

HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 5



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Operating System Overview

- An operating system (OS) is a platform that manages computer hardware and software resources. It is required for the normal operation of a computer. During the development of personal computers (PCs), there have been many different operating systems - the most commonly used include DOS, Windows, Linux, Unix (Mac), and OS/2.
- This course describes the Windows and Linux operating systems.

Objectives

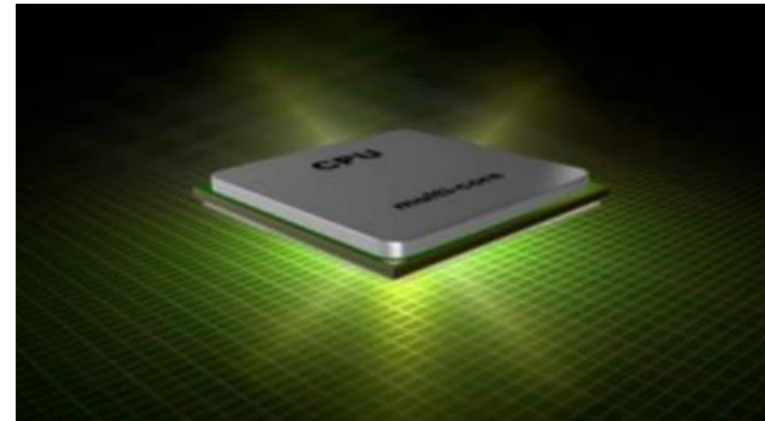
- **Upon completion of this course, you will be able to:**
 - ❑ **Describe the main functions of an operating system.**
 - ❑ **Describe features of the Windows operating system.**
 - ❑ **Describe the development history of the Linux operating system.**

- **An operating system:**
 - ❑ **is an interface between users and computers**
 - ❑ **manages all hardware resources and controls the execution of software**
 - ❑ **improves the human-machine interaction interface**
 - ❑ **is a (system) software program**

- The main task of processor management is to allocate, control, and manage processor resources. In a multiprogramming environment, a process is the basic unit for the allocation and running of processor resources. Therefore, processor management can be included in process management.

Processor management includes:

- ☐ Process control
- ☐ Process synchronization
- ☐ Process communication
- ☐ Process scheduling



- **Process control:** Process control refers to controlling and managing resources of running processes.
- **Process synchronization:** Process synchronization is a technique used to ensure the concurrent execution of collaborative processes using shared data.
- **Process communication:** Process communication refers to data transmission between processes.
- **Process scheduling:** When multiple programs run concurrently, each program requires processor resources. The OS dynamically allocates processor resources to a process for process running. This is called process scheduling.

- The main task of memory management is to allocate memory resources to programs and manage these resources. Memory management facilitates memory usage and logical expansion. Therefore, memory management should provide:

- ☐ Memory allocation
- ☐ Memory protection
- ☐ Memory expansion



- **Memory allocation:** Memory allocation refers to the process of allocating memory during process execution.
- **Memory protection:** Before memory is allocated, the OS must be protected from the impact of the user processes, and the running user process must be protected from being affected by other user processes.
- **Memory expansion:** The execution of large or multiple programs may require more memory than the system supports or has installed. Therefore, memory management needs to support memory expansion.

• The main task of device management is to execute I/O requests, classify I/O devices, and facilitate CPU and I/O device usage. To achieve this, device management should provide:

- ☐ Buffer management
- ☐ Device allocation
- ☐ Device virtualization

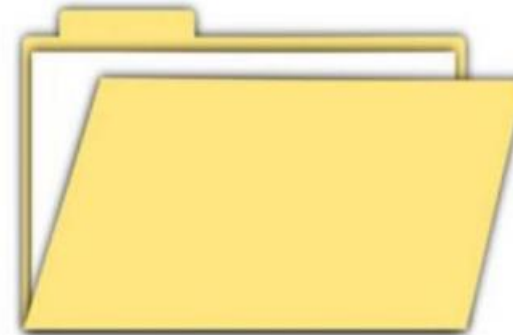


• **Buffer management:** To mitigate the difference in speed between the CPU and I/O device and improve the concurrent running of the CPU and I/O device, in modern OSes, almost all I/O devices use buffers when exchanging data with the processor. The main task of buffer management is to organize these buffers and provide means to obtain and release buffers.

