



Data Forensics Glossary

Active Data: Active data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction (i.e., word processing and spreadsheet files, programs and files used by the computer's operating system).

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.

Active Records: Active records are records related to current, ongoing or in process activities and are referred to on a regular basis to respond to day-to-day operational requirements. An active record resides in native application format and is accessible for purposes of business processing with no restrictions on alteration beyond normal business rules.

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: An application is a collection of one or more related software programs that enables a user to enter, store, view, modify or extract information from files or databases. The term is commonly used in place of "program," or "software." Applications may include word processors, Internet browsing tools and spreadsheets.

Archival Data: Archival data is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats (i.e., data stored on backup tapes or disks, usually for disaster recovery purposes).

Archive/Electronic Archive: Archives are long term repositories for the storage of records. Electronic archives preserve the content, prevent or track alterations and control access to electronic records.

Attachment: An attachment is a record or file associated with another record for the purpose of storage or transfer. There may be multiple attachments associated with a single "parent" or "master" record. The attachments and associated record may be managed and processed as a single unit. In common use, this term refers to a file (or files) associated with an e-mail for transfer and storage as a single message unit. Because in certain circumstances the context of the attachment—for example, the parent e-mail and its associated metadata—can be important, an organization should consider whether its policy should authorize or restrict the disassociation of attachments from their parent records.

Attribute: An attribute is a characteristic of data that sets it apart from other data, such as location, length, or type. The term attribute is sometimes used synonymously with "data element" or "property."

ASCII (Acronym for American Standard Code): ASCII is a code that assigns a number to each key on the keyboard. ASCII text does not include special formatting features and therefore can be exchanged and read by most computer systems.

Author /Originator: The author of a document is the person, office or designated position responsible for its creation or issuance. In the case of a document in the form of a letter, the author or originator is usually indicated on the letterhead or by signature. In some cases, the software application producing the document may capture the author's identity and associate it with the document.

Backup: To create a copy of data as a precaution against the loss or damage of the original data. Most users backup some of their files, and many computer networks utilize automatic backup software to make regular copies of some or all of the data on the network. Some backup systems use digital audio tape (DAT) as a storage medium.

Backup Data: Backup data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster.

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

Backup Tape: Backup or disaster recovery tapes are portable media used to store data that is not presently in use by an organization to free up space but still allow for disaster recovery.

Backup Tape Recycling: Backup tape recycling is the process whereby an organization's backup tapes are overwritten with new backup data, usually on a fixed schedule (i.e., the use of nightly backup tapes for each day of the week with the daily backup tape for a particular day being overwritten on the same day the following week; weekly and monthly backups being stored offsite for a specified period of time before being placed back in the rotation).

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).

Bates Production Number: A bates production number is a tracking number assigned to each page of each document in the production set.

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

Binary: Mathematical base 2, or numbers composed of a series of zeros and ones. Since zero's and one's can be easily represented by two voltage levels on an electronic device, the binary number system is widely used in digital computing.

Bit: A measurement of data. It is the smallest unit of data. A bit is either the "1" or "0" component of the binary code. A collection of bits is put together to form a byte.

Blog: Blogs, also referred to as Web logs, are frequent, chronological Web publications consisting of links and postings. The most recent posting appears at the top of the page.

Burn: Slang for making (burning) a CD-ROM copy of data, whether it is music, software, or other data.

Byte: Eight bits. The byte is the basis for measurement of most computer data as multiples of the byte value. A "megabyte" is one million bytes or eight million bits or a "gigabyte" is one billion bytes or eight billion bits.

1 gigabyte = 1,000 megabytes

1 terabyte = 1,000 gigabytes

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

Cache: A fast storage buffer in the central processing unit of a computer that temporarily stores frequently used information for quick access.

CD-ROM: Data storage medium that uses compact discs to store about 1,500 floppy discs worth of data.

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.

Coding: Document coding is the process of capturing case-relevant information (i.e. author, date authored, date sent, recipient, date opened, etc.) from a paper document.

Compression: A technology that reduces the size of a file. Compression programs are valuable to network users because they help save both time and bandwidth.

Computer Forensics: Computer forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

Computer Forensics: 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.

Cookie: Small data files written to a user's hard drive by a Web server. These files contain specific information that identifies users (i.e., passwords and lists of pages visited).

DAT: (Digital Audio Tape): Used as a storage medium in some backup systems.

Data File: See File

Data: Information stored on the computer system and used by applications to accomplish tasks.

De-Duplication: De-Duplication (“De-Duping”) is the process of comparing electronic records based on their characteristics and removing duplicate records from the data set.

Deleted Data: Deleted data is data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or “wiped” with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

Deleted file: A file with disk space that has been designated as available for reuse. The deleted file remains intact until it has been overwritten with a new file.

Deletion: Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except using special data recovery tools designed to recover deleted data.

