

Digital Forensics Terms Very Handy In Court

❖ *!DigitalSherlock.com | SafeHack.com*

❖ *!Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *!GNU Free Documentation License*

❖ *!Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ *!Document Name: incident_response*

❖ *!Version 1.00*

❖ *!Date: 2005/06/06*

❖ **Address Resolution Protocol (ARP)**

- A protocol used on the Internet to map computer network addresses to hardware addresses.

❖ **Admissible evidence**

- Evidence that meets all regulatory and statute requirements, and has been properly obtained and handled.

❖ **ASCII**

- Stands for American Standard Code for Information Interchange. It is a singlebyte character encoding scheme used for text-based data.

❖ **Auditing**

- The process of keeping track of who is logging in and accessing what files.

❖ **backdoor**

- A software program that allows access to a system without using security checks.

❖ **Basic Input Output System (BIOS)**

- Responsible for booting the computer by providing a basic set of instructions.

❖ **BeOS File System (BFS)**

- Designed for the BeOS, BFS has the builtin capability to work with FAT 12, FAT 16, VFAT, and HPFS partitions.

❖ **Best evidence rule**

- When a document is presented as evidence, you must introduce the original document. You cannot introduce a copy.

❖ **Best practices**

- A set of recommended guidelines that outline a set of good controls.

❖ **Bluetooth**

- A standard developed to allow various types of electronic equipment to make their own connections by using a shortrange (10 meter) frequency-hopping radio link between devices.

❖ **Browser**

- An application that allows you to access the World Wide Web. The most common ones are Microsoft Internet Explorer and Netscape.

❖ **Brute force**

- Systematically trying every conceivable combination until a password is found, or until all possible combinations have been exhausted.

❖ **Cache**

- Space on a hard disk used to store recently accessed data in an effort to improve performance speed.

❖ **CD/DVD-ROM/RW drive**

- A drive accessible from outside the computer that is used to read and/or write CDs and

DVDs. A compact disc (CD) can store huge amounts of digital information (783MB) on a very small surface. CDs are incredibly inexpensive to manufacture.

❖ **Chain of custody**

- Documentation of all the steps that evidence has taken from the time it is located at the crime scene to the time it's introduced in the courtroom. All steps include collection, transportation, analysis, and storage processes. All accesses of the evidence must be documented as well.

❖ **CMOS**

- Complementary Metal Oxide Semiconductor. An on-board semiconductor chip used to store system information and configuration settings when the computer is either off or on.

❖ **Computer evidence**

- Any computer hardware, software, or data that can be used to prove one or more of the five Ws and an H of a security incident (i.e., who, what, when, where, why, and how).

❖ **Computer Forensic**

- Computer investigation and analysis techniques that involve the identification, preservation, extraction, documentation, and interpretation of computer data to determine potential legal evidence.

❖ **cookies**

- Small text files that are placed on your computer's hard drive when you browse a website. The file contains a simple unique number that identifies you to the website's computers when you return.

❖ **Covert channels**

- A method by which an entity receives information in an unauthorized manner.

❖ **Cross examination**

- Questions asked by opposing counsel to cast doubt on testimony provided during direct examination.

❖ **Cryptography**

- The science of hiding the true meaning of a message from unintended recipients.
- Encrypt
 - Obscure a message's meaning to make it unreadable.
- Decrypt
 - Translate an encrypted message back into the original unencrypted message.
- Cipher
 - An algorithm for encrypting and decrypting.
- Substitution cipher
 - A cipher that substitutes each character in the original message with an alternate character to create the encrypted message.
- Plaintext
 - The original unencrypted message.
- Ciphertext
 - The encrypted message.
- Private key algorithm
 - An encryption algorithm that uses the same key to encrypt and decrypt.
- Symmetric algorithm
 - Another name for a private key encryption algorithm.

