Designation: E2916 – 13

Standard Terminology for Digital and Multimedia Evidence Examination[1]

This standard is issued under the fixed designation E2916; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This is a compilation of terms and corresponding definitions used in the examination of digital and multimedia evidence to include the areas of computer forensics, image analysis, video analysis, forensic audio, and facial identification.

1.2 Legal or scientific terms that generally are understood or defined adequately in other readily available sources may not be included.

2. Referenced Documents

2.1 *ASTM Standards:*[2]

C670 Practice for Preparing Precision and Bias Statements for Test Methods for Construction Materials

E177 Practice for Use of the Terms Precision and Bias in ASTM Test Methods

E456 Terminology Relating to Quality and Statistics

E691 Practice for Conducting an Interlaboratory Study to Determine the Precision of a Test Method

E1732 Terminology Relating to Forensic Science

E2808 Guide for Microspectrophotometry and Color Measurement in Forensic Paint Analysis

2.2 *ANSI/NIST Standards:*[3]

ANSI/NIST-ITL 1-2011 Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information

NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response

NIST SP 800-88 Guidelines for Media Sanitization

2.3 *ISO Standards:*[4]

ISO 9000 Quality Management

ISO/IEC Guide 2:2004 Standardization and Related Activities — General Vocabulary

ISO/IEC 19794-5 Information Technology — Biometric Data Interchange Formats — Part 5: Face Image Data

2.4 *IEEE Standards:*[5]

IEEE 100-2000 The Authoritative Dictionary of IEEE Standards Terms, 7th Edition

2.5 *ASCLD/LAB Publication:*[6]

ASCLD/LAB International Supplemental Requirements (Testing), 2011 Edition

3. Significance and Use

3.1 This terminology includes general as well as discipline-specific definitions as they apply across the spectrum of image analysis, computer forensics, video analysis, forensic audio, and facial identification.

4. Terminology: Terms and Definitions

4.1 *Definitions:*

achievable resolution, resolving power, *n*—the measure of imaging system's practical limit to distinguish between separate adjacent elements, typically by imaging a known reference standard.

acquisition, *n—in computer forensics*, the process of using an access interface to read digital data from a digital source and to create a destination object.

ad hoc image, *n*—see **uncontrolled image**.

administrative review, *n*—a procedure used to check casework for consistency with agency/laboratory policy and editorial practice.

allocated space, allocated storage, *n—in computer forensics*, the portions of storage that are assigned or reserved for active instructions or for data.

IEEE 100-2000, (C) 610.10-1994w

[1] This terminology is under the jurisdiction of ASTM Committee E30 on Forensic Sciences and is the direct responsibility of Subcommittee E30.12 on Digital and Multimedia Evidence.

Current edition approved June 1, 2013. Published July 2013. DOI: 10.1520/E2916-13.

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[4] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036, http://www.ansi.org.

[5] Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., Piscataway, NJ 08854, http://www.ieee.org.

[6] Available from American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD/LAB), 139 J Technology Drive, Garner, NC 27529, http://www.ascld-lab.org.

anthropometric analysis, *n—in facial identification*, an explicit measurement of landmarks on a face and a comparison of these measurements between two samples.

anti-forensics, *n*—the application of a process to modify, conceal or destroy information to inhibit or prevent the effectiveness of forensic science examinations.

archive, *n*—data stored for long-term availability and retrieval.

archive, *v*—to store data in a manner suitable for long-term availability and retrieval.

archive image, *n—in computer forensics*, a **bit stream** duplicate of data placed on media that is suitable for long-term storage

artifact, *n*—a by-product, artificial feature, or change resulting from human activity or a technical process. (Compare **noise**).

DISCUSSION—Examples include speckles in a scanned picture, "blocking" in compressed images, distortion in over-saturated audio, and the automatic creation of temporary files due to normal usage of a computer.

aspect ratio, *n*—the ratio of the width to the height of a rectangle, such as an image, a pixel, or an active video frame.

attempt, *n—in facial identification*, a submission of a single set of biometric samples to a biometric system for identification or verification. (Compare **biometric search**).

audio enhancement, *n*—the processing and filtering of audio recordings to improve the signal quality and intelligibility of the signals of interest, such as speech, by attenuating noise or otherwise increasing the signal-to-noise ratio.

authentication, *n*—(*1*) the process of substantiating that the asserted provenance of data is true; (*2*) the process of substantiating that data are accurate representations of what they are purported to be.

backlight, *n—in facial identification*, a light source placed behind a subject in a controlled capture that reduces background shadows.

backlit, *adj*—a characteristic of a subject or an object that is illuminated from behind.

batch mode search, *n—in facial identification*, a mode of searching records in an automated system in which a group of probes are simultaneously or sequentially launched.

batch search mode, *n*—see **batch mode search**.

bias, *n*—the difference between the expectation of the test results and an accepted reference value.

