

Chapter

1

Computer Hardware

ENCE EXAM TOPICS COVERED IN THIS CHAPTER:

- ✓ Computer hardware components
- ✓ The boot process
- ✓ Partitions
- ✓ File systems

COPYRIGHTED MATERIAL



Computer forensics examiners deal most often with the media on which data is stored. This includes, but is not limited to, hard drives, CDs, DVDs, Flash memory devices, floppies, and tapes.

While those devices might be the bane of the examiner's existence, media devices don't exist in a void, and knowledge of a computer's various components and functions is a must for the competent examiner.

As an examiner, you may be called upon to explain how a computer functions to a jury. To do so requires that you not only know a computer's function from a technical standpoint, but also be able to translate those technical concepts into real-world, easy-to-understand terms.

As an examiner, you may also be subjected to a *voir dire* examination by opposing counsel to challenge your competence to testify. Acronyms are hardly in short supply in the field of computing, some well known and meaningful, and others more obscure. Imagine being asked during such an examination to explain several of the common acronyms used with computers, such as RAM, CMOS, SCSI, BIOS, and POST. If you were to draw a blank on some obscure or even common acronym, picture its impact on your credibility.



TWAIN – “Technology Without An Interesting Name”

You may encounter problems with a computer system under examination or with your own forensic platform. Troubleshooting and configuration require knowledge of the underlying fundamentals if you are to be successful.

Thus, the purpose of this chapter is to develop a solid understanding of the various components of a computer and see how a single spark of electricity brings those otherwise dead components to life through a process known as *booting* the computer. In addition, you'll learn about the drive partitions and file systems used by computer systems.

Computer Hardware Components

Every profession has, at its core, a group of terms and knowledge that is shared and understood by its practitioners. Computer forensics is certainly no exception. In this section, I discuss the various terms used to describe a computer's components and systems.

Case The case, or chassis, is usually metal, and it surrounds, contains, and supports the computer system components. It shields electrical interference (both directions) and provides

protection from dust, moisture, and direct-impact damage to the internal components. It is sometimes erroneously called the central processing unit (CPU), which it is not.

ROM (read-only memory) This is a form of memory that can hold data permanently, or nearly so, by virtue of its property of being impossible or difficult to change or write. Another important property of ROM is its nonvolatility, meaning that the data remains when the system is powered off. Having these properties (read-only and nonvolatile) makes ROM ideal for files containing startup configuration settings and code needed to boot the computer (ROM BIOS).

RAM (random access memory) A computer's main memory is its temporary workspace for storing data, code, settings, and so forth. It has come to be called RAM as it exists as a bank of memory chips that can be randomly accessed. Before chips, tape was the primary media, and accessing tape was—and still is—a slow, linear or sequential process. With the advent of chips and media on drives (both floppy and hard drives), data could be accessed randomly and directly, and therefore with much greater speed. Hence, *random access memory* was the name initially given to this type of memory to differentiate from its tape predecessor. Today most memory can be accessed randomly, and the term's original functional meaning, differentiating it from tape, has been lost to history. What distinguishes RAM from ROM, among other properties, is the property known as *volatility*. RAM is usually volatile memory, meaning that upon losing power, the data stored in memory is lost. ROM, by contrast, is nonvolatile memory, meaning that the data remains when the power is off. It is important to note that there are non-volatile forms of RAM memory known as NVRAM (nonvolatile random access memory), and thus you should not be quick to assume that all RAM is nonvolatile.



The computer forensic examiner more often than not encounters computers that have been shut down, seized, and delivered for examination. Important information in RAM (the computer's volatile memory) is lost when the plug is pulled. All is not lost, however, as this data is often written to the hard drive in a file called the *swap file*. This swap file can grow and shrink by default in most Microsoft Windows systems, which means this data can be in the swap file itself as well as in unallocated clusters and in file slack as the swap file is resized. Unallocated clusters and file slack are areas containing data that is no longer in an allocated file. We'll cover them in detail in a later chapter. What's more, if the computer was in the "hibernate" mode, the entire contents of RAM are written to a file named *hiberfil.sys* so that the contents of RAM can be restored from disk and the system restored in the time it takes to read the *hiberfil.sys* file into RAM. It should be no surprise to learn that the *hiberfil.sys* file size is the same size as the system's RAM memory size!

Power supply The power supply transforms supply voltage (120VAC or 240VAC) to voltages and current flows required by the various system components. DC voltages of 3.3 volts, 5 volts, and 12 volts are provided on a power supply for an ATX form factor motherboard.

4 Chapter 1 • Computer Hardware



The standard molex power connector used frequently by examiners has four wires providing two different voltages (yellow = 12VDC+, black = ground, black = ground, red = 5VDC+).

Motherboard or mainboard This component is the largest printed circuit card within the computer case. It is mounted on “stand-offs” to raise it above the case, providing a space for air-flow and preventing contact or grounding of the printed circuits with the case. The motherboard typically contains the following: the CPU socket, BIOS, CMOS, CMOS battery, Real-Time Clock (RTC), RAM memory slots, Integrated Drive Electronics (IDE) controllers, Serial Advanced Technology Attachment (SATA) controllers, Universal Serial Bus (USB) controllers, floppy disk controllers, Accelerated Graphics Port (AGP) or Peripheral Component Interconnect (PCI) Express video slots, PCI or PCI Express expansion slots, and so forth. Many features that once required separate expansion cards are now offered as “on-board,” such as Small Computer System Interface (SCSI) controllers, network interface (Gigabit Ethernet and wireless), video, sound, and FireWire (1394a and b).

Microprocessor or CPU The brains of the unit, this is a massive array of transistors arranged in microscopic layers. The CPU performs data processing, or interprets and executes instructions. Accordingly, most of the computer’s function and instructions are carried out in this unit. Modern processors generate enormous amounts of heat, and quickly and efficiently eliminating heat is essential to both function and survival.

Heat sink and fan At the very least, a heat sink and fan will be attached to the CPU to keep it cool. The heat sink interfaces directly with the CPU (or other heat-generating chip), usually with a thermal compound sandwiched between. The heat sink is made of a high-thermal conductance material whose job it is to draw the heat from the chip and to dissipate that heat energy into the surrounding air (with the assistance of the fan, with an array of cooling fins). Some high-end platforms will have thermal solutions (heat sinks and fans) mounted to RAM memory, chipsets, hard drives, and video cards. Water-cooling systems are becoming more popular with gamers. Use caution working around these systems as water and electricity are usually at odds and damage to systems can occur.

Hard drive This is the main storage media for most computer systems, holding the boot files, operating system files, programs, and data. It consists of a series of hard thin platters revolving at speeds ranging from 4,800 to 15,000 revolutions per minute (RPMs). These platters (which are magnetized) are accessed by heads moving across their surfaces as they spin at high speed. The heads can read or write, detecting or creating microscopic changes in polarity, with positive changes being 1s and negative changes being 0s—hence the binary system of “1s and 0s.”

