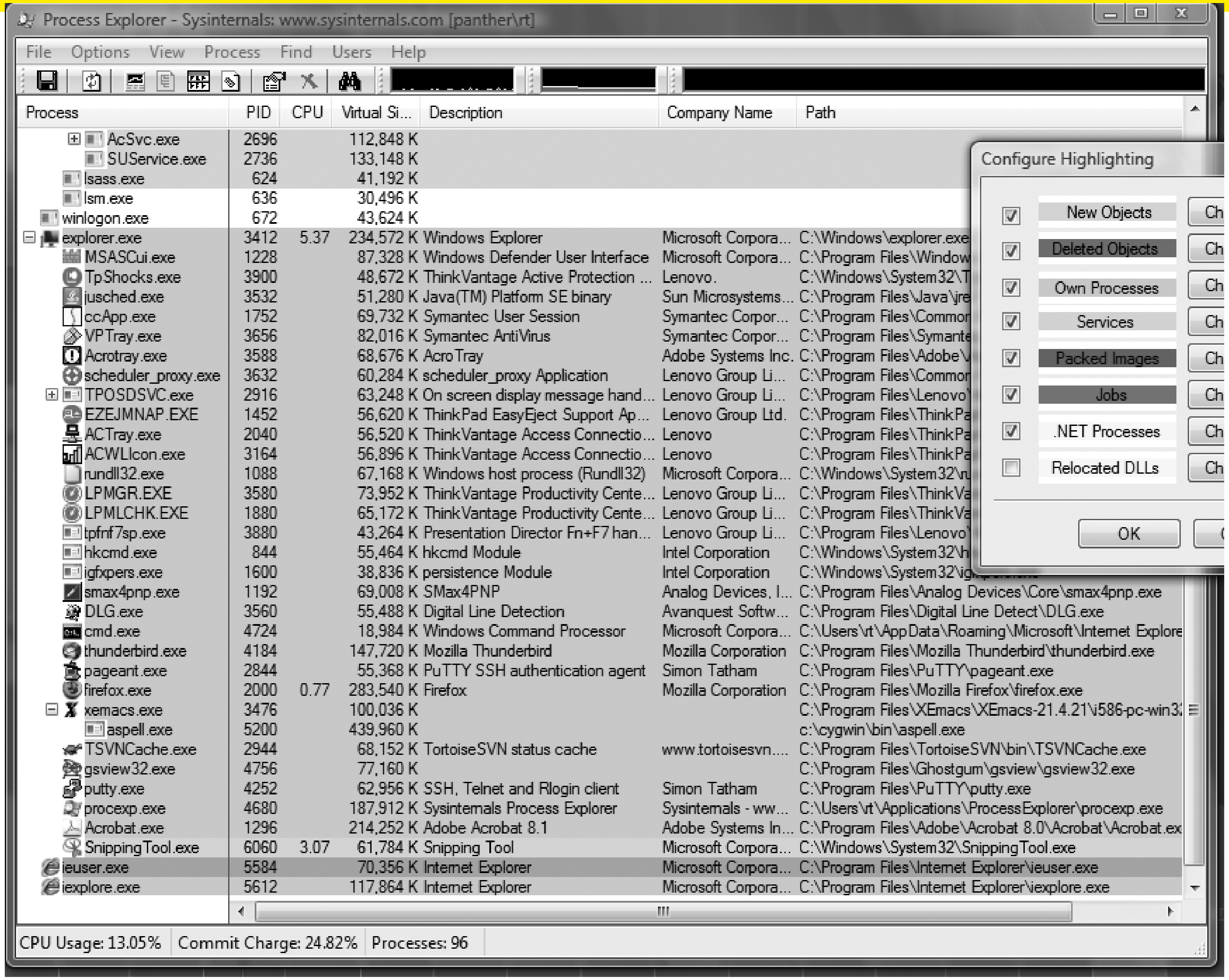
Hibernation - example

- Later, when the user needs to resume their work, they power on the laptop again.
- The operating system detects the hibernation file and restores the computer's exact state from when it was hibernated.
- The laptop resumes the document editing session, allowing the user to pick up right where they left off without any data loss.

Event Logging

- Keeping track of
  - ➢what processes are running,
  - ➢what other machines have interacted with the system via the Internet, and
  - ➢if the operating system has experienced any unexpected or suspicious behavior
  - ➢can often leave important clues not only for troubleshooting ordinary problems, but also for determining the cause of a security breach.

