

# Basic Computer course book

Edition 6 (16 February 2012)

Free University of Bolzano Bozen – Prof. Paolo Coletti

## Introduction

This book contains course's lessons held at the Free University of Bolzano Bozen. It contains only the first part of the courses, namely the lessons on:

- computer introduction,
- Microsoft Windows,
- computer networks,
- computer dangers and security.

It does not contain the parts on Microsoft Word, Microsoft Excel, financial functions, Microsoft Access, computer algorithms, SPSS, Visual Basic for Applications, which are very well covered by the respective courses' suggested books.

This book is usually updated every year, please take a look at the edition date.

## Disclaimers

This book is designed for very novice computer users. It often contains oversimplifications of reality and every technical detail is purposely omitted. Expert users will find this book useless and, for certain aspects, partially wrong.

This book supposes that the user is using English Microsoft Windows Vista operating system. However, most of the book is perfectly readable with other Windows versions, while some menus and instructions can be rather different if the language is not English (Windows language may be changed on multi-language installations: see page 7 for further information).

The novice user in this book is, for simplicity, always considered male. This is not meant to be gender discrimination.

## Table of contents

Introduction.....	1	3.3.	Addresses.....	15
Table of contents.....	1	3.4.	Communication programs.....	16
1. Computers .....	2	3.5.	World Wide Web.....	19
1.1. Terminology .....	2	3.6.	Internet connections.....	20
1.2. Hardware .....	2	4.	Computer security .....	22
1.3. Software.....	4	4.1.	Encryption.....	22
2. Microsoft Windows.....	6	4.2.	Passwords .....	23
2.1. First glance .....	6	4.3.	External threats .....	24
2.2. Regional and language settings .....	7	4.4.	Emails .....	25
2.3. File system.....	8	4.5.	Navigation.....	27
3. Computer networks .....	13	4.6.	Backup .....	28
3.1. What is a computer network.....	13	Index .....		31
3.2. Network components.....	14			

# 1. Computers

This chapter presents with a brief description of computer main components, of the most common devices and of the typical software components for novice user.

## 1.1. Terminology

### 1.1.1. Bits, bytes, Kilobytes, Megabytes

Before starting with the computer description, it is useful to become proficient with the data size terminology, which will often be used in this book.

Computers have a very elementary way to store data: they can remember only 0 or 1. A value of 0 or 1 is called bit and all computer data are stored as sequences of bits. A sequence of 8 bits is called a byte, which is a quantity large enough to store usually a letter or a digit (even though sometimes 2 bytes are necessary). Modern computers are able to deal with enormous quantity of bytes, forcing us to introduce other quantities:

- Kilobyte (KB), approximately 1,000 bytes,
- Megabyte (MB), approximately 1,000 KB or one million bytes,
- Gigabyte (GB), approximately 1,000 MB or one billion bytes,
- Terabyte (TB), approximately 1,000 GB or one trillion bytes.

Usually the text of a whole book can fit in some KB, while for an image in a good resolution (let's say ready to be printed on A4 paper) or for a modern song some MB are required, and a film in high quality needs some GB.

### 1.1.2. Hardware and software

When talking about computer, we divide the topic into hardware and software.

Hardware consists of all the physical components of a computer, those which can be touched (and is therefore "hard"). Hardware is designed and built by engineers.

Software is everything which cannot be touched contained by a computer (and is therefore unsubstantial, "soft"), including programs, data, operating system. Software is developed by programmers and must be transported and stored on hardware devices.

## 1.2. Hardware

Over the last 40 years, computer hardware has been continuously improving its performances with an exponential growth. This growth is summarized by the famous Moore's law which says that the number of transistors in a processor doubles every 18 months. This law can be extended to almost every aspect of hardware and we may say that the performance (be it speed or capacity) of hardware doubles every 18 months, thus leading to a general exponential growth. Unfortunately software's performance does not increase with the same rate.

### 1.2.1. Computer box

The computer appears as a big rectangular metal box, which is usually never opened by the user and which contains its internal components.



The most popular component is the processor, which is the brain of the computer. Here all the calculations and logical operations are carried on, and the whole computer is administered. The last generation of processors on the market is the quad core generation, processors which contain inside four processors.



The RAM memory is the place where the computer stores its ready-to-be-used information. In this place information is quickly reached by the processor. Modern computers are typically equipped with 4 GB of memory. When the computer is turned off, the memory is erased and all its content is lost. This is the short term memory of the computer, where data can be quickly accessed.



The hard disk is the place where the computer stores permanent data, those which must not be lost when it is turned off. Here data are kept forever (unless the disk is physically damaged), until they are explicitly deleted by the user. Hard disk capabilities for modern computers are around 1 TB. In comparison with a human being, hard disks are the books of the computer, where information stays until explicitly deleted.



There are a lot of different cards plugged-in into the motherboard, the main computer card, which serve for various purposes such as communicating with the outside network (network card), using the telephone (fax/modem card), producing sound (sound card), producing images for the monitor (video card). These are the nerves of the computer, used to interface the inner world with the outside world.

### 1.2.2. Input-output devices

The computer uses different devices to communicate with the outside world. Some are the ears, nose and the eyes of the computer, used only to receive information, while others are the hands and mouth of the computer, used to send information. Some devices can be used both for input and output operations.



The monitor is the most evident output device, which displays images projected by the computer. Modern monitors are LCD-TFT, the new slim elegant ones. Monitor size is measured in diagonal inches, modern ones commonly are 23".



The printer is the output device used to print text and images on paper. There are two types of printers: the old, cheap and unreliable color inkjet printers, which however use expensive ink cartridges and the expensive reliable laser printer.



Multifunction printers have a printer, a scanner and often a fax integrated into the same machine, and are therefore input-output devices.



Another common output device is the speakers, used to produce sound.



The keyboard is the most evident input device, used to transmit letters, digits and some commands to the computer, together with the mouse used to move the mouse cursor on the screen.



Other common input devices are the microphone, used by the computer to catch sound, the camera, used to transmit videos to the computer, and the scanner, used to send written text or images inside the computer.



Common input-output devices are the fax/modem, used to send and receive faxes and to connect to the Internet, the network router, used to connect to the Internet or to the local network, the multifunction-printer, used both as a printer and a scanner, or the infrared and Bluetooth devices to connect the computer with a notebook or a cellular phone, or the VoIP telephone, which let the user make telephone calls via Internet.

### 1.2.3. Data storage and moving devices

The computer uses several devices to permanently store and move data, which vary a lot in terms of capability, cost, speed and portability.

The most used is the internal hard disk, which usually is inside the computer box and can not be moved. Its size currently ranges from 500 GB to 2 TB. On the other hand, an external hard disk is outside the computer and can be moved with a similar size.

Slowly SSD Solid State Disks are starting to invade the market. They are not disks at all, but very large memory cards shaped like an hard disks which can entirely replace the internal hard disk. Their main advantages are that they do not have moving parts (they do not rotate at high speed like hard disks) and therefore are suited for portable devices and that in most situation they are faster than hard disks (up to 10 times faster). Their disadvantage is the limited size which currently is 250 GB and their high price.



CD and DVD are the two modern ways to store data. They contain about 700 MB and 4 GB, respectively. They are divided into R which may only be written once and RW which may be written are re-written several times. They require a CD-reader or a DVD-reader to be read, which are available on most computers, and a CD-writer or DVD-writer to be written, which are available only on some computers.

A new generation of high capacity DVD has appeared on the market, the Blu-ray with 25 GB size.



Memory stick or USB pen drive is the most used way to temporary store and move data. Its size is now up to 64 GB and it works on every modern computer. However its reliability is not perfect, therefore it is used mostly to move data.



Other common ways to store and move data are through memory card, used by external devices such as photo cameras, cellular phones or music players, while big companies have tape devices to be used for backup.

## 1.3. Software

Software can be divided into three big categories: operating systems, programs and data.

The operating system takes care, through the processor and the motherboard, of controlling the computer hardware and the human-computer interaction. There are currently three widely used operating systems:



Microsoft Windows (with its versions XP, Vista and Windows 7), which is the expensive and user-friendly market leader,



Linux/Unix (it is a family of very similar operating systems), which is the new costless operating system,



Macintosh computers have their own operating system Mac OS X.

Programs are software which is used to do particular tasks, e.g. Word for document writing, Explorer for Internet navigation, the Calculator for mathematical operations.

Data is everything which is produced either by the user or by programs (sometimes even by the operating system) to store information, e.g. a document file produced by Word is data, a downloaded web page is data.

### 1.3.1. Software categories

Software can be divided, from a commercial point of view, using two features: the cost and the permission to be modified.

Subdivision by cost is:

- freeware, software which is completely costless. The producers of this software are either public institutions such as universities, or developers who do it for personal interest or advertisement or private company who do it for dumping reasons. Some examples are Microsoft Internet Explorer or Linux operating system;
- shareware, software which is initially costless but after a certain period the user is asked to pay a fee or delete it; or software which has two versions: a free one, but incomplete or with advertisement banners, and a complete advertisement-free one, for which the user must pay. The most common example is WinZip compression program;
- commercial, software for which the user has to pay a license to use it. Common examples are Microsoft Windows operating system and Microsoft Word;
- private, software uniquely built, under payment, for a specific customer to fit his needs. Only the costumer may use it. A typical example is the university's students-courses-professors database system.

The permission to be modified can seem a trivial question for the novice user, however for program developers and computer experts being authorized to modify a software is a great advantage since it can be improved, checked for errors and tailored to specific needs. The "open source versus proprietary software" is a strong ethical and economical debate in the computer scientists' community. Subdivision by permission to modify is:

- open source software may be modified by anyone, sometimes under certain restriction (usually not converting it into commercial software and redistributing it as free software). The software developers at the same time legally authorize any modifications and they distribute the source of the software to put other developers in a condition to easily modify it. Open source software is also freeware. The most typical example is Linux operating system.
- proprietary software is distributed (costless as Microsoft Internet Explorer, or as a shareware as WinZip, or most often sold as commercial software as Microsoft Word) with the explicit legal warning not to modify it and technically locked to prevent other developers to see or modify its source.

Software is usually identified by a name, for example "Linux" or "Microsoft Office", sometimes by a distribution/edition name "Linux Ubuntu", "Microsoft Office Professional" and very often by a version number, a sequence of numbers, points and letters which distinguishes the changes made by developers with time, such as "Linux Ubuntu 11.04" or "Microsoft Office Professional 2010". Obviously the version numbers of open source software changes rapidly, due to the many developers working on them.

## 2. Microsoft Windows

Microsoft Windows is currently the market leader operating system, it is the usual interface which appears when the user turns a personal computer on.

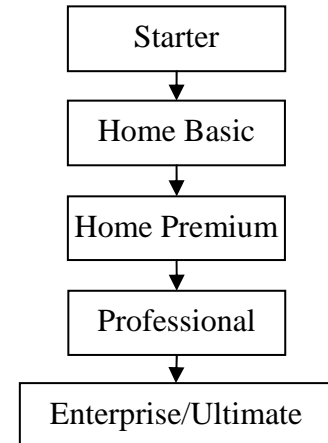
### 2.1. First glance

Microsoft released Windows XP in 2001 and for many years it has been, with its three major upgrades Service Pack 1, 2, and 3, the official Microsoft operative system. In January 2012 it is installed on approximately 35% of computers (source gs.statcounter.com).