E177, E456, E691, C670

binning, *n—in facial identification*, (*1*) any technique used by a facial recognition (FR) system to organize or optimize searching based upon some piece(s) of metadata; (*2*) the process of parsing (examining) or classifying data to accelerate or improve biometric matching.

biometric match, *n—in facial identification*, determination that two samples correspond to the same source based on some level of computer-evaluated similarity.

DISCUSSION—Does not inherently imply that the probe and candidate is the same person.

biometrics, *n*—(*1*) a set of measureable anatomical, physiological, or behavioral characteristic that can be used to discriminate members of a population; (*2*) collectively, a set of automated processes used to discriminate members of a population using measureable anatomical, physiological, behavioral characteristics, or combinations thereof.

biometric search, *n*—the submission of a biometric reference as a probe against a biometric system for identification (one-to-many) or verification (one-to-one). (Compare **attempt**).

bit stream, *n*—a continuous stream of bits transmitted over a channel with no separators between the character groups.

IEEE 100-2000, (C) 610.7-1995, 610.10-1994w

bit stream duplicate, *n—in computer forensics*, an exact, bit-for-bit reproduction of all data objects independent of any physical media upon which that data is stored. (Compare **copy**).

cache, *n—in computer forensics*, a temporary storage area set aside on a processor, in memory, or in a filesystem to keep frequently needed data readily available, designed to speed up processing and improve performance.

capture, *n*—(*1*) the process of recording data such as an image, video sequence, or audio stream; (*2*) *in facial identification*, the process of collecting a biometric sample from an individual via a sensor.

capture, *v*—to record data, such as an image, video sequence, audio stream, or biometric sample to digital storage, often by means of a sensor.

capture card, frame grabber, *n*—a piece of computer hardware that accepts an analog or digital signal and outputs the signal as digital data.

capture device, *n*—device used in the recording of data.

carve, *v—in computer forensics*, to extract a portion of data for the purpose of analysis.

certification authority, *n*—(*1*) *in computer forensics*, a trusted third party entity that issues digital certificates certifying the ownership of a public key by the subject named in the certificate, and trusted by both entities engaged in a digital transaction; (*2*) *in facial identification*, a body that issues biometric documents and certifies that the data stored on the documents are genuine.

chain of custody, *n*—the procedures and documents that account for the possession of a sample by tracking its handling and storage from its point of collection to its final disposition.

E1732

clarification, *n*—see **enhancement**.

clarify, *n*—see **enhance**.

class characteristics, *n—in facial identification and image analysis*, characteristics common to many objects or individuals (for example, the color, make, or model of objects, and for faces, the overall shape of the nose, eyes, or mouth).

clear, *v—in computer forensics*, to overwrite storage space on a medium with non-sensitive data, which may include overwriting not only the logical storage location of files, but may include all addressable locations. **NIST SP 800-88**

cluster, *n—in computer forensics*, a group of contiguous sectors on storage media, typically the smallest unit of allocation in a filesystem.

codec, *n*—an algorithm to encode and decode digital data, typically to reduce the amount of data for transmission or storage.

DISCUSSION—A codec is not a storage format, but may be required to interpret stored data.

cognitive bias, *n*—(*1*) a mental error caused by one's simplified information processing strategies; it does not result from any emotional or intellectual predisposition toward a certain judgment but rather from subconscious mental procedures for processing information; (*2*) a mental error that is consistent and predictable; (*3*) a set of influences that may affect the reliability and validity of one's observations and conclusions.

cognitive image analysis, *n—in image and video analysis*, a process used to extract visual information from an image by human evaluation.

colorimetry, *n*—the conversion of instrumental light measurements into psychophysical descriptions or numerical notations that can be correlated with visual evaluations of color and color differences. **E2808**

color range, *n*—see **gamut**.

competency test, *n*—an evaluation of a person's knowledge and ability before performing independent work in forensic casework. **ASCLD/LAB**

composite video signal, *n*—a single analog video signal that combines a base-band luminance signal with color information by modulating a subcarrier with chroma signals, typically using one of the National Television System Committee (NTSC), Phase Alternating Line (PAL), or Sequential Color with Memory (SECAM_ systems.

compression, *n*—a process to reduce the size of a data file or stream while attempting to retain the original semantic meaning of that data.

compression ratio, *n*—the ratio of the size of the data before compression to that of after compression.

computer forensics, *n*—the scientific examination, analysis, or evaluation of digital evidence in legal matters.

conclusion, *n*—a position reached after consideration of a set of facts or examination results.

confirmation bias, *n*—the tendency to search for data or interpret information in a manner that supports one's preconceptions.

contextual bias, *n*—a deviation in human judgment caused by factors external to the data that is logically relevant to the decision at hand.

control, *n*—material of established origin that is used to evaluate the performance of a test or comparison. **E1732**

controlled image, *n—in facial identification*, a photographic image captured in accordance with facial identification (FI) or facial recognition (FR) standards or guidelines (for example, a driver's license photo).

copy, *v*—to reproduce information with some level of accuracy.