• **Device allocation:** When a process sends an I/O request to the system, the device allocation program allocates the device to the process in accordance to specific policies.

• **Device virtualization:** Device virtualization is the act of creating multiple logical versions of a physical device for multiple user processes to use.

- In modern computer systems, programs and data are stored as files.
- The main task of file management is to manage user and system files. File management facilitates file usage and security. To achieve this, file management should provide functions such as file storage space management, file read and write management, directory management, and file sharing and protection.



• The main task of job management is to provide a stable environment suitable for users to effectively organize their workflows. Job management should provide:

- ☐ Task and interface management
- ☐ Human-machine interaction
- ☐ Graphical interfaces
- ☐ Language control



Different operating systems are difficult to categorize due to their diverse nature. However, some general categorization types are as follows:

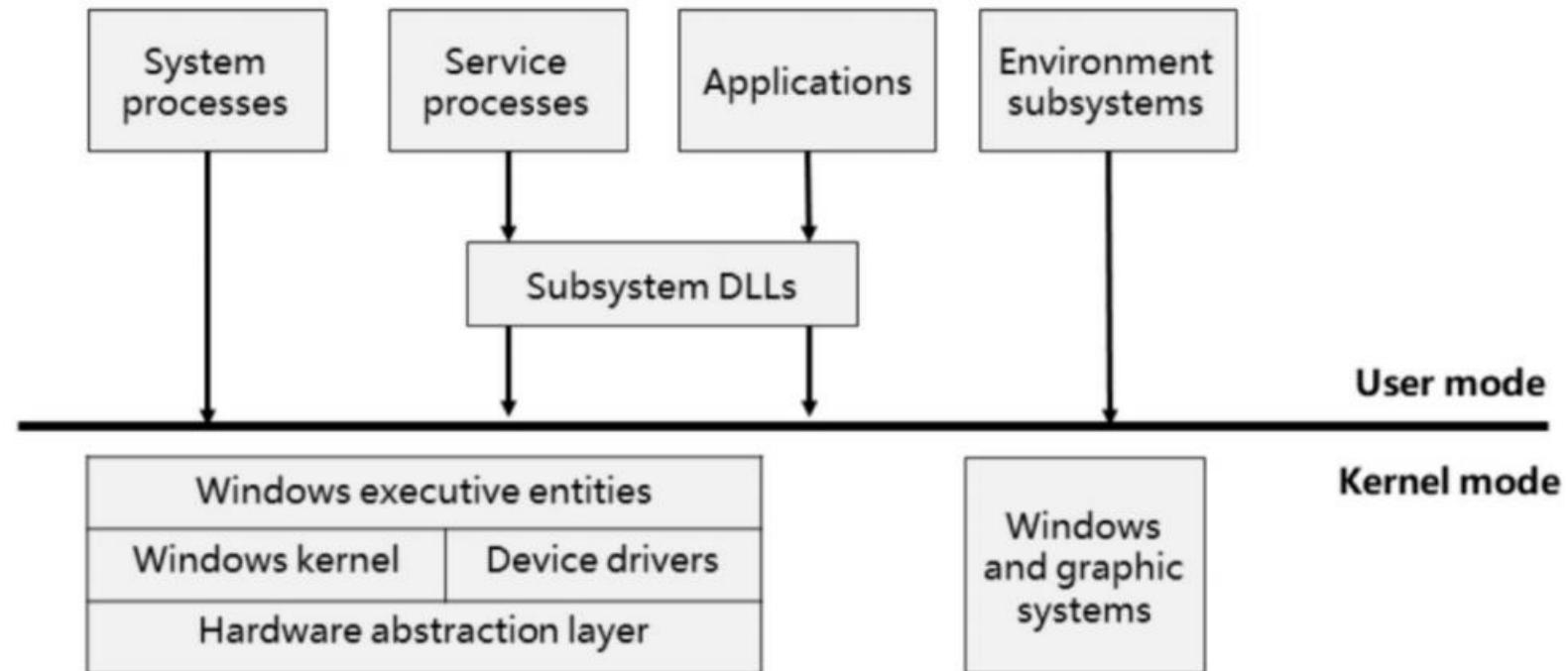
- **By application domain:** Operating systems can be categorized into desktop operating systems, server operating systems, and embedded operating systems.
- **By the number of supported users:** Operating systems can be categorized into single-user operating systems (such as MS-DOS and OS/2) and multi-user operating systems (such as Unix, Linux, and Windows).
- **By the openness of source code:** Operating systems can be categorized into open- source operating systems (such as Linux and FreeBSD) and closed-source operating systems (such as Mac OS X and Windows).

