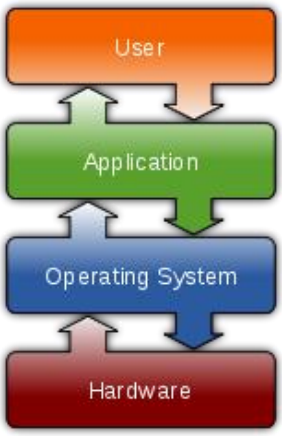
SOFTWARE CONCEPTS

Types of Software

Operating System:

An **operating system** (**OS**) is a collection of software that manages computer hardware resources and provides common services for computer programs. The operating system is a vital component of the system software in a computer system. Application programs require an operating system to function. For hardware functions such as input and output and memory allocation, the operating system acts as an intermediary between programs and the computer hardware . The most popular and latest ones include the Windows XP, Mac, UNIX, Linux, Windows Vista, etc.



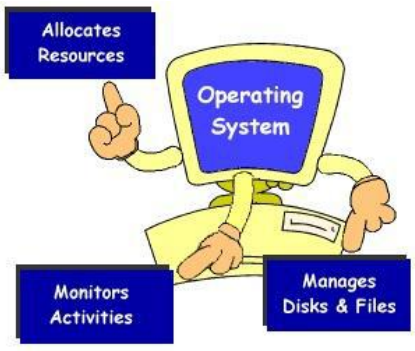
Functions of an Operating System

The major functions of an OS are:

-resource management,
-data management,
-job (task) management, and
-standard means of communication between user and computer.

The resource management function of an OS allocates computer resources such as CPU time, main memory, secondary storage, and input and output devices for use.

The data management functions of an OS govern the input and output of the data and their location, storage, and retrieval



Need of an Operating System:

At the simplest level, an operating system does two things:

1. It manages the hardware and software resources of the system. In a desktop computer, these resources include such things as the processor, memory, disk space, etc. (On a cell phone, they include the keypad, the screen, the address book, the phone dialer, the battery and the network connection.)
2. It provides a stable, consistent way for applications to deal with the hardware without having to know all the details of the hardware.

The first task, managing the hardware and software resources, is very important, as various programs and input methods compete for the attention of the **central processing unit** (CPU) and demand memory, storage and input/output (I/O) bandwidth for their own purposes. In this capacity, the operating system plays the role of the good parent, making sure that each application gets the necessary resources while playing nicely with all the other applications, as well as husbanding the limited capacity of the system to the greatest good of all the users and applications.

The second task, providing a consistent application interface, is especially important if there is to be more than one of a particular type of computer using the operating system, or if the hardware making up the computer is ever open to change. A consistent **application program interface** (API) allows a software developer to write an application on one computer and have a high level of confidence that it will run on another computer of the same type, even if the amount of memory or the quantity of storage is different on the two machines.

In earlier day's user had to design the application according to the internal structure of the hardware. Operating System was needed to enable the user to design the application without concerning the details of the computer's internal structure. In general the boundary between the hardware & software is transparent to the user.

1. Easy interaction between the human & computer.
2. Starting computer operation automatically when power in turned on.
3. Loading & scheduling users program.
4. Controlling input & output.
5. Controlling program execution.
6. Managing use of main memory.
7. Providing security to users program.

For hardware functions such as input and output and memory allocation, the Operating System acts as an intermediary between application programs and the computer hardware, although the application code is usually executed directly by the hardware and will frequently call the OS or be interrupted by it.

Process management:

It deals with running multiple processes. Most operating system allows a process to be assigned a priority which affects its allocation of CPU time. Interactive operating systems also employ some level of feedback in which the task with which the user is working receives higher priority. In many systems there is a background process which runs when no other process is waiting for the CPU.

Memory management:

It is the act of managing computer memory. The essential requirement of memory management is to provide ways to dynamically allocate portions of memory to programs at their request, and freeing it for reuse when no longer needed. This is critical to the computer system.