DISCUSSION—Depending on the process used, copying might result in the loss of data. (Compare **bit stream duplicate**).

CSI effect, *n*—perception of the near infallibility of forensic science in response to popular media.

data, *n*—information in analog or digital form that can be transmitted or processed.

data file, *n*—a file consisting of stored data (that is, text, numbers, graphics, etc.) as compared to a program file of commands and instructions for a digital device.

deblur, *v*—to restore an image by attempting to reverse degradation caused by blur.

decryption, *n*—a process to return encrypted data to its original unencrypted condition.

deinterlace, *v*—to separate an interlaced video frame into its two discrete fields.

demonstrative comparison, *n—in video analysis*, a method of presenting similarities or differences, or both among images or objects, or both without rendering an opinion regarding identification or exclusion.

depth of field, *n*—the distance that is in focus (sharp) when capturing an image based upon the camera and lens, and their settings.

digital device, *n*—electronic equipment which can create, process or store digital data.

digital evidence, *n*—information of probative value that is stored or transmitted in binary form.

digital image, *n—in image analysis*, a photographic image that is represented by discrete numerical values organized in a two-dimensional array.

Focal Encyclopedia of Photography[7]

digital object, *n*—a collection of logically related information.

digital source, *n*—a container of digital data that can be acquired by an acquisition tool.

[7] *Focal Encyclopedia of Photography*, 3rd edition, Richard D. Zakia and Leslie Stroebel, Eds., Focal Press, 1996.

digital video recorder, DVR, *n*—a stand-alone embedded system or a computer-based system for recording video and, optionally, audio data.

digital zoom, *n*—a digital camera function that simulates an optical zoom by cropping and enlarging a digital image without increasing the resolution or detail.

directory, *n—in computer forensics*, an object or structure used to group files together within a filesystem.

directory listing, *n—in computer forensics*, a list of files and, optionally, file properties contained within a filesystem.

download, *v*—(*1*)*in audio, image, and video analysis*, to retrieve audio, video, image, or transactional data from a recording device (for example, DVR system); (*2*) *in computer forensics*, to receive data from another digital source.

dynamic range, *n*—(*1*) *in image analysis*, the difference between the brightest highlight and darkest value that a sensor can detect and record in a single image; (*2*) *in audio and video analysis*, the ratio of the strongest (undistorted) signal to that of the weakest (discernible) signal in a unit or system as expressed in decibels (dB); (*3*) a way of stating the maximum signal-to-noise ratio.

enhance, *v—in audio, image, and video analysis*, to improve the perceptual recognition or quality of a signal of interest.

enhancement, *n—in audio, image, and video analysis*, the process of improving the perceptual recognition or quality of a signal of interest.

enroll, *v*—to capture a biometric sample, extract the relevant features, convert them to a template, and use it to form a reference for matching.

DISCUSSION—Enrollment most often is performed to populate a gallery, but it can also refer to the creation of a probe.

export, *n*—see **download** (*1*).

extraction, *n*—any method of exporting data from a source.

face detection, *n—in facial identification*, the automated determination of the locations and sizes of human faces in digital images.

face recognition, *n—in facial identification*, (*1*) in automated systems, the automated searching of a facial image as a probe in a biometric system (one-to-many), typically resulting in a group (candidate list) of facial images being returned to a human operator in ranked order based on system-evaluated similarity for a decision; (*2*) *by humans*, the mental process by which an observer identifies a person as being one they have seen before.

facial examination, *n—in facial identification*, the formal systematic comparison of two images to determine if the same person is depicted in both.

facial identification, FI, *n*—the manual, one-to-one examination of the differences and similarities between two images of human faces, or a live subject and a single image, for the purpose of determining if they represent the same person.

facial mapping, *n—in facial identification*, the process of landmarking defined anthropological points.

facial recognition, FR, *n*—see **face recognition**.

facial review, *n—in facial identification*, (*1*) the review of a facial recognition (FR) system candidate list to identify a possible match; (*2*) the one-to-one comparison (verification) conducted in a high-throughput environment (for example, border crossing).

feature, *n—in facial identification and image analysis*, (*1*) an observable class or individual characteristic; (*2*) a component of biometric templates.

field, *n—in video analysis*, a set of odd or even scan lines comprising one half of an interlaced video frame.