- In 1985, Microsoft officially released the first-generation window-based multitasking system—Windows 1.0. Due to the hardware limitation at that time, Windows 1.0 did not draw the expected social attention and did not play its advantages. However, the launch of the operating system indicated that PCs entered the era of GUI. In GUI operating systems, most operation objects are represented by icons, which are intuitive and user-friendly and can better meet actual needs of some users.



- Microsoft Windows is a group of operating systems developed by the American multinational technology company Microsoft. Windows was first introduced by Microsoft in 1985 as a Microsoft-DOS simulation environment. Its later versions were gradually developed into operating systems designed mainly for PCs and server users and came to dominate the world's PC market. The Windows operating systems can run on multiple different types of platforms, such as PCs, mobile devices, servers, and embedded systems. They are most commonly used on PCs.
- Modern Windows operating systems use GUIs and are more user-friendly than text based DOS operating systems, which required users to enter instructions for use. As computer hardware and software has developed, Microsoft Windows has evolved from 16 bits to 32 bits and then to 64 bits. Different versions have also evolved, from Windows 1.0 to Windows 95, Windows 98, Windows ME, Windows 2000, Windows 2003, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, and Windows Server. Microsoft continues to develop and improve the Windows operating systems.
- The latest stable Windows operating system is Windows 10, which was released on July 29, 2015. The latest stable operating system of Windows Server is Windows Server 2016, which was released on September 26, 2016.

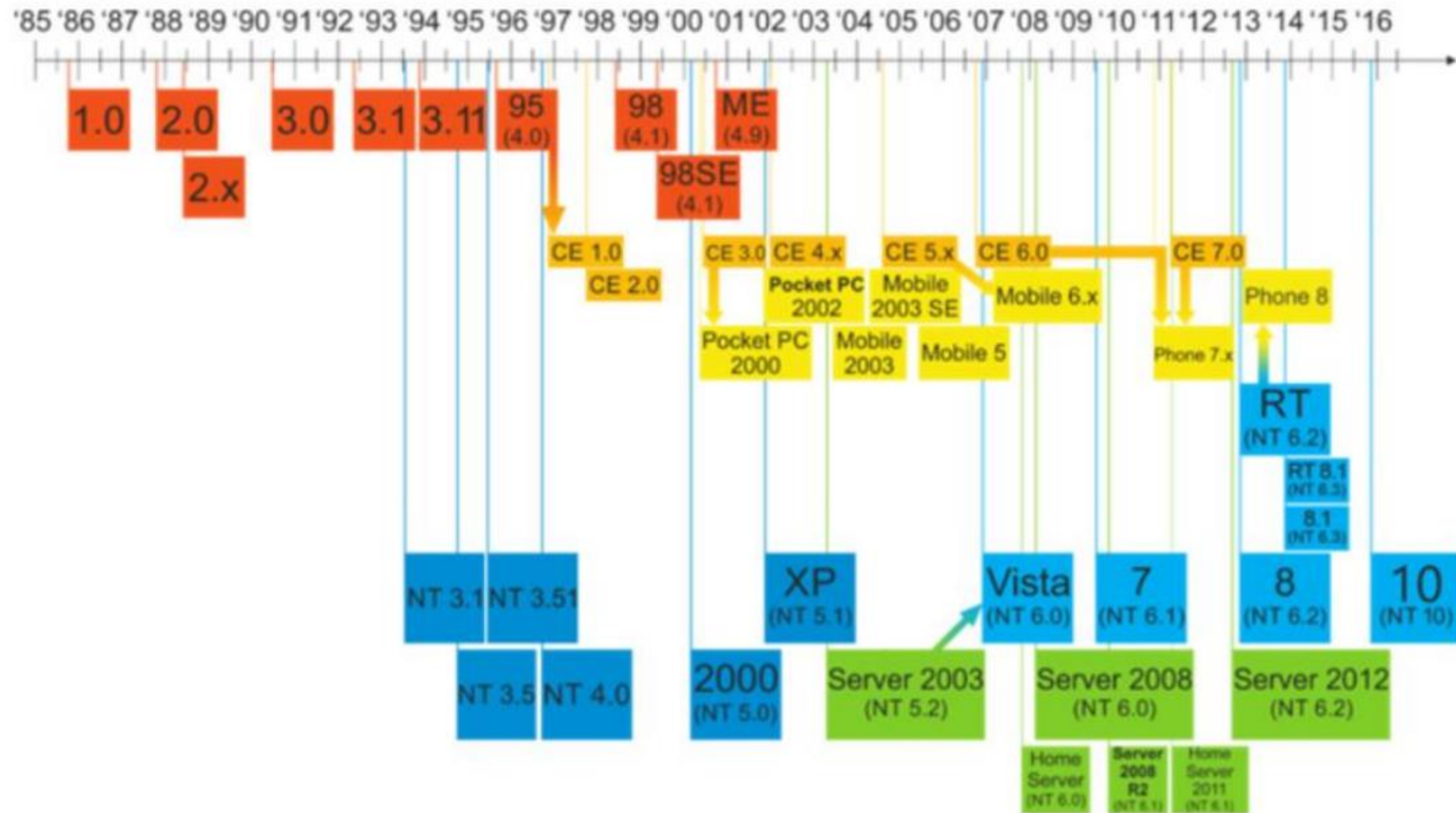
- The following figure shows the simplified architecture of the Windows operating system.