Hard drive platters have an addressing scheme so that the various locations where data is stored can be located for reads and writes. Originally this addressing scheme involved the CHS system (C = Cylinder, H = Head, and S = Sector). A *sector* is the smallest amount of space on a drive that can be written to at a time. A sector contains 512 bytes that can be used by the operating system. Each side of the platter is formatted with a series of concentric circles known as *tracks*.

Sectors are contained in the tracks, and originally each track contains the same number of sectors. A *cylinder* is a logical construct; it is a point on all the platters where the heads align along a vertical axis passing through the same sector number on all the platters. There are two *heads* for each platter, one for each side (side 0 and side 1). Depending on the number of platters present, the heads will be numbered. To determine the number of bytes present on a hard drive, a formula is used: $C \times H \times S \times 512 = \text{total storage bytes}$. The “C” is the total number of cylinders, the “H” is the total number of heads, the “S” is the number of sectors per track, and 512 is a constant that represents the number of bytes in a sector usable by the operating system (OS).

This formula holds true as long as the number of sectors per track remains the same for all tracks, which applies as well to older, lower-capacity hard drives. This system, however, has limitations for hard drive storage capacity. The limitations reflect how densely populated (sectors per track) the inner tracks are. The outer tracks, by contrast, can always hold more data than the inner tracks and contain wasted storage space. To overcome this limitation, Zoned-Bit Recording (ZBR) was developed; in ZBR, the number of sectors per track varies in zones, with the outer zones containing more sectors per track than the inner zones. This system has vastly improved data storage capacities.

The formula, however, is not valid for modern drives, because the number of sectors per track is no longer constant if ZBR is present. To address the larger-capacity hard drives, a new addressing scheme has been developed, called Logical Block Addressing (LBA). In this system, sectors are addressed simply by sector number, starting with sector zero, and the hard drive’s electronics translate the sector number to a CHS value understood by the drive. To determine the storage capacity of hard drives using ZBR, you determine the total LBA sectors and multiply that number by 512 (bytes per sector). The product yields the total storage capacity of the drive in bytes (total LBA sectors \times 512 = total storage capacity in bytes).

Hard drives can be ATA (now often called PATA to differentiate parallel from serial with the advent of SATA), SATA (Serial ATA), and SCSI, depending on their electrical interface or controller.

SCSI (Small Computer Systems Interface) SCSI is an electronic interface that originated with Apple computer systems and migrated over to other systems. It is a high-speed, high-performance interface, used on devices requiring high input/output, such as scanners and hard drives. The SCSI BIOS is an intelligent BIOS that queues read/write requests in a manner that improves performance, making it the choice for high-end systems. SCSI drives do not use the master/slave pin configurations of the IDE counterparts. Rather, they are assigned ID numbers that are most often set by pinning jumpers.

IDE (Integrated Drive Electronics) controller IDE is a generic term for any drive with its own integrated drive controller. Originally there were three types, but only one survived; it is known as ATA (Advanced Technology Attachment). Officially, the IDE interface today is called ATA, and the two names will often be used interchangeably. Two IDE connectors are found on the motherboard, one labeled *primary IDE* and the other *secondary IDE*. Each is capable of handling two IDE devices (hard drive, CD, DVD), for a maximum of four IDE devices. Of the two devices on same IDE ribbon cable, one is the “master” and the other is the “slave.” One places jumpers on pins to designate the “master” or “slave” status. Typically the boot hard drive will be attached to the primary controller, and it is the master if two devices are present on that IDE

6 Chapter 1 • Computer Hardware

channel. Alternatively, you could use the CS, or “cable select,” method of pinning by which the assignment of master/slave is done “automatically,” provided you use a cable that properly supports CSEL (another way of abbreviating Cable SElect) signaling. On an 80-conductor IDE/ATA cable using CS, the drive at the end of the cable will be assigned as master and the drive assigned to the middle connector will be the slave.

SATA (Serial Advanced Technology Attachment) controller By the beginning of this century, IDE (ATA) hard drives had been around for a long time, but the electronic circuitry by which the data was sent had reached its upper limit (133MB/s). In August 2001 a new standard, known as SATA 1.0, was finalized and approved. SATA uses serial circuitry and data can be sent, initially, at 150MB/s, with 300 or more on the near horizon as SATA II standards (released in October 2002) find their way into the market. Unlike IDE drives, SATA drives require no “pinning.” SATA ports can be found on most modern motherboards and often have RAID 0 available to them. IDE drives are starting to phase out and are being replaced by SATA drives. Even though IDE drives are being phased out forensic examiners can expect to see them around for a long time, as they were in use for over 10 years.

RAID (Redundant Array of Inexpensive Disks) A RAID is an array of two or more disks combined in such a way as to increase performance or increase fault tolerance. In a RAID 0, data is striped over two or more disks, which increases performance by reducing read and write times. However, if any disk fails in a RAID 0, all data is lost. In a RAID 1, data is mirrored over the drives in the array. A RAID 1 does not increase performance, but it does create redundant data, thereby increasing fault tolerance. In a RAID 5 configuration, typically data is stored on three drives, although other configurations can be created. Data is striped over two drives, and a parity stripe is created on the third. Should any one drive fail, it can be “rebuilt” from the data of the other two. RAID 5 achieves fault tolerance and increased performance. RAID 0 + 1 is a relatively new type of RAID. It is typically configured with four drives; one pair is used for striping data and the other pair is a mirror of the striped pair. With this configuration, you again achieve high performance and fault tolerance.

Floppy drive Floppy drives used to be primary storage devices. Currently they are used to store and move small amounts of data, since the capacity of the 3.5-inch floppy is only 1.44MB of data. They are often used by forensic examiners as boot drives to boot systems for DOS acquisitions, which is a method of acquiring data using a DOS boot disk. We’ll cover this extensively in a later chapter. Floppy drives are being phased out in lieu of CD/DVD and USB thumb drives.



When going out into the field to image a system, always pack a spare internal 3.5-inch floppy drive. You may have to do a DOS acquisition, and the target system may not be equipped with a floppy, or the one present may be defective, and a CD boot may not be an option.

CD-ROM (Compact Disc – Read-Only Memory) or CD-RW (Compact Disc – Read/Write) drive CD drives use laser beams to read indentations and flat areas as 1s and 0s. The data is formatted into a continuous spiral emanating from the center to the outside, whereas, by comparison, hard

drive data is formatted into concentric circles. The former CD-ROM is read-only technology whereas the latter, CD-RW, permits writing to CD media in addition to reading.

DVD-ROM (Digital Versatile Disc – Read-Only Memory) or DVD-RW (Digital Versatile Disc – Read/Write) DVD drives use a technology similar to that of CDs. The laser beam used with DVDs is a shorter wavelength, creating smaller pits and lands, which are actually depressions and elevations in the physical surface. The result is a spiral track that is more densely populated with data. Couple this gain with layered spiral tracks, and the gain in data storage capacity is tremendous. Whereas a CD stores, at most, approximately 700MB of data, a DVD can hold 8 to 17GB of data, with higher densities on the horizon.