DISCUSSION—For interlaced video, the scanning pattern is divided into two sets of spaced lines (odd and even) that are displayed sequentially. Each set of lines is called a field, and the interlaced set of the two sets of lines is a frame.

file, *n—in computer forensics*, a collection of information logically grouped into a single object and referenced by an identifier, such as a filename

file format, *n—in computer forensics*, a standard structure by which data is organized in a file for a specific purpose.

file header, *n—in computer forensics*, the data within a file that contains identifying information about the file and possibly metadata with information about the file contents.

filename, *n—in computer forensics*, an identifier used to uniquely identify a file object within a directory object in a filesystem.

file slack, *n—in computer forensics*, the data between the logical end of a file and the end of the last storage unit for that file.

filesystem, file system, *n—in computer forensics*, a specified method for naming, storing, organizing, and accessing files on logical volumes.

fixed focal length lens, prime lens, *n*—a lens with a focal length that is not adjustable.

focal length, *n*—the distance from the optical center of a lens to its point of focus at the sensor or image plane when focused at infinity.

forensic, *adj*—the use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime.

forensic audio, *n*—the scientific examination, analysis, comparison, or evaluation of audio.

forensic cloning, *v*—creating a **bit stream duplicate** of the available data from one physical media to another.

forensic image, *n*—see **image**.

forensic wipe, *n—in computer forensics*, a verifiable procedure for sanitizing a defined area of digital media by overwriting each byte with a known value.

format, *n*—the structure by which data are organized on a device.

DISCUSSION—A format can refer to a physical medium, a type of signal, a file format, encoding parameters, or combinations thereof.

format, *v*—to prepare a hard disk or a removable data storage device to enable data storage using a specified filesystem or data structure.

format conversion, *n—in audio, image, and video analysis*, the transfer of audio or video information, or both, from one format to another.

frame, *n—in video analysis*, the lines of spatial information of a video signal.

DISCUSSION—For interlaced video, a frame consists of two fields, one of odd lines and one of even lines, displayed in sequence. For progressive scan (non-interlaced) video, the frame is written through successive lines that start at the top left of the picture and finish at the bottom right.

free space, *n*—see **unallocated space**.

frontal pose, *n—in facial identification*, a facial image captured from directly in front of the subject with the focal plane approximately parallel to the plane of the subject's face.

gallery, *n—in facial identification*, a FR system's database, which typically contains all known-person biometric references (samples or templates, or both).

gamut, *n*—the portion of the colorspace that can be represented or reproduced by a device or process.

Gaussian blur, *n—in image and video analysis*, a function typically used to reduce image noise and detail using a specific mathematical function known as the "Gaussian Kernel" or "bell-curve."

guideline, *n*—recommended practice that allows some discretion or leeway in its interpretation, implementation, or use.

hash, hash value, *n*—a string of numerical values used to substantiate the integrity of digital evidence or for inclusion/exclusion comparisons against known value sets or both.

hashing function, *n*—an established mathematical calculation that generates a numerical value based on input data.

hidden data sector, *n—in computer forensics*, a sector in the current configuration of a drive that cannot be accessed by read and write commands without changing the drive configuration. Discussion—Sectors in a host protected area would be hidden data sectors.

histogram, *n*—a graph of a frequency distribution in which rectangles with bases on the horizontal axis are given widths equal to the class intervals and heights equal to the corresponding frequencies.

DISCUSSION—In digital images, a histogram is frequently used to document the number of pixels of a given brightness value (for example, 0-255).

holistic comparison, *n—in facial identification*, a process of comparing faces by looking at the face as a whole and not the component parts in isolation.

hot spot, *n—in facial identification*, a bright area of light reflecting on a face that reduces the visibility of features.

identification, *n*—(*1*) a classification process intending to discriminate individual members of a set; (*2*) the conclusion that the sources of two samples cannot be distinguished from each other; (*3*) in computer forensics, a process involving the search for, recognition and documentation of potential digital evidence; (*4*) in facial identification, a task in which a biometric system searches a database for a reference matching a submitted biometric sample and, if found, returns a corresponding identity. (Compare **individualization**).

identity, *n—in facial identification*, the collective set of biographic data, images, and templates assigned to one person within a biometric system.

image, *v—in computer forensics*, to create a bit stream duplicate of the original data.

image, *n*—(*1*) *in image and video analysis*, an imitation or representation of a person or thing drawn, painted, or photographed; (*2*) *in computer forensics*—see bit stream duplicate.

