Designation: E2678 – 09

StandardGuide for Education and Training in Computer Forensics[1]

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 June 15, 2009. Published August 2009. DOI: 10.1520/E2678-09.

2.1.18 *intrusion detection system (IDS), n*—software or hardware that are used to identify attacks or anomalies on computers or networks or both.

2.1.19 *link analysis, n*—type of analysis often used by law enforcement that uses visual or other means of showing relationships between people, places, events, and things by linking them through timelines, telephone calls, emails, or any other consistent scheme.

2.1.20 *local area network (LAN), n*—computer network covering a local area such as a home, office, or small group of buildings, such as a college.

2.1.21 *malware, n*—malicious software designed to cause unexpected and frequently undesirable actions on a system (for example, viruses, worms, spyware, or Trojan horses).

2.1.22 *mock trial, n*—often referred to as "moot court," role-playing court proceedings intended to prepare students for courtroom testimony.

2.1.23 *new technology file system (NTFS), n*—advanced file system with security features commonly used with the Windows and all subsequent sytems.

2.1.24 *open system interconnect (OSI), n*—layered model that describes the way computers communicate on a network.

2.1.25 *personal area network (PAN), n*—networking scheme that enables computers and other electronic devices to communicate with each other over short distances either with or without wires.

2.1.26 *partitioning, v*—software method of dividing a physical hard drive into logical containers that will appear as multiple logical drives.

2.1.27 *peer to peer (P2P), n*—communications network that allows multiple computers to share files.

2.1.28 *personal electronic device (PED), n*—consumer electronic device that is typically mobile or handheld (for example, personal digital assistant (PDA), cell phone, or iPOD).

2.1.29 *photogrammetry, n*—science of obtaining dimensional information of items depicted in photographs.

2.1.30 *public key infrastructure (PKI), n*—system that uses encryption to verify and authenticate network transactions.

2.1.31 *random access memory (RAM), n*—computer's read/write memory; it provides temporary memory space for the computer to process data.

2.1.32 *redundant array of inexpensive/independent disks (RAID), n*—system that uses two or more drives in combination for fault tolerance or performance.

2.1.33 *steganography, n*—technique for embedding information into something else, such as a text file in an image or a sound file, for the sole purpose of hiding the existence of the embedded information.

2.1.34 *thumb drive, n*—small digital storage device that uses flash memory and a universal serial bus (USB) connection to interface with a computer.

2.1.35 *topology, n*—physical layout or logical operation of a network.

2.1.36 *virtual private network (VPN), n*—computer network that uses encryption to transmit data in a secure fashion over a public network.

2.1.37 *voice over internet protocol (VoIP), n*—technique for transmitting real-time voice communications over the internet or another transmission control protocol/internet