USB controller Universal serial bus (USB) is a relatively new external peripheral bus standard capable of high-speed serial input/output (USB 1.1 = 1.5Mb/s and USB 2 = 480Mb/s). It was developed to facilitate Plug and Play for external devices without the need for expansion cards and configuration issues.

USB port This is a rectangular-shaped port connected to the USB controller, with pins for four conductors (one cable power, two data negative, three data positive, four ground—all surrounded by shielding). These ports are used for USB connections, which can be external storage devices, cameras, license dongles, keyboards, mice, and so forth.

IEEE 1394 Also known as FireWire (the name licensed by Apple) or iLink (Sony), 1394 is yet another high-speed serial I/O standard. Its plug-and-play capabilities are on a parallel with USB. 1394 comes now in two flavors, or speeds. 1394a is the original version, moving data at 400Mb/s. 1394b is the latest version, moving data at 800 Mb/s, with gigabit speeds planned soon. 1394 allows “daisy chaining” of devices, with a maximum of 63 nodes.

IEEE 1394a ports FireWire ports are similar to USB ports, except that one end is slightly rounded or pointed. There are six wires/pins in a 1394 connection, with two pairs of clock and data lines, plus two for power (one positive, one negative). FireWire ports are used primarily for external high-speed storage devices, cameras, multimedia systems, and so forth.

Expansion slots (ISA, MCA, EISA, VL-Bus, PCI, AGP, PCI Express) Expansion slots are populated by “cards” whose purpose is to connect peripheral devices with the I/O bus on the motherboard so that these peripheral devices can communicate with the CPU. There are several types of peripheral devices, and they expand the capabilities of the PC. Expansion slots come in different flavors, or speeds, that have evolved over time. Rarely do you encounter the older types, such as the ISA (Industry Standard Architecture 8 bit and 16 bit in 1981 and 1984, respectively), MCA (IBM Micro Channel Architecture, 32 bit in 1986), or the EISA (Extended Industry Standard Architecture – Compaq and Generic, 32 bit in 1986). The VL-Bus (VESA Local Bus, named after the VESA Committee who developed it) was in use during 1992 to 1994, and appears as a legacy slot on some older PCI bus systems still in use. The VL-Bus slot uses the 16-bit ISA plus an extension to handle legacy 16-bit and newer 32-bit cards. The PCI (Peripheral Component Interconnect) bus was born in 1992 and is still in use today. It exists primarily as a 32-bit card, but some high-end systems provide a 64-bit PCI interface. After 10 years, in July 2002 the PCI design had reached its upper speed limit and was replaced with the PCI Express 1.0 specification, which is finding its way into the mainstream market. The former was

8 Chapter 1 • Computer Hardware

based on parallel data communications whereas the latter was based on serial data communications, with serial facilitating faster data communications. Sandwiched between the PCI and the PCI Express was the AGP (Accelerated Graphics Port). AGP was based on PCI, with enhancements, but was connected separately from the PCI bus and joined via a direct pathway for exclusive video/graphics use by the system. PCI Express replaces AGP altogether for graphics. PCI Express coexists on most new boards with “legacy” PCI slots, with the latter slated for extinction as the market shifts to PCI Express (which is expected to be the dominant PC bus architecture for the next 10 to 15 years). In laptops, extension cards are called PC Cards (also called PCMCIA cards after the organization that created them, the Personal Computer Memory Card International Association). “PC Card” is the trademarked name assigned by the PCMCIA. These cards, which are about the size of a credit card, plug into an externally accessible slot, and serve the same purpose for laptops as do the other extension cards for PCs.

Sound card A sound card is the circuitry for recording or reproducing multimedia sound. The circuitry can be found in the form of an extension card, a sound codec (Compression/Decompression Module) chip on the motherboard, or hardware integrated into the motherboard’s main chipset. These hardware devices have interfaces for microphones, headphones, amplified speaker output, line-in, CD player input, and so forth. The sound card hardware requires a software counterpart in the form of a driver in order to function.

Video card (PCI, AGP, PCI Express) In its most basic form, the video card is the circuitry or interface for transmitting signals that appear as images on the computer display or monitor. High-end cards can perform video capture as well. The circuitry can be found, as with the sound card, in the form of an extension card, as a dedicated chip on the motherboard, or integrated into the motherboard’s main chipset. Current display adapters use the 15-pin video graphics array (VGA) analog connectors or the Digital Video Interface (DVI) analog/digital connector. Like the sound card, the video card requires a software counterpart in the form of a driver in order to function. Both sound and video have undergone extreme improvements over time. Sound used to be used only for troubleshooting and in the form of beeps. Video used to be monochrome for text-only displays. Both are now capable of combining to deliver rich sound and three-dimensional (3-D) graphics for movies and games.

RTC (Real-Time Clock) RTC is the system clock for storing the system date and time, which is maintained by means of a battery when the system powers down. This battery is often called the CMOS battery, and the chip hosting the RTC is often called the CMOS chip (as the chip material itself is produced using the Complementary Metal-Oxide Semiconductor process). Officially, however, the CMOS chip is called the RTC/NVRAM. The RTC component has already been explained. NVRAM stands for nonvolatile RAM memory, meaning that the data remains when the system powers down and the data can be accessed randomly rather than in linearly. The NVRAM stores the basic configuration data that we have come to call CMOS data, which is the amount of installed memory, type of floppy and hard disk drives, and other startup configuration settings.

CMOS The process by which the RTC/NVRAM chip is produced (Complementary Metal-Oxide Semiconductor). CMOS is often used in lieu of RTC/NVRAM (the official term) and may be used in the context of the “CMOS settings,” which includes the system date/time (RTC) and the basic configuration data.

CMOS battery To maintain critical configuration data when the system is turned off, the RTC/NVRAM chip is powered by a battery. These batteries have a long service life. They are usually mounted on the motherboard and appear as a dime-sized, silver disk. On some systems (Dallas Semiconductor or Benchmarq), the battery is built into the chip itself. The expectation is that they will last ten years, which is usually more than the service life of most systems. Some systems use no battery at all, instead using a capacitor to store a charge to be used when the system is off. Some systems use a combination of battery and capacitor, so that the capacitor can power the chip during battery changes so that the data is never lost.



One of the configuration settings retained by the RTC/NVRAM aka CMOS is the boot or BIOS access passwords. One of the methods for bypassing these passwords is to remove the CMOS battery and allow the chip to lose its settings when the power is removed, reverting to factory defaults.

BIOS BIOS stands for Basic Input Output System, and is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system. They load into RAM from three possible sources: 1) from the motherboard ROM (ROM BIOS), 2) from the adapter card ROM (examples: video card, SCSI card), and 3) from disk in the form of device drivers. The terms BIOS and CMOS (RTC/NVRAM) are often confused and erroneously used interchangeably. They are separate systems, although closely interrelated and interdependent. The user interface for the settings that are stored in RTC/NVRAM memory are accessed through a setup program contained within the BIOS. The settings stored in RTC/NVRAM are read by the BIOS during boot to apply settings for your system configuration.

