NIJ

APR. 08

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

Glossary

NCJ 219941

Glossary

Analog: Also spelled analogue. A device or system that represents changing values as continuously variable physical quantities. A typical analog device is a clock on which the hands move continuously around the face. Such a clock is capable of indicating every possible time of day. In contrast, a digital clock is capable of representing only a finite number of times (every 10th of a second, for example).

Bandwidth: The amount of information or data that can be sent over a network connection in a given period of time. Bandwidth is usually stated in bits per second (bps), kilobits per second (kbps), or megabits per second (mps).

Bit-by-bit duplicate copy: The process of copying data stored on digital media so that it replicates the data at the lowest level. The term "bit copy" refers to the duplication of the zeros and ones (bits) that are the binary form of digital data.

BIOS: Basic Input Output System. The set of routines stored in read-only memory on a system circuit board that starts a computer, then transfers control to the operating system. The BIOS opens communication channels with computer components such as the hard disk drives, keyboard, monitor, printer, and communication ports.

Blackberry: A handheld device that functions as a cellular phone, personal organizer, wireless Internet browser, speakerphone, long-range digital walkie-talkie, and mini-laptop. Can be used to send and receive e-mail and text messages.

Blog: Derived from Weblog. A series of online journal entries posted to a single Web page in reverse-chronological order. Blogs generally represent the personality of the author or reflect the purpose of the Web site that hosts the blog.

BMP: A filename extension for Bitmap, an image file format generally used to store digital images or pictures.

Buffer: A block of memory that holds data temporarily and allows data to be read or written in larger chunks to improve a computer's performance. The buffer 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.

Cables: A collection of wires or optical fibers bound together, used as a conduit for components and devices to communicate or transfer data.

CAT-5/Category-5: A cable capable of transmitting data at high speeds (100 megabits per second and faster). CAT-5 cables are commonly used for voice and data applications in the home.

CAT-5e: Enhanced CAT-5. Similar to a CAT-5 cable, but with improved specifications.

CAT-6/Category-6 (ANSI/TIA/EIA-568-B.2-1): A cable standard for Gigabit Ethernet and other interconnect that is backward compatible with CAT-5, CAT-5e and Cat-3 cables. A Cat-6 cable features more stringent specifications for crosstalk and system noise. The cable standard is suitable for 10BASE–T, 100BASE–TX, and 1000BASE–T (Gigabit Ethernet) connections.

CD/CD-ROM: Compact Disc—Read-Only Memory. A compact disc that contains data accessible by a computer.

CD-R: Compact Disc—Recordable. A disc to which data can be written but not changed or erased.

CD-RW: Compact Disc—Rewritable. A disc to which data can be written, rewritten, changed, and erased.

Chat Room: An Internet client that allows users to communicate in real time using typed text, symbols, or audio.

Compact Flash Card: A small, removable mass storage device that relies on flash memory technology—a storage technology that does not require a battery to retain data indefinitely. There are two types of compact flash cards: Type I cards are 3.3mm thick; Type II cards are 5.5mm thick.

Compressed File: A file that has been reduced in size by use of an algorithm that removes or combines redundant data for ease of transfer. A compressed file is generally unreadable to most programs until the file is uncompressed.

Cookies: Small text files on a computer that store information about what information a user accessed while browsing the Internet.

CPU: Central Processing Unit. The computer microprocessing chip that contains several thousand to several million transistors that perform multiple functions simultaneously.

Deleted Files: Files no longer associated with a file allocation table or master file table. Deleted files are still resident on the media but are not accessible by the operating system.

DHCP: Dynamic Host Configuration Protocol. A set of rules used by communications devices such as computers, routers, or network adapters to allow the device to request and obtain an IP address from a server that has a list of addresses available for assignment.

Digital (photographs, video, audio): A digital system uses discrete values rather than the continuous spectrum values of analog. The word "digital" can refer to the type of data storage and transfer, the internal working of a device, or the type of display.

Digital Camera: A still camera that records images in digital format. Unlike traditional analog cameras that record infinitely variable intensities of light, digital cameras record discrete numbers for storage on a flash memory card or optical disk.

Digital Evidence: Information stored or transmitted in binary form that may be introduced and relied on in court.