Desktop: Usually refers to an individual PC -- a user’s desktop computer.

Digital: Storing information as a string of digits – namely “1”s and “0”s.

Digital Evidence

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

Disc (disk): It may be a floppy disk, or it may be a hard disk. Either way, it is a magnetic storage medium on which data is digitally stored. A disc may also refer to a CD-ROM.

Distributed Data: Distributed data is that information belonging to an organization which resides on portable media and non-local devices such as home computers, laptop computers, floppy disks, CD-ROMs, personal digital assistants (“PDAs”), wireless communication devices (i.e., Blackberry), zip drives, Internet repositories such as e-mail hosted by Internet service providers or portals, Web pages, and the like. Distributed data also includes data held by third parties such as application service providers and business partners.

Document: Fed. R. Civ. P. 34(a) defines a document as “including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations.” In the electronic discovery world, a document also refers to a collection of pages representing an electronic file. E-mails, attachments, databases, word documents, spreadsheets, and graphic files are all examples of electronic documents.

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.

Electronic Discovery: The discovery of electronic documents and data including e-mail, Web pages, word processing files, computer databases, and virtually anything that is stored on a computer. Technically, documents and data are “electronic” if they exist in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes.

Electronic Mail Message: Commonly referred to as “e-mail”, an electronic mail message is a document created or received via an electronic mail system, including brief notes, formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

Electronic Record: Information recorded in a form that requires a computer or other machine to process it and that otherwise satisfies the definition of a record.

E-mail Message Store: A top most e-mail message store is the location in which an e-mail system stores its data. For instance, an Outlook PST (personal storage folder) is a type of top most file that is created when a user’s Microsoft Outlook mail account is set up. Additional Outlook PST files for that user can be created for backing up and archiving Outlook folders, messages, forms and files. Similar to a filing cabinet, which is not considered part of the paper documents contained in it, a top most store generally is not considered part of a family.

Encryption: A procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it.

Ethernet: A common way of networking PCs to create a LAN.

Extranet: An Internet based access method to a corporate intranet site by limited or total access through a security firewall. This type of access is typically utilized in cases of joint venture and vendor client relationships.

Family Range: A family range describes the range of documents from the first Bates production number assigned to the first page of the top most parent document through the last Bates production number assigned to the last page of the last child document.

Family Relationship: A family relationship is formed among two or more documents that have a connection or relatedness because of some factor.

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).

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

File extension: A tag of three or four letters, preceded by a period, which identifies a data file's format or the application used to create the file. File extensions can streamline the process of locating data. For example, if one is looking for incriminating pictures stored on a computer, one might begin with the .gif and .jpg files.

File Server: When several or many computers are networked together in a LAN situation, one computer may be utilized as a storage location for files for the group. File servers may be employed to store e-mail, financial data, word processing information or to back-up the network.

File Sharing: One of the key benefits of a network is the ability to share files stored on the server among several users.

Firewall: A set of related programs that protect the resources of a private network from users from other networks.

Floppy: Once the standard and now an increasingly rare storage medium consisting of a thin magnetic film disk housed in a protective sleeve.

Format: The internal structure of a file, which defines the way it is stored and used. Specific applications may define unique formats for their data (i.e., "MS Word document file format"). Many files may only be viewed or printed using their originating application or an application designed to work with compatible formats. Computer storage systems commonly identify files by a naming convention that denotes the format (and therefore the probable originating application) (i.e., "DOC" for Microsoft Word document files; "XLS" for Microsoft Excel spreadsheet files; "TXT" for text files; and "HTM" (for Hypertext Markup Language (HTML) files such as Web pages). Users may choose alternate naming conventions, but this may affect how the files are treated by applications.

Fragmented Data: Fragmented data is live data that has been broken up and stored in various locations on a single hard drive or disk.

FTP (File Transfer Protocol): An Internet protocol that enables you to transfer files between computers on the Internet.

GIF (Graphic Interchange Format): A computer compression format for pictures.

Gigabyte (GB): A gigabyte is a measure of computer data storage capacity and is a billion (1,000,000,000) bytes.

GUI (Graphical User Interface): A set of screen presentations and metaphors that utilize graphic elements such as icons in an attempt to make an operating system easier to use.

Hard Drive: The primary storage unit on PCs and servers, consisting of one or more magnetic media platters on which digital data can be written and erased magnetically.

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.

HTML (Hypertext Markup Language): The tag-based ASCII language used to create pages on the Web.

Inactive Record: Inactive records are those Records related to closed, completed, or concluded activities. Inactive Records are no longer routinely referenced, but must be retained in order to fulfill reporting requirements or for purposes of audit or analysis. Inactive records generally reside in a long-term storage format remaining accessible for purposes of business processing only with restrictions on alteration. In some business circumstances, inactive records may be reactivated.

Instant Messaging ("IM"): Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously.