The four types of processes in the user mode are:

- **Fixed system processes**, such as the login process and session manager. They are not Windows services (that is, they are not started through the service control manager [SCM]).
- **Service processes**, such as the task dispatcher and printer service. Users can run these processes after login. Many service applications, such as SQL server and exchange server, run as services.
- **Applications**: Applications can be 32-bit or 64-bit Windows, 16-bit Windows 3.1, 16-bit MS-DOS, or 32-bit or 64-bit POSIX. Note that the 16-bit applications can run only on the 32-bit systems.
- **Environment subsystems**: Environment subsystems expose the operating system functions to applications through application programming interfaces (APIs), including Windows API, POSIX, and OS/2 APIs (available in earlier versions of Windows NT). Windows 2000 is the last subsystem with POSIX and OS/2. The flagship versions and enterprise editions of Windows also support an enhanced POSIX subsystem named SUA (Unix-based application).
- **Note the "subsystem DLL" under the service processes and applications**. In Windows, applications can only invoke local Windows services through the subsystem DLLs. The role of a subsystem DLL is to translate a documented function into a required non documented system service (undisclosed).

- The kernel mode consists of the following components:
 - Windows executive entities, including basic system services such as memory manager, process and thread manager, security manager, I/O manager, network, and inter-process communication.
 - The Windows kernel, including underlying system functions such as thread dispatching, interruption, exception distribution, and concurrent running of multiple CPUs. It also provides some routines and basic objects that implement the high-level structure.
 - Device drivers, including hardware device drivers (translating user I/O to hardware I/O) and software drivers (such as file and network drivers).
 - Hardware abstraction layer, a layer of programming independent of the kernel. It isolates the operating system from platform-specific hardware differences.
 - Windows and graphics systems, which implement GUI functions and process user interfaces and rendering.



- **What is the difference between an operating system designed for servers and an operating system designed for individuals?**
 - ❑ **The performance of an operating system designed for servers is more stable than that of an operating system designed for individuals.**
 - ❑ **In file management or network applications, an operating system designed for servers provides higher performance.**
 - ❑ **In graphics and entertainment, an operating system designed for individuals provides better functionality.**
 - ❑ **In terms of security and coordination, an operating system designed for servers outperforms an operating system designed for individuals.**
- **An operating system designed for servers supports special hardware, contains dedicated functions and management tools for server operation, and has stricter requirements on security and stability. Therefore, such an operating system may provide relatively lower speed.**
- **An operating system designed for individuals does not need, nor does it provide, professional functions. However, it adds media management software and functions for individual users.**

