What does Basic Input/Output System (BIOS)?

A basic input/output system (BIOS) is a preinstalled program used during startup on Windows-based computers. The CPU initially accesses the BIOS, after which the operating system is loaded.

The BIOS is built-in software that contains generic code required to control the keyboard, display screens, disk drives and other functions. The primary purpose of the BIOS is to set up hardware and further load and start an operating system. BIOS is placed in a nonvolatile ROM chip inside the computer, ensuring the availability of BIOS at all times and preventing accidental disk failure. The BIOS checks every hardware connection and locates the devices, after which the operating system is loaded into computer memory.

BIOS software is designed to work with the various devices that make up a complimentary system chipset. The BIOS library has certain functions used to operate and control system peripherals, which can be initiated by external software.

Users using the BIOS user interface can perform functions such as:

- Setting the system clock
- Enabling and disabling certain system components
- Hardware configuration
- Selecting boot drives
- Set password prompts for secured access to BIOS user interface function

Modern PCs have BIOS stored in rewritable memory, permitting contents to be rewritten or replaced. Such content rewriting is called flashing and is executed through a special program provided by system manufacturers.

What is booting process?

In computing, booting is starting up a computer or computer appliance until it can be used. It can be initiated by hardware such as a button press or by software command. After the power is switched on, the computer is relatively dumb and can read only part of its storage called read-only memory (ROM). There, a small program is stored called firmware. It does power-on self-tests and, most importantly, allows accessing other types of memory like a hard disk and main memory. The firmware loads bigger programs into the computer's main memory and runs it. In general purpose computers, but additionally in smartphones and tablets, optionally a boot manager is run. The boot manager lets a user choose which operating system to run and set more complex parameters for it. The firmware or the boot manager then loads the boot loader into the memory and runs it. This piece of software is able to place an operating system kernel like Windows or Linux into the computer's main memory and run it. Afterwards, the kernel runs so-called user space software – well known is the graphical user interface (GUI), which lets the user log in to the computer or run some other applications. The whole process may take seconds to tenths of seconds on modern day general purpose computers.

Restarting a computer also is called reboot, which can be "hard", e.g. after electrical power to the CPU is switched from off to on, or "soft", where the power is not cut. On some systems, a soft boot may optionally clear RAM to zero. Both hard and soft booting can be initiated by hardware such as a button press or by software command. Booting is complete when the operative runtime system, typically operating system and some applications,[NB 1] is attained.

The process of returning a computer from a state of hibernation or sleep does not involve booting. Minimally, some embedded systems do not require a noticeable boot sequence to begin functioning and when turned on may simply run operational programs that are stored in ROM. All computing systems are state machines, and a reboot may be the only method to return to a designated zero-state from an unintended, locked state.

In addition to loading an operating system or stand-alone utility, the boot process can also load a storage dump program for diagnosing problems in an operating system.

Boot is short for bootstrap or bootstrap load and derives from the phrase to pull oneself up by one's bootstraps. The usage calls attention to the requirement that, if most software is loaded onto a computer by other software already running on the computer, some mechanism must exist to load the initial software onto the computer. Early computers used a variety of ad-hoc methods to get a small program into memory to solve this problem. The invention of read-only memory (ROM) of various types solved this paradox by allowing computers to be shipped with a startup program that could not be erased. Growth in the capacity of ROM has allowed ever more elaborate start up procedures to be implemented.

What is UEFI?

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace BIOS.

Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on. It checks to see what hardware components the computing device has, wakes the components up and hands them over to the operating system. The new specification addresses several limitations of BIOS, including restrictions on hard disk partition size and the amount of time BIOS takes to perform its tasks.

Difference between RAID and LVM

S.No.	RAID	LVM
1.	RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
2.	A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.	LVM is a logical layer that that can be manipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
3.	RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.	LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without losing data, resize the volumes, create snapshots, etc.
4.	RAID is either software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.	LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.

5.	RAID is NOT any kind of Data backup solution. It’s a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.	LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.

WhatsApp Security

From day one, we built WhatsApp to help you stay in touch with friends, share vital information during natural disasters, reconnect with separated families, or seek a better life. Some of your most personal moments are shared with WhatsApp, which is why we built end-to-end encryption into our app. When end-to-end encrypted, your messages, photos, videos, voice messages, documents, and calls are secured from falling into the wrong hands.

Security by Default

WhatsApp's end-to-end encryption is available when you and the people you message use our app. Many messaging apps only encrypt messages between you and them, but WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp. This is because your messages are secured with a lock, and only the recipient and you have the special key needed to unlock and read them. For added protection, every message you send has its own unique lock and key. All of this happens automatically: no need to turn on settings or set up special secret chats to secure your messages.

See for Yourself

WhatsApp lets you check whether the calls you make and messages you send are end-to-end encrypted. Simply look for the indicator in contact info or group info.

Speak Freely

WhatsApp Calling lets you talk to your friends and family, even if they're in another country. Just like your messages, WhatsApp calls are end-to-end encrypted so WhatsApp and third parties can't listen to them.

Messages that Stay with You

Your messages should be in your hands. That's why WhatsApp doesn't store your messages on our servers once we deliver them, and end-to-end encryption means that WhatsApp and third parties can't read them anyway.