Digital Evidence Dictionary

Definitions

- **Binary** – A base-2 representation for numbers that uses a sequence of 1's and 0's to write a number.
- **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.
- **Chip-Off Extraction –** A method of data extraction which involves the removal of a flash memory chip from the printed circuit board (PCB) of a device and directly reading the binary data from the flash memory chip. This type of data extraction is considered destructive as the device will be permanently inoperable after the memory chip is removed from the PCB.
- **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.
- **Control Image –** A forensic image of a known piece of media.
- **Control Media –** A standard piece of media with a known hash value.
- **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.
- **Data Acquisition –** The general process of making a copy of digital data. This can be an entire digital device, just a partition from a storage device, or selected files from a file system.
- **Digital Evidence –** Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.
- **Device Interface Board (DIB) –** An adapter affixed to a circuit board to enable connection between the circuit board and the forensic computer.
- **Disk** – An actual piece of hardware that can be held physically. It could be a floppy disk, hard disk, ZIP disk, etc.
- **Disk Imaging** – The process of acquiring the digital contents of a storage device (fxed disk, removable disk, flash drive, etc.). This acquires all the data on a device including files, metadata, and contents of unallocated areas of the device.
- **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.
- **Electrostatic Discharge (ESD) –** An uncontrolled and sudden flow of electrons from one object to another caused by contact between the two objects.
- **Encrypt –** To encode information in a way that prevents unauthorized access. For example, decryption with a key is required to access the information.
- **ExFAT –** Extensible File Allocation Table. A revised implementation of the FAT file system introduced in 2006 that addresses some shortcomings in the FAT file system e.g., allows files larger than 4GB, and faster performance.
- **EXT2** - The primary file system used on the Linux operating system.
- **FAT-** File Allocation Table
- **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 System –** A method of organizing files on a storage device. Common file systems on Windows systems are NTFS< ExFAT, and FAT> LINUX systems use ext4 and FAT. Apple Macs use HFS+, APFS, FAT and ExFAT.
- **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.
- **Filter Set – A collection of filters and/or processes designed to clarify a specific audio recording.**
- **Finalize –** To format a CD such that no additional data can be added or removed.
- **Forensic Image –** A bit stream copy of available data (i.e. an exact copy), which may result in an encapsulated proprietary format
- **Forensic Tool –** Forensic software tool or standalone hardware device utilized to conduct acquisitons in casework.
- **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).
- **Hash Value –** An alphanumeric value that uniquely represents a set of data.
- **Hash Value Set (File Filter) –** A list of hash values of known files used within a forensic software tool to show or mask files on a forensic image that have a hash value contained within the list. A file filter does not alter any data on a forensic image
- **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.
- **HFS Plus –** Hierarchical File System Extended. Apple file system introduced in 1998, replaced by APFS in 2017.
- **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.
- **Initial Hash –** A hash value that has been established before conducting any examination to be used to compare to other hash values.
- **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.
- **JTAG –** Joint Action Test Group. An industry standard for verifying designs and testing printed circuit boards after manufacture.
- **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.
- **Logical extraction –** A method of extraction that includes user data available through the device's Application Program Interface but does not include deleted data or unallocated space.
- **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.
- **MAC Times** – Time stamp metadata maintained by a file system to track events in the life cycle of a file. The exact events recorded depends on the operating system and the file system. The usual meaning are Modify, Access, and Create with slight differences in meaning for each type of file system and differences in meaning for files and directories.
- **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** – Message Digest 5. A 128-bit value that uniquely describes the contents of a file. This is a standard hash code used in forensics.

