Active Files. Files residing on disk drives of PCs, LAN file servers, laptops, etc. Include backup files created by application software such as Microsoft Word.

Address: The term address can be used to mean:

- An Internet address - a unique location on the Internet.
- An e-mail address or
- A web page address (also known as a URL)

Application Software. Software that performs more visible operations such as word processing creating spreadsheets and database management systems

Archival Files. Aged data no longer in use; based on date of last access, removed and stored separately on various kinds of media (including tapes, floppy or hard disks, zip drives, optical disks, etc), freeing space on the active drive.

Backup Files. Files copied to diskettes, portable disk drives, backup tapes and compact disks, providing the user with access to data in case of emergency. Some backup files are created automatically by certain applications or operating systems, are not readily apparent to the user and are maintained (as hidden files) on computers' disk drives

Best Evidence Rule. The Best Evidence Rule states that to prove the content of a written document, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required

BIOS: Basic input output system

Cache: A fast storage buffer in the central processing unit of a computer. Also called cache memory

Chain of Custody: A chain of custody tracks evidence from its original source to what is offered as evidence in court

Client/Server Architecture. A computer network design involving desktop PCs that depend on other (generally larger) computers to provide the PCs with information and/or applications. In the client/server environment, the client (PC) and the server are symbiotic and processing occurs in both places.

Client- server networks connect individual PCs called "clients" to a central "server" computer.

Computer forensics is the science of obtaining, preserving, and documenting evidence from digital electronic storage devices, such as computers, pagers, PDAs, digital cameras, cell phones, and various memory storage devices. All must be done in a manner designed to preserve the probative value of the evidence and to assure its admissibility in a legal proceeding.

Computer forensics - the collection, preservation, analysis and court presentation of computer-related evidence - has developed as a specialized field in order to harness the power of the vast amounts of digital information for use in litigation. Increasingly, such computerized information does not exist in hard copy, paper form.

Computer Crime: See Cybercrime

Computer System refers to the entire computing environment. This environment may consist of one large computer serving many users (e.g. a mainframe or mini- computer) or one or more personal computers working individually or linked together through a network. A computer system includes all hardware and peripherals used (e.g. terminals, printers, modems, data storage devices), as well as the software.

Copy: A copy is an accurate reproduction of information contained in the data objects independent of the original physical

Cybercrime: Any offense where the modus operandi involves the use of a computer network in any way

Cybercrime investigation includes such endeavors as detecting and stopping hackers, as well as other criminals who use the Internet as the instrumentality of their criminal enterprises. Catching them often involves tracing and verifying e-mail messages, or setting traps on the Internet in the hope of reeling them in.

Cyberspace: The term originally coined by William Gibson in his novel *Neuromancer* that refers to the connections and conceptual locations created using computer networks

Data File. See File

Denial of Service (DOS) Attacks are attacks made against a specific web site to deny access to legitimate users by tying up the system

Digital Evidence Information stored or transmitted in binary form that may be relied upon in court.

Dongle: An external hardware devices with some memory inside it.

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

Files are groups of information collectively placed under a name and stored on the computer. Files are organized in various directories and subdirectories.

File Allocation Table (FAT). Where the operating system stores information about a disk's structure. The FAT is a road map, which allows a computer to save information on the disk, locate and retrieve it. Different operating systems have more or less sophisticated FAT capabilities and therefore are more or less wasteful of space on the disk. Newer operating systems utilize FAT 32 systems while older systems utilize FAT 16 systems (the principal difference being, for present purposes, that FAT 16 operating systems waste a lot of space where old deleted files can languish).

Hearsay evidence; Hearsay can be defined as "a statement , other than one made by the declarant while testifying at the trial or hearing , offered in evidence to prove the truth of the matter asserted."

Hearsay evidence is considered secondhand; it is not what the witness knows personally, but what someone else told him or her. Gossip is an example of hearsay. In general, hearsay may not be admitted in evidence, because the statements contained in it were not made under oath but there are exceptions.