Several methods have been devised that increase the effectiveness of memory management. Virtual memory systems separate the memory addresses used by a process from actual physical addresses, allowing separation of processes and increasing the effectively available amount of RAM using paging or swapping to secondary storage. The quality of the virtual memory manager can have an extensive effect on overall system performance.

Disk and file systems:

Operating systems have a variety of native file systems that controls the creation, deletion, and access of files of data and programs.

Networking:

A **computer network**, or simply a **network**, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information.[1] Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network.

Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

Security:

Most operating systems include some level of security.

Language Processor

Assembler:

It is a computer program to translate between lower-level representations of computer programs; it converts basic computer instructions into a pattern of bits which can be easily understood by a computer and the processor can use it to perform its basic operations

Compiler:

A **compiler** is a computer program (or set of programs) that transforms source code written in a programming language (the *source language*) into another computer language (the *target language*, often having a binary form known as *object code*). The most common reason for wanting to transform source code is to create an executable program.
A compiler can translate the programs of only that language for which it is written. For example C++ compiler can translate only those programs, which are written in C++. Each machine requires a separate compiler for each high level language.

Interpreter:

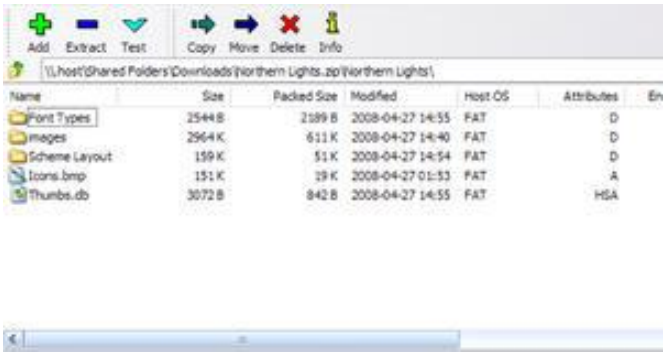
An interpreter is a program that converts one statement of a program at a time. It executes this statement before translating the next statement of the source program. If there is an error in the statement, the interpreter will stop working and displays an error message. The advantage of interpreters over compilers is that an error is found immediately. So the programmer can make corrections during program development.

Utility Software:

Utility software is system software designed to help analyze, configure, optimize or maintain a computer. A single piece of utility software is usually called a **utility** or **tool**.

Utility software usually focuses on *how* the computer infrastructure (including the computer hardware, operating system, application software and data storage) operates. Due to this focus, utilities are often rather technical and targeted at people with an advanced level of computer knowledge - in contrast to application software, which allows users to do things like creating text documents, playing games, listening to music or viewing websites.

Compression Tools: Data compression can be used for many purposes on computers and achieved in many ways. There are two types of data compression, lossy and lossless. Lossy compression makes data smaller by removing excess data so that the end result is still acceptable for its purpose. This is a one-way process and the compressed data is the result. Lossless compression makes data smaller by looking for patterns that can be written more concisely. This is a reversible process and a compressed file is the result. This file will have to be decompressed to access the original data. Advantages of data compression are that compressed data will take up less space on a computer and be quicker to transmit. Ex: 7-Zip, IZArc, WinRAR, PeaZip, The Unarchiver,