Windows Vista was released in 2007 and it was not a market success. Currently it is installed on 10% of computers.

Microsoft released Windows Seven in 2009, which is the currently default Microsoft operative system. It is installed on approximately 44% of computers and the first Service Pack has already been released. Its editions are:

- Starter and Home Basic, cheap versions with severe limitations;
- Home Premium, home user's edition;
- Professional, personal business' edition which includes more network programs;
- Enterprise/Ultimate, Professional edition with more network utilities available to companies/individual users. Enterprise edition is currently (February 2012) installed at UNIBZ



#### 2.1.1. Keyboards and languages

Before starting this section it is necessary to take a close look at your keyboard. Locate these keys since they will be used in the rest of this manual and are very useful in many programs:

English keyboard	German keyboard	Italian Keyboard	Main function
CTRL	STRG	CTRL	
ALT	ALT	ALT	
ALTGR	ALTGR	ALTGR	Produce character on the key's right left
F1 to F12	F1 to F12	F1 to F12	
DEL	ENTF	CANC	Delete next character
INS	EINFG	INS	Toggle insert/overwrite mode
HOME or ⌵	POS1	⌵	Go to beginning
END	ENDE	FINE	Go to end
PG↑ and PG↓	BILD↑ and BILD↓	PAG↑ and PAG↓	Go one page up or down
BACKSPACE or ←	←	←	Delete last character
ENTER or ↵	↵	INVIO or ↵	Enter data
TAB or ⇄	⇄	TAB or ⇄	Move through the window
SHIFT or ⇧	⇧	⇧	Capitalize letters
CAPS LOCK or ⇩	⇩	⇩	Keep SHIFT pressed
ARROWS ←↑→↓	←↑→↓	←↑→↓	Move the cursor

In this book the English name for keys will be indicated. When A+B is indicated, it means that the user must press key A, then press key B, and then release both keys.

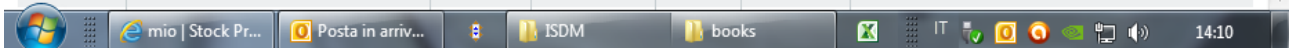
## 2.2. Regional and language settings

With a multilanguage Windows installation, keyboard settings or menus' languages may be changed clicking on the Start icon", choosing "Control panel", then "Clock, Language and Region", then "Change Display Language", and modifying the appropriate setting.

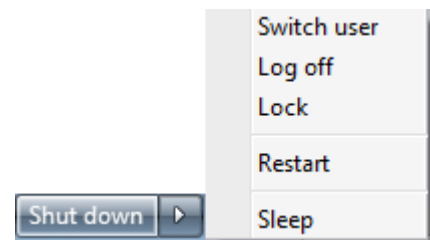
Another interesting option, available on every Windows installation, is the numbers' and dates' formats. When in "Clock, Language and Region", choosing "Region and Language" and clicking on "Formats" then on "Additional Settings" the user is able to change the format of numbers, especially the decimal separator, the currency and the date format, especially the English (month-day) and European (day-month) formats.

### 2.2.1. Desktop and application bar

The first thing commonly seen after typing the login name and password (on those computers which require them) is the user's Desktop, a large area where the user drops the most commonly or recently used things. The Desktop is different for every user, if the computer asks for login name. It contains, usually on the bottom, the application bar with the start menu on the left. When clicking the left mouse key on this menu a long list of things appears; the most interesting ones are:



- Programs, with the complete list of programs installed on this computer,
- Disconnect icons from which the user can disconnect from the computer or turn it off,
- Computer, from which the user can access the computer's hard disks,
- Network, from which the user can access the network connected to the computer,
- Control panel, which contains the operating system configuration and should not be accessed unless the user perfectly knows what he is going to do,
- User's home and Documents, which contains all the user's files.



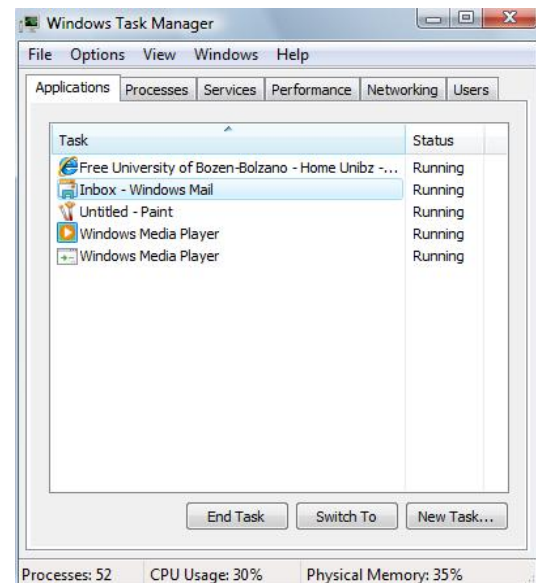
In the application bar, usually next to the start menu's icon, there are the quicklaunch icons, small images which start, when clicked on, the most common programs. At the center of the application bar there are the currently running programs and on the extreme right other running programs, usually those controlled by the operating system. Note that this is not an exhaustive list of running programs, since most technical programs which are not considered interesting to the user (including viruses!) are not displayed on the application bar. The current keyboard language and the clock are also displayed in the application bar: to change their setting simply double click the mouse left key on their indication.

### 2.2.2. Computer locking problem

Microsoft Windows sometimes becomes unstable: it can unpredictably, without any warning and when the user does not expect it and typically when he is doing something very important and urgent, lock and refuse to respond to user's actions. When this happens, it is usually caused by the program that was used and therefore the first thing to do is to try to close the current program. If this does not improve the situation, the only other solution left is to turn off the computer. The list of operations to try until the computer answers to user's commands is:

1. if the mouse works, click the X button on the program window or otherwise press ALT+F4;
2. press CTRL+SHIFT+ESC; select the program from the list and press End Program;
3. press CTRL+ALT+DEL and, from the bottom right icon, choose Shut Down;
4. press the computer on/off button;
5. unplug the electric power.

In any case all the current unsaved work will be lost; in the last two cases the operating system can sometimes be damaged but very often it will repair by itself the next time the computer is turned on. Therefore it is always a very good idea to save very often the current work, especially when it is important, urgent, or difficult to redo.




## 2.3. File system


Before starting this section it is necessary to do the following operations:

1. open the Control Panel from the start menu icon
2. choose Appearance and Personalization
3. choose Folder Options
4. choose View
5. deselect “Hide extensions for known file types”.

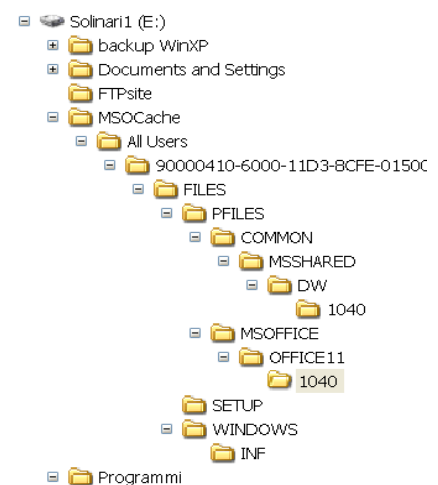
In this way extensions (see section 2.3.3) are shown and file types are better recognized.

### 2.3.1. Files and directories

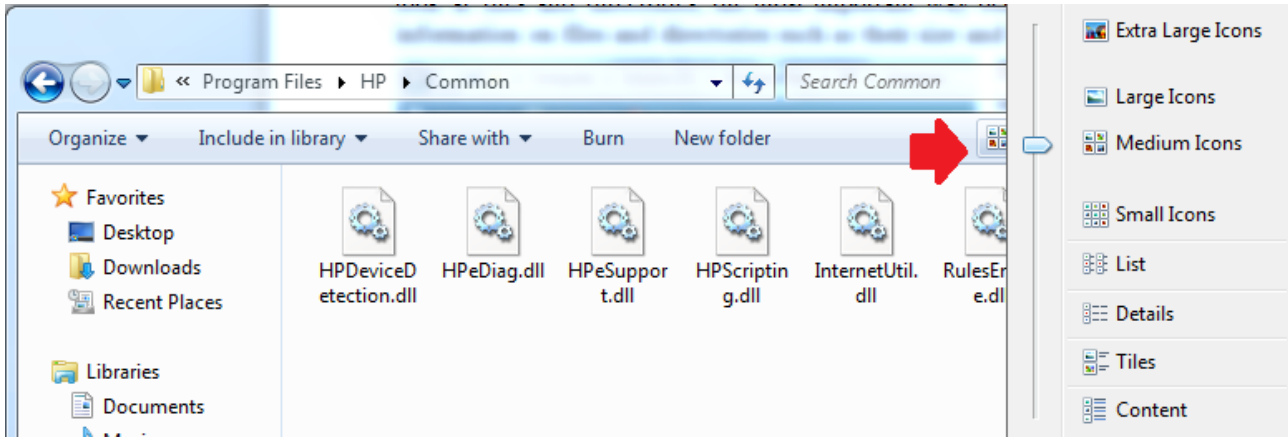
Software is stored on storage devices in a special container called file. The operating system uses a lot of files for itself and for its data, a program usually uses one file for itself and other files for its data, and the user uses some files for his data. A file is represented by a small picture called icon. 

Another special object is the directory or folder, which is basically a container for files and other directories and is represented with an icon depicting a yellow closed or open folder. Double clicking on a directory opens a new window which presents the directory content. 

Each storage device is a big directory, accessible from My Computer window, which contains directories and files. Each of these subdirectories may contain other files and other subsubdirectories, and so on in a hierarchical way, forming a tree with the hard disk (or another storage device) as the root, directories as branches and files as leaves. On UNIBZ computers, the usual hard disk are “C:” which contains programs, “E:” which contains courses information and “F:” which contains user’s reserved space. Disks directories “A:” and “B:” are usually reserved for floppy disks, and “D:” or “Z:” for CD-reader.



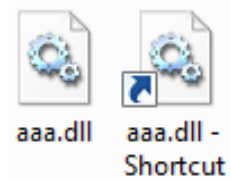
Choosing the “Change your view” menu of a directory windows will provide the user with five different ways to look at files and directories, the most important way being the Details which can show interesting information on files and directories such as their size and date of last modification.



Each file and directory can be univocally identified by its absolute path or address. For directories it is the path which appears on the address bar of the directory window, while for files it is the path of their containing directory followed by “\” and the file name. For example, the absolute path of directory “Common” in “HP” directory in “Program Files” directory in the C: hard disk is “C:\Program Files\HP\Common” as can be seen from the address bar. While, the HPeDiag.dll file has the absolute path “C:\Program Files\HP\Common\ HPeDiag.dll”.

Note that, for Windows operating system, capital or small caps letters in paths are perfectly equal.

