

# Glossary

**Access token:** In Windows NT, an internal security card that is generated when users log on. It contains the security IDs (SIDs) for the user and all the groups to which the user belongs. A copy of the access token is assigned to every process launched by the user.

**BIOS:** Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

**Buffer:** An area of memory, often referred to as a “cache,” used to speed up access to devices. It is used for temporary storage of data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer, or tape drive.

**Click!™:** A portable disk drive, also known as a PocketZip disk. The external drive connects to the computer via the USB port or a PC card, the latter containing a removable cartridge slot within the card itself.

**CD-R:** Compact disk-recordable. A disk to which data can be written but not erased.

**CD-RW:** Compact disk-rewritable. A disk to which data can be written and erased.

**Compressed file:** A file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

**Cookies:** Small text files stored on a computer while the user is browsing the Internet. These little pieces of data store information such as e-mail identification, passwords, and history of pages the user has visited.

**CPU:** Central processing unit. The computational and control unit of a computer. Located inside a computer, it is the “brain” that performs all arithmetic, logic, and control functions in a computer.

**Deleted files:** If a subject knows there are incriminating files on the computer, he or she may delete them in an effort to eliminate the evidence. Many computer users think that this actually eliminates the information. However, depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data.

**Digital evidence:** Information stored or transmitted in binary form that may be relied upon in court.

**Docking station:** A device to which a laptop or notebook computer can be attached for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors, and printers.

**Documentation:** Written notes, audio/videotapes, printed forms, sketches, and/or photographs that form a detailed record of the scene, evidence recovered, and actions taken during the search of the scene.

**Dongle:** Also called a hardware key, a dongle is a copy protection device supplied with software that plugs into a computer port, often the parallel port on a PC. The software sends a code to that port and the key responds by reading out its serial number, which verifies its presence to the program. The key hinders software duplication because each copy of the program is tied to a unique number, which is difficult to obtain, and the key has to be programmed with that number.

**DSL:** Digital subscriber line. Protocols designed to allow high-speed data communication over the existing telephone lines between end-users and telephone companies.

**Duplicate digital evidence:** A duplicate is an accurate digital reproduction of all data objects contained on the original physical item.

**DVD:** Digital versatile disk. Similar in appearance to a compact disk, but can store larger amounts of data.

**Electromagnetic fields:** The field of force associated with electric charge in motion having both electric and magnetic components and containing a definite amount of electromagnetic energy. Examples of devices that produce electromagnetic fields include speakers and radio transmitters frequently found in the trunk of the patrol car.

**Electronic device:** A device that operates on principles governing the behavior of electrons. See chapter 1 for examples, which include computer systems, scanners, printers, etc.

**Electronic evidence:** Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device.

**Encryption:** Any procedure used in cryptography to convert plain text into ciphertext in order to prevent anyone but the intended recipient from reading that data.

**First responder:** The initial responding law enforcement officer and/or other public safety official arriving at the scene.

**Hidden data:** Many computer systems include an option to protect information from the casual user by hiding it. A cursory examination may not display hidden files, directories, or partitions to the untrained viewer. A forensic examination will document the presence of this type of information.

**ISDN:** Integrated services digital network. A high-speed digital telephone line for high-speed network communications.

**ISP:** Internet service provider. An organization that provides access to the Internet. Small Internet service providers provide service via modem and ISDN, while the larger ones also offer private line hookups (e.g., T1, fractional T1).

**Jaz®:** A high-capacity removable hard disk system.

**Latent:** Present, although not visible, but capable of becoming visible.

**LS-120:** Laser Servo-120 is a floppy disk technology that holds 120MB. LS-120 drives use a dual-gap head, which reads and

writes 120MB disks as well as standard 3.5-inch 1.44MB and 720KB floppies.

**Magnetic media:** A disk, tape, cartridge, diskette, or cassette that is used to store data magnetically.

**Misnamed files and files with altered extensions:** One simple way to disguise a file's contents is to change the file's name to something innocuous. For example, if an investigator was looking for spreadsheets by searching for a particular file extension, such as ".XLS," a file whose extension had been changed by the user to ".DOC" would not appear as a result of the search. Forensic examiners use special techniques to determine if this has occurred, which the casual user would not normally be aware of.

**Modem:** A device used by computers to communicate over telephone lines. It is recognized by connection to a phone line.

**Network:** A group of computers connected to one another to share information and resources.

**Networked system:** A computer connected to a network.

**ORB:** A high-capacity removable hard disk system. ORB drives use magnetoresistive (MR) read/write head technology.

**Original electronic evidence:** Physical items and those data objects that are associated with those items at the time of seizure.

**Password-protected files:** Many software programs include the ability to protect a file using a password. One type of password protection is sometimes called "access denial." If this feature is used, the data will be present on the disk in the normal manner, but the software program will not open or display the file without the user entering the password. In many cases, forensic examiners are able to bypass this feature.

**Peripheral devices:** An auxiliary device such as a printer, modem, or data storage system that works in conjunction with a computer.

**Phreaking:** Telephone hacking.

**Port:** An interface by which a computer communicates with another device or system. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

**Port replicator:** A device containing common PC ports such as serial, parallel, and network ports that plugs into a notebook computer. A port replicator is similar to a docking station but docking stations normally provide capability for additional expansion boards.

**Printer spool files:** Print jobs that are not printed directly are stored in spool files on disk.

**Removable media:** Items (e.g., floppy disks, CDs, DVDs, cartridges, tape) that store data and can be easily removed.

**Screen saver:** A utility program that prevents a monitor from being etched by an unchanging image. It also can provide access control.

**Seizure disk:** A specially prepared floppy disk designed to protect the computer system from accidental alteration of data.

**Server:** A computer that provides some service for other computers connected to it via a network.

**Sleep mode:** Power conservation status that suspends the hard drive and monitor resulting in a blank screen to conserve energy, sometimes referred to as suspend mode.

**Stand-alone computer:** A computer not connected to a network or other computer.

**Steganography:** The art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

**System administrator:** The individual who has legitimate supervisory rights over a computer system. The administrator maintains the highest access to the system. Also can be known as sysop, sysadmin, and system operator.

**Temporary and swap files:** Many computers use operating systems and applications that store data temporarily on the hard drive. These files, which are generally hidden and inaccessible, may contain information that the investigator finds useful.

**USB:** Universal Serial Bus. A hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

**Volatile memory:** Memory that loses its content when power is turned off or lost.

**Zip®:** A 3.5-inch removable disk drive. The drive is bundled with software that can catalog disks and lock the files for security.