



Standard Guide for Education and Training in Computer Forensics¹

This standard is issued under the fixed designation E2678; 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 guide will improve and advance computer forensics through the development of model curricula consistent with other forensic science programs.

1.2 Section 4 describes the alternative paths by which students may arrive at and move through their professional training. Sections 5 through 7 cover formal educational programs in order of increasing length: a two- year associate degree, a four-year baccalaureate degree, and graduate degrees. Section 8 provides a framework for academic certificate programs offered by educational institutions. Section 9 outlines model criteria and implementation approaches for training and continuing education opportunities provided by professional organizations, vendors, and academic institutions.

1.3 Some professional organizations recognize computer forensics, forensic audio, video, and image analysis as subdisciplines of computer forensics. However, the curricula and specific educational training requirements of subdisciplines other than computer forensics are beyond the scope of this guide.

1.4 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Terminology

2.1 Definitions of Terms Specific to This Standard:

2.1.1 *assembler*, *n*—software that translates a low-level program into a form that can be executed by a computer.

2.1.2 *capstone project*, *n*—design and implementation-oriented project typically completed during the final year of a degree program that requires students to apply and integrate knowledge and skills gained from several courses.

2.1.3 *central processing unit (CPU)*, *n*—computer chip that interprets commands and runs programs.

2.1.4 *compiler*, *n*—software that translates a high- level program into a form that can be executed by a computer.

2.1.5 *digital forensics*, *n*—science of identifying, collecting, preserving, documenting, examining, and analyzing evidence from computer systems, the results of which may be relied upon in court.

2.1.6 *cryptography*, *n*—using the sciences of encryption to transform data to hide its information content and decryption to restore the information to its original form.

2.1.7 *data fusion*, *n*—process of associating, correlating, and combining data and information from single and multiple sources.

2.1.8 *debugger*, *n*—software that is used to find faults in programs.

2.1.9 *demultiplexing*, *v*—process of isolating individual images from a video flow.

2.1.10 *digital evidence*, *n*—information of probative value that is stored or transmitted in binary form that may be relied upon in court.

2.1.11 *computer forensics*, *n*—science of identifying, collecting, preserving, documenting, examining, and analyzing evidence from computer systems, networks, and other electronic devices, the results of which may be relied upon in court.

2.1.12 *distributed denial of service (DDoS)*, *n*—intentional paralyzing of a computer or a computer network by flooding it with data sent simultaneously from many locations.

2.1.13 *Electronic Communications Privacy Act (ECPA)*, *n*—regulates interception of wire and electronic communications (18 USC §2510 et seq.) and retrieval of stored wire and electronic communications (18 USC §2701 et seq.).

2.1.14 *embedded device*, *n*—special-purpose computer system that is completely encapsulated by the device it controls.

2.1.15 *enterprise system*, *n*—computer systems or networks or both integral to the operation of a company or large entity, possibly global in scope.

2.1.16 *ext2/ext3 (Linux-extended 2/Linux-extended 3) file system*, *n*—file system typically used with Linux-based operating systems.

2.1.17 *file allocation table (FAT) file system*, *n*—original file system used with Microsoft and IBM-compatible operating systems still in common use.

¹ This guide 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 Oct. 1, 2014. Published October 2014. Originally approved in 2009. Last previous edition approved in 2009 as E2678 – 09. DOI: 10.1520/E2678-09R14.