A special and tricky object is the link or shortcut. Although its icon looks like a file icon, the small curved arrow on the left corner clearly indicates that this object is a link. A link is simply an address to a file or directory, it is not a real file or directory. When the user clicks on the link, the computer behaves exactly as if the user is clicking on the real file or directory (if Windows can find the real one, which is not the case if in the meantime somebody deleted or moved it). However, any copy/move operation on the link will simply copy/move the link and not the real file or directory; especially copying/moving the link to another disk will probably cause it to malfunction. Therefore it is a good idea for novice users to avoid using links at all.



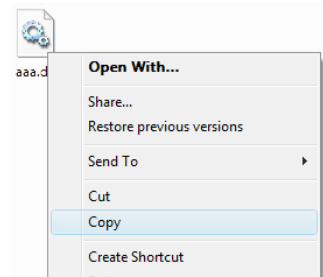
### 2.3.2. Files' operations

When double clicking on a file, Windows usually starts a program. The user is totally unaware of an important difference:

- double clicking on a program runs the program which was double clicked
- double clicking on a file calls the program associated with that file and runs it, at the same time telling the program to open the file. If no program is associated with that file type, Windows asks the user which program should open the file.

Copying a file means reproducing it to another location or to the same location with a different name. Copying a directory means reproducing it to another location, or to the same location with a different name, together with its entire tree of subdirectories and files. To copy a file or directory windows offers several methods, the most used being:

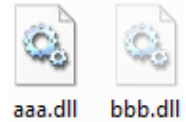
- drag the object to the destination. If a plus symbol does not appear, press CTRL key to have it appear while dragging. Release the object in the destination;
- select the object and click the right mouse button. Select “copy”. Point the mouse to the destination and click the right mouse button. Select “paste”. If the destination is the original location, the file name changes to “copy of ...”;



- select the object and press CTRL+C. Point the mouse to the destination and press CTRL+V. If the destination is the original location, the file name changes to “copy of ...”.

Moving a file means moving it to another location losing the file in the original place. Moving a directory means moving it to another location together with its entire tree of subdirectories and files. To move a file or directory windows offers several methods, the most used being:

- drag the object to the destination. If a plus or a link symbol does appear, press CTRL or SHIFT key to remove it. Release the object in the destination;
- select the object and click the right mouse button. Select “cut” and the icon becomes lighter. Point the mouse to the destination and click the right mouse button. Select “paste”;
- select the object and press CTRL+X and the icon becomes lighter. Point the mouse to the destination and press CTRL+V.



To create a link to a file or directory:

- drag the object to the destination of the link. If a link symbol does not appear, press CTRL+SHIFT until it appears. Release the object in the destination;
- select the object and click the right mouse button. Select “create shortcut”. A link is created in the same directory.

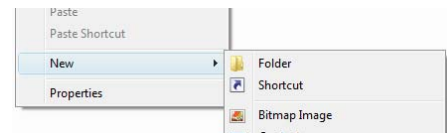
Deleting a file means often putting it into the trash can where it can be recuperated unless the trash can is emptied. Deleting a directory mean putting it to the trash can together with its entire tree of subdirectories and files. Pay special attention, since not always the trash can works correctly and sometimes files are deleted without passing through the trash can. To delete a file or directory windows offers several methods, the most used being:



- drag the object to the trash can and release it;
- select the object and click the right mouse button. Select “delete”;
- select the object and press DEL key.

To rename a file or directory, simply select the object, click on the name and retype it. Usually Windows accepts every name, but novice users should stick with letters and numbers and spaces, since other characters may be forbidden.

To create a new directory, simply right click the mouse and choose “New” and “Folder”. After the creation, rename it.



Sometimes files occupy a lot of space and need to be reduced to save disk space or to be sent by email; other times files must be put in a package to remain together or to be sent as a single file via email. These two operations are accomplished compressing a set of files and directories, which means using a special program (WinZip or IZArc or the operative system itself) to reduce (from 0% to 90% depending on the file type) the file size and produce a new single file called zip-archive containing all the selected files and directories.

To compress a set of files and directories:

1. select the files and directories all together,
2. click the right mouse key,
3. select “IzArc” or the installed compression program and select something like “Add to Archive File...”,
4. a dialog box appears asking you to choose the zip-archive name and its destination;
5. in this dialog box you must also choose the compression method, which is strongly suggested to be ZIP to be compatible with other programs;
6. in this dialog an encryption method (see section 4.1 on page 22) may be chosen. If your zip-archive should be opened by anybody, then choose “None”: Otherwise, if you want the zip-

archive to be uncompressed only by people knowing a proper password, choose any of the encryption methods, such as “AES 128 bit”, and provide the password.

Other files or directories may be added later to the zip-archive simply dragging them on the zip-archive file (this is a copy and not a move operation) if it is not encrypted.

To extract files from a zip-archive file, simply click the right mouse key on the file and from the drop-down menu choose the appropriate extract option: the content will appear in the location you have chosen, together with all its directories’ structure.

When double clicking on a compressed file, if the compression program is properly installed, it will open in a window as if it were a directory. But it is not a normal directory, it is simply a window, produced by the compression program, with the list of the zip-archive’s content: the user should not open files from this window since it is a very unreliable way to modify files! Files can be copied from this window to a real directory simply dragging them to the directory. When the entire content of the zip-archive has to be extracted or when the user wants to preserve the original tree structure, it is better to use the Extract button of this special window.

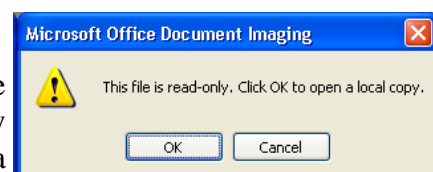
### 2.3.3. File types

Windows identifies a file type by its extension, which is everything after the last dot in the filename. Usually it is a 3 or 4 character acronym. Using the file extension, Windows knows the file type and decides which program will open that file. If the file extension does not show up, follow the instructions at section 2.3 on page 8. The most important file types are:

File type	Typical programs that open it	Typical extensions	Typical icons
Program	itself	.exe .com .bat	
Compressed	WinZip / IZArc	.zip	
Text	Notepad	.txt .csv	
Document	Word / Acrobat / Powerpoint	.docx .doc .rtf .pdf .ppt	
Sheet	Excel	.xlsx .xls .csv	
Image	Explorer / Picture Fax Viewer / Paint / Office Picture Manager	.jpg .jpeg .gif .bmp	
Video	Media Player	.avi .mov .mpg .mpeg	
Audio	Media Player / WinAmp	.mp3 .wav	
Web page	Explorer	.html .htm	

### 2.3.4. File sharing

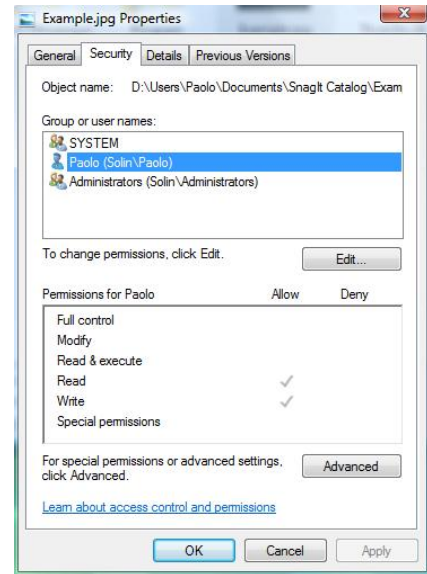
On the same computer different programs can try to access the same file at the same time, or on a network different users can try to do it. When this happens, Windows locks the file as soon as a program, able to write on it, opens it. Other programs trying to open it will be allowed to open it in read-only mode: they may read, but are not allowed to modify



it, nor users are allowed to move or delete it but simply to copy it. As soon as the locking program closes the file, Windows releases the lock and another program may take it.

Another way to forbid use of files is through permissions. Click the right button of the mouse on a file or directory and select “Properties” and “Security”. The security dialog box shows the list of users or groups of users who may access this object, while not listed users may not access it. For each user or group this dialog box displays the permissions, the most important being:

- read permission, to copy and open the object;
- read and execute, same as read, plus run the object if it is a program;
- list content (for directories), to see the content;
- write permission (for directories), to create files and subdirectories;
- modify permission, same as read and execute, plus delete, move, rename, save modifications;
- full control, same as modify, plus change permissions.



The owner of the file usually has full control on it and may change permissions or add new authorized groups or users. A special group is the Administrators group (containing the users involved in technical administration of computers) which has full control on every object.

### 2.3.5. Network folders at UNIBZ

On UNIBZ LAN there are shared hard disks on which common information is stored, so that it is accessible from every computer. These are called network folders. Some of them are:

- \\ubz01fst\courses\course\_coletti which contains utility files that will be used during the course. These files must never be opened double-clicking from here, otherwise they will be locked (see section 2.3.4 on page 11); they should be copied on each user’s desktop before opening them;
- \\ubz01fst\courses\exam\_coletti\, followed by user’s login name, which will contain exam files and which is accessible only by the user;
- \\ubz01fst\students\, followed by faculty, year and user’s login name, contains a copy of the student’s disk F, desktop, and configuration. This folder is updated every time the user logs off, only if the user is not using too much disk space (which is usually 150 MB, but it is a good idea to stay below 80 MB). Otherwise, it is not updated and the next time the user logs in he will not find the new files on the desktop. Therefore it is a good idea to periodically, especially if a warning email has been received, go through this network folder and delete your huge files (which sometimes appear only here and not on disk E nor on the Desktop).

### 3. Computer networks

This part of the book is dedicated to computer networks from a user's perspective. Nowadays a computer is very likely to belong to some company's network, or to be connected to the Internet via an Internet provider, and is therefore exposed to all the typical network problems. Without entering into technical details, this section will explore the situations in which a novice user can find himself in troubles and how he can try to survive dialoguing with network administrators in their own strange technical language.

#### 3.1. What is a computer network

A computer network is a set of devices which communicate and share resources. These devices are mostly computers, and sometimes stand-alone hard disks, telephones, printers and terminals (processorless computers which must rely on other computers to work).

##### 3.1.1. Resources sharing

Resources sharing is what makes computer networks different from a general networks and this is often overlooked by the novice user. Resources which can be shared are:

- the processor or the memory: computers and terminals may use the computational resources of a more powerful computer;
- hard disks: computers and terminals often access each other hard disks to read data and sometimes may use a special computer as a storage machine;
- CD-reader or DVD-reader: computers may read CD and DVD physically inside the reader of another computer;
- programs: usually due to license's problems, a program may be installed only on some computers and others must use it through these computers;
- connection: due to security or commercial reasons, only some computers are connected to the Internet or to another network or to the telephone system and other computers must pass through these ones to connect.

##### 3.1.2. Server and client

A computer network interaction is based on the client server architecture. When considering a single interaction, one computer is the server and the other one is the client. The server is the computer which is offering its resource, usually programmed to wait until someone asks for its resource. The client is the computer which uses the resource, which sends the request to a waiting server.

For example, when sending a document to the printer, the user's computer is the client while the printer is the server; when retrieving personal emails, the user's computer is the client which connects to the mailserver asking for available emails. When talking to a friend on an Internet chat, the interaction is composed of two different interactions: the user's computer as a client is connected to the chat room's computer acting as a server, and the friend's computer does the same interaction.