Two Important Settings in RTC/NVRAM for Examiners

Computer forensic examiners should be concerned with at least two important settings stored in RTC/NVRAM, which is accessed by the BIOS software most often called Setup. Setup is accessed during system boot using a special key or combination of keys, such as F1, F2, Esc, or Delete. Those two settings are:

- System date and time
- Boot order

The first setting is important to help establish a baseline for system time, and the second may have to be changed by the examiner if the drive must be imaged "in place" through the use of a boot floppy disk or CD.

10 Chapter 1 • Computer Hardware

Mouse port This is the interface port in which the mouse is connected to the computer. Older systems use a serial port, and newer systems use a PS2 connection. Although most computers still provide the PS2 port option, the mouse you purchase today will probably ship with the USB interface with a PS2 adapter as the industry moves away from PS2 in favor of USB.

Keyboard port This is the interface port into which the keyboard is connected to the computer. Old systems use a five-pin round port, and newer systems use the PS2 (mini-DIN type) connection. As with the mouse, most systems today ship with PS2 ports, but keyboards ship normally with USB connections with PS2 adapters as the industry moves toward USB.

Network interface card (NIC card) The NIC card is an extension card used to connect the computer to a network. This functionality is now available via USB connection and is built into the motherboard on most workstation-grade motherboards currently manufactured. Ethernet is the most common type of network in use, but Token Ring is still found in some environments. The type of network deployed determines which type of network adapter, Ethernet or Token Ring, will be used. Each NIC has a unique hardware address or serial number coded into its memory. This address is called its MAC (Media Access Control) address. The Data Link Layer protocol uses this address to identify and communicate with other NICs on the same network. This address is 48 bits, or six sets of hexadecimal values, and consists of two parts. The first three hexadecimal values identify the manufacturer. The second set of three hexadecimal values is a unique serial number applied by the manufacturer. Most network cards today are rated at 10/100Mbps; however, Gigabit Ethernet (1,000Mbps) is becoming quite common and will soon be standard. Another type of network is the wireless network, whereby the network packets are sent via radio waves instead of over wires. Wireless NIC cards are typically PCI or USB, or are offered as “on-board” the motherboard. All three types require an antenna to receive the signal.

Modem A modem, which stands for modulate/demodulate, is used to connect a computer to other computers using a telephone as the signal carrier. The modem takes your computer’s digital signals and modulates, or transforms, them to analog signals for transmission over telephone lines. On the receiving end, the modem demodulates, or transforms, the analog signals from the telephone line back to digital signals that the receiving computer can understand.



First Responder Hint: Upon discovering that a target computer is connected to a network (telephone, wired, wireless), one of your first concerns should be the potential for destruction of data via remote connection. Disconnect the network connection or, if it’s wireless, power down the machine immediately. Keep in mind, though, that a decision to “pull the plug” must be weighed against the loss of possible evidence by doing so. Running processes, network connections, and data in volatile RAM will be lost once you pull the plug. If your case depends on this volatile data, you may opt to provide a shield to block wireless transmissions while you capture the volatile data.

Parallel port The parallel port is a relatively large port used primarily for legacy printer connections, although some other devices are known to use this connection. *Parallel* describes a method of transmitting data in which data is sent down parallel electrical paths at the same time. Parallel data transmission suffers limitations at high speeds with timing issues, cable length limitations, and other problems. It is being replaced by serial data transmission methods and technologies.

Serial port The serial port is an I/O port used for connecting devices that use serial data transmission connections. The most common serial port you'll encounter is the RS-232 connection. Most workstations have two serial ports but can support four; however, only two at a time can be used because each pair uses the same hardware resources.

Watch That Terminology!

The realm of computer forensics is still relatively new, and newer still with regard to law enforcement. Our job as computer forensic examiners is not limited to just conducting examinations. We find ourselves having to explain and educate those around us. This includes coworkers, supervisors, attorneys, judges, and, most important of all, the jury.

I have witnessed countless reports, search warrants, and testimonies in which improper terms were used to describe a computer. I have read police reports where officers have requested examinations on CPUs and computer cases. Better yet, I have observed one search warrant signed by a judge allowing the computer forensic examiner to conduct a search of a computer monitor. Apparently, the officer witnessed something of evidentiary value on the screen and wanted it examined!

If as an examiner you are confronted with inaccurate terminologies describing the device to be examined, you do not have the legal authority to actually examine the device just because the request has been approved. In such scenarios, the police reports have to be corrected and the search warrant amended before you perform any examinations.

The Boot Process

At this point, we have discussed a vast array of computer system components and systems. Next we are going to look at the boot process. Computer system components are useless pieces of silicon, copper, gold, and tin until they are awakened by a spark of electricity, which follows a predetermined path, testing the various system components, establishing configuration settings, loading pieces of code—all of which culminates in the loading of a functional operating system, custom-configured to your particular hardware and software environment. The process by which this occurs is the *boot process*, named for the process of “pulling yourself up by the bootstraps.” It is the process by which PC computer systems come to life, and the process that computer forensics examiners must understand and may be called upon to describe.

12 Chapter 1 • Computer Hardware

The boot process begins when the user presses the power switch and starts the system. When this occurs, the following steps take place regardless of the operating system:

1. When you press the power switch, the process initiates the Power On Self-Test (POST). Before the power leaves the power supply, the power supply conducts its own POST, making sure that voltages and current levels are acceptable. The electrical current from the power supply follows a predetermined path to the CPU. Any residual data in the CPU is erased. This signal also resets a CPU register called the program counter. In the case of ATs and later computers, this value is F000. The value describes the address of the next piece of code to be processed. In this case, the address of F000 corresponds to the beginning of a boot program in the ROM BIOS.
2. The boot program (sometimes called “bootstrap”) in the ROM BIOS initiates a series of system checks. The first step in the process is to run a set of instructions or code intended to check the CPU and the POST process, matching it against a set of values stored in the BIOS chipset. The CPU and POST must first be checked before they can be relied on to check the rest of the system. As long as the values match and they “pass,” the POST process continues to the next step.
3. Signals are sent from the CPU to the system bus (main electrical pathway) to ensure that the bus is properly functioning. If this test passes, POST continues to the next step.
4. The CPU next tests the RTC, or system clock. This clock keeps all system electrical signals in synchronization. If the RTC passes its POST check, POST continues to the next step.
5. POST next tests the system’s video components. The video memory is tested, as are the signals sent by this device. The video’s BIOS is added to the overall system BIOS, which is stored in RAM. It is only at this point in the boot process that the user will see anything on the screen.
6. In the next phase of POST, the system’s main memory, RAM, is tested. Data is written to RAM. The data is read and compared to the original data sent. If it matches, it passes; if it doesn’t match, it doesn’t pass. Depending on the system settings, the user may see the “countdown” as the volume of RAM is tested. If all the RAM memory passes this test, POST continues with the next step.
7. The CPU next tests to see if a keyboard is properly attached and if any keys are pressed. If you’ve ever accidentally left a book or papers on a keyboard during boot, you’ll no doubt recall the error beep and screen message from this test! Assuming a successful test, POST continues to the next step.
8. POST next sends signals over specific bus pathways to determine which drives (floppies, CDs, hard drives, etc.) are available to the system.
9. The results of the POST are compared to the expected system configuration settings that are stored in CMOS, which we have learned is properly called RTC/NVRAM. If the settings do not match, the user is given the opportunity to update the configuration through the Setup utility. If it passes, the next step in POST occurs.
10. If any other system component contains its own BIOS, it is loaded into the overall BIOS in RAM at this time. A typical example is a SCSI BIOS. Plug and Play runs next, configuring

any Plug and Play devices, configuring systems resources, and writing those settings to RAM. At this point, the system is ready to load a specific operating system.