Main Frame Architecture. A computer network design where large (main frame) computers maintain and process data and send information to users' terminals. In a classic mainframe set up, no processing occurs at the desktop, which is merely a means of viewing information contained in and processed on the main frame (host) computer.

Memory Card: Memory cards, sometimes referred to as Flash Memory Cards, are removable solid-state storage devices employing flash memory technology.

Some popular types of flash memory cards for use in digital cameras are: CompactFlash (CF), SmartMedia (SM), Memory Stick (MS), MultiMediaCard (MMC) Secure Digital (SD) and xD-Picture Card (xD) and PCMCIA Type I and Type II memory cards

Media is the generic term for the various storage devices computers use to store data. For PCs the most common media are the computer's internal hard drive, Cds, floppy diskettes, backup tapes and microchips

Non-Printing Information The non-printing information carried by most data files is another excellent source of information. A common example is the date and time stamp an OS may put on a file. Some word-processing programs store revisions to documents, allowing a viewer to follow the thought process of the author as a document is edited. Some word-processing packages allow users to insert "hidden" or non-printing comments. Many schedule programs track who made changes to a calendar and when the changes were made. This information may never appear in hard copy form, but may be found in the electronic version.

Networks are the hardware and software combinations that connect computers and allow them to share data. Two common ways PCs are networked are peer-to- peer and client-server.

Operating Systems [OS]: System software that controls the workings of the computer (e.g., Windows, Unix, Linux). The OS handles essential, but often invisible, tasks such as maintaining files.

Original Digital Evidence: Physical items and those data objects, which are associated with those items at the time of seizure.

Peer-to-peer networks physically connect each computer in the network to every other computer in the network. Files are stored on the hard drives of the individual PCs with no centralized file storage.

Probative Value: Evidence that is sufficiently useful to prove something important in a trial. However, probative value of proposed evidence must be weighed by the trial judge against prejudicing in the minds of jurors toward the opposing party or criminal defendant.

Prima Facie Evidence: Prima Facie evidence that is sufficient to raise a presumption of fact or to establish the fact in question unless rebutted.

QUERY To search or ask. In the context of online computing, this often refers to the process of requesting information in a search engine, index directory, or database.

RAM: Random access memory is short-term memory that provides working space for the computer to work with data. Information stored in RAM typically is lost when the device is turned off.

Real evidence: Evidence afforded by the production of physical objects for inspection or other examination by the court

Residual data. Residual data includes deleted files that have not been overwritten and/or file slack space that has not been wiped clean by specialized software. Also called "recoverable files."

When a file is deleted, the data in that file is not erased. Rather, the computer marks the file space as free and the file remains retrievable. Data in a deleted file is not erased until it is overwritten with data from a newly saved file or until specialized programs wipe it. Residual data can also include portions of files distributed on the drive surface or embedded within other files. These files are commonly referred to as ‘file fragments’ and ‘unallocated data.’

Removable Media: Digital media such as floppy disks, CDs, DVDs, cartridges, tapes or removable media cards (small-sized data storage media typically found in cameras, PDAs or music players) that store data and can be easily removed.

Shareware: Software distributed free on a trial basis with the understanding that the user will pay if the software is used beyond the trial period.

Slack Space: The unused space in a disk cluster.

Smart Card: Plastic, credit card sized cards with an embedded integrated electronic chip. The Hong Kong SmartID card is an example of a smart card used for identification purposes and the Octopus card is an

example of a stored value smart cards.

System Unit: Usually the largest part of a PC, the system unit is a box that contains the major components including disk drives and the ports for connecting the keyboard, mouse, printer and other devices.

Tape: A long strip of magnetic coated plastic used to record computer data.

Trojan Horse: A malicious computer program that is disguised as or hidden within another program

URL: Uniform Resource Locator,.

Virus: A piece of malicious programming code designed to create an unexpected and, for the victim, usually undesirable event.

Word Processor: A software program used for preparing documents

Worm: A malicious software program capable of moving from computer to computer over a network without being carried by another program.

Zip: A popular data compression format.