The same computer may be the client for a service and the server for another service. For example, a library computer may have a CD inside its reader shared to the network (server for the CD) and may be at the same time used by a user to print his own documents (client for the printer).

##### 3.1.3. Peer to peer

In the last years peer to peer architecture has also become very popular. It is composed of two computers connected together, typically through the Internet, exchanging files or information

without any server client relationship. The popularity of this architecture depends on its easy technical implementation and on its typical use to exchange multimedia files.

### 3.1.4. Areas

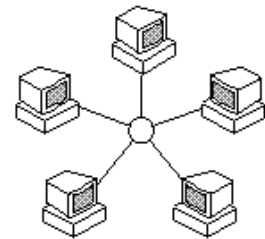
Computer networks are commonly divided into three categories:

- Local Area Network (LAN or Intranet), usually the network of computers in the same building or belonging to the same owner. Inside the LAN every computer is well identified and usually every user is known. It is considered a trusted area.
- Wide Area Network (WAN or Internet), which is everything which connects LANs. Computers' and users' identification is very hard and anonymity is possible. It is considered a dangerous area.
- Virtual Private Network (VPN) is a way to recognize a computer outside the LAN as a trusted computer: the user is identified with a password and his computer, even though connected via Internet, will be considered as part of the LAN, for as long as it remains connected. VPN is typically required to identify portable computers connected via wireless connection.

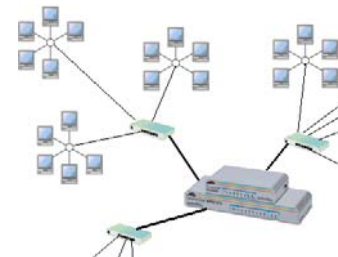
## 3.2. Network components

### 3.2.1. Topology

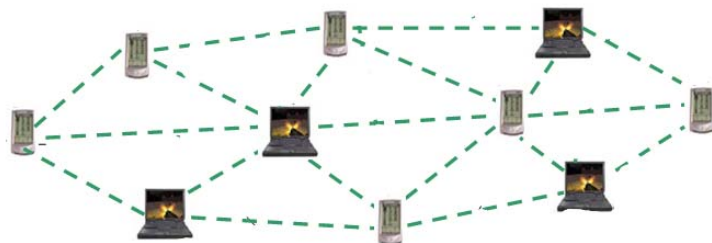
Computers and devices can be connected in different ways. The topology of a very small LAN, for home or small office environments, is a single star network, with a main device called hub or switch to which all computers are connected and through which all communications must pass. Usually this device is also connected to the Internet and in this case it takes the name of router.



The most typical topology of large site's LAN is the star network: computers are divided into groups and are connected directly to hub. Every hub is connected to a main hub; in very large companies there are many main hub connected to a higher level hub, and so on.



On the other hand, Internet's topology is very different, due to the non hierarchical structure of the organization and to the fact that each site is independent from the others. Internet network has a net topology, where each site is connected to other sites and there are always several possible routes to go from one site to another.<sup>1</sup>



<sup>1</sup> This solution derives from the original military use of Internet. In case of a site's destruction, the rest of the Internet is able to continue to work without communication's interruption.

### 3.2.2. Cables

The network connecting components are the cables, which often determine the speed of the LAN. Cables have a speed measure in bps (bits per second) which indicates how many bits can flow through the cable in one second.

- Ethernet cables have a speed of 10 Mbps and can thus carry 1.25 MB each second, meaning that, for example, a 600 MB movie can be transferred in 8 minutes from one computer to another one, supposing no one (neither users nor computers) is using that network tract for other purposes during the transfer.
- Fast Ethernet cables have a speed of 100 Mbps.
- Giga Ethernet cables have a speed of 1 Gbps.
- A wireless network, a cableless network where computers use radio signals to communicate, has usually a speed around 10-300 Mbps, depending on the wireless generation.

To find out how much time does it take to transfer a file with a size expressed in bytes, divide the connection speed in bps by 8 to find out the byte rate per second and then divide the file size by the speed to find out the number of seconds it takes for the file transfer. For example, to transfer a 600 MB file through an Fast Ethernet connection, find out the speed of 12.5 MB per second (12,500,000 bytes per second) and then divide 600 MB (or 600,000,000 bytes) by 12.5 (or by 12,500,000) to find out the time of 48 seconds.

### 3.2.3. Gateway

When a LAN is connected to the Internet, there is one, or sometimes more than one, special computer called gateway dedicated to this connection and to keep relations with the outside world. Other network devices are internal and this special portion of the network is called Intranet. The gateway is the only computer physically connected to the Internet and on it several administrative and security programs run. The main ones are:

- the firewall, a program in charge of rejecting unwanted incoming connection attempts (which can be attacks to the internal security) and sometimes of forbidding unauthorized outgoing connections (which can be users trying to perform operations the network owner does not want);
- the Domain Name Server (DNS), a program in charge of dealing with computer addresses, whose exact behavior will be seen later on page 16;
- the webserver, a program in charge of publishing web pages. The webserver offers the local web pages to users outside, answering to requests coming from external users;
- the mailserver, in charge of receiving emails from the Internet and dispatching them to the right local user (according to the name before the @) and of receiving emails from the local users and dispatching them to the right external mailserver (according to the domain name after the @).

These programs usually all run on the gateway for large companies' networks, while for smaller networks, such as the ones of small office or home environments, DNS, mailserver and webserver run on the Internet Provider computers (implying that the local network depends on external resources for emails, its own web pages and domain names) and the firewall usually runs on every computers.

## 3.3. Addresses

### 3.3.1. IP numbers

Computer networks use the Internet Protocol version 4 (IPv4) address system: every network device is identified by an IP number composed of four numbers from 0 to 255 separated by dots. For example, 15.0.234.65 or 255.54.9.23 are valid IP numbers.

As it can easily be calculated, there are about 4 billion of possible IP addresses, meaning that not every computer and connected device may have its own public IP address. Therefore, usually LANs have private IP numbers, using traditionally those starting with 10 (for example 10.0.1.5). Moreover, every computer identifies itself via the name "localhost" with address 127.0.0.1.

Unfortunately IPv4 numbers have turned out to be not enough for a very fast growing Internet and thus a new standard has been introduced, called IPv6, which consists of eight hexadecimal numbers (numbers with digits and letters up to f), such as 2001:db8:85a3:8d3:1319:8a2e:370:7348.

### 3.3.2. Ports

Many incoming and outgoing connections can arrive and leave a single computer at the same time. To keep correctly track of all the connections, the computer lets them in and out through different ports, according to the service they are asking or giving. For example, outgoing emails travels on port 25, incoming emails on port 110 and web pages on port 80. Addresses with ports are indicated with a colon after the IP number followed by the port number, for example a connection to port 572 of computer 167.34.54.23 is 167.34.54.23:572.

### 3.3.3. Internet names

Human users often dislike numbers and prefer meaningful names, which can be more easily remembered. Therefore, many computers and devices have also an Internet name. These names have the special form subdomain.domain.extension, where the extension usually indicates the network type or nationality:

- .eu for Europe, .it for Italy, .de for Germany, .at for Austria, .nl for Netherlands;
- .com formerly for US commercial companies, now for every company;
- .org and .net formerly for independent organizations and networks, now for every company;
- .to for tourism, .tv for television;
- .edu for United States' universities, .gov for US government, .mil for US military;
- .ac.uk for United Kingdom's universities, .bz.it for the Province of Bolzano Bozen.

The domain is chosen by the network's owner to reflect the company name or to be easily remembered by web surfers, such as unibz.it for University of Bolzano Bozen, vodafone.it for Vodafone Italia telephone company, or lastminute.com for a travel agency. The subdomain usually indicates the service offered by the computer (www for a webserver, pop or mail or smtp for a mailserver) or simply the computer's name.

The Domain Name Server (DNS) takes care of converting every Internet name to the corresponding IP number.

## 3.4. Communication programs

Inside a computer network many communication programs are installed on Intranet computers to connect to the Internet or even to internal computers.

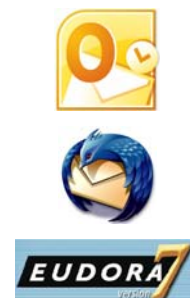
### 3.4.1. Web browser

A web browser is a client program to navigate the WWW and retrieve web pages. It runs directly on the user's computer and passes through the gateway at port 80 to reach outside web servers. It is one of the most vulnerable programs, since it is widely installed and often used by novice users. The market leader (about 70% of uses according to recent statistics) is Microsoft Internet Explorer, a freeware proprietary software. Its main competitors are Mozilla Firefox, an open source software, Safari, the browser for Mac OS X, and Chrome, the new browser from Google.



### 3.4.2. Mail reader

A mail reader is a client program to send and retrieve emails. It runs directly on the user's computer and connects to the local mailserver, or sometimes to remote mailservers. This is also a vulnerable program, since it is often used by novice users and since emails can carry attached files. The market leader is Microsoft Outlook, a commercial proprietary software. It has many competitors, the most famous being Mozilla Thunderbird, freeware and free, and Qualcomm Eudora, shareware and proprietary.



To communicate with the mailserver the mail reader uses special languages, called protocols:

- POP3 to retrieve emails at port 110,
- SMTP to send emails at port 25,
- IMAP is a more modern protocol to retrieve and, in rare cases, to send emails.

Big Internet providers and large networks usually have three different mailserver, one for each protocol: the POP3 server only for incoming emails, the SMTP server only for outgoing emails and the IMAP server for every connection using the new protocol.

This is the typical call sequence exchanged between the user's mailclient and the mailserver:

POP3 connection			SMTP connection		
User's mailclient		Mailserver		User's mailclient	Mailserver
Open POP3 connection	→		A	Open SMTP connection	→
		Check connection's origin	B		Check connection's origin
	←	Get name and password	C		Get name and password
Name and password	→		D	Name and password	→
		Check name and password	E		Check name and password
	←	Arrived email messages	F	Sent email messages	→

Network policies usually restrict access to mailservers only to identified users (with username and password) or only to users physically connected to the same provider, due to security and commercial reasons. These are the restrictions policies for Internet providers and for UNIBZ:

	Internet providers		UNIBZ and gmail.com	
	POP3 server	SMTP server	POP3 server	SMTP server
<b>Authentication required (steps C, D, E)</b>	Yes	No	Yes	Yes
<b>Only same provider (step B)</b>	Yes: tin.it, libero.it, wind.it No: tiscali.it, email.it	Yes	No	No

As it seems clear, the fact that Internet providers do not require authentication for outgoing emails makes it very easy to send anonymous emails or even emails with a fake sender address. The Internet provider can always trace back who is the real sender, since it is a user connected to its network probably through a telephone line, but this procedure requires time and usually a request from a judge. Therefore emails do not offer the guarantee of the real sender and novice users should beware of possible fraudulent use of this fact.