- Public key algorithm
 - An encryption algorithm that uses one key to encrypt plaintext and another key to decrypt ciphertext.
- Passcode
 - A character string used to authenticate a user ID to perform some function, such as encryption key management.
- Asymmetric algorithm
 - Another name for a public key encryption algorithm.
- Known plaintext attack
 - An attack to decrypt a file characterized by comparing known plaintext to the resulting ciphertext.
 - If you have both the unencrypted and encrypted versions of a file, you can analyze the relationship between the two and deduce the encryption key.
- Chosen plaintext attack
 - An attack to decrypt a file characterized by comparing ciphertext to a plaintext message you chose and encrypted.
 - In a chosen plaintext attack, you encrypt a file of your choosing and compare it to the resulting encrypted file. After you create the plaintext and ciphertext, the attack progresses just as the known plaintext attack.
- ❖ **Cyclic redundancy check (CRC)**
 - A common technique for detecting data transmission errors. Each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving device then applies the same formula to the message and checks to make sure the accompanying numerical value is the same, thereby verifying the data integrity.
- ❖ **dd utility**
 - Copy and convert utility. Originally included with most versions of Unix and Linux, versions now exist for Windows as well.
- ❖ **Demonstrative evidence**
 - Evidence that illustrates, helps explain, or demonstrates other evidence. Many times, demonstrative evidence consists of some type of visual aid.
- ❖ **Deposition**
 - Testimony that is reduced to written form.
- ❖ **Desktop**
 - A PC designed to be set up in a permanent location because the components are too large to easily transport.
- ❖ **Direct examination**
 - Initial questions asked to a witness to extract testimony.
- ❖ **Disaster recovery**
 - The ability of a company to recover from an occurrence inflicting widespread destruction and distress.
- ❖ **Distributed denial of service (DDoS) attack**
 - An attack that uses one or more systems to flood another system with so much traffic that the targeted system is unable to respond to legitimate requests.
- ❖ **Documentary evidence**
 - Written evidence, such as printed reports or data in log files. Such evidence cannot stand on its own and must be authenticated.
- ❖ **Dual-boot system**

- A system that has the ability to boot, or start, and run more than one operating system.
- ❖ **EBCDIC**
 - Stands for Extended Binary Coded Decimal Interchange Code. It is a character encoding set used by IBM mainframes. Most computer systems use a variant of ASCII, but IBM mainframes and midrange systems, such as the AS/400, use this character set primarily designed for ease of use on punched cards.
- ❖ **Electromagnetic fields**
 - Produced by the local buildup of electric charges in the atmosphere. They can be damaging to computer components. They are present everywhere in our environment but are invisible to the human eye.
- ❖ **electronic discovery**
 - The process whereby electronic documents are collected, prepared, reviewed, and distributed in association with legal and government proceedings.
- ❖ **Electrostatic discharge (ESD)**
 - Buildup of electrical charge on one surface that is suddenly transferred to another surface when it is touched.
- ❖ **E-mail header**
 - Data contained at the beginning of an electronic message that contains information about the message.
- ❖ **Expert witness**
 - A person called to testify in a court of law who possesses special knowledge or skill in a specific area that applies to a case.
- ❖ **Extension checker**
 - A utility that compares a file's extension to its header. If the two do not match, the discrepancy is reported.
- ❖ **fdisk**
 - A utility that can be run from a bootable floppy disk that displays current disk partition information and allows you to repartition a hard disk.
- ❖ **File Allocation Table (FAT)**
 - A simple filesystem used by DOS, but supported by later operating systems. The FAT resides at the beginning of a disk partition and acts as a table of contents for the stored data.
- ❖ **File viewer**
 - A utility that provide thumbnail images of files. Such tools are useful for visually scanning a group of files.
- ❖ **Filesystem**
 - The operating system's method of organizing, managing, and accessing files through logical structuring on the hard drive.
- ❖ **FireWire**
 - An IEEE-1394 technology that is a highperformance, external bus standard that supports data transfer and multimedia.
- ❖ **Floppy drive**
 - A drive accessible from the outside of the computer into which you can insert and/ or remove a floppy disk. One floppy disk holds up to 1.4MB of data.
- ❖ **Forensic compression**
 - The compacting of an image file by compressing redundant sectors to reduce the

amount of space it takes up.