Internet: The interconnecting global public network made by connecting smaller shared public networks. The most well-known Internet is the Internet, the worldwide network of networks which use the TCP/IP protocol to facilitate information exchange.

Intranet: A network of interconnecting smaller private networks that are isolated from the public Internet.

IP address: A string of four numbers separated by periods used to represent a computer on the Internet.

IS/IT (Information Systems or Information Technology): Usually refers to the people who make computers and computer systems run.

ISP (Internet Service Provider): A business that delivers access to the Internet.

JPEG (Joint Photographic Experts Group): An image compression standard for photographs.

Keyword search: A search for documents containing one or more words that are specified by a user.

Kilobyte (K): One thousand bytes of data is 1K of data.

LAN (Local area network): Usually refers to a network of computers in a single building or other discrete location.

Legacy Data: Legacy Data is information in the development of which an organization may have invested significant resources and which has retained its importance, but which has been created or stored by the use of software and/or hardware that has been rendered outmoded or obsolete.

Legal Hold: A legal hold is a communication issued as a result of current or anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records. The specific communication to business or IT organizations may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

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.

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

Megabyte (Meg): A million bytes of data is a megabyte, or simply a meg.

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

Metadata: Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed. (Typically referred to by the less informative shorthand phrase "data about data," it describes the content, quality, condition, history, and other characteristics of the data.)

Migrated Data: Migrated Data is information that has been moved from one database or format to another, usually as a result of a change from one hardware or software technology to another.

Mirror Image: Used in computer forensic investigations and some electronic discovery investigations, a mirror image is a bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination. May also be referred to as "disc mirroring," or as a "forensic copy."

MIS: Management information systems.

Modem: A piece of hardware that lets a computer talk to another computer over a phone line.

Mount/Mounting: The process of making off-line data available for on-line processing. For example, placing a magnetic tape in a drive and setting up the software to recognize or read that tape. The terms "load" and "loading" are often used in conjunction with, or synonymously with, "mount" and "mounting" (as in "mount and load a tape"). "Load" may also refer to the process of transferring data from mounted media to another media or to an on-line system.

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.

Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the "native format" of the document. Because viewing or searching documents in the native format may require the original application (i.e., viewing a Microsoft Word document may require the Microsoft Word application), documents are often converted to a standard file format (i.e., tiff) as part of electronic document processing.

Nesting: Document nesting occurs when one document is inserted within another document (i.e., an attachment is nested within an email; graphics files are nested within a Microsoft Word document).

Networks: The hardware and software combinations that allow the exchange of data and sharing of resources. Two common ways PCs are networked are peer-to-peer and client-server.

Node: Any device connected to network. PCs, servers, and printers are all nodes on the network.

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.

OCR (Optical Character Recognition): Optical character recognition is a technology which takes data from a paper document and turns it into editable text data. The document is first scanned. Then OCR software searches the document for letters, numbers, and other characters.

Offline: Not connected (to a network).

Off-line data: The storage of electronic data outside the network in daily use (i.e., on backup tapes) that is only accessible through the off-line storage system, not the network.

On-line storage: The storage of electronic data as fully accessible information in daily use on the network or elsewhere.

Online: Connected (to a network).

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.

Paper Discovery: Paper discovery refers to the discovery of writings on paper that can be read without the aid of some devices.

Parent-child Relationships: Parent-child relationships is a term used in e-discovery to describe a chain of documents that stems from a single e-mail or storage folder. These types of relationships are primarily encountered when a party is faced with a discovery request for e-mail. A "child" (i.e., an attachment) is connected to or embedded in the "parent" (i.e., an e-mail or Zip file) directly above it.

PC: Personal computer.

PDA (Personal Digital Assistant): Handheld digital organizers.

PDF (Portable Document Format): An Adobe technology for formatting documents so that they can be viewed and printed using the Adobe Acrobat reader.

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.

Petabyte (PB): A petabyte is a measure of computer data storage capacity and is one thousand million million (1,000,000,000,000,000) bytes.

Plaintext: The least formatted and therefore most portable form of text for computerized documents.

Pointer: A pointer is an index entry in the directory of a disk (or other storage medium) that identifies the space on the disc in which an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. In most cases, when an electronic document is "deleted," the pointer is deleted, which allows the document to be overwritten, but the document is not actually erased.

Preservation Notice, Preservation Order: See Legal Hold.

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

Private Network: A network that is connected to the Internet but is isolated from the Internet.

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.

PST (Personal Folder File): The place where Outlook stores its data (when Outlook is used without Microsoft® Exchange Server). A PST file is created when a mail account is set up. Additional PST files can be created for backing up and archiving Outlook folders, messages, forms and files. The file extension given to PST files is .pst.

Public Network: A network that is part of the public Internet.

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 the short-term memory that provides working space into which application programs can be loaded and executed and for the computer to work with data within. 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.