DivX: A brand name of products created by DivX, Inc., including the DivX Codec, which has become popular due to its ability to compress lengthy video segments into small sizes while maintaining relatively high visual quality. It is one of several codecs, or digital data encoding and decoding programs, commonly associated with ripping, where audio and video multimedia are transferred to a hard disk and transcoded. As a result, DivX has been a center of controversy because of its use in the replication and distribution of copyrighted DVDs.

Docking Station: A device that enables laptop and notebook computers to use peripheral devices and components normally associated with a desktop computer such as scanners, keyboards, monitors, and printers.

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

Dongle: A copy protection or security device supplied with software. The dongle hinders unauthorized use or duplication of software because each copy of the program requires a dongle to function.

DSL: Digital Subscriber Line. A high-speed digital modem technology that allows high-speed data communication over existing telephone lines between end users and telephone companies.

DVD: Digital Versatile Disk. A high-capacity compact disk that can store up to 28 times the amount of data that a standard CD-ROM can hold. DVDs are available in DVD-R, DVD-RW, DVD+R, DVD+RW, and BlueRay formats.

Electromagnetic Field: The field of force associated with electric charge in motion that has both electric and magnetic components and contains a definite amount of electromagnetic energy. Speakers and radio transmitters frequently

found in the trunks of patrol cars are examples of devices that produce electromagnetic fields.

Electronic Device: A device that operates on principles governing the behavior of electrons. Examples of electronic devices include computer systems, scanners, and printers.

Electronic Evidence: Information or data of investigative value that is stored on or transmitted by an electronic device.

Electronic Storage Device: Any medium that can be used to record information electronically. Examples include hard disks, magnetic tapes, compact discs, videotapes, and audiotapes. Examples of removable storage devices include thumb drives, smart media, flash cards, floppy disks, and Zip® disks.

Encryption: Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient with the corresponding key from reading that data.

EPROM: Erasable programmable read-only memory. A type of computer memory chip that retains its data when its power supply is switched off. Once programmed, an EPROM can be erased only by exposing it to strong ultraviolet light.

Ethernet: The standard local area network (LAN) access method that connects electronic devices to a network, cable modem, or DSL modem for Internet access.

Exculpatory Evidence: Evidence that shows that a criminal charge is not substantiated by the evidence.

Faraday: A dimensionless unit of electric charge quantity, equal to approximately 6.02×10^{23} electric charge carriers. This is equivalent to one mole, also known as Avogadro's constant. Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals.

File Format: Refers to file type based on file structure, layout, or how a particular file handles the information (sounds, words, images) contained within it. A file's format is usually indicated by the three- or four-letter file extension in the MS-DOS filename, e.g., .doc or .jpg.

Firewall: A firewall allows or blocks traffic into and out of a private network or a user's computer, and is the primary method for keeping a computer secure from intruders. Also used to separate a company's public Web server from its internal network and to keep internal network segments secure.

FireWire: A high-speed serial bus that allows for the connection of up to 63 devices. Widely used for downloading video from digital camcorders to the computer.

First Responder: The initial responding law enforcement officer or other public safety official to arrive at a scene.

GPS: Global Positioning System. A system of satellites and receiving devices used to compute positions on Earth. GPS is used in navigation and real estate assessment surveying.

GIF: Graphics Interchange Format. One of the two most common file formats for graphic images; the other is the jpg. Widely used on the Internet due to its high compression and subsequent small file size. GIF files have a .gif file extension and can be created or edited in most popular graphics applications.

Hard Copy: A permanent reproduction of data on any media suitable for direct use by a person, e.g., printed pages and facsimile pages.

Hard Drive: A data storage device that consists of an external circuit board; external data and power connections; and internal glass, ceramic, or magnetically charged metal platters that store data. The most common types of hard drives are IDE and SCSI.

Hardware: The physical components that make up a computer system such as the keyboard, monitor, and mouse.

Header: In many disciplines of computer science, a header is a unit of information that precedes a data object. In a network transmission, a header is part of the data packet and contains transparent information about the file or the transmission. In file management, a header is a region at the beginning of each file where bookkeeping information is kept. The file header may contain the date the file was created, the date it was last updated, and the file's size. The header can be accessed only by the operating system or by specialized programs.

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

Host: A computer on a network that provides resources or services to other computers on the same network. One host machine may provide several services, such as SMTP (e-mail) and HTTP (Web).

IM: Instant Messenger. A type of communications service that enables users to communicate in real time over the Internet. Analogous to a telephone conversation but communication is text-based.