❖ **Forensic compression**

- The compacting of an image file by compressing redundant sectors to reduce the amount of space it takes up.

❖ **Forensic duplicate**

- A process used to copy an entire hard drive that includes all bits of information from the source drive and stores it in a raw bit stream format.

❖ **Forensic suite**

- A set of tools and/or software programs used to analyze a computer for collection of evidence.

❖ **Forensically sound**

- Procedures whereby absolutely no alteration is caused to stored data so that all evidence is preserved and protected from all contamination.

❖ **Hard evidence**

- Real evidence that is conclusively associated with a suspect or activity.

❖ **Hardware write blocker**

- A hardware device that is plugged in between the disk controller and the physical disk, and blocks any write requests.

❖ **Hardware-protected areas (HPAs)**

- Areas of a hard drive created to specifically allow manufacturers to hide diagnostic and recovery tools.

❖ **HASH**

- A mathematical function that creates a fixed-length string from a message of any length. The result of a hash function is the hash value, sometimes called a message digest. Hash functions are one-way functions. That is, you can create a hash value from a message, but you cannot create a message from a hash value.

❖ **High-Performance File System (HPFS)**

- A filesystem designed for the OS/2 operating system. HPFS automatically sorts the directory based on the filename, and it includes the super block and spare block.

❖ **Honeypot**

- A specially equipped system deployed to lure hackers and track their use of the system's resources.

❖ **HyperText Markup Language (HTML)**

- A web-based programming language used to create documents that are portable from one platform to another.

❖ **IACIS**

- International Association of Computer Investigative Specialists. An international volunteer corporation comprised of law enforcement professionals, including federal, state, local, and international law enforcement, who are committed to education in the field of forensic computer science.

❖ **IDE port**

- The Integrated Drive Electronics (IDE) port is a system-level interface that allows the operating system to recognize a hard drive as part of the system.

❖ **Incident**

- A threatening computer security breach that can be recovered from in a relatively short period of time.

- ❖ **Incident response**
 - The action taken to respond to a situation that can be recovered from relatively quickly.
- ❖ **Incident response plan**
 - The actions an organization takes when it detects an attack, whether ongoing or after the fact.
- ❖ **Incident response team (IRT)**
 - A team of individuals trained and prepared to recognize and immediately respond appropriately to any security incident.
- ❖ **Input/output (I/O)**
 - Data transfer that occurs between the thinking part of the computer or CPU and an external device or peripheral. For example, when you type on your keyboard, the keyboard sends input to the computer which, in turn, outputs what you type on the screen.
- ❖ **Internet service provider (ISP)**
 - Provides a gateway to the Internet and other online services, primarily as a paid service.
- ❖ **Intrusion detection**
 - Software and hardware agents that monitor network traffic for patterns that may indicate an attempt at intrusion.
- ❖ **IP address**
 - An identifier for a computer or device on a TCP/IP network.
- ❖ **Jaz drive**
 - A true, replaceable hard disk. Each Jaz cartridge is basically a hard disk, with several platters, contained in a hard, plastic case.
- ❖ **key logger**
 - Device that intercepts, records, and stores everything that the user types on the keyboard into a file. This includes all keystrokes, even passwords.
- ❖ **KISS method**
 - KISS stands for “Keep It Simple, Stupid” and is an acronym that reminds us to avoid making things overly complex.
- ❖ **logic bomb**
 - A virus or other program that is created to execute when a certain event occurs or a period of time passes. For example, a programmer might create a logic bomb to delete all his code from the server on a future date, most likely after he has left the company.
- ❖ **Malware**
 - Another name for malicious code. This includes viruses, logic bombs, and worms.
- ❖ **Message Digest 5 (MD5)**
 - A method of verifying data integrity that is more reliable than CRC. MD5 is a oneway hash function, meaning that it takes a message and converts it into a fixed string of digits, which is then used to verify that the message hasn't been altered.
- ❖ **Metadata**
 - A data component that describes the data. In other words, it's data about data.
- ❖ **Mirror image**
 - A process used to create a bit-for-bit copy from one hard drive to another.
- ❖ **Modem**
 - A shortened version of the words modulator-demodulator. A modem is used to send