Process Explorer


Process Explorer - Sysinternals: www.sysinternals.com [panther\rt]

File Options View Process Find Users Help

Process	PID	CPU	Virtual Si...	Description	Company Name	Path
AcSvc.exe	2696		112,848 K			
SUService.exe	2736		133,148 K			
lsass.exe	624		41,192 K			
lsm.exe	636		30,496 K			
winlogon.exe	672		43,624 K			
explorer.exe	3412	5.37	234,572 K	Windows Explorer	Microsoft Corpora...	C:\Windows\explorer.exe
MSASCui.exe	1228		87,328 K	Windows Defender User Interface	Microsoft Corpora...	C:\Program Files\Window
TpShocks.exe	3900		48,672 K	ThinkVantage Active Protection ...	Lenovo.	C:\Windows\System32\T
jusched.exe	3532		51,280 K	Java(TM) Platform SE binary	Sun Microsystems...	C:\Program Files\Java\jre
ccApp.exe	1752		69,732 K	Symantec User Session	Symantec Corpor...	C:\Program Files\Common
VPTray.exe	3656		82,016 K	Symantec AntiVirus	Symantec Corpor...	C:\Program Files\Symante
Acrotray.exe	3588		68,676 K	AcroTray	Adobe Systems Inc.	C:\Program Files\Adobe\
scheduler_proxy.exe	3632		60,284 K	scheduler_proxy Application	Lenovo Group Li...	C:\Program Files\Common
TPOSDSVC.exe	2916		63,248 K	On screen display message hand...	Lenovo Group Li...	C:\Program Files\Lenovo
EZEJMNAP.EXE	1452		56,620 K	ThinkPad EasyEject Support Ap...	Lenovo Group Ltd.	C:\Program Files\ThinkPa
ACTray.exe	2040		56,520 K	ThinkVantage Access Connectio...	Lenovo	C:\Program Files\ThinkPa
ACWLIcon.exe	3164		56,896 K	ThinkVantage Access Connectio...	Lenovo	C:\Program Files\ThinkPa
rundll32.exe	1088		67,168 K	Windows host process (Rundll32)	Microsoft Corpora...	C:\Windows\System32\ru
LPMGR.EXE	3580		73,952 K	ThinkVantage Productivity Cente...	Lenovo Group Li...	C:\Program Files\ThinkVa
LPMLCHK.EXE	1880		65,172 K	ThinkVantage Productivity Cente...	Lenovo Group Li...	C:\Program Files\ThinkVa
tpfnf7sp.exe	3880		43,264 K	Presentation Director Fn+F7 han...	Lenovo Group Li...	C:\Program Files\Lenovo
hkcmd.exe	844		55,464 K	hkcmd Module	Intel Corporation	C:\Windows\System32\h
igfxpers.exe	1600		38,836 K	persistence Module	Intel Corporation	C:\Windows\System32\ig
smax4pnp.exe	1192		69,008 K	SMax4PNP	Analog Devices, I...	C:\Program Files\Analog Devices\Core\smax4pnp.exe
DLG.exe	3560		55,488 K	Digital Line Detection	Avanquest Softw...	C:\Program Files\Digital Line Detect\DLG.exe
cmd.exe	4724		18,984 K	Windows Command Processor	Microsoft Corpora...	C:\Users\rt\AppData\Roaming\Microsoft\Internet Explore
thunderbird.exe	4184		147,720 K	Mozilla Thunderbird	Mozilla Corporation	C:\Program Files\Mozilla Thunderbird\thunderbird.exe
pageant.exe	2844		55,368 K	PuTTY SSH authentication agent	Simon Tatham	C:\Program Files\PuTTY\pageant.exe
firefox.exe	2000	0.77	283,540 K	Firefox	Mozilla Corporation	C:\Program Files\Mozilla Firefox\firefox.exe
xemacs.exe	3476		100,036 K			C:\Program Files\XEmacs\XEmacs-21.4.21\i586-pc-win3
aspell.exe	5200		439,960 K			c:\cygwin\bin\aspell.exe
TSVNCache.exe	2944		68,152 K	TortoiseSVN status cache	www.tortoisesvn....	C:\Program Files\TortoiseSVN\bin\TSVNCache.exe
gsview32.exe	4756		77,160 K			C:\Program Files\Ghostgum\gsview\gsview32.exe
putty.exe	4252		62,956 K	SSH, Telnet and Rlogin client	Simon Tatham	C:\Program Files\PuTTY\putty.exe
procexp.exe	4680		187,912 K	Sysinternals Process Explorer	Sysinternals - ww...	C:\Users\rt\Applications\ProcessExplorer\procexp.exe
Acrobat.exe	1296		214,252 K	Adobe Acrobat 8.1	Adobe Systems In...	C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrobat.ex
SnippingTool.exe	6060	3.07	61,784 K	Snipping Tool	Microsoft Corpora...	C:\Windows\System32\SnippingTool.exe
ieuser.exe	5584		70,356 K	Internet Explorer	Microsoft Corpora...	C:\Program Files\Internet Explorer\ieuser.exe
iexplore.exe	5612		117,864 K	Internet Explorer	Microsoft Corpora...	C:\Program Files\Internet Explorer\iexplore.exe

CPU Usage: 13.05% Commit Charge: 24.82% Processes: 96

Configure Highlighting

✓	New Objects	Ch
✓	Deleted Objects	Ch
✓	Own Processes	Ch
✓	Services	Ch
✓	Packed Images	Ch
✓	Jobs	Ch
✓	.NET Processes	Ch
	Relocated DLLs	Ch

OK

Seeing Processes

- On Windows, ctrl/alt/del ➔ choose task manager ➔ select processes
- On Linux, ps lists your processes. Various switches allow access to system wide processes.
  - ➢For example,

    ```
    ps –e
    ```

    lists all processes on the machine.