



Designation: **E2916—13 E2916 – 18**

Standard Terminology for Digital and Multimedia Evidence Examination¹

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.

1.3 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

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~~

2.1 ANSI/NIST Standards:²

~~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~~

2.2 IEEE Standards:³

~~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.

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~~ Nov. 1, 2018. Published ~~July 2013~~ November 2018. Originally approved in 2013. Last previous edition approved in 2013 as E2916 – 13. DOI: ~~10.1520/E2916-13~~ 10.1520/E2916-18.

² Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, <http://www.nist.gov>.

³ Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., Piscataway, NJ 08854, <http://www.ieee.org>.

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

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.

candidate list, *n*—*in facial identification*, a rank ordered list generated from a facial recognition search.

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**. iteh.ai/catalog/standards/sist/f1288546-4a71-47fb-8d5e-5d9906a36eca/astm-e2916-18

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 Photography⁴

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.

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.

⁴ *Focal Encyclopedia of Photography*, 3rd edition, Richard D. Zakia and Leslie Stroebel, Eds., Focal Press, 1996.

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.

examiner, *n*—*in facial identification*, an individual whose role it is to perform a **facial examination**.

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 presence of human faces in digital images.

face recognition, *n*—*in facial identification*, (1) *inby automated systems*, the automated searching of a facial image as a probe in a biometric facial recognition 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; similarity; (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, comparison, *n*—*the manual, one-to-one in facial identification*, examination of the differences and similarities between two images of human faces, or a manual process to identify similarities or dissimilarities between two (or more) facial images or facial image(s) and a live subject and a single image, for the purpose of determining if they represent the same person or different person.

facial mapping, examination, *n*—*in facial identification*, the process of a formal systematic landmarking defined facial comparison. anthropological points.

facial identification, FI, *n*—the discipline of image-based comparisons of human facial features.

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

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

facial review, *n*—*in facial identification*, (an)1) the review of a facial recognition (FR) system candidate list to identify a possible match; (2) adjudication of a 2candidate) the list. 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~~^{subject's} face.

gallery, *n*—*in facial identification*, a FR ~~system~~^{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.