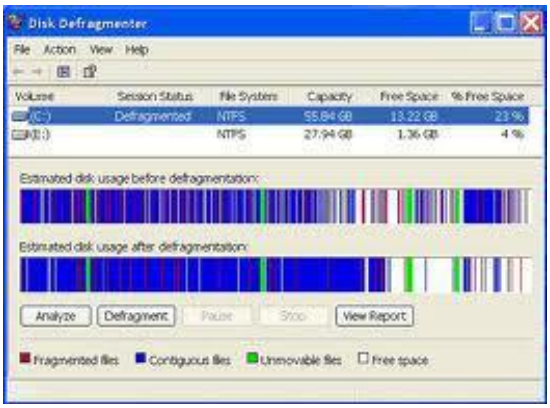


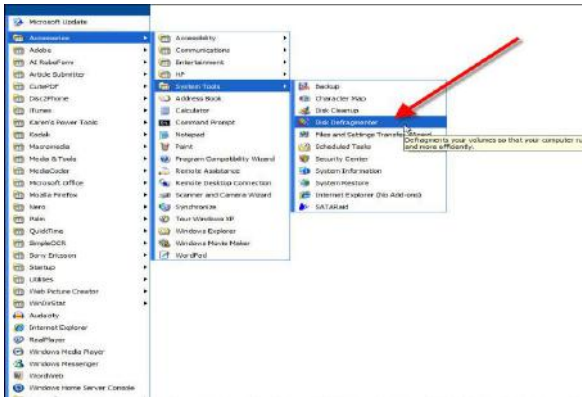
Data compression for computer files is a lossless compression
Data compression for audio can be lossy or lossless

Data compression of images can be either lossy or lossless depending on the compression format used.

Data compression of video is primarily lossy

Disk Defragmenter:





Disk Defragmenter is a utility in Microsoft Windows designed to increase access speed by rearranging files stored on a disk to occupy contiguous storage locations, a technique called defragmentation. Defragmenting a disk minimizes head travel, which reduces the time it takes to read files from and write files to the disk.[1] Beginning with Windows XP, Disk Defragmenter also reduces system startup times

Antivirus:

Antivirus or **anti-virus software** is software used to prevent, detect and remove malware (of all descriptions), such as: computer viruses, adware, backdoors, malicious BHOs, dialers, fraudtools, hijackers, keyloggers, malicious LSPs, rootkits, spyware, trojan horses and worms. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies.Commonly used Antivirus are Norton, Kaspersky, Quick heal etc.

Application Software:

Application software, also known as an **application** or an **app**, is computer software designed to help the user to perform specific tasks. Examples include enterprise software, accounting software, office suites, graphics software and media players. Many application programs deal principally with documents. Apps may be bundled with the computer and its system software, or may be published separately. Some users are satisfied with the bundled apps and need never install one.

There are two types of Application software

General purpose Application Software e.g. Word, Excel, DBMS etc.

Specific Purpose Application Software e.g. Inventory Management System, Payroll System, Railway Reservation System, Hotel Management System etc.

Computer Security Threats:

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats varies considerably. Some affect the confidentiality or integrity of data while others affect the availability of a system.

Malware:

Short for "malicious software," Malware refers to software programs designed to damage or do other unwanted actions on a computer system. In Spanish, "mal" is a prefix that means "bad," making the term "badware," which is a good way to remember it (even if you're not Spanish).

Common examples of Malware include viruses, worms, Trojan horses, and Spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers.

Virus :

Like a biological virus, a computer virus is something you don't want to get. Computer viruses are small programs or scripts that can negatively affect the health of your computer. These malicious little programs can create files, move files, erase files, consume your computer's memory, and cause your computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.

We all know it's hard enough to get a computer to work well when it is healthy, let alone when it has been attacked by a virus. Therefore, it is better to prevent an attack than to try and cure it. There are many antivirus programs available that scan incoming files for viruses before they can cause damage to your computer. Some of these programs include Norton Antivirus, McAfee Virus Scan, and Virex

Trojan Horse:

A **Trojan horse**, or **Trojan**, is a type of malware that masquerades as a legitimate file or helpful program possibly with the purpose of granting a hacker unauthorized access to a computer. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems.[1] Trojans may use drive-by downloads or install via online games or internet-driven applications in order to reach target computers. The term is derived from the Trojan Horse story in Greek mythology because Trojan horses employ a form of "social engineering," presenting themselves as

harmless, useful gifts, in order to persuade victims to install them on their computers. For example, a Trojan horse might appear to be a computer game, but once you double-click it, the program starts writing over certain parts of your hard drive, corrupting your data. While this is certainly something you want to avoid, it is good to know that these malicious programs are only dangerous if they are given a chance to run. Also, most antivirus programs can catch Trojan horses when scanning for viruses. Unlike viruses, however, Trojan horses don't replicate themselves. Though it is possible for a Trojan horse to be attached to a virus file that spreads to multiple computers.