digital data over a phone line. The sending modem converts data into a signal that is compatible with the phone line, and the receiving modem then converts the signal back into digital data.

❖ **Network File System (NFS)**

- Provides remote access to shared file systems across networks. The primary function of NFS is to mount directories to other computers. These directories can then be accessed as though they were local.

❖ **New Technology File System (NTFS)**

- A file system supported by Windows NT and higher Windows operating systems.

❖ **Operating system OS**

- Acts as a director and interpreter between the user and all the software and hardware on the computer.

❖ **Packets**

- Unit of information routed between an origin and a destination. A file is divided into efficient-size units for routing.

❖ **Password**

- A string of characters used to authenticate a user by comparing the provided value to a value that has previously been stored and is associated with a specific user ID. Passwords are routinely stored when an account is created or the password is changed.

❖ **Password cracking**

- Attempting to discover a password by trying multiple options and continuing until a successful match is found.
- Dictionary attack
 - An attack that tries different passwords defined in a list, or database, of password candidates.
- Brute force attack
 - An attack that tries all possible password combinations until the correct password is found.
- Hybrid attack
 - A modification of the dictionary attack that tries different permutations of each dictionary entry.

❖ **PC**

- A personal computer intended for generic use by an individual. PCs were originally known as microcomputers because they were built on a smaller scale than the large systems most businesses used.

❖ **Personal digital assistant (PDA)**

- A tightly integrated handheld device that combines computing, Internet, and networking components. A PDA can use flash memory instead of a hard drive for storage.

❖ **Port scanners**

- A program that attempts to connect to a list of computer ports or a range of IP addresses.

❖ **Protocol**

- A set of rules and conventions that governs how computers exchange information over the network medium.

❖ **Real evidence**

- Any physical objects that you can bring into court. Real evidence can be touched, held, or otherwise observed directly.

- ❖ **Relevant evidence**
 - Evidence that serves to prove or disprove facts in a case.
- ❖ **Request for Comments (RFC)**
 - Started in 1969, RFCs are a series of notes about the Internet. An Internet document can be submitted to the Internet Engineering Task Force (IETF) by anyone, but the IETF decides if the document becomes an RFC. Each RFC is designated by an RFC number. Once published, an RFC never changes. Modifications to an original RFC are assigned a new RFC number.
- ❖ **Routers**
 - Devices used to forward packets.
- ❖ **Search warrant**
 - A court order that allows law enforcement to search and/or seize computer equipment without providing advance warning to the equipment owner.
- ❖ **Second/Third Extended Filesystems (ext2/ext3)**
 - State-based filesystems used by the Linux operating system.
- ❖ **Security policies**
 - Specifications for a secure environment, including such items as physical security requirements, network security planning details, a detailed list of approved software, and human resources policies on employee hiring and dismissal.
- ❖ **Seized**
 - A program developed by New Technologies, Inc. (NTI) that locks a seized computer and warns the computer operator that the computer contains evidence and should not be operated.
 - <http://www.forensics-intl.com/seized.html>
- ❖ **Server**
 - A computer that has the capacity to provide services to other computers over a network. Servers can have multiple processors, a large amount of memory, and many hard drives.
- ❖ **Signature analysis**
 - A technique that uses a filter to analyze both the header and the contents of the datagram, usually referred to as the packet payload.
- ❖ **Site survey**
 - Notes, photographs, drawings, and any other documentation that describes the state and condition of a scene.
- ❖ **Slack space**
 - The space on a hard disk between where the file ends and where the cluster ends.
- ❖ **Social engineering**
 - A method of obtaining sensitive information about a company through exploitation of human nature.
- ❖ **Software write blocker**
 - Software that lives between the operating system and disk driver and blocks any write requests.
- ❖ **Spam**
 - Unsolicited “junk” e-mail often sent to a large number of people.
- ❖ **Spanning across multiple discs**
 - Breaks the image file into chunks of a certain size so the image file can be backed up

onto multiple CD recordable discs or other media types.