Another way to read and send emails is through webmail systems, which are websites where the user can enter and read his received email and send new ones acting directly, through his web browser, on the mailserv. It can be useful for various reasons: it does not require the installation of a mail reader program; old received emails are always available on the website and can thus be accessed from home, office and while traveling, even without a personal laptop; the mailserv takes care of emails backup. But on the other hand it requires a continuous fast connection even to write a single long email, which can be costly and, in some situations, impossible and usually the email space is limited. The most famous website interfaces are the Microsoft Outlook Web App, where the web interface looks exactly like Microsoft Outlook, and the Webmail interface, used and personalized by most Internet providers.

### 3.4.3. Posta Elettronica Certificata PEC

When sending an email, the sender has no proof that it has been sent, for example to be used in a court of justice, and no guarantee that the email has been dispatched. Some mail readers use a receipt system, but the receiver is not obliged to send back the receipt.

In order to overcome these problems, many solutions have been proposed. The Italian Posta Elettronica Certificata (PEC) system has become one of the most widespread solutions, thanks to law Decreto Ministeriale 6 May 2009 which guarantees a free PEC email address to every citizen and thanks to Decreto Legislativo 82/2005 which determines that PEC receipts are legal proves.

When an email is sent from a PEC address to another PEC address, the sender receives two receipt: the first one is a proof that the email has been sent with date and time, while the second one is a proof that the email has been dispatched to the mailbox of the receiver. This does not represent a proof that the email has been actually read, but from the moment the email is dispatched to the mailbox it is the receiver's responsibility to read it. Under this circumstances, it is perfectly equivalent to "raccomandata con ricevuta di ritorno". Emails can be send also from a PEC address to a non-PEC address, and in this case the receiver gets only the sent proof but not the dispatched proof, like the "raccomandata semplice". When an email is sent from a non-PEC address to a PEC address, no receipt is produced and this is equivalent to a standard letter.

It is important to note that PEC alone offers only the two receipts for the sender, but does not guarantee that the sender is really the person who claims to be nor that the email's content has not been altered. In order to overcome these problems, encryption and digital signature (see section 4.1 on page 22) must be used.

### 3.4.4. Voice over IP programs

Voice over IP (VoIP) programs are able to use the computer connection as a substitute for standard telephone. Equipped with either microphone and headphones or with a real telephone-like device, the user can send his voice through the Internet to remote computers or even to real remote telephones, thus saving on telephone bills.

VoIP requires a subscription to a VoIP's website, the most famous being Skype, who decides the telephone fares. Typically calling other VoIP's users is free all over the world, while calling fixed telephones depends only on the destination country and is independent from the caller's country, with a fare which is comparable to the standard local telephone call (about 2 €cent/minute in August 2011). On the other hand, calling mobile telephones is, for the moment, still very expensive (about 25 €cent/minute in August 2011); for this reason, special VoIP telephones, which can be

programmed to automatically decide between VoIP and the standard telephone line according to the dialed number, are appearing on the market.

### 3.4.5. Other communication programs

Other commonly used communications programs are:

- chat programs, like Yahoo! Messenger, to write instant messages to other users;
- File Transfer Protocol (FTP) programs, used to transfer files from and to external computers (while often for Intranet computers transfer is simply a drag and drop of the file);
- Telnet, SSH and other remote access programs, used to take full control of a computer as if the user were sitting in front of it;
- peer to peer programs, used to share files with unknown Internet users; these programs are used to exchange files.

## 3.5. World Wide Web

The World Wide Web (WWW), born in the mid-90s, is a huge collection of electronic documents, which are accessible from all over the Internet using a web browser. The two strengths of the WWW are the hyperlinks, a system which allows the user to click on some keywords and access documents related to the chosen word, and the easy technical tools that let anybody build a set of web pages, called website.

At the beginning of the 2000s the WWW saw the developing of Web 2.0, dynamic web pages which actively interact with the user and let him contribute to the website and access and modify personal information contained in the web site's databases. Interactive web services are pushing users to take an active role in the WWW, especially via forums, a place for common discussions on predefined topics, via blogs, a personal diary with the possibility for other users to put comments and multimedia material. The most famous production of Web 2.0 is Wikipedia, "a multilingual, web-based, encyclopedia project" built entirely by web users under their own mutual supervision with more than 20 million articles in 283 languages.

### 3.5.1. Search engines

A search engine is a special program running on a website which offers to the user the possibility of searching other websites for specific web pages. The user needs to connect to the search engine website and digit the keywords, or sometimes even a complete question, and the website returns the list of relevant web pages.

Search engines use a crawler technique: they continuously go through the known web pages memorizing their content and trying to discover other web pages through the contained links. In this way they are able to memorize most of the WWW's pages (more than 8 billion pages), even though some not linked websites can remain unknown to search engines.

The most popular search engines are Google, the current market leader, Yahoo! and Bing. In order to choose the order in which web pages are displayed to the user, search engines use scoring system. The most famous one is Google's which relies on the idea that a linked page is very important and useful; therefore a web page receives a score proportional to the number of web pages which put a link to it. According to recent researches, the percentage of use of these engines are Google 83%, Yahoo 6%, and Bing 4%.



There are many tricks to speed up the web search and arrive quickly to the right result:

- most novice users search the WWW using only a single keyword, which often produces the right result but in some cases can result in long lists of wrong results, for example when

looking for Java Island using simply “java”. Using as many keywords as possible often avoids wrong results, even though sometimes returns no pages if too many words are used;

- writing AND and OR commands between keywords allows the user to look for all the words (AND) or at least one of the words (OR), such as “center OR centre”. Usually search engines use AND if the user does not specify any logical command;
- putting some words between quotation marks forces the search engine to look for the exact phrase, i.e. exactly for those words in that order and with no words in between;
- in the advanced search menu often there are very good options, such as the search of pages only in a specified language or only in a specified format, for example .doc or .pdf.



- when looking simply for some images, it is more convenient to use the specific search rather than trying to find web pages containing them.

### 3.6. Internet connections

There are many different ways to connect to the Internet, divided by the physical mean of connection: the telephone cable, a dedicated cable or electromagnetic signals.

Names	Equipment	Subscription cost	Use cost	Effective speed	Notes
PSTN Plain Standard Telephone Network <u>analogical</u> <u>dial-up</u>	telephone modem	free	telephone call	56 Kbps	Telephone is busy during connection.
<u>ISDN</u> Integrated Service Digital Network	ISDN telephone ISDN modem	free	telephone call	128 Kbps	Telephone is busy during full speed connection.
<u>ADSL</u> Asymmetric Digital Subscriber Line	telephone ADSL modem	necessary	free	500 Kbps in upload	Speed depends on subscription fee and network traffic
		free	time fee	1-20 Mbps download	
T3 E3 / T4 E4	special cable	necessary	free	40 / 300 Mbps	
<u>GPRS</u> General Packet Radio Service	GSM cellular phone	free	traffic fee	100 Kbps	

<u>UMTS</u> <u>3G</u> Universal Mobile Telecommunications System	UMTS cellular phone	free	traffic fee	<u>7 Mbps</u>	Speed depends strongly on environment.
new <u>Wireless Wi-Fi</u>	wireless card	depends on the LAN policy	free	<u>30-80 Mbps</u>	Speed depends on wireless generation.
<u>WiMax</u>	antenna in line of sight	still to go on the market		<u>2 Mbps</u>	Speed depends strongly with distance.

Many fast connections, especially ADSL, suffer from network congestion: too many users are connecting at the same time and the Internet provider's main cables are not able to support the users' maximum speed multiplied by the number of users, and therefore must reduce the practical connection speed. Therefore the maximum speed is often only theoretical and some providers are offering a "minimum band guaranteed": a minimum speed under which the connection may never fall.

Unfortunately, even in technologically advanced countries, there are still many areas where nor ADSL neither UMTS arrives, mostly due to the geographic conditions (mountains, islands or long desert distances) and to the low inhabitants' density. This phenomenon is called digital divide: there are people (e.g. 5,400,000 of inhabitants of Italy) that even willingly to pay cannot get a broadband connection, and, on the other hand, Internet services and especially the WWW is continuously going towards large size contents, cutting these people off. In order to overcome this social problem, WiMax is spreading, a sort of very long range Wireless which arrives up to 50 Km but works only if the transmitting and receiving antennas are in line of sight and whose theoretical speed of 70 Mbps decreases with distances to about 2 Mbps.

## 4. Computer security

Being connected to the Internet means giving anybody access to the computer. Despite the traditional novice user's belief that he is the one who goes outside, it is instead the Internet world which is coming inside, with all its benefits and dangers. Knowing a little bit of security issues is nowadays necessary even to the non-expert user, to avoid being lured into traps or adopting potentially dangerous behaviors.

Moreover, the recent Italian [law 196/2003](#) on [privacy](#) issues contains in the Allegato B the minimal security techniques which must be adopted by system administrators but also by normal users. Every user who has access to [personal data](#) protected by privacy must take care of these procedures, in particular:

- each user must be [authenticated](#) by a personal username and a password or a biometric device (fingerprint, hand shape, eye);
- each user has its [own permissions](#), limited only to the data he needs for his work, and the permissions must be revoked when the user does not need them anymore;
- users must receive [specific training](#) to be able to use their authentication and to be aware of their responsibilities, duties and the possible dangers;
- a [firewall](#) and an [antivirus](#) must protect the network and they must be [updated at least every 6 months](#);
- software used to handle data must be [updated](#) at least every year;
- [sensitive data](#) must be stored and transmitted using [encryption](#);
- sensitive data must have a [backup](#) copy and, in case of loss, they must be [restored within 7 days](#).

### 4.1. Encryption

[Encryption](#) is a text masking technique, derived from military use, which transforms information in such a way that it may be correctly read only with a special password called [key](#). It uses two keys, a [private key](#) for encrypting, usually known only to one computer or person, and a [public key](#) for decrypting, usually known by all the computers or people which legitimately may read the information. The size of these keys, and thus the difficulty to be guessed, is expressed in bits, with [128 bits](#) being the typically most secure size used.

Its first computer use has been in encrypting users' passwords and important information in such a way that only specific programs or users are able to decrypt it. Then it started to be used in computers' communications, where the two involved computers start by exchanging their respective decryption keys and then they can conduct a protected exchange of information, for example to send passwords or credit card numbers, being sure that no other computer can understand the communication and that the arrived information comes surely from the other computer (otherwise it would not be decrypted).

#### 4.1.1. Digital signature

A digital signature, or electronic signature, is an encryption technique for documents which guarantees, at the same time, the document's author's identity and that the document's content has not been altered. The author writes the document and encrypts it with his private key, while his public key is given to official certification authorities. When anybody opens the document, the program used to view it connects to the certification authority which decrypts it and, if decryption is possible, then the document has really been encrypted with the author's private key and thus author's identity is guaranteed. On the other hand, if decryption is not possible it means that either public key does not match private key and thus the author is not who claims to be or that document has been altered after the encryption.

In this way, digital signature used in combination with PEC can guarantee also sender's identity and email's content. Unfortunately, certification authority require a payment for the deposit of a public key: VeriSign, the market leader authority, charges 400 \$ per year.