image analysis, *n*—the application of image science and domain expertise to examine and interpret the content of an image, the image itself, or both in legal matters.

image averaging, *n—in image and video analysis*, the process of averaging similar images, such as sequential video frames, to reduce noise in stationary scenes.

image comparison, photographic comparison, *n—in image analysis*, the process of comparing images of questioned objects or persons to known objects or persons or images thereof and making an assessment of the correspondence between features in these images for rendering an opinion regarding identification or elimination.

image content analysis, *n—in image analysis*, the drawing of conclusions about an image and targets for content analysis include, but are not limited to, the subjects/objects within an image; the conditions under which, or the process by which, the image was captured or created; the physical aspects of the scene (for example, lighting or composition); or the provenance of the image.

image data recovery, *n—in image analysis*, the process of retrieving viewable image(s) from a data set.

image enhancement, *n*—any process intended to improve the visual appearance of an image or specific features within an image.

image output, *n—in image analysis*, a means by which an image is presented for examination or observation.

image processing, *n—in image analysis*, any activity that transforms an input image into an output image.

image processing log, *n—in image analysis*, a record of the steps used in the processing of an image.

image registration, *n*—the process by which two images are aligned with each other using a geometric transformation.

image restoration, *n*—see **restoration**.

image synthesis, *n—in image and video analysis*, any process that renders an image, using computer graphics techniques, for illustrative purposes (that is, age progression, facial reconstruction, and accident/crime scene reconstruction).

imaging technology, *n—in image and video analysis*, any system or method used to capture, store, process, analyze, transmit, or produce an image.

DISCUSSION—Such systems include film, electronic sensors, cameras, video devices, scanners, printers, computers, and so forth.

image transmission, *n—in image and video analysis*, an act of moving images from one location to another.

individualization, *n—theoretically*, a determination that two samples derive from the same source; practically, a determination that two samples derive from sources that cannot be distinguished within the sensitivity of the comparison process. (Compare **identification**.)

DISCUSSION—Theoretical individualization is the asymptotic upper bound of the sensitivity of a source identification process.

individual characteristic, *n*—a measurable feature that differentiates a single member of a set from every other member of that set. (Compare **class characteristic**.)

integrity verification, *n*—a process of confirming that the data presented is complete and unaltered since time of acquisition.

intermediate storage, *n*—any media or device on which data is temporarily stored for transfer to permanent or archival storage.

interlaced scan, *n*—in video analysis, a technique of combining two television fields to produce a full frame in which the two fields are composed of only odd and only even lines that are displayed one after the other but with the physical position of all the lines interleaving each other, hence, interlace. **CCTV**[8]

interpolation, *n*—the estimation of the value of a sampled function at an arbitrary ordinal using the closest samples.

known image, *n—in facial identification and image analysis*, an image of an individual or object associated with a known or claimed identity or object and recorded electronically or by other medium (also known as exemplars). (Compare **questioned image**).

levels of conclusion, *n—in facial identification*, a verbal or numeric scale that indicates the level of confidence regarding identification or exclusion of a subject.

lights out, *n—in facial identification*, an automated conclusion based upon threshold scores with no human involvement.

log file, *n*—a record of actions, events, and related data.

logical acquisition, logical copy, *n—in computer forensics*, an accurate reproduction of information contained within a logical volume (for example, mounted volume, logical drive assignment, and so forth).

DISCUSSION—Logical acquisitions or copies may not reproduce deleted data, or data otherwise not accessible easily by a user.

logical volume, *n*—in computer forensics, a partition or a collection of partitions acting as a single entity that has been formatted with a filesystem. **NIST SP 800-86**

lossless compression, *n*—a data reduction process that is completely reversible, such that all of the original data can be retrieved in its original form.

lossy compression, *n*—a data reduction process that is not completely reversible, and some original data is irretrievably lost.

match, *v*—see **identification**.

media, storage media, *n*—objects on which data can be stored.

media characterization, *n*—the process of inspecting, identifying, and noting the properties of media.

memory, *n—in computer forensics*, (*1*) hardware used for the temporary storage of operating instructions and data while a digital device is running; (*2*) see **random access memory**.

metadata, *n*—data, frequently embedded within a file, that describes a file or directory.

mobile phone forensics, *n*—for legal purposes, the utilization of scientific methodologies to recover data stored by a cellular device.

morphological analysis, *n—in facial identification*, direct comparison of class and individual facial characteristics without explicit measurement.

multimedia evidence, *n*—analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and the information contained therein.

multiplex, *v*—to combine multiple signals into a single signal which can later be separated.

native file format, *n*—the original format of a file.

network, *n*—a group of two or more computers or other digital devices that communicate with each other electronically to transfer and share data.

network traffic, *n*—network communications that are carried over wired or wireless networks between hosts or devices.

noise, *n*—a part of a signal that is not the target signal.