- 11. The bootstrap code (boot program) has finished one of its two primary missions, that of conducting the POST. Its final task is that of searching the available drives for an operating system according to the order set forth in the boot sequence. Thus, the ROM BIOS boot code looks to the very first sector of the default boot hard drive (first on the list in the boot sequence) for the master boot record (MBR) and, finding it, reads it into memory and tests it for a valid signature. The “signature” is hex 55AA, located at the last two bytes of this sector. If this doesn’t match, an error message is returned; otherwise the boot process continues. Figure 1.1 shows a hard drive with both an MBR and a VBR while Figure 1.2 shows a floppy disk that has only a VBR.



The MBR pertains to hard disk drives only. If the bootable media is removable media (floppy disk), there is no MBR. Rather, only a volume boot record (VBR) is located at the very first sector. Thus, when the boot is from a floppy, the VBR only is read and executed as there is no MBR on a floppy.

FIGURE 1.1 Hard disk drive with MBR and VBR

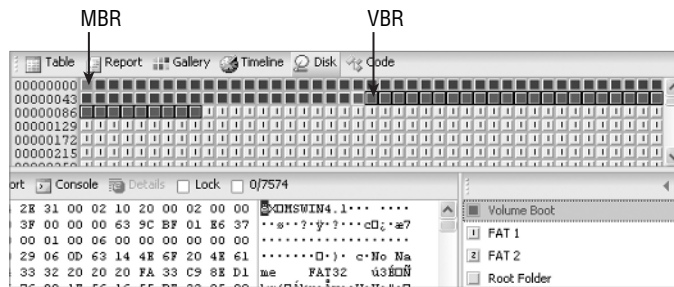
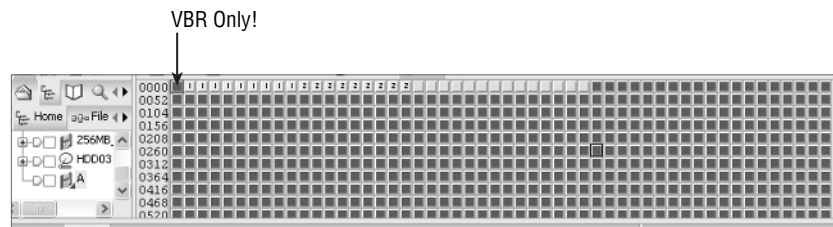


FIGURE 1.2 Floppy disk drive with VBR only



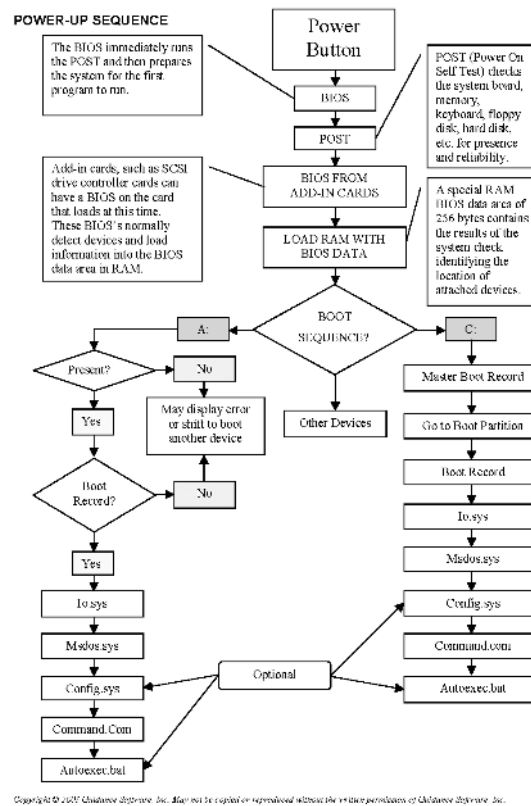
14 Chapter 1 • Computer Hardware

12. The MBR contains a 64-byte partition table located at byte offsets 446 to 509. Each of up to four partitions is described by 16 bytes in the 64-byte table. The MBR reads its own partition table for the “boot indicator byte” that marks one as the active partition. One must be active to boot, and there can’t be more than one marked as active. The absence of the active partition or having more than one marked as active will result in an error message. The MBR reads the VBR of the partition marked as active, loads it into memory, and conducts the same “signature” test carried out with the MBR, looking for the last two bytes of the VBR to read as hex 55AA. If the signature test fails, an error message is returned. If it passes, the VBR code executes or runs. The VBR code or program searches for and runs the operating system on that volume. What happens next in the boot process depends on the operating system that is loaded on that active bootable partition.

Up through Step 12, the boot process is the same whether you’re booting to DOS or to Windows. We will first boot to DOS, which will be described in steps 13 through 17. Next, we will boot to Windows. Steps 13 to 17 will be different for DOS and Windows.

DOS boot:

13. The code in the VBR locates and executes the initial or primary system file, which is IO.SYS (IBMBIO.COM for IBM systems). As part of execution, SYSINIT (a subroutine of IO.SYS) runs. This code copies itself into the highest region of contiguous DOS memory. The code next locates and reads MSDOS.SYS, copying it into low memory and overwriting that portion of IO.SYS in low memory that contains the initialization code (SYSINIT), as it is no longer needed there.
14. SYSINIT runs MSDOS.SYS (or IBMDOS.COM for IBM systems). MSDOS.SYS initializes basic device drivers and checks on the status of system equipment. It also resets the disk system, resets and initializes various devices that are attached to the system, and sets default system parameters. It works with the system BIOS to manage files, execute code, and respond to hardware signals.
15. With the DOS file system running and active, SYSINIT (contained within IO.SYS) resumes control of the boot process. SYSINIT reads the CONFIG.SYS file as many times as there are statements within it to process. The DEVICE statements are processed first in the order in which they appear, followed next by the INSTALL statements in the order of their appearance. Once they are done, if a SHELL statement is present, it is run. If none is present, the default shell with default parameters (COMMAND.COM) is run. SYSINIT is now complete, so COMMAND.COM is written into the section of memory previously occupied by SYSINIT.
16. If the file AUTOEXEC.BAT (.BAT is the extension for batch files) is present, COMMAND.COM will run it. Each command in the batch file is executed. If one of the batch commands calls for launching an application or shell, then the user is presented with that interface or prompt. Otherwise, when the batch commands have been executed, the user sees a blinking cursor at a DOS prompt.
17. If no AUTOEXEC.BAT file is present, COMMAND.COM runs the DATE and TIME commands and displays a copyright message, and then the user is shown a blinking cursor at a DOS Prompt. The entire process appears in Figure 1.3.