Record: Information, regardless of medium or format that has value to an organization. Collectively the term is used to describe both documents and electronically stored information.

Record Custodian: A records custodian is an individual responsible for the physical storage and protection of records throughout their retention period. In the context of electronic records, custodianship may not be a direct part of the records management function in all organizations.

Record Lifecycle: The time period from when a record is created until it is disposed.

Records Hold: See Legal Hold.

Records Management: Records Management is the planning, controlling, directing, organizing, training, promoting and other managerial activities involving the lifecycle of information, including creation, Records Retention Period, Retention Period: The length of time a given records series must be kept, expressed as either a time period (i.e., four years), an event or action (i.e., audit), or a combination (i.e., six months after audit).

Records Retention Schedule: A plan for the management of records, listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to historical archives.

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.

Repository for Electronic Records: Repository for Electronic Records is a direct access device on which the electronic records and associated metadata are stored. Sometimes called a "records store," "online repository" or "records archive."

Residual Data: Also called "recoverable files." Residual Data (sometimes referred to as "Ambient Data") refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted, in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques. 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.'

Restore: To transfer data from a backup medium (such as tapes) to an on-line system, often for the purpose of recovery from a problem, failure, or disaster. Restoration of archival media is the transfer of data from an archival store to an on-line system for the purposes of processing (such as query, analysis, extraction or disposition of that data). Archival restoration of systems may require not only data restoration but also replication of the original hardware and software operating environment. Restoration of systems is often called "recovery".

Router: A piece of hardware that routes data from a local area network (LAN) to a phone line.

Sampling: Sampling usually (but not always) refers to the process of statistically testing a data set for the likelihood of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions as to which repositories of data should be preserved and reviewed in a particular litigation, and determinations of the validity and effectiveness of searches or other data extraction procedures. Sampling can be useful in providing information to the court about the relative cost burden versus benefit of requiring a party to review certain electronic records.

Sandbox: A network or series of networks that are not connected to other networks.

Scanning: Scanning is the process of converting a hard copy paper document into a digital image for use in a computer system. After a document has been scanned, it can be reviewed using field and full-text searching, instant document retrieval, and a complete range of electronic document review options.

Server: Any computer on a network that contains data or applications shared by users of the network on their client PCs.

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.

Sibling: A sibling is a document that shares a common parent with the document in question (e.g. two attachments that share the same parent email or are sibling documents in the same Zip file).

Slack Space: A form of residual data, slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. It is unused space in a disk cluster. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments and other information useful for forensic analysis of computer systems.

Smart Card: Plastic, credit card sized cards with an embedded integrated electronic chip.

Spoilation: Spoilation is the destruction of records which may be relevant to ongoing or anticipated litigation, government investigation or audit. Courts differ in their interpretation of the level of intent required before sanctions may be warranted.

Software: Coded instructions (programs) that make a computer do useful work.

Stand alone computer: A personal computer that is not connected to any other computer or network, except possibly through a modem.

System administrator (sysadmin, sysop): The person in charge of keeping a network working.

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.

Terabyte (TB): A terabyte is a measure of computer data storage capacity and is one thousand billion (1,000,000,000,000) bytes.

TIFF (Tagged Image File Format): One of the most widely supported file formats for storing bit-mapped images. Files in TIFF format often end with a .tif extension.

Transmission Control Protocol/Internet Protocol (TCP/IP): A collection of protocols that define the basic workings of the features of the Internet.

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

URL: The Uniform Resource Locator is commonly known as the address for a website such as www.ianusassociates.com.

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

Vlog (Videoblog): A vlog is a Weblog that uses video as its primary medium for distributing content. Vlog posts are usually accompanied by text, image, and other metadata to provide a context or overview for the video.

VPN (Virtual Private Network): A virtually private network that is constructed by using public wires to connect nodes.

Web site: A collection of Uniform Resource Indicators (URIs, including URLs (Uniform Resource Locators)) in the control of one administrative entity. May include different types of URIs (i.e., file transfer protocol sites, telnet sites, as well as World Wide Web sites).

World Wide Web: The WWW is made up of all of the computers on the Internet which use HTML-capable software (Netscape, Explorer, etc.) to exchange data. Data exchange on the WWW is characterized by easy-to-use graphical interfaces, hypertext links, images, and sound. Today the WWW has become synonymous with the Internet, although technically it is really just one component.

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: An open standard for compression and decompression used widely for PC download archives. ZIP is used on Windows-based programs such as WinZip and Drag and Zip. The file extension given to ZIP files is .zip.

JANUS is a certified, woman-owned small business. Please call 203.251.0200 to speak with a Data Forensics Specialist about how your organization would benefit from our information security services.

JANUS Associates, Inc. 9 West Broad Street Stamford, CT 06902

www.JANUSassociates.com

DFG032206