DISCUSSION—In audio, image, and video signals, sources of noise can include film grain, electronic variations in the input device sensor and circuitry, and stray electromagnetic fields in the signal pathway.

nominal resolution, *n*—the number of horizontal and vertical pixels an imaging system or sensor is capable of capturing. **Focal Encyclopedia of Photography**[7]

normal lens, *n*—a lens designed to approximate the field of view of the human eye without magnification or reduction.

[8] Damjanovski, V., *CCTV: Networking and Digital Technology*, 2nd edition, Butterworth-Heinemann, 2000.

occlusion, *n—in facial identification*, the obscureness of features (that is, features blocked by sunglasses or objects in the environment, such as a tree).

operating system, *n*—a specific set of programs that run on a computer or other digital device and provides a software platform for the device to function and on which other programs can run. **NIST SP 800-86**

original image, *n*—an accurate and complete replica of the primary image, irrespective of media.

DISCUSSION—For film and analog video, the primary image is the original image.

partition, *n—in computer forensics*, a logical portion of a media that functions as though it were physically separate from other logical portions of the media. **NIST SP 800-86**

password recovery, *n—in computer forensics*, the process of locating and identifying a series of characters used to restrict access to data or a system.

peer review, *n*—(*1*) the review of a paper submitted to a scientific journal by an equally competent independent party to evaluate the methods, claims, and conclusions before publication; (*2*) see **technical review**.

peripheral, *n—in computer forensics*, a hardware device connected externally to a computer or other digital device that adds more functionality.

perspective, *n—in image and video analysis*, camera-to-subject geometry, including both camera-to-subject distance and orientation of the camera relative to the subject.

perspective distortion, *n—in image and video analysis*, a warping or transformation of an object's appearance in an image introduced by insufficient subject to camera distance (for example, larger nose or smaller ears).

photo-anthropometry, *n—in facial identification*, the application of anthropometric analysis to images.

photogrammetric analysis, *n*—process of obtaining dimensional information regarding objects and people depicted in an image.

photogrammetry, *n*—the art, science, and technology of obtaining reliable information about physical objects and the environment through the processes of recording, measuring, and interpreting photographic images and patterns of electromagnetic radiant energy and other phenomena.
The Manual of Photogrammetry[9]

photographic comparison, *n—in image analysis and facial identification*, the assessment of the correspondence between features in images and known objects or images for the purpose of rendering an opinion regarding identification, elimination, or a qualified conclusion (as opposed to a demonstrative exhibit).

photometry, *n—in image analysis*, the measurement of light values of objects in an image.

physical copy, *n—in computer forensics*, an accurate reproduction of information contained on a physical digital data storage device.

physical image, *n—in computer forensics*, a **bit stream duplicate** of data contained on a physical digital data storage device.

pitch, *n—in facial identification*, rotation in degrees about the (horizontal) X-axis. **ISO/IEC 19794-5**

DISCUSSION—Frontal poses have a pitch angle of 0°. Positive angles represent faces looking down (a counter-clockwise rotation around the X-axis).

playback, *v*—recorded material viewed and heard as recorded, facilitated by camcorder, cassette recorder, or other device.

playback optimization, *n—in audio and video analysis*, the process of determining the most suitable equipment and settings for producing the highest quality output signal.

pose, *n—in facial identification*, the orientation of the face with respect to the camera, consisting of pitch, roll, and yaw.

preservation, *n—in computer forensics*, a process undertaken to maintain the integrity of potential digital evidence.

primary image, *n*—the first instance in which an image is recorded onto any media that is a separate, identifiable object.

DISCUSSION—Examples include a digital image recorded on a flash card or a digital image downloaded from the internet.

probe, *n—in facial identification*, a facial image or template searched against the gallery in a facial recognition (FR) system.

processed image, *n—in image and video analysis*, any image that has undergone enhancement, restoration, or other operation.

production switcher, *n—in forensic audio and video analysis*, a device or software or both used to mix video or audio signals or both from two or more sources. (Compare **routing switcher**.)

proficiency test, *n*—test to evaluate analysts, technical support personnel, or the quality performance of an organization.

DISCUSSION—Four examples are:

(*1*) *Open test*—Analyst(s) and technical support personnel are aware they are being tested.

(*2*) *Blind test*—Analyst(s) and technical support personnel are not aware they are being tested.

(*3*) *Internal test*—Conducted by the organization itself.