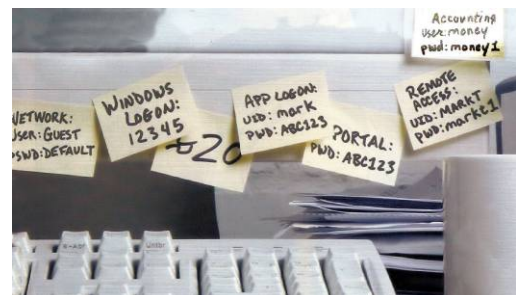


## 4.2. Passwords

On the Intranet the user is identified only by his username, known to everybody, and his password, known only to him. The password is what makes an unknown person an authenticated user, with all his privileges and his identity's responsibilities. If somebody else uses the right user's password, for the Intranet this other person is exactly the user. Law 196/2003 explicitly forbids users from giving their password to other users, even when they are absent from work. These are some, often underestimated, malign actions a passwords' thief can do:

- steal personal information: the thief can read the user's emails and personal information;
- steal privacy protected data: the thief can gain access to data about other people protected by privacy, or read emails received from other people. The legal responsible of this privacy violation is the thief as well as the user who did not protect other people's data;
- steal money: the thief can find the user's bank account numbers and passwords, sometimes directly from the user's web browser's history;
- delete and modify data: the thief can delete user's important data, or even worse he can modify these data without the user's knowledge (bank numbers, friend's email addresses, degree thesis content, add illegal pictures);
- steal identity: for the computer the thief is now the user, and therefore he can act to the outside world exactly as if it were the user, for example answering to emails, subscribing to websites, withdrawing from exams;
- start illegal activities: anybody who wants to start an illegal Internet activity will obviously use somebody else identity, so he will not get into troubles when the activity is discovered.

Therefore it is absolutely necessary to keep passwords secret. However, there are some ways to discover easy passwords by trial: special automatic programs are able to try one million passwords each second, and they usually start trying combinations of words and numbers (the complete set of all Italian, German and English words can be tried in less than 30 seconds). Law 196/2003 explicitly requires that password do have some features:



- change the password often, at least every three months;
- avoid words related to yourself, such as names, birth dates, birth places and addresses;
- use minimum 8 characters.

Moreover, other good procedures are:

- use as password a good mix of numbers, strange characters, small caps and capital letters;
- use different passwords for different purposes. Unfortunately every website asks the user to register with a password and users who use always the same password are giving it away to every website they register, even untrustworthy ones. It is a good procedure to have at least three passwords: one for important use (bank account), a second one for everyday use and a last one for unimportant use (registering to unknown websites or to services that will not be used anymore).
- beware of passwords stored in programs: Outlook, Outlook Express, Internet Explorer and many other programs store your password masked with asterisks. They seem to be unreadable, but computer

Account name:	username
Password:	*****
	<input checked="" type="checkbox"/> Remember password

experts can reveal them instantly. Store passwords in programs only if that computer has a single user (i.e. the home computer or the personal laptop) or if access to that computer is on a username basis, but never in public places such as an Internet café.

#### 4.2.1. Token key

The token key is a modern password system which consists of a very small electronic device which displays a password changing every few seconds. The system is perfectly time-aligned with the token key and each password is accepted only if entered in those seconds. Therefore, even if a password is intercepted or guessed, it expires after a few seconds.

### 4.3. External threats

From the Internet many unauthorized connection attempts arrive. Some of these are mistakenly authorized and manage to reach the Intranet or at least to come in contact with programs which are behind the firewall. If these connections carry malign intentions, usually their aim is to explore and use the Intranet computers, to destroy Intranet data or to stop some Intranet services (which is a dangerous attack if these services are managing stock trades or telephone calls). Defense against these kinds of attacks is in charge system administrators.

#### 4.3.1. Viruses

While normal external attacks do not involve normal users, the virus is a special attack which arrives directly on the user's computer and must be prevented and stopped by him.

The virus is a little program which has this name because its life cycle is the same of a biological organism: survive and duplicate.

1. It arrives on the computer through email attachments, downloaded files, CDs and floppy disks or directly from the Intranet. It is often hidden inside other good files or programs, which are called infected.
2. As soon as the user mistakenly runs it (often trying to run the good program or to open the good file), the virus orders the computer to run itself every time the computer is turned on, thus assuring its survival.
3. It starts duplicating itself, infecting other files, CDs and floppy disks, and trying to send itself around by email or on the Intranet.
4. Most viruses are programmed to do damage to the computer and to the user, altering or deleting files, sending emails with user's personal data, preventing firewalls and antiviruses from running, or turning the computer off. No viruses are known to be able to damage hardware.

Many names are used for viruses' types according to their different behaviors.

- trojan horse is a virus which looks like a good program and, when downloaded and run by the user, it performs the user's wanted task but at the same time does other actions;
- key logger is a virus which records keyboard's activity and then sends the keystrokes to its creator, mostly to get user's passwords;
- back door is a virus which opens a port on the computer to let external users in;
- adware is a virus which displays advertisement;
- spyware is a virus which spies user's activity to get passwords or to target the user with specific advertisement;
- dialer is a virus which dials expensive numbers using the PSTN modem.

These types are not exclusive: for example a Trojan horse which is at the same time a spyware and an adware.

An infected computer can be recognized by some symptoms. These are the most frequent ones:

- when the computer is turned on, unwanted programs start, advertisement appears, and the desktop presents some new bars or features which were not present nor installed before;
- the computer starts very slowly and unknown programs give strange operating system errors;
- commercial or pornographic web pages appear on the web browser without the user's consent;
- the analogical modem makes typical connection noises even when the computer is not connected or the operating system asks the user to stop the current connection and start a new one to a strange telephone number;
- the Task Manager window (see page 8) presents unknown programs.

Most of the time, a responsible user's behaviour is the best weapon against viruses: it protects him from getting viruses, helps him removing them and prevents him from diffusing them. Responsible behavior means:

- never open downloaded files and email attachments, especially when they come from a friend with a text such as "please open it, urgent!", since simulating to be a user's friend is a typical virus tactics. To open these files, save them on the desktop, check them with an antivirus and then open them;
- do not insert in your computer CDs, DVDs, USB keys and floppy disks coming from other people or which were inserted in other computers, unless you have an antivirus running or unless you scan them immediately with an antivirus;
- avoid visiting strange websites, especially pornographic or hackers' website, or websites which open a lot of pop-up windows;
- have an antivirus always running or at least run an updated antivirus on your whole hard disks every week; keep your antivirus always up to date: more than 50 new viruses appear every week;
- keep communication programs and Microsoft products up to date. Microsoft and most software companies offer free updates and automatic updating tools.

To check the computer for viruses and to try to remove viruses from the computer, the user can run a special program called antivirus. The antivirus basically has three possible different actions:

- it can scan all the storage devices (hard disks, the floppy disk inside the computer, the CD or DVD inside the reader) for viruses. If a virus is found, it tries to remove it and to repair damaged files. Some files can be unrecoverable. Complete devices scanning takes usually some hours;
- it can scan a single file or an entire directory for viruses. If there is an infected file, it tries to delete the virus and repair it. Some files can be unrecoverable. Single file scanning takes some seconds;
- it can be always running. In this case, whenever a virus or a suspect file is run, the antivirus prevents it from running and warns the user.

A lot of antivirus programs, free and commercial, exist. Their most important feature is obviously the possibility to be constantly updated through the Internet.

## **4.4. Emails**

### **4.4.1. Attachments**

For viruses, email attachments are a first class way of traveling, since they are very often opened by users without any precaution. Sometimes viruses hide inside files which were really sent by the sender, unaware of having an infected computer. Other times a virus takes control of the mail reader program and sends itself to the whole address book, counterfeiting the sender address (often using

an address taken from the address book) in order to avoid that the real infected computer be identified and to gain the trust of the receiver, and writing in the email text smart sentences pretending to be a regular friend of the receiver. The arrival of this kind of email usually creates havoc, since the receiver is sure that the fake sender has a virus, while the original infected computer is another one.

The basic rule is never open any attachment from the mail reader program. Save the attached files on the desktop and run an antivirus program to check these files before opening them. Even when the email comes from a friend: he cannot know that to have got a virus, or he can not be the real sender.

#### 4.4.2. Spam

Spam messages are unsolicited unwanted bulk emails. They are unsolicited, meaning that the user did not ask to receive them, they are unwanted, meaning that the user did not want to receive them, and they are bulk, meaning that they are sent to millions of addresses. They are used mainly for four different purposes:

- advertisement emails are the most innocuous version. The email message contains commercial information usually on medicines, pornography, software or investments. Sometimes these messages are purposely written with orthographic mistakes or with strange characters, to avoid being intercepted by antispam programs;
- chain letters are electronic versions of letters circulating in the XX century. They promise good luck to anyone resending it and bad luck to anyone trashing it, or they contain a sad story of an ill child desiring postcards or an urgent warning about a terrible virus: their content is probably false or too old, and a search on the WWW will reveal this immediately. Sending it around will probably cause complains from other users;
- frauds are usually long letters proposing the user a semi-legal bargain or a big lottery prize. Their only aims are to get the user's bank coordinates for further illicit activities and to lure him into paying small expenses hoping to get the promised imaginary money;

**Da:** Gralnick  
**Data:** martedì 21 febbraio 2006 12:59  
**A:** aditn@ing.unitn.it  
**Oggetto:** ATI-Network: probabile SPAM \*\*\* Best love dr@gs at best store!

Hot Weekly Specials			
1	Cialis	\$89	<a href="#">BUY NOW</a>
2	Viagra	\$69	<a href="#">BUY NOW</a>
3	Valium	\$99	<a href="#">BUY NOW</a>

World Wide Shipping Save Up to 80%  
 Discreet Shipping  
 Complete Order Tracking  
 Best Pricing  
 World Wide Shipping

**Da:** miccam@marfino.net  
**Data:** venerdì 24 febbraio 2006 13:55  
**A:** miccam@marfino.net  
**Oggetto:** Equity in Friendship

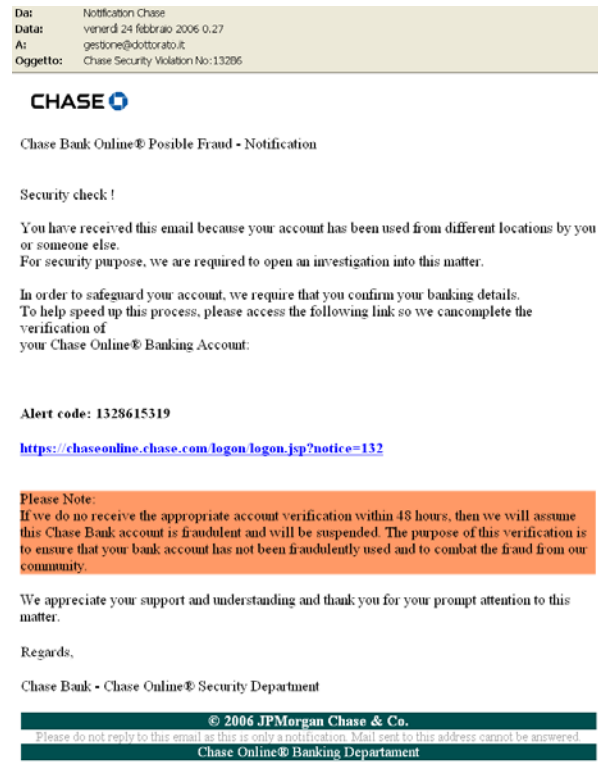
Phone: +234 802 554 9993  
 reply to [adioms@marfino.net](mailto:adioms@marfino.net)

I am the chairman of the contract award committee of the National Petroleum Corporation here in Nigerian, for security reasons, I may not wish to disclose how I got your email address for now.