- **Metadata –** A description of stored data. Categories of metadata include: (1) application metadata, (2) file system metadata, (3) partition metadata that identifies the type of file system the partition contains and global file system parameters, and (4) device metadata describes the layout of partitions on a device.
- **microSD Card –** The microSD (Secure Digital) card found in some devices that may contain user data.
- **M26 Dataport Download Kit –** Kit containing the hardware and software needed to download the firing information from a Serial Connection Taser.
- **Non-Standard Audio Video Result Statements –** Result statements which vary in their content due to the nature of the audio or video being enhanced and/or due to the nature of the case being worked.
- **NTFS** - New Technology File System. The file descriptors for every file on an NTFS volume are stored in the Master File Table.
- **Operating System –** The software that creates the digital environment for running software on a computer or other digital device. Most operating systems use variants of either MS Windows (95, 98, 2000, Vista, XP, 10, etc.) or UNIX (BSD, Linux, Mac OS, iOS, etc.).
- **Partition –** A contagious area of a storage device used to contain a formatted file system.
- **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 Extraction –** A method of extraction that includes a bit-by-bit image of the flash memory of a device that contains system and user data to include deleted data, hidden data, and unallocated space.
- **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.
- **Post Exam Hash –** A hash value that is used to ensure data has not been corrupted/changed by comparing the data's initial hash value to the calculated hash value after completing an exam.**Power-On Self Test –** A series of diagnostic tests that are performed when a computer powers on and determines proper functioning of the hardware components.
- **PPE –** Personal Protective Equipment
- **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.
- **Removable Media –** A storage device that is either (1) a data container that is inserted and removed from a data reader or (2) a storage device that can be connected or removed from a computer while the computer is running.
- **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.
- **SATA –** Serial ATA. A protocol for connecting storage devices to a host computer.
- **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.
- **SHA –** Secure Hash Algorithm..
- **SHA-1 -** A 160-bit value that uniquely describes the contents of a file. This is a standard hash code used in forensics.
- **SHA- 256 -** A 256-bit value that uniquely describes the contents of a file. This is a standard hash code used in forensics.
- **SIM Card –** The Subscriber Identity Module card used in some devices that allows the device to connect to a carrier network (AT&T, Verizon, Sprint, etc.). SIM cards may contain identifying information and other data.
- **SIM Card Adapter –** A device used to connect the various types of SIM cards (micro or nano) to the forensic tool for extraction
- **Spam** - Unsolicited "junk" e-mail which is sent to persons who did not request it. It is usually commercial e-mail.
- **Standard Audio Video Result Statements –** Result statements which are common for all audio video cases regardless of the type of case being examined

- **Storage Device –** An electronic or optical device that can store data for later retrieval. A storage device usually has some type of file system to organize the stored data as files. There are several types including fixed media physically installed in a computer, removable media, memory card, or optical disk.
- **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 drive that contains the operating system (OS)
- **System Image –** Backup of the system drive that contains a clean install of the operating system (OS).
- **Target Drive** - A sterile piece of media used to store forensic image(s) and case related data
- **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.
- **USB Data Interface Module –** Kit containing the hardware and software need to download the firing information from the USB connection Taser.
- **USB DPM –** Connecter from the interface module which plugs into the battery compartment of the USB Taser.
- **Verification Hash –** A hash value that is used to ensure data has not been corrupted/changed by comparing the data's hash value to a previously calculated value.
- **Video Mixdown –** Duplicate copy of video already created. These are generally created to add additional processing to a previously processed video.
- **VIN –** Vehicle Identification Number
- **Virtual Machine (VM)** – A software emulation of a computer that executes programs like a real machine.
- **Volatile** – data stored on a device that is lost when power is removed from the device, Removing power usually resets all binary digits to zero.
- **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.
- **Write-Blocker –** A read-only software or hardware device that protects the integrity of the original evidence by not allowing any writes or alterations to occur during the acquisition process.
- **Write Blocking –** Techniques designed to prevent any modification to digital media during acquisition or browsing.
- **Write Protection –** A method by which media content is protected from inadvertent alteration or deletion.

References –

Lyle, James R., et al. "Digital Investigation Techniques: A NIST Scientific Foundation Review." May 2022. *https://doi.org/10.6028/NIST.IR.8354-draft.* May 2022.