- ❖ **Steganography**
 - Passing information in a manner such that the very existence of the message is unknown.
- ❖ **Subpoena**
 - A court order that compels an individual or organization to surrender evidence.
- ❖ **Summons**
 - A court order that compels a witness to appear in court and answer questions.
- ❖ **Swap file**
 - Space on the hard disk used as the virtual memory extension of a computer's actual memory.
- ❖ **TCP/IP**
 - Transmission Control Protocol/Internet Protocol (TCP/IP) network
 - A network that uses the TCP/IP protocol.
 - between 1 and 126 are Class A.
 - between 128 and 191 are Class B.
 - between 192 and 223 are Class C.
 - between 224 and 239 are Class D.
 - between 240 and 255 are Class E.
- ❖ **Temporary Internet files**
 - Copies of all the HTML, GIF, JPG, and other files associated with the sites a user has visited on the Internet.
- ❖ **Testimonial evidence**
 - Evidence consisting of witness testimony, either verbal or in written form. Testimonial evidence can be presented in person by the witness in a court or through a recorded deposition.
- ❖ **Trace evidence**
 - Traces of data either left behind or found with a criminal that can be used to prove that a crime was committed.
- ❖ **Traceroute**
 - A command used to see where a network packet is being sent and received in addition to all the places it goes along the way to its destination.
- ❖ **Unerase tool**
 - A utility that assists in recovering previously deleted files. In some cases, files can be completely recovered. At other times, only portions of the file can be recovered.
- ❖ **Universal Serial Bus (USB)**
 - A connectivity standard that allows for the connection of multiple devices without the need for software or hardware.
- ❖ **User ID**
 - A string of characters that identifies a user in a computing environment.
- ❖ **Virtual FAT (VFAT)**
 - Also called FAT32, an enhanced version of the FAT filesystem that allows for names longer than the 8.3 convention and uses smaller allocation units on the disk.
- ❖ **Virus**
 - A program or piece of code that is loaded onto your computer without your knowledge

and is designed to attach itself to other code and replicate. It replicates when an infected file is executed or launched.

❖ **Voluntary surrender**

- Permission granted by a computer equipment owner to search and/or seize the equipment for investigative purposes.

❖ **War dialing**

- Uses an automated software application that attempts to dial numbers within a given range of phone numbers to determine if any of those numbers are actually used by modems accepting dial-in requests.

❖ **WinHex**

- A universal hexadecimal editor used in computer forensics, data recovery, lowlevel data processing, and IT security.

❖ **Wireless access point (WAP)**

- Network device that contains a radio transmitter/receiver and that is connected to another network. A WAP provides wireless devices access to a regular wired network.

❖ **Workstation**

- A desktop computer that has enhanced processing power, memory, and capabilities for performing a special function, such as software or game development.

❖ **Worm**

- Similar in function and behavior to a virus, with the exception that worms do not need user intervention. A worm takes advantage of a security hole in an existing application or operating system and then finds other systems running the same software and automatically replicates itself to the new hosts.

❖ **Zip drive**

- A small, portable, high-capacity floppy disk drive developed by Iomega Corporation and used primarily for backing up or archiving PC files.

❖ **Reference**

- Book Computer Forensics Jumpstart 2005 Sybex
- Book CRC Press Investigating Computer-Related Crime
- Book Computer Network & Internet Security
- Book Cyber Crime Investigator's Field Guide