FIGURE 1.3 The boot process (DOS)**Windows NT/2000/XP boot:**

13. The code in the VBR locates and runs the primary system file, which in the case of the various flavors of Windows NT is NTLDR (often called “NT Loader”). NTLDR places the processor in the “protected” mode, starts the file system, and reads the contents of the BOOT.INI file. Startup options and initial boot menu options are determined by the contents of the BOOT.INI file. If dual booting is configured, and the other OS is a non-NT type such as Linux, BOOTSEC.DOS runs. If SCSI drives are attached to the system, another file (NTBOOTDD.SYS) containing the SCSI drivers executes.
14. NTDETECT.COM executes and searches the system for installed hardware and passes configuration data to NTLDR. If more than one hardware profile exists, NTDETECT determines the correct profile for the current hardware and runs that profile.

16 Chapter 1 • Computer Hardware

15. The configuration data obtained in the previous step by NTDETECT is passed by NTLDR to NTOSKRNL.EXE. NTOSKRNL.EXE is the code that loads the kernel, the Hardware Abstraction Layer (HAL), and the system registry information.
16. The next step in the NT boot process is that of loading drivers and code for networking systems, typically TCP/IP. Simultaneously, services that are configured to run at startup load and run. One of the services is the logon service that provides the user with a logon prompt, unless configured otherwise. When the user successfully logs on, the current configuration status is considered “good” and is updated into the system registry as “Last Known Good Configuration.”
17. As logon occurs, device detection takes place as a simultaneous process. If new devices are detected, Plug and Play assigns system resources, extracts drivers from the DRIVER.CAB file, and completes configuration and mounting of those devices. If drivers can’t be found, the user is prompted to provide them. When done, the user has a graphical user interface (GUI) that allows them to interact with their system and its unique environment of software and hardware.

Partitions

Partitions and *volumes* are terms that are often used interchangeably. Usually this doesn’t cause a problem because typically they are the same thing. There are, however, some subtle differences, and defining the terms and understanding the differences is an important part of being a professional. A partition is a collection of consecutive sectors within a volume, and those sectors are addressable by a single file system specific to and contained within that partition. A volume, by subtle contrast, is a collection of addressable sectors that are used by an operating system or an application to store data. The addressable sectors in a volume do not have to be consecutive—and therein lies the difference. Rather, they need only give the appearance of being consecutive. When a volume consists of a single partition, they are functionally the same. When a volume spans more than one partition or drive, the difference becomes self-evident.

Volumes are logical storage units that are assigned drive letters by the operating systems. Theoretically, most operating systems can support up to 24 volumes, using the letters C through Z, and reserving A and B for floppy drives. If a single physical hard drive were installed in a system, that drive could, in theory, be partitioned into 24 volumes. Recall, however, from our earlier discussion that the partition table contained in the master boot record only permitted four 16-byte entries for four partitions. How then could such a system support 24 logical volumes?

The answer lies with the extended partition system. One of the four defined partitions in the MBR partition table must be an extended partition. The disk space assigned to the “extended partition” is further subdivided into logical volumes by the operating system. Each subpartition of the extended volume contains a partition table located in the first sector of that subpartition. That table defines its own subpartition and, optionally, points to another partition table in yet another subpartition. This “nesting” of subpartitions within the extended partition can extend as far as letter assignments permit, and each “nested” subpartition will have a partition table

describing itself and pointing to the next level down until done. Seldom will you ever encounter more than few partitions, but in theory, you could encounter the upper limit of 24!

The partition types you can encounter are many and are usually specific to the operating system(s) on the host computer. The fifth byte within each 16-byte partition entry (byte offset 446–509 of the MBR) will determine the partition type/file system for each defined partition. The same holds true for partition tables within the extended partition and their subpartitions. The first byte of each of the four partition table entries determines which partition is “active” and therefore is the “boot” partition. Only one can be active. Hex 80 denotes the active partition. The other three partition entries, if defined, will have hex 00 for the first byte in their respective entries. Table 1.1 defines the partition table fields.

TABLE 1.1 Partition Table Fields Defined*

Offset (Dec)	Name	Length	Description
446	Boot Byte	1 byte	Boot status; hex 80 is active and bootable. Otherwise, it is hex 00.
447	Starting Head	1 byte	For CHS mode, this is the start head or side of the partition.
448	Starting Cylinder & Sector	2 bytes (16 bits)	For CHS mode, the starting cylinder is 10 bits and the starting sector is the next 6 bits, for a total of 16 bits.
450	Partition Type	1 byte	This is the partition type/file system.
451	Ending Head	1 byte	For CHS mode, this is the ending head or side of the partition.
452	Ending Cylinder & Sector	2 bytes (16 bits)	For CHS mode, the ending cylinder is 10 bits and the ending sector is the next 6 bits, for a total of 16 bits.
454	Relative Sector	4 bytes (32 bits or dword)	For LBA mode, this is the number of sectors before the partition, which is the starting sector of the partition.
458	Total Sectors	4 bytes (32 bits or dword)	For LBA mode, this is the total number of sectors in the partition.

* Fields repeat three more times, if partitions defined, starting at offsets 462, 478, and 494.

Typically FAT12, FAT16, FAT32, and NTFS partitions and file systems are used when running the various flavors of the Windows operating systems. These partitions can be created by

18 Chapter 1 • Computer Hardware

utilities that ship with the Windows operating system, such as FDISK, DISKPART, or Disk Manager. Other partition types that are often encountered are Linux Native (EXT2/3 and Reiser) and Swap partitions, Solaris (UFS), and Mac OSX (HFS+), all of which are supported under EnCase Version 5. As with Windows operating systems, partitioning utilities ship with these operating systems. Third-party partitioning utilities are also available that you can use to create partitions of varied types, such as Symantec's PartitionMagic and V-Communications' Partition Commander.

Using Disk Manager (Windows 2000/XP), the formatting is done when you use the Create a New Partition wizard. If a partition is created with FDISK, the partition must be formatted with the high-level format command before it can be used. When you use the format command to format a FAT12/16/32 partition, the following occurs:

1. The disk is scanned for errors and bad sectors are marked.
2. Drive heads are placed at the first cylinder of the partition and a DOS VBR is written.
3. FAT 1 is written to Head 1 Sector 2. Immediately following FAT 1, FAT 2 is written. The entries in the FAT are mostly null, except that bad clusters are marked.
4. A blank root directory is written.
5. If the /s parameter is selected, the system files are transferred.
6. If the /v parameter is selected, the user is prompted for a volume label.

It is during the FDISK or disk partitioning process that the MBR is written, which contains the MBR booting code; the partition table entries are written; and the MBR signature is written. It is during the high-level formatting process (FORMAT) that the VBR is typically written, along with other file system features.