Spyware:

Spyware is a type of malware (malicious software) installed on computers that collects information about users without their knowledge. The presence of spyware is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

As the name implies, this is software that "spies" on your computer. Nobody likes to be spied on, and your computer doesn't like it either. Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person's computer over the Internet.

Worm:

A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself. This is due to security shortcomings on the target computer. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Worms are hard to detect because they are typically invisible files. They often go unnoticed until your computer begins to slow down or starts having other problems. Unlike viruses and Trojan horses, worms can replicate themselves and travel between systems without any action from the user. For these reasons, it is good to have an antivirus program installed on your system that can detect and remove worms before they have a chance to replicate or spread to other computers. Security updates such as Windows Update also patch security holes that allow worms to infect your computer. So keep your security updates and virus definitions up-to-date and you should be able to keep your computer worm-free.

Virus detection and its removal:

Virus detection and its removal are made through an antivirus program which finds out viruses in a computer and then possibly removes or repairs the virus problem. Some of commonly used Virus detection and its removable tools are Norton Antivirus, McAfee, Virus Scan, Kaspersky and Quick Heal etc.

Digital Certificate:

A digital certificate is a pair of files on your computer that you can use to create the digital equivalent of handwritten signatures and sealed envelopes. Each pair of files is divided into two parts: the public key and the private key. The public key is the portion that is shared; the private key is the portion that you, and only you, should have access to. Your computer and programs understand how to share only the public portion of your keys so that others can see them, while still keeping your private keys secure.

For example, when sending an e-mail message, you can digitally sign the message by attaching your digital certificate. Once they receive the message, recipients can verify that it came from you by viewing the small attachment on the e-mail, which contains your public key information. This protects you from people who might try to "spoof" an e-mail that looks like it came from you but is really sent from a different e-mail account.

Digital Signature:

A digital signature authenticates electronic documents in a similar manner a handwritten signature authenticates printed documents. This signature cannot be forged and it asserts that a named person wrote or otherwise agreed to the document to which the signature is attached. The recipient of a digitally signed message can verify that the message originated from the person whose signature is attached to the document and that the message has not been altered either intentionally or accidentally since it was signed. Also, the signer of a document cannot later disown it by claiming that the signature was forged. In other words, digital signatures enable the “authentication” and “non-repudiation” of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

A digital signature is issued by a Certification Authority (CA) and is signed with the CA’s private key. A digital signature typically contains the: Owner’s public key, the Owner’s name, Expiration date of the public key, the Name of the issuer (the CA that issued the Digital ID), Serial number of the digital signature, and the digital signature of the issuer. Digital signatures deploy the Public Key Infrastructure (PKI) technology.

Cookies:

A **cookie**, also known as an **HTTP cookie**, **web cookie**, or **browser cookie**, is usually a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website. When the user browses the same website in the future, the data stored in the cookie can be retrieved by the website to notify the website of the user's previous activity.[1] Cookies were designed to be a reliable mechanism for websites to remember the state of the website or activity the user had taken in the past. This can include clicking particular buttons, logging in, or a record of which pages were visited by the user even months or years ago.

How Do They Work

A command line in the HTML of a document tell the browser to set a cookie of a certain name or value? Here is an example of some script used to set a cookie. Set-Cookie: NAME=VALUE; expir es=DATE; path=PATH; domain=DOMAIN_NAME; secure Cookies are usually run from CGI scripts, but they can also be set or read by JavaScript.

Firewall:

A **firewall** can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not,
based on a predetermined rule set. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted

Hardware Firewall
Hardware firewall providing protection to a Local Network.

Software Firewall:

Computer running firewall software to provide protection

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

Password:

A **password** is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (example: an access code is a type of password). The password should be kept secret from those not allowed access. The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or *watchword.* Sentries would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online.