After due deliberation with my partner, I decided to forward to you this business proposal, we want you to assist us receive the sum of Twenty eight million, six hundred thousand united state bills(us28.6m) into your account. This fund resulted from an over-invoiced contract awarded by us under the budget allocation to my ministry and the bill was approved for payment by the concerned ministries. The contract was executed, commissioned and the contractor was paid his actual cost of the contract. Now, we are left with the balance of us28.6m as the over invoiced amount, which we have deliberately over estimated for our own use. Please note that the law forbids civil servants to operate or own foreign accounts hence this contact, we have agreed to share the money in the following percentages: 30 for you, 60 for us 10 for tax as may be required by your government.

Note that this transaction is very much free from all sorts of risk hence the business was carefully planned before it was successfully executed and we the officials involved in the deal have put many years in service to our ministry. We have been exercising patience for this privilege for so long

- phishing emails look as completely plausible emails from banks and credit card companies, asking the user to enter their website to update his passwords or credit card number. They often carry real bank logos, seem to address to the correct bank's website and even cite the real bank's anti-phishing campaign! However, this website address is a trap, and the user will be sent to a false website, who looks exactly like the bank's one, whose only scope is to get his passwords or credit card number. Phishing has become a big problem for Internet banking system, and the user's best defenses are entering the bank's website always typing the address directly in the web browser (never clicking on addresses contained in emails) and calling immediately the bank at the telephone whenever believing of having been victim of phishing.



The best behavior to adopt against spam messages is to ignore them. Complaining is worthless, since their sender address is always false; clicking on their links, especially if they suggest to click there to be removed from their lists, usually has the only effect of letting the spammer know that the user's address is really read by someone.

The best ways to defend from spammers are to avoid giving the user's real email address during registration in forums, newsgroups and unnecessary websites, and to avoid publishing it on the personal or the company's website. These are the places where spammers get their millions of addresses. If it is really necessary, a good strategy is to have an alternative email address for registrations, which will receive all the spam.

There are antispam programs, which put the supposed spam messages in a separate junk email folder, but they are not completely reliable and sometimes they trash even good messages. These programs relies on analysis of the email's content and on blacklists, which contains the Internet mailservers which are supposed to let spammers send their emails; it may happen that a good mailserver ends up into those blacklists and that emails send from customers or employees of that Internet site are marked as spam by other sites.

#### 4.5. Navigation

Navigation is the second most dangerous Internet activity. It has more or less the same dangers as emails: the user's computer can get viruses if he does not run an antivirus before opening downloaded files, and the user can be lured into phishing websites if he does not type personally the bank's address in the web browser. Moreover, the computer can get viruses even when simply visiting some websites, and therefore two good suggestions are to avoid visiting strange (pornographic websites, websites with a lot of pop-up windows and illegal websites) or untrustworthy websites and to keep Internet Explorer and Windows operating system always up to date.

The other security problem while navigating is data interception. When connecting to a website, the user's data travels long distances, passing through a large number of computers (to connect from unibz.it to www.athesia.it the data go to Padua, Milan and Bologna passing through at least 13 computers). Data on the Internet travel without any protection, any computer administrator can read

them. Therefore, when sending passwords and other private data to a website, the user should take special care that the address in the address bar starts with `https://` (instead of `http://`) and on some browser a lock icon appears in the lower right part of the windows: these indications mean that the connection is secure (SSL) since data are traveling encrypted. Beware that the SSL connection guarantees only that data are not intercepted and that the user is connected to the same website from which he started the connection, while it does not guaranteed this website is the right one.

## 4.6. Backup

Backup is the process of copying important data to another location to prevent their loss. Sometimes programs and even entire operating systems are copied, to be able to immediately continue working even when a computer breaks. There are three very good reasons to do regular backups:

- against the user, who can accidentally delete some files or who can modify files and then change his mind. Having a recent backup handy can often save hours of work;
- against the system, which can suddenly break due to hardware or software problems. Even hard disks tend to be unreliable after some years of continuous activity. A recent backup saves the user from redoing all the work of the previous months;
- against viruses and other users, which can delete and alter files: a backup can save a user coming back from vacations.

Usually the operating system's and the programs' backup are done by system administrators: law 196/2003 explicitly requires an instantaneous backup for all sensitive data and that data are restored within 7 days in case of loss. However, there are some files which should be taken in charge by the user himself:

- personally created data files, including all documents and images created by the user, and any other file which is a result of the user's personal work;
- the address book and the emails (mail readers usually offer a way to save them into files to be used for backup), and for strong navigators also web browser's configuration;
- some programs require a lot of configuration and store their configuration in configuration files, which are usually in the program's directory;
- all the stuff which is difficult to find again, such as documents from other people or downloaded from forgotten websites.

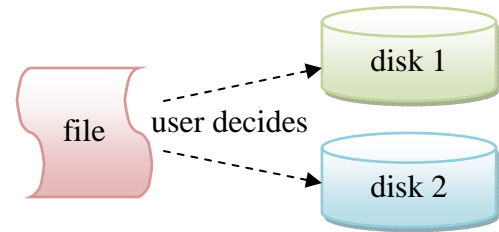
The place where the files are copied determines the reliability of the backup. It should be a large, cheap and fast storage device. It should also be handy, since the typical problem with backup is that the user does not takes time to do it regularly and, when the backup is too old, it is worthless. For home or simple office users, the Friday morning backup is a good timing solution. Good storage devices to be used are:

- a second hard disk, used only for backup, which is very fast and very large and always ready to be used;
- online backup systems, where user's data are uploaded and are ready from anywhere in the world (given a broadband connection);
- four sets of rewritable DVDs, to be used in circle (one for each month's week, for example);
- USB pen drive, to be used only in emergency when no other appropriate storage device is available;
- big companies usually have special tape devices for backups.

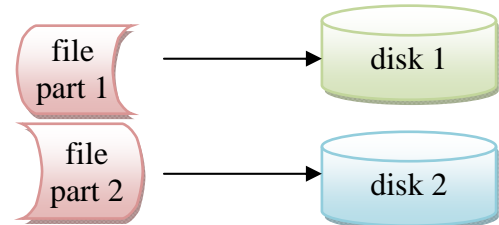
### 4.6.1. RAID

A very popular backup solution is RAID (Redundant Array of Independent Disks) technology, which consists of several identical hard disks. There are different types of RAID implementations, which vary a lot in functionalities and security.

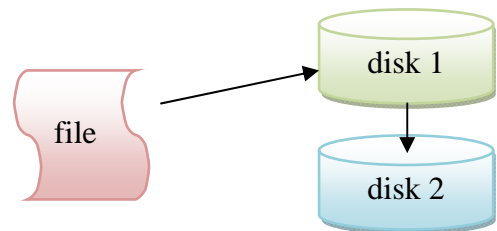
**JBOD** (Just a Bunch Of Disks) is a primitive form of RAID in which all the disks are seen by the user simply as disks on which they can write as usual. The advantage is that the available space is the sum of the space of all the disks, however there is no form of data protection: if a disk breaks, anything on that disk is lost.



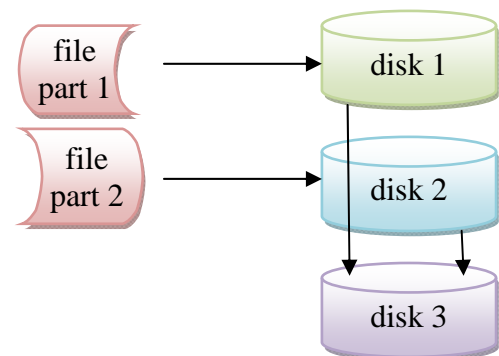
**RAID0** uses two identical disks which are seen by the user as a single disk. Every time he writes a file, the first part of the file is written on the first disk while the second on the second this. This strategy has the big advantage that writing speed doubles, with a total available space which is the sum of the size of the two disks. But if a disk breaks, all the content of both disks is lost, since the user will lose half of all the files.



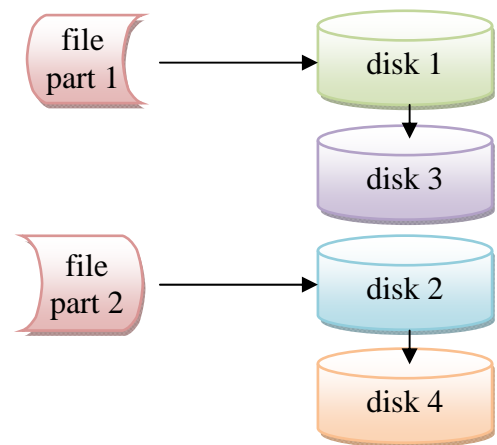
**RAID1** is the most common implementation of RAID. It uses two identical disks but the user sees only the first one. The second disk is simply an identical and instantaneous copy of the first one. The disadvantage is that the speed does not improve and the available space is the size of one disk only, but in case a disk breaks, no file is lost since the other one is its identical copy. This is a very good backup solution to protect data against physical failure, especially suited for 24h services. However, it is not a backup solution against viruses or user's incidental cancellations, since any modification on the first disk is immediately performed on the second one.



**RAID5** is a complicated implementation of RAID. It uses three identical disks and the user sees only the first two as a single big disk. Every file written is split between the first two disks as for RAID0, however at the same time the difference between first and second disk is saved on the third disk. In case one of the first two disks breaks, the computer is able to automatically reconstruct its content with a complicated technique which uses the differences stored on the third disk. This has the speed advantage of RAID0 and the safety of RAID1, giving the user an available space equivalent to the sum of two disks sizes. Its only drawback is that, with respect to RAID1, in case of hard disk failure a lot of time is required to reconstruct the missing disk's content.



RAID10 is an overlay of RAID1 and RAID0. It uses four disks, writing files on the first and on the third as if they were on RAID0 and then duplicating their content on disks two and four. This technique has the speed of RAID0, the reliability of RAID1, but gives the user a space equivalent to the sum of two disks sizes, while four disks are effectively used.



All the RAID techniques are good at either improving the speed or improving the reliability against hardware failure, but are not good against other threats and therefore they must always be coupled with another form of backup, such as tape backup for large companies or weekly/daily copy on DVD or on another hard disk for home users.