EXERCISE 1.1**Examining the Partition Table**

In this exercise, you will use EnCase to decode the information contained in the partition table.

1. With EnCase open, and a case started, choose Add Device > Local Drives. Select your own boot drive and select the physical device, not the logical device.
2. In the left pane, select your drive. In the right pane, choose the Disk View tab.
3. Go to the very first sector, which should appear in red in EnCase Version 5. Place your cursor on that sector. In the bottom pane, choose the Hex View. Locate and sweep (select by clicking and dragging) bytes 446–509. With these 64 bytes selected, right-click in the selected area and choose Bookmark Data. With the Bookmark dialog box open, under View Types, choose Windows/Partition Entry. The partition table is decoded and displayed.



Often FDISK is used to remove the partition, rendering the drive unreadable and causing the user to believe that the data is gone. All that really occurs is that the partition table entry is removed. As each defined and formatted partition contains a VBR, which is untouched by FDISK, the examiner can use EnCase to recover a deleted partition. Simply locate and select the VBR, right-click, and choose Add Partition from the context menu.

File Systems

We have, thus far, made reference to *file systems* in our discussion of partitions and volumes, but we have not yet defined them or described their function and importance in data storage and retrieval. In this section, we'll discuss file systems in a generic sense. In the chapter that follows, we'll cover specific file systems in detail.

A file system is nothing more than a system or method of storing and retrieving data on a computer system that allows for a hierarchy of directories, subdirectories, and files. File systems must be consistent between systems using the same file system. If a library used the Dewey Decimal System to store books in one library, a user could go to another library using the same file system and locate a book in that library. Even though the book would be stored in different physical locations in both libraries, a common file system would enable the user to find the book using a common filing and locating system. Computer systems are no different in this regard.

A file system needs its own structural or organization files and data, and the other component is the user data. Because a file system is contained within a partition, there must be data or files that describe the layout and size of the file system, as well as how large the data storage units (clusters, blocks, etc.) will be. The data storage units, which are groups of sectors that hold content data, are referred to as allocation units, clusters, blocks, and similar names depending on the file system being used. A file system needs to have a method or convention for naming data and therefore a system of file names. File names are usually contained in directory entries or as an attribute or field in a database of file and directory names. File names have to be linked to actual data comprising that file name so that the operating system can locate the data. Thus, there must be an attribute or *metadata* (data within data describing data) to point to where the data starts. This is done, usually, via a directory entry (FAT systems) or an entry (field or attribute) in a file table such as the master file table (MFT) in NTFS systems.

Because the data may be larger than one allocation unit can hold, there must be a system that tracks the containing data storage units (clusters, blocks, etc.). In a FAT system, these clusters are linked together in the FAT table (file allocation table). In NTFS, the clusters containing the data are described by data runs in the MFT. The operating system must know the size of the data so it knows where the data ends in an allocation unit, and that data is typically stored in a directory entry or as an attribute or field in a database of file names, such as the MFT.

Finally, any file system must have a system that tracks allocation unit usage and availability. Without this function, data could be overwritten. In a FAT system, this is accomplished with the

FAT table. In NTFS and other systems, this is accomplished by the single-purpose volume bit map (VBM), which is an array of bits, with each representing an allocation unit. A 0 means it is available for use, and a 1 means it is allocated.

At a minimum, a file system needs to have the functions described thus far. Most file systems contain much more information about the files it stores and has metadata in the form of file attributes about the data. This information may take the form of dates and times for last written, file creation, and last modified. It may also take the form of file permissions or access control lists (ACLs).

In summary, when a partition is created, its boundaries and type are set forth in a partition table. The “type” is something akin to a zoning ordinance where a given piece of real estate is “supposed” to be used for a specific purpose. A piece of real estate could be zoned as “residential” while a partition type could, similarly, be declared as having a type of “Linux Swap.” A real estate parcel is described in a deed by its meets and bounds as determined by a survey. A partition’s “meets and bounds” are described, similarly, in a partition table by its starting point, ending point, and size, based on a survey conducted by the partitioning utility.

When a partition is formatted, among other things, the data structures needed for its specific file system are created. While these file system type structures are usually consistent with the file system type declared in the partition table, they do not have to be. One could have a FAT32 file system located in a partition type declared as a Linux Swap. This would be somewhat analogous to someone placing a business on real estate zoned for residential use. If you were using Linux for the operating system, Linux does not rely on the partition type; if instructed to mount the partition as FAT32, it would do so since the structure for FAT32 is present regardless of the declared type. Linux ignores the “zoning laws.” Windows, however, strictly obeys “zoning laws” and would not permit an office in a residential zone. Windows relies on declared partition types for mounting partitions and file systems and would not mount a FAT32 partition declared as a Linux Swap partition or any other type not a FAT32. In this manner, partitions and file systems can be hidden from Windows.

File systems are the management tools for storing and retrieving data in a partition. Some operating systems require certain file systems for them to function. Windows needs a FAT or NTFS file system, depending on its “flavor,” or version, and won’t recognize or mount other systems with its own native operating system. Third-party software can enable mounting and reading (sometimes writing) other file systems from within the Windows environment. EnCase and VMWare are two examples. Many different file system schemes have been developed, and more will be forthcoming as computing evolves. In the next chapter, we examine the FAT file system in detail.

Summary

This chapter explained the computer’s components, its boot process, partitions, and file systems. We covered computer hardware components, including their acronyms, attributes, functions, and purpose. In addition, we examined the two major components of the boot process.

The first is the POST (Power On Self-Test), in which the major components are tested and initialized (added to the system). The second consists of the bootstrap code locating a bootable drive and loading the specified operating system.

We also defined and described partitions and volumes. A partition is a collection of consecutive sectors within a volume and is a container for a file system, with specific boundaries and properties. A volume is a collection of addressable sectors that are used by an operating system or an application to store data. A volume is assigned a drive letter by the OS; it may be limited to a single partition, or it may span partitions or physical hard drives. Finally, we discussed file systems and their purpose, function, and necessary generic components.

Exam Essentials

Know computer hardware components. Understand the proper terminology, acronyms, purpose, and function of the various computer hardware components.

Be familiar with the boot process. Understand and be able to describe the POST process. Understand and be able to describe the process by which the system boots and loads an operating system.

Understand partitions and volumes. Understand and be able to describe partitions and volumes, what the differences are, and how they are created. Understand the MBR and VBR, where they are found, their contents (boot code, partition table, signature), and how and when they are created. Understand a partition table, where it is located, its structure, length, and general properties.

Understand file systems in general. Understand the purpose of a file system as a means to store and retrieve data. Be familiar with the functional components of any generic file system so as to be able to apply them to specific file systems.