Internet Protocol (IP) Address: A 32-bit binary number that uniquely identifies a host connected to the Internet or to other Internet hosts for communication through the transfer of data packets. An IP address is expressed in "dotted quad" format consisting of decimal values of its four bytes separated with periods, e.g.,127.0.0.1.

IRC: Internet Relay Chat. A multiuser Internet chat client through which users communicate on channels referred to as chat rooms.

ISDN: Integrated Services Digital Network. A high-speed digital telephone line Internet connection.

ISP: Internet Service Provider. A business that provides access to the Internet. Small Internet service providers provide service via modem and ISDN, while larger ones also offer private line hookups.

JPG: Joint Photographic Experts Group. Also JPEG. A compression technique used for saving images and photographs. Reduces the file size of the images without reducing their quality; widely used on the World Wide Web.

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

MAC Address: Also known as the hardware address or ethernet address. A unique identifier specific to the network card inside a computer. Allows the DHCP server to confirm that the computer is allowed to access the network. MAC addresses are written as XX–XX–XX–XX–XX–XX, where the Xs represent digits or letters from A to F.

Magnetic Media: Includes hard disk drives, tapes, cartridges, diskettes, or cassettes used to store data magnetically.

Media Storage Devices: Examples include disk drives, tape drives, Zip® drives, thumb drives, floppy disks, CDs, and DVDs. Unlike main memory, media storage devices retain data even when the computer is turned off.

Memory Card: A removable data storage device commonly used for storing images in digital cameras but can also be used to store any type of data. These devices are made up of nonvolatile flash memory chips in various forms such as CompactFlash, SmartMedia, and Memory Stick.

MiniDV: A videocassette designed for use in MiniDV digital camcorders. MiniDV cassettes can have up to 530 lines of video resolution.

MP3: An acronym for MPEG-1 or MPEG-2 audio layer 3. MP3 is the file extension for MPEG audio layer 3. Layer 3 is one of three coding schemes for the compression of audio signals. Layer 3 uses perceptual audio coding and psychoacoustic compression to remove the redundant and irrelevant parts of a sound signal.

MPEG: Moving Picture Experts Group. A standard for compressing full motion video. MPEG files frequently have an .mpg file extension.

Multimedia Player: A hard disk or flash memory-based electronic device, such as an MP3 player, capable of storing and playing files in one or more media formats including: MPEG, DivX, and Xvid, audio, MP3, WAV, Ogg Vorbis, BMP, JPEG, GIF, images, and interactive media Adobe Flash and Flash LITE.

Network: A configuration of independent computers, peripherals, and devices connected through data communication wires or wireless technologies capable of sharing information and resources.

Network Connection: A wired or wireless communication link between a group of computers or devices for the purpose of sharing information and resources.

Ogg Vorbis: An open-source audio encoding and streaming technology.

Operating System: A computer program that controls the components of a computer system and facilitates the operation of applications. Microsoft® Windows® Me, Microsoft® Windows® XP, Vista®, Linux, and Apple® MacOS are common operating systems.

Original Electronic Evidence: Physical devices and the data contained by those items at the time of seizure.

Palm: Any of the various models of personal digital assistants marketed by Palm, Inc.

Password-Protected File: A file configured to deny access to users who do not enter the correct password (a specific character or combination of characters). Access denial security does not modify the content of the file; it only prevents those without the password from accessing it.

PCMCIA: Personal Computer Memory Card International Association. A trade association responsible for promulgating standards for integrated circuit cards, including PC cards and Express Cards.

PCMIA: Personal Computer Manufacturer Interface Adaptor. Used to expand the function of personal computers.

PDA: Personal Digital Assistant. A handheld device that can function as a cellular phone, fax sender, and personal organizer. Many PDAs incorporate handwriting and voice recognition features. Also referred to as a palmtop, handheld computer, or pocket computer.

Peripheral: Any device used in a computer system that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external such as a mouse, keyboard, printer, monitor, external Zip® drive or scanner; or internal such as a CD-ROM drive, CD-R drive, or internal modem.

Personal Computer (PC): A computer whose price, size, and capabilities make it useful for individuals.

Phishing: Internet fraud perpetrated through an e-mail linking to a Web site simulating a legitimate financial organization; once on the fake Web site, victims are tricked into revealing a security access code, credit card or Social Security number, user ID, or password, which is then used by the thieves to steal the victim's financial resources.