(*4*) *External test*—Conducted by an organization independent of the organization being tested.

program, *n—in computer forensics*, a list of coded instructions causing a computer to perform a specific task or set of tasks.

progressive scan, *n—in video analysis*, a display scan pattern in which each line of the frame is scanned out sequentially.

proprietary file format, *n*—any file format that is unique to a specific manufacturer or product.

[9] *Manual of Photogrammetry*, 4th edition, ASPRS, 1980.

protocol, *n—in computer forensics*, a set of conventions governing the format and timing of message exchanges to control data movements and correct errors.

quality assurance, *n*—all the planned and systematic activities implemented within the quality system, and demonstrated as needed, to provide adequate confidence that an entity will fulfill requirements for quality.

ISO/IEC Guide 2:2004, E1732

quantitative image analysis, *n*—any process used to extract measurable data from an image.

questioned image, *n—in image analysis and facial identification*, an image of an individual or object whose identity is unknown or in question and has been recorded electronically or by other medium. (Compare **known image**).

random access memory, RAM, *n—in computer forensics*, volatile memory that can be written to as well as read, which can be used to execute operating instructions or store data for processing on a computer or device.

raw, *n—in image analysis*, a digital camera or scanner file format, usually proprietary, for minimally processed digital image data.

read only memory, ROM, *n—in computer forensics*, a memory device that is programmed with a permanent program or data that cannot be erased.

reconstruction, *n*—process of repairing damaged media to allow the retrieval of data.

registration, *n—in facial identification*, (*1*) the enrollment of an identity in an application using a biometric system; (*2*) see **image registration**.

relative frequency, *n—in facial identification*, a measure of how often facial features or combinations thereof occur in a given population.

reproducibility, *n*—the extent to which a process yields the same results on repeated trials.

residue, *n—in computer forensics*, (*1*) data that are contained in unallocated space or file slack; (*2*) data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place. **NIST SP 800-88**

resolution, *n—in facial identification*, image and video analysis, a measure of the limit of an imaging system's capability to distinguish between two separate but adjacent stimuli, such as elements of spatial detail in an image, or similar colors.

restoration, *n*—(*1*) *in computer forensics*, the process of restoring data from an image; (*2*) *in image and video analysis*, any process applied to an image that has been degraded by a known cause (for example, defocus or motion blur) to remove partially or totally the effects of that degradation.

roll, *n—in facial identification*, a rotation in degrees about the z-axis (the horizontal axis from front to back).

ISO/IEC 19794-5

DISCUSSION—Frontal poses have a roll angle of 0°. Positive angles represent faces tilted toward their right shoulder (counter-clockwise rotation around the X-axis). A roll angle of 0° denotes that the left and right eye centers have identical Y coordinates.

routing switcher, *n—in forensic audio and video analysis*, device or software or both used to direct the path of one or more signals into one or more devices. (Compare **production switcher**.)

search, *v—in facial identification*, to compare a probe against a gallery.

search result set, *n—in facial identification*, a candidate list returned from a search.

sharpening, *n—in image and video analysis*, a process used to emphasize edge detail in an image by enhancing the high-frequency components.

source code, *n*—list of instructions written in a programming language used to construct a computer program.

spoofing, *n—in facial identification*, the process by which an imposter intentionally attempts to be recognized as another person in a biometric system or intentionally attempts to be missed as an existing identity in the gallery.

standard conversion, *n—in video analysis*, the transformation of one television system signal to another, for example, National Television System Committee (NTSC) to Phase Alternating Line (PAL).

storage, *n—in computer forensics*, retrievable retention of data; electronic, electrostatic, or electrical hardware or other media into which data may be entered, and from which data may be retrieved.

storage media, *n*—any object on which data is preserved.

subdirectory, *n—in computer forensics*, a directory object contained within another directory object in a filesystem.

subject acquisition profile, *n—in facial identification*, the facial image capture criteria described in ANSI/NIST-ITL 1-2011.

superimposition, *n*—use of a registered overlay as an aid to comparison.

system bias, *n*—(*1*) errors repeatedly introduced through automation (for example, errors in template generation or comparison); (*2*) errors repeatedly introduced through operational practices in an organization or unit (for example, improper lighting or camera position guidance).

system time, *n—in computer forensics*, the time generated by the system clock and used by the operating system.

technical review, *n*—the evaluation conducted by a second qualified individual of reports, notes, data, conclusions, and other documents.

template, *n—in facial identification*, a set of biometric measurement data prepared by a facial recognition (FR) system from a facial image.

third-party imagery, *n—in facial identification*, images used in facial recognition (FR) or facial identification (FI) that were not captured by the agency performing the comparison (for example, family snapshots of a missing person).