Review Questions

1. What is the definition of a CPU?
 - A. The physical computer case that contains all its internal components
 - B. The computer's internal hard drive
 - C. A part of the computer whose function is to perform data processing
 - D. A part of the computer that stores and manages memory
2. What is the BIOS?
 - A. BIOS stands for Basic Input Output System, and is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system.
 - B. BIOS stands for Bootstrap Initialization Operating System, and is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system.
 - C. BIOS stands for Boot-level Input Output System and is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system.
 - D. BIOS stands for Boot Initialization Operating System and is a combination of low-level software and drivers that function as the interface, intermediary, or layer between a computer's hardware and its operating system.
3. What is the definition of POST?
 - A. A set of computer sequences the operating system executes upon a proper shutdown
 - B. A diagnostic test of the computer's hardware and software for presence and operability during the boot sequence prior to running the operating system
 - C. A diagnostic test of the computer's software for presence and operability during the boot sequence prior to running the operating system
 - D. A diagnostic test of the computer's hardware for presence and operability during the boot sequence prior to running the operating system
4. Is the information stored on a computer's ROM chip lost during a proper shutdown?
 - A. Yes
 - B. No
5. Is the information contained on a computer's RAM chip accessible after a proper shutdown?
 - A. Yes
 - B. No
6. Can information stored in the BIOS ever change?
 - A. Yes
 - B. No

7. What is the purpose or function of a computer's ROM chip?
 - A. Long-term or permanent storage of information and instructions
 - B. Temporary storage area to run applications
 - C. Permanent storage area for programs and files
 - D. A portable storage device
8. Information contained in RAM memory (system's main memory), which is located on the motherboard, is _____.
 - A. Volatile
 - B. Nonvolatile
9. What is the maximum number of drive letters assigned to hard drive(s) partitions on a system?
 - A. Four
 - B. Sixteen
 - C. Twenty-four
 - D. Infinity
10. The smallest area on a drive that data can be written to is a _____ while the smallest area on a drive that a file can be written to is a _____.
 - A. Bit and byte
 - B. Sector and cluster
 - C. Volume and drive
 - D. Memory and disk
11. The size of a physical hard drive can be determined by which of the following?
 - A. Multiplying the cylinder x head x sector
 - B. Multiplying the cylinder x head x sector x 512 bytes
 - C. Multiplying the total LBA sectors times 512 bytes
 - D. Adding the total size of partitions
 - E. Both B and C
12. Which is not considered an output device?
 - A. Monitor
 - B. Printer
 - C. CD-RW drive
 - D. Speaker

24 Chapter 1 • Computer Hardware

- 13.** The electrical pathway used to transport data from one computer component to another is called?
- A.** Bus
 - B.** RAM
 - C.** CMOS
 - D.** BIOS
- 14.** What is the main component of a computer that essential internal devices such as CPU, memory chips, and other chipsets are attached to?
- A.** BIOS
 - B.** Motherboard
 - C.** Expansion card
 - D.** Processor
- 15.** IDE, SCSI, and SATA are different types of interfaces describing what device?
- A.** RAM chips
 - B.** Flash memory
 - C.** CPUs
 - D.** Hard drives
- 16.** What do the terms *Master*, *Slave*, and *Cable Select* refer to?
- A.** External SCSI devices
 - B.** Cable types for external hardware
 - C.** Jumper settings for internal hardware such as IDE hard drives and CD drives
 - D.** Jumper settings for internal expansion cards
- 17.** What can you assume about a hard drive that is pinned as CS?
- A.** It's an IDE drive.
 - B.** It's a SATA drive.
 - C.** It's a SCSI drive.
 - D.** All of the above.
- 18.** What is found at Cylinder 0, Head 0, Sector 1 on a hard drive?
- A.** Master boot record
 - B.** Master file table
 - C.** Volume boot record
 - D.** Volume boot sector

19. What is the first sector on a volume called?
- A. File allocation table
 - B. Volume boot record or sector
 - C. Master boot record
 - D. Volume boot device
20. Which of the following is incorrect?
- A. The MBR is typically written when the drive is partitioned with FDISK or DISKPART.
 - B. A file system is a system or method of storing and retrieving data on a computer system that allows for a hierarchy of directories, subdirectories, and files.
 - C. The VBR is typically written when the drive is high-level formatted with a utility such as FORMAT.
 - D. The partition table is contained within the MBR and consists of a total of 16 bytes, which describes up to four partitions using 4 bytes each to do so.

Answers to Review Questions

1. C. A CPU is the central processing unit, a microprocessor that performs data processing, or interprets and executes instructions.
2. A. BIOS stands for Basic Input Output System and consists of all the low-level software that is the interface between the system hardware and its operating system. It loads, typically, from three sources: the ROM/BIOS on the motherboard; the various BIOS ROMs on video cards, SCSI cards, and so forth; and finally, device drivers.
3. D. POST (Power On Self-Test) is a diagnostic test of the computer's hardware, such as the motherboard, memory, CD-ROM drive, and so forth. POST does not test the computer's software.
4. B. Information contained on a ROM chip, read-only memory, is not lost after the computer has been shut down.
5. B. Unlike a ROM chip, information contained on a computer's RAM chip is not readily accessible after a proper shutdown.
6. A. Although not very common, information stored in the BIOS can change, such as when the BIOS needs to be upgraded to support new hardware.
7. A. ROM (read-only memory) contains information about the computer, such as hardware configuration. Unlike RAM, the information is not lost once power is disconnected.
8. A. Information contained in RAM memory is considered volatile, which means that the data is lost after the computer has been disconnected.
9. C. The answer is 24 drive letters (C–Z), with drive letters A and B reserved for floppy drives.
10. B. Data is written to sectors, and files are written to clusters.
11. E. Multiplying C/H/S gives the total amount of sectors in older systems if the number of sectors per track is constant. When it's not, total LBA sectors give total sectors. Multiplying the total number of sectors from the appropriate method times 512 bytes per sector gives the total number of bytes for the physical drive. Adding up the total size of partitions does not include areas outside the partitions, such as Unused Disk Area.
12. C. A CD-RW (rewritable) drive is both an input and output device, as opposed to a CD drive, which only reads and inputs data to the computer system.
13. A. A Bus performs two functions: it transports data from one place to another and directs the information where to go.
14. B. The motherboard is the main circuit board used to attach internal hardware devices to its connectors.
15. D. IDE (Integrated Drive Electronics), SCSI (Small Computer System Interface), and SATA (Serial ATA, or Serial Advanced Technology Attachment) describe different hard drive interfaces.

16. C. Master, Slave, and Cable Select are settings for internal devices such as IDE hard drives and CD drives to identify and differentiate the devices on the same channel.
17. A. SATA and SCSI hard drives are not configurable as Master, Slave, or Cable Select. Only IDE drives are configured as Master, Slave, or Cable Select. Thus, any jumper setting denoting “CS” would apply only to an IDE drive.
18. A. The master boot record is always located at the first physical sector on a hard drive. This record stores key information about the drive itself, such as the master partition table and master boot code.
19. B. The first sector on a volume is called the volume boot record, or volume boot sector. This sector contains the disk parameter block and volume boot code.
20. D. All are true statements, except for a portion of D. The partition table is contained within the MBR and consists of a total of 64 bytes, not 16 bytes, which describes up to four partitions using 16 bytes each to do so, not 4 bytes each.