- **Intuitive and efficient object-oriented GUIs that are easy to learn and use**
- **The most widely used and most compatible operating system worldwide**
- **Unified, friendly, and neat UIs**
- **Various device-independent graphical operations**
- **Multi-user and multitasking**



Personal office



Enterprise servers



Bank ATMs



Mobile phones

- Before the Linux operating system was developed, UNIX and Microsoft Windows dominated the computer operating system market.
 - UNIX had many enterprise users and was the de facto operating system standard for many small-, medium, and large-sized computers, workstations, and high-end microcomputers.
 - Microsoft Windows occupied most of the microcomputer operating system market due to its ease of use.
- However, both operating systems are commercial software. UNIX in particular was not popular among common users due to its high purchase price. In response to this issue, several free operating systems with most functions of the Unix operating system were launched.

- Multics program

- In the 1960s, computers were not very popular, and only a handful of people could use them. Computer systems at that time only supported batch processing, that is, users submitted a batch of tasks and then waited for the results. Users could not interact with computers during task processing. A computer took a long time to process a batch of tasks, during which period the computer could not be used by others, resulting in a waste of computer resources.

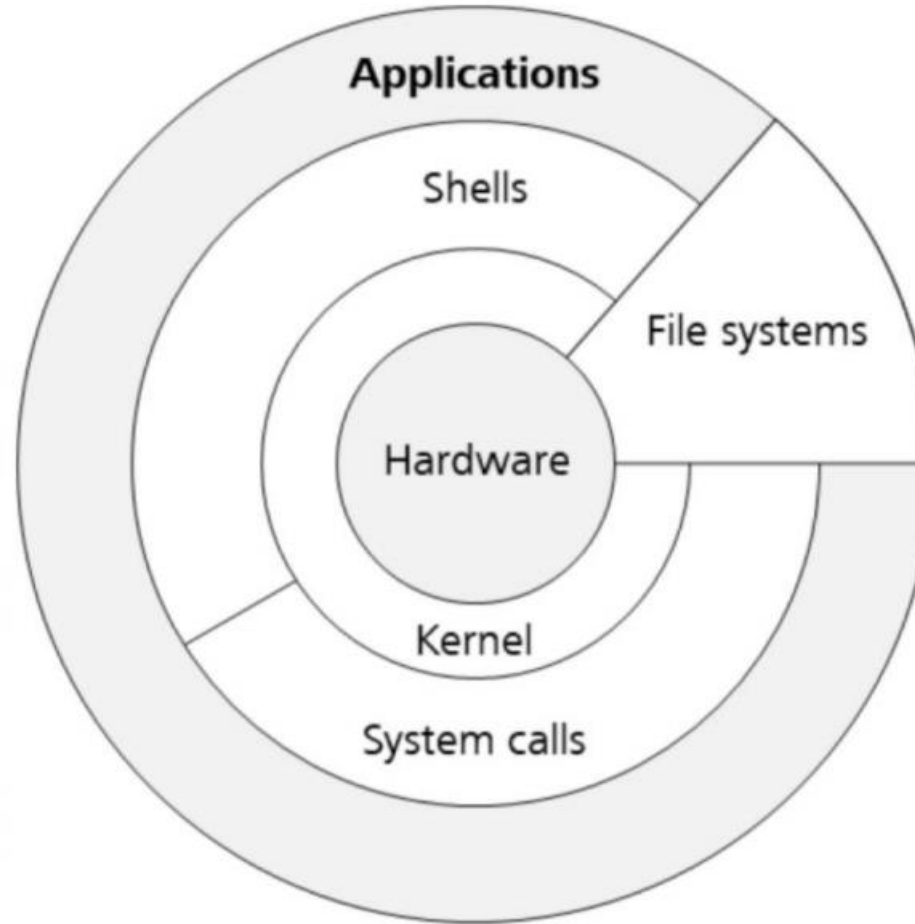
- To address this situation, in the mid-1960s, AT&T Bell Labs, the Massachusetts Institute of Technology (MIT), and General Electric (GE) worked together to develop an experimental time-sharing multitasking processing system called Multiplexed Information and Computing Service (Multics), which was intended to allow multiple users to access a mainframe simultaneously. Due to the project complexity and dissatisfied with the project's progress, Bell Labs management ultimately withdrew.