time-base corrector, TBC, *n—in video analysis*, a electronic device used to correct timing inconsistencies, stabilize, and synchronize video signals for optimum quality.

timed expiry, *n—in video analysis*, a feature of digital video recorders (DVRs) that allows the equipment to adhere to data retention policies that may be mandated in certain parts of the world which results in video data becoming inaccessible after a certain date.

time-lapse video recording, *n*—process by which images are recorded at less than the standard rate of frames per second (National Television System Committee (NTSC) – 29.97; Phase Alternating Line (PAL) – 25.00) thus extending the period of time that can be covered by the storage medium.

timeline sequence reconstruction, *n*—process of relating images, audio, or other data to one another in a chronologically ordered succession.

timestamp, *n—in computer forensics*, a point in time with respect to system time used by a file system to annotate creation, access or modification of file system objects.

traditional enhancement technique, *n—in image analysis*, a technique that has a direct counterpart in traditional darkroom photography.

unallocated space, *n—in computer forensics*, (*1*) areas on storage media which a file system has marked as available for use for data storage; (*2*) the portions of storage media that are unassigned external to a file system.

DISCUSSION—The area may already contain previously stored information. Also referred to as free space.

uncontrolled image, ad hoc image, *n—in facial identification*, an image not captured in accordance with facial identification/facial recognition (FI/FR) standards or guidelines (for example, a surveillance image). (See **image**.)

validation, *n*—the confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

ISO 9000:2005(E), E1732

DISCUSSION—(*1*) The term "validated" is used to designate the corresponding status; (*2*) the use conditions for validation can be real or simulated.

validation test, *n*—an evaluation to determine if a tool, technique, or procedure functions correctly and as intended.

variable focal length lens, zoom lens, *n*—a lens having a focal length that can be continuously changed between set limits.

vectorscope, *n—in video analysis*, an electronic device that measures the chrominance (color) performance of a video signal.

verification, *n*—(*1*) a review and independent analysis of the conclusion of another examiner; (*2*) confirmation that a tool, technique, or procedure performs as expected; (3) process of confirming the accuracy of an item to its original; (*4*) in facial identification, the process of conducting a one-to-one comparison in a biometric system. (See **verification** in ISO 9000:2005(E) and E1732.)

video analysis, *n*—the scientific examination, comparison, or evaluation of video in legal matters.

video enhancement, *n*—any process intended to improve the visual appearance of video sequences or specific features within video sequences.

video stabilization, *n*—the process of positioning individual frames so that a selected object or person will remain in the same location as the video is played.

volatile data, *n—in computer forensics*, data on a live system or digital device that is lost after the device is powered down.

waveform monitor, *n—in video analysis*, an electronic device that provides a graphic display of a video signal.

work copy, working copy, *n*—a copy of a recording or data that can be used for subsequent processing or analysis or both.

write block, write protect, *v*—to prevent the content of storage media from being modified.

write blocker, *n*—a hardware or software method, or both that prevents the modification (addition, deletion, or alteration) of media content.

yaw, *n*—in facial identification, a rotation in degrees about the Y-axis (vertical axis). **ISO/IEC 19794-5**

DISCUSSION—Frontal poses have a yaw angle of 0°. Positive angles represent faces looking to their left (a counter-clockwise rotation around the Y-axis).

5. Arconyms

5.1 *Acronyms:*

AFR, *n*—automated facial recognition

CCD, *n*—charge coupled device

CD, *n*—compact disc

codec, *n*—coder/decoder or compressor/decompressor

DMV, *n*—Department of Motor Vehicles or Division of Motor Vehicles

DVD, *n*—digital versatile disc

DVR, *n*—digital video recorder

FI, *n*—facial identification

FR, *n*—facial recognition

GSM, *n*—Global System for Mobile Communications, originally Groupe Spécial Mobile

JPEG, *n*—Joint Photographic Experts Group

LZW, *n*—Lempel-Ziv-Welch

NTSC, *n*—National Television System Committee, also referred to as National Television Standards Committee

PAL, *n*—phase alternating line

SAP, *n*—subject acquisition profile

6. Keywords

6.1 computer forensics; definitions; digital evidence; facial identification; forensic audio; image analysis; multimedia; terminology; video analysis

BIBLIOGRAPHY

(1) Joint Publication from the Scientific Working Group on Digital Evidence (SWGDE) and the Scientific Working Group on Imaging Technology (SWGIT), *SWGDE and SWGIT Digital and Multimedia Evidence Glossary*, Version 2.6.

(2) Facial Identification Scientific Working Group (FISWG), *Glossary, Version 1.1*.

(3) Newton, H., *Newton's Telecom Dictionary*, Flatiron Publishing, 2007.