Phreaking: Telephone system hacking.

Printer Cable: A cable that connects a printer to a computer.

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 that contains common computer ports (e.g., serial, parallel, and network ports) that plug 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 File: The temporary file created when a print command is executed.

Processor: The logic circuitry that responds to and processes the basic instructions that drive a computer. The term processor has generally replaced the term central processing unit (CPU). The processor in a personal computer or that is embedded in small devices is often called a microprocessor.

PS2: PlayStation 2. A popular video game console.

PSP: PlayStation Portable. A handheld videogame console released in 2005 by Sony. Uses a Universal Media Disc and Memory Stick PRO Duo card for storage. The PSP also plays music and displays photos.

Quarantine: The status of any item or material isolated while pending a decision on its use.

RAM: Random Access Memory. Computer memory that stores data and can be accessed by the processor without accessing the preceding bytes, enabling random access to the data in memory.

Remote: Files, devices, and other resources that are not connected directly to a computer.

Removable Media: Items that store data and can be easily removed from a computer system or device such as floppy disks, CDs, DVDs, cartridges, and data backup tape.

Screen Name: The name a user chooses to use when communicating with others online. A screen name can be a person's real name, a variation of the person's real name, or it can be a pseudonym (handle). Screen names are required for instant messaging (IM) applications.

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 configured to boot a computer system and protect it from accidental or unintentional alteration of data.

Serial Cable: Provided with a digital camera. Used to connect a digital camera to a personal computer so that images can be downloaded on to the computer hard disk.

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

SIM: Subscriber Identity Module. The SIM card is the smart card inserted into GSM cellular phones. The SIM identifies the user account to the network, handles authentication, and provides data storage for basic user data and network information. It may also contain some applications that run on a compatible phone.

Sleep Mode: Also Suspend Mode. A power conservation state that suspends power to the hard drive and monitor; results in a blank screen.

Smart Card: Also chip card, or integrated circuit card. A pocket-sized card with embedded integrated circuits which can process information. There are two broad categories of smart cards. Memory cards contain only nonvolatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components.

Software: Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Web site development, file management, or inventory management.

Stand-Alone Computer: A computer not connected to a network or other computer.

Steganography: The process of hiding files within other files.

System Administrator: A user who has the most comprehensive access privileges over a computer system.

Temporary and Swap Files: To improve computer performance, many computer operating systems and applications temporarily store data from system memory or RAM in files on the hard drive. These files, which are generally hidden and inaccessible, may contain information useful to the investigator.

Thumbnail: A miniature representation of a page or an image used to identify a file by its contents. Clicking the thumbnail opens the file. Thumbnails are an option in file managers, such as Windows Explorer, and they are found in photo editing and graphics program to quickly browse multiple images in a folder.

Touch Screen: A video display screen that has a touch-sensitive transparent panel covering the screen. A user can touch the screen to activate computer functions instead of using a pointing device such as a mouse or light pen.

USB: Universal Serial Bus. A computer hardware interface connection that facilitates the use of many peripheral devices including keyboards, mice, joysticks, scanners, printers, external storage devices, mobile phones, smart phones, PDAs, and software dongles.

Virus: A software program capable of spreading and reproducing itself on connected computers and damaging or corrupting legitimate computer files or applications.

VoIP: Voice over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet protocol. Data network may be the Internet or a corporate Intranet.

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

WAV: An abbreviation of WAVeform. A type of audio file. Usually has a .wav file extension.

Wireless: Any computing device that can access a network without a wired connection.

Wireless Modem: A modem that accesses a wireless telephone system to provide a connection to a network.

Wireless Router: A network device that consists of a wireless access point (base station), a wired LAN switch, and a router to connect computers and peripheral devices to an Internet service. Wireless routers are a convenient way to connect a small number of wired and any number of wireless computers to the Internet.

Write Protection: Software or hardware that prevents data from being written to a storage device. Write protection ensures that digital evidence is not modified after it is seized.

Xvid: An open-source video codec library (video compression software) that follows the MPEG–4 standard.

Zip®: A removable 3.5-inch data storage disk drive.

Zip® File: A file that has been reduced in size to allow faster transfer between computers or to save storage space. Some compressed files have a .exe file extension, which indicates that the file is self-extracting.