Glossary for Computer Forensics

1.0 Purpose - This procedure contains the specific definitions of the terms and abbreviations used in the computer forensics technical procedures.

2.0 Scope – These definitions are to be used to explain any terms within the computer forensics technical procedures.

3.0 Definitions

- **BIOS -** Basic Input Output System. A number of machine code routines that are stored in ROM and available for execution at boot time.
- **Browser -** Browser is short for Web Browser. A browser is a computer program that locates and displays pages from the Internet.
- **Cache -** A computer’s cache is an area where the computer can temporarily store frequently used data that would otherwise have to be loaded from a slower source. The computer’s cache speeds up the operation of the computer.
- **CDFS -** The standard used to describe the file structure on a CD.
- **Clone -** The process of performing a sector-by-sector copy operation from the suspect drive to the destination drive. The number of sectors copied is determined by the size of the suspect drive.
- **Cluster bitmaps -** Used by NTFS to track free clusters by using a bitmap. This file contains one bit for every cluster on the volume.
- **Clusters -** A group of sectors in a logical volume that is used to store files and folders.
- **Compressed file -** A file that has been reduced in size via one or more compression techniques.
- **Compression -** A method of storing files resulting in great savings in disk storage space. Compressed blocks are checked for validity in the same way as uncompressed blocks.
- **Cookie -** A cookie is a short piece of data that Web servers place on your computer to help identify Web users. Cookies can be used by Web servers to track your Internet browsing habits.
- **Cylinder -** The set of tracks on the drive platters that are at the same head position.
- **Disk** – An actual piece of hardware that can be held physically. It could be a floppy disk, hard disk, ZIP disk, etc.
- **DOS -** Disk Operating System - usually refers to MS-DOS. This operating system, which was developed by Microsoft for IBM compatible PCs, is still used today to help control operation on computers and operates beneath the Windows environment.
- **Drive Geometry -** The number and position of the bytes, sectors, tracks located on the physical drive.
- **EXT2 -** The primary file system used on the Linux operating system.
- **Fdisk -** DOS program that provides information about, and editing of, the partitions on a hard drive.
- **File entries -** Each folder contains a starting cluster and can be expanded or contracted as files are added or removed from the folder. Each file in the folder is represented by a 32-byte entry in the table. The content of a folder “file” is an array of records containing information about the files in the folder. Each entry in the folder can be either a file or another folder. In this way, a “tree” structure can be built.
- **File slack -** The space between the logical end and the physical end of a file.
- **File signature -** A few bytes at the beginning of some files (such as graphic or document files) that constitute a unique signature of the file type, regardless of the file extension used.
- **File allocation table (FAT) -** An array of numbers that sits near the beginning of a DOS volume. The length of the numbers is determined by the size of the volume. Each entry in the FAT corresponds directly to one cluster and there is always one FAT entry for every cluster.

- **Format -** DOS command used to prepare a storage medium (hard drive, floppy disk) for reading and writing. Format does not erase data on the disk. It checks for bad sectors and resets the internal address tables (FAT).
- **Head -** A device that rides very close to the surface of the platter and allows information to be read from, and written to, the platter.
- **Hyperlink** – A hyperlink is a text phrase (which often is a different color that the surrounding text) or a graphic that conceals the address of a website. Clicking on the hyperlink takes you to the website.
- **Image drive -** Same as the target drive.
- **Internet -** The Internet is a worldwide network with more than 100 million computer users that are linked for the exchange of data, news, conversation, and commerce. The Internet is a decentralized network that no one person, organization, or country controls.
- **ISDN Line -** Integrated Services Digital Network - A phone line that connects two computers to transmit a digital signal between them, as opposed to the analog signal transmitted over normal phone lines. This allows data to be transferred more than twice as fast as with an analog phone line with a 56kbps modem.
- **Logical file size -** The exact size of a file in bytes and is the number represented in the properties for a file. This is different than physical file size.
- **Logical drive -** A drive named by a DOS drive specifier, such as C: or D:. A single physical drive can act as several logical drives, each with its own specifier.
- **Master boot record (MBR) -** The very first sector of a physical disk (sector zero). It contains machine code that allows the computer to find the partition table and the operating system.
- **MD5 -** A 128-bit value that uniquely describes the contents of a file. This is the standard hash code used in forensics.
- **NTFS -** New Technology File System. The file descriptors for every file on an NTFS volume are stored in the Master File Table.
- **Partition table -** Describes the first four partitions, their location on the disk, and which partition is bootable.
- **PGP -** Pretty Good Privacy - Program used to encrypt data on a computer, such as messages on the Internet.
- **Physical drive -** A single disk drive. A single physical drive may be divided into multiple logical drives.
- **Physical file size -** The amount of space that a file occupies on a disk. A file or folder always occupies a whole number of clusters even if it does not completely fill that space.
- **Plug-ins -** Computer hardware or software that adds a specific feature or service to a larger system.
- **RAM slack -** The space from the end of the file to the end of the containing sector. Before a sector is written to disk, it is stored in a buffer somewhere in RAM.
- **RAM -** Random Access Memory. Volatile read/write memory whose contents are lost when the power is turned off.
- **ROM -** Read Only Memory. Chips contain a permanent program that is burned on the chip at the factory and maintained when the power is turned off. The information on these chips can be read; however, information cannot be written to the chip.
- **Root folder -** Stored in a known location, this is a tree structure that supports files and folders within folders to an arbitrary depth.
- **Sector -** A group of bytes within a track and the smallest group of bytes that can be addressed on a drive. The number of bytes in a sector can vary, but is almost always 512.
- **Spam -** Unsolicited “junk” e-mail which is sent to persons who did not request it. It is usually commercial e-mail.

- **Suspect drive -** The drive (or drives) that are removed from a subject's computer, or in the possession of a subject, that will be imaged for later analysis. This drive is never analyzed; rather is copied so the analysis can be conducted on the forensic image.
- **System drive -** The forensic hard drive used to boot the forensic tower. This is the drive which contains the forensic search tools.
- **Target drive -** The drive to which information from the suspect drive is being written.
- **Track -** Each platter on a disk is divided into thin concentric bands called tracks. Tracks are established when the disk is low level formatted.
- **Upload -** To send or transmit data from one computer to another computer or network.
- **URL -** Universal Resource Locator - An address at which documents or other resources can be found on the Web.
- **Virtual Machine (VM)** – A software emulation of a computer that executes programs like a real machine.
- **Volume -** A mounted partition. There may be only one volume on a floppy or ZIP disk, or there may be several on a hard disk.
- **Wipe** – a procedure for sanitizing a defined area of digital media by overwriting each byte with a known value.
- **World Wide Web -** A group of Internet servers that supports HTML formatting. The World Wide Web is one part of the Internet.

4.0 Equipment, Materials and Reagents – N/A

5.0 Procedure – N/A

6.0 Limitations – N/A

7.0 Safety – N/A

8.0 References – N/A

9.0 Records - N/A

10.0 Attachments – N/A

Revision History		
Effective Date	Version Number	Reason
09/17/2012	1	Original Document
10/31/2013	2	Added issuing authority to header