## Index

- .ac.uk, 16
- .at, 16
- .avi, 11
- .bat, 11
- .bmp, 11
- .bz.it, 16
- .com, 11, 16
- .csv, 11
- .de, 16
- .doc, 11, 20
- .edu, 16
- .eu, 16
- .exe, 11
- .gif, 11
- .gov, 16
- .htm, 11
- .html, 11
- .it, 16
- .jpeg, 11
- .jpg, 11
- .mil, 16
- .mov, 11
- .mp3, 11
- .mpeg, 11
- .mpg, 11
- .net, 16
- .nl, 16
- .org, 16
- .pdf, 11, 20
- .ppt, 11
- .rtf, 11
- .to, 16
- .tv, 16
- .txt, 11
- .wav, 11
- .xls, 11
- .zip, 11
- @, 15
- \ubz01fst, 12
- 127.0.0.1, 16
- 128 bits, 22
- 3G, 21
- absolute path, 9
- access, 11
- Acrobat, 11
- address, 9, 15, 25, 27
- address book, 28
- Administrators, 12
- ADSL, 20
- ADSL modem, 20
- advanced search, 20
- advertisement, 26
- adware, 24
- ALT, 6
- AltaVista, 19
- ALTGR, 6
- AMD Ahtlon 64 X2, 2
- analogical, 20, 25
- AND, 20
- anonymous, 18
- antispam, 26, 27
- antivirus, 22, 24, 25, 26, 27
- application bar, 7
- ARROWS, 6
- asterisks, 23
- Asymmetric Digital Subscriber Line, 20
- attachment, 25, 26
- audio, 11
- authenticated user, 23
- authentication, 17, 18, 22
- back door, 24
- BACKSPACE, 6
- backup, 4, 22, 28
- bank, 26, 27
- BILD, 6
- biometric, 22
- bit, 2
- bits per second, 15
- blacklist, 27
- blog, 19
- bluetooth, 4
- bps, 15
- bulk, 26
- byte, 2
- cables, 15
- camera, 3
- CANC, 6
- CAPS LOCK, 6
- cards, 3
- CD, 4, 24, 25
- CD-reader, 4, 8, 13
- CD-writer, 4
- certification authority, 22, 23
- chain letter, 26
- chat, 13, 19
- Chrome, 16
- client, 13
- commercial, 5
- communication program, 16, 18, 19, 25
- compress, 10
- compressed file, 11
- computer box, 2
- computer network, 13
- configuration file, 28
- congestion, 21
- connection, 13, 14, 24, 25
- Control panel, 7
- copy, 9
- counterfeit, 25
- crawler, 19
- create a new directory, 10
- create shortcut, 10
- CRT, 3
- CTRL, 6, 10
- CTRL+ALT+DEL, 8
- CTRL+C, 10
- CTRL+SHIFT+ESC, 8
- CTRL+V, 10
- CTRL+X, 10
- curved arrow, 9
- cut, 10
- dangerous area, 14
- data, 4, 5, 28
- data interception, 27
- data storage, 4
- DEL, 6, 10
- delete, 10
- desktop, 25, 26
- Desktop, 7
- Details, 9
- dialer, 24
- dial-up, 20
- digital divide, 21
- digital signature, 22
- directory, 8, 25, 28
- distribution, 5
- DNS, 15, 16
- document, 11, 28
- documents, 28
- domain, 16
- Domain Name Server, 15, 16
- double click, 9
- download, 20
- downloaded file, 27
- dual core, 2
- DVD, 4, 25, 28
- DVD-reader, 4, 13
- DVD-writer, 4
- E3, 20
- edition, 5
- EINFG, 6
- electronic signature, 22
- email, 10, 13, 15, 16, 23, 24, 25, 26, 27, 28
- email attachment, 24, 25
- encrypted, 28
- encryption, 10, 22
- END, 6
- ENDE, 6
- ENTER, 6
- Enterprise, 6
- ENTF, 6
- external hard disk, 4
- Ethernet, 15
- Excel, 11
- execute, 12
- Explorer, 11
- extension, 11, 16
- external threat, 24
- extract, 10
- F1, 6
- F12, 6
- Fast Ethernet, 15
- fax/modem, 4
- fax/modem card, 3
- file, 8, 25, 26, 28
- file system, 8
- File Transfer Protocol, 19
- file type, 9, 11
- FINE, 6
- firewall, 15, 22, 24
- floppy disk, 8, 24, 25
- folder, 8
- Folder Options, 8
- forum, 19, 27
- fraud, 26
- free, 17
- freeware, 5, 16, 17
- full control, 12
- gateway, 15
- Gbps, 15
- General Packet Radio Service, 20
- Giga Ethernet, 15
- Gigabyte, 2
- Google, 19
- GPRS, 20
- group of users, 12
- GSM cellular phone, 20
- hard disk, 3, 4, 8, 12, 13, 25, 28
- hardware, 2, 24, 28
- Hide extensions, 8
- hierarchical, 8
- HOME, 6
- Home Premium, 6
- http, 28
- https, 28
- hub, 14
- hyperlink, 19
- icon, 8
- identity, 23
- image, 11, 20, 28
- IMAP, 17
- IMAP server, 17
- inches, 3
- infrared, 4
- inkjet, 3
- input, 3
- INS, 6
- Integrated Service Digital Network, 20
- interaction, 13
- interception, 27
- internal hard disk, 4
- Internet, 14, 15, 16, 21, 22, 27
- Internet connection, 20
- Internet name, 16
- Internet Protocol, 15
- Internet provider, 17, 18
- Intranet, 14, 15, 16, 23, 24
- INVIO, 6
- IP, 15, 16
- IP number, 16
- IPv4, 15, 16
- IPv6, 16
- ISDN, 20
- ISDN modem, 20
- ISDN telephone, 20
- IZArc, 10, 11
- JBOD, 29
- junk, 27
- Kbps, 20
- key, 22
- key logger, 24
- keyboard, 3, 6, 7
- keyword, 19
- Kilobyte, 2
- LAN, 12, 14, 21
- language, 7
- laser, 3
- law 196/2003, 22, 23, 28
- LCD, 3
- link, 9, 10, 19, 27
- Linux, 4

- list content, 12
- local area network, 14
- localhost, 16
- lock icon, 28
- locking, 7
- locks, 11, 12
- login name, 7
- Lycos, 19
- Mac OS X, 5, 16
- Macintosh, 5
- mail reader, 17, 25, 26, 28
- mailserver, 15, 16, 17
- maximum speed, 21
- Mbps, 15, 20, 21
- Media Player, 11
- Megabyte, 2
- memory, 3
- memory card, 4
- memory stick, 4
- microphone, 3
- Microsoft Internet Explorer, 16, 23, 27
- Microsoft Outlook, 17, 23
- Microsoft Outlook Express, 23
- Microsoft Outlook Web App, 18
- Microsoft Windows, 4, 6, 27
- Microsoft Windows 7, 4
- Microsoft Windows Seven, 6
- Microsoft Windows Vista, 4, 6
- Microsoft Windows XP, 4, 6
- minimum band, 21
- minimum speed, 21
- modem, 20, 25
- modify, 12
- monitor, 3
- Moore's law, 2
- motherboard, 3, 4
- mouse, 3
- move, 10
- Mozilla Firefox, 16
- Mozilla Thunderbird, 17
- mp3 players, 4
- multifunction, 3
- multifunction-printer, 4
- multilanguage, 7
- navigation, 27
- net, 14
- network card, 3
- network folder, 12
- network router, 4
- network traffic, 20
- new directory, 10
- newsgroup, 27
- Notepad, 11
- Office Picture Manager, 11
- open, 9, 26, 27
- open source, 5
- operating system, 4, 25, 27, 28
- OR, 20
- output, 3
- owner, 12
- PAG, 6
- Paint, 11
- password, 7, 17, 22, 23, 27, 28
- paste, 9, 10
- PEC, 18, 23
- peer to peer, 13, 19
- permission, 22
- permissions, 12
- personal data, 22
- PG, 6
- phishing, 27
- photo cameras, 4
- Picture Fax Viewer, 11
- Plain Standard Telephone Network, 20
- plus symbol, 9
- pop, 16
- POP3, 17
- POP3 server, 17
- port 110, 16, 17
- port 25, 16, 17
- port 80, 16
- ports, 16
- POS1, 6
- Posta Elettronica Certificata, 18
- PowerArchiver, 11
- Powerpoint, 11
- printer, 3, 13
- privacy, 22
- private, 5
- private key, 22
- processor, 2, 4, 13
- Professional, 6
- program, 4, 5, 11, 23, 25, 28
- proprietary, 5, 16, 17
- Proprieties, 12
- protocol, 17
- provacy, 22, 23
- PSTN, 20
- public key, 22
- Qualcomm Eudora, 17
- quicklaunch icons, 7
- quotation mark, 20
- RAID, 28
- RAID0, 29
- RAID1, 29
- RAID10, 30
- RAID5, 29
- RAM, 3
- read, 12
- read and execute, 12
- read-only, 11
- Regional and Language Options, 7
- registration, 27
- remote access, 19
- rename, 10
- resources, 13
- restrictions policies, 17
- root, 8
- router, 14
- run, 9, 26
- Safari, 16
- save, 26
- scanner, 3
- scoring, 19
- search engine, 19
- secure, 28
- security, 15, 22
- Security, 12
- sender, 25, 26
- sender address, 18, 25, 27
- sensitive data, 22, 28
- server, 13
- service pack, 6
- shareware, 5, 17
- sharing, 13
- sheet, 11
- SHIFT, 6, 10
- shortcut, 9
- Skype, 18
- smtp, 16
- SMTP, 17
- SMTP server, 17
- software, 2, 4, 28
- solid state disk, 4
- sound card, 3
- spam, 26, 27
- spam message, 26
- speakers, 3
- speed, 15
- spyware, 24
- SSD, 4
- SSH, 19
- SSL, 28
- star, 14
- start menu, 7
- storage device, 25, 28
- STRG, 6
- subdirectories, 8
- subdomain, 16
- swith, 14
- T3, 20
- TAB, 6
- tape device, 4, 28
- Task Manager, 25
- telephone, 20
- Telnet, 19
- terminal, 13
- text, 11
- TFT, 3
- token key, 24
- topology, 14
- trash can, 10
- tree, 8
- trojan horse, 24
- trusted area, 14
- Ultimate, 6
- UMTS, 21
- UMTS cellular phone, 21
- Universal Mobile Telecommunications System, 21
- Unix, 4
- unsolicited, 26
- unwanted, 26
- upload, 20
- USB pen drive, 4, 28
- username, 17, 22, 23, 24
- users, 12
- VeriSign, 23
- version number, 5
- video, 11
- video card, 3
- Virtual Private Network, 14
- virus, 24, 25, 26, 27, 28
- vlog, 19
- Voice over IP, 18
- VoIP, 18
- VPN, 14
- WAN, 14
- Web 2.0, 19
- web browser, 16, 18, 19, 25, 27, 28
- web page, 11, 15, 16, 19, 25
- web service, 19
- webmail, 18
- webserver, 15, 16
- website, 19, 25, 27, 28
- Wide Area Network, 14
- Wi-Fi, 21
- Wikipedia, 19
- WiMax, 21
- WinAmp, 11
- WinZip, 10, 11
- wireless, 14, 15, 21
- wireless card, 21
- Word, 11
- World Wide Web, 19
- write, 12
- www, 16
- WWW, 16, 19, 21, 26
- Yahoo!, 19
- Yahoo! Messenger, 19
- zip-archive, 10