- UNIX

- While working on Multics, Ken Thompson, a programmer in Bell Labs' computing research department, programmed a game called Space Travel. After Bell Labs withdrew from the Multics project, Ken Thompson and Dennis Ritchie found an idle PDP-7 machine and wrote a revised edition of Multics using the C language on the machine. The operating system they wrote was officially released in 1971 and later became the UNIX recognized today.



- Andrew S. Tanenbaum, a Dutch computer scientist, developed the Unix-like operating system Minix, which was mainly used for educational purposes.
- Linus Torvalds, a Finnish college student, created an operating system kernel based on Minix. The kernel was further developed and released in October 1991 as Linux 0.02. Since then, enthusiasts and hackers around the world have contributed to its development.
- Source code of the Linux kernel can be obtained free of charge. Many companies pack and improve the kernel source code to form their own products, that is, Linux distributions.
- Apple Inc., Microsoft, and Linux use a bitten apple, a window, and a penguin named Tux, respectively, as their logos.
- History of Linux's logo
 - ❑ When the official Linux kernel 1.0 was published in 1994, Linus Torvalds was invited to find a mascot for Linux. He chose a penguin as the mascot after remembering an incident in an Australian zoo, where he was bitten by a penguin.
 - ❑ Another more widely accepted view is that the penguin represents the South Pole, which is shared globally without any one country having ownership. That is, Linux does not belong to any particular company. It is a technology shared by everyone.



- Generally, the Linux system has four major parts: the kernel, shells, file systems, and applications.
- The kernel, shells, file systems, and applications are used to manage files and use the system.
- Linux kernel
 - The kernel is the core of the operating system and provides many basic functions. It manages the processes, memory, device drivers, files, and network systems of the operating system, and determines the system performance and stability.
 - The Linux kernel consists of components such as memory manager, process manager, device drivers, file systems, and network manager.
- Linux Shells
 - The shell is the user interface (UI) provided by the operating system for users to interact with the kernel. It receives user-input commands and sends the commands to the kernel for execution. A shell is a command interpreter. The shell programming language shares many characteristics of common programming languages. Shell programs written in this programming language have the same functions as other applications.
- Linux file systems
 - A file system controls how data is stored on storage devices such as disks. Linux supports multiple popular file systems, such as EXT2, EXT3, FAT, FAT32, VFAT, and ISO 9660.
- Linux applications
 - Generally, a standard Linux system has a set of applications, including text editors, programming languages, X Window, office suites, Internet tools, and databases.

- Linux has two defining features:
 - ❑ Everything is a file.
 - ❑ Each software program has a defined purpose.
- The first feature means that, in Linux, the Linux kernel regards everything (including commands, hardware and software devices, operating systems, and processes) as a file of a specific type with its own features. Linux is based on Unix, which is largely because they share this basic idea.



- **Free of charge:**

- ❑ Linux is a free-of-charge operating system that can be downloaded from the Internet or obtained in other ways. Its source code can be changed by users as required. This is a unique advantage that attracts countless programmers worldwide to modify and change Linux as they want, which in turn helps Linux continue to develop.

- **Multi-user and multitasking:**

- ❑ Linux allows multiple users to use the computer without other users affecting them. This is because each user has their own special rights to their own file devices. Multitasking is the most important feature of current computers. Linux allows multiple applications to run concurrently without being affected by others.

- **User-friendly interfaces:**

- ❑ The Linux operating system supports both the command line interface (CLI) and GUI. On a CLI, users can enter commands. The Linux system also provides an X- Window system similar to the Windows GUI. Through the X-Window system, users can use a mouse to perform operations.

- **Supporting multiple platforms:**

- ❑ The Linux system can run on multiple hardware platforms, such as platforms with x86, 680x0, SPARC, and Alpha processors. Linux is an embedded operating system that can run on various devices, such as handheld computers, set-top boxes (STBs), and games consoles. The Linux kernel 2.4, released in January 2001, fully supported the 64-bit Intel chips. Linux also supports the multi-processor technology, which allows multiple processors to work at the same time, greatly improving system performance.



Military equipment



Enterprise servers



Network devices



Gaming consoles

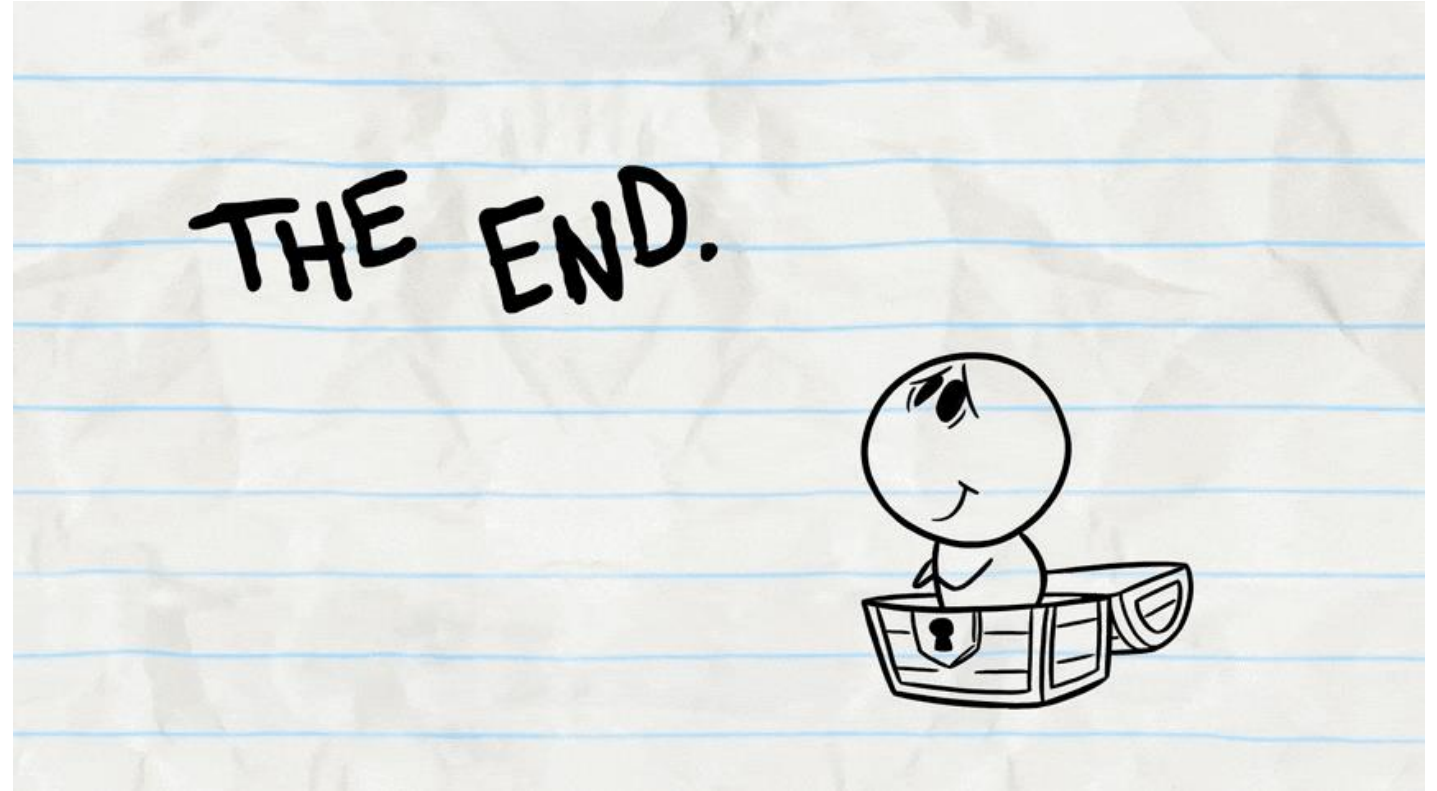
Comparison Between Windows and Linux

Operating System	Cost	Software Support	Security	Usage	Customizability
Linux	Free or minimal charge	A relatively small number of software programs can run directly in Linux	Low risks of virus infection	Difficult for beginners to use; learning and guidance required	Open source code
Windows	Charged	Many software titles, including games, can run in Windows	Frequent system patching and a high risk of virus infection	Easy to use for beginners	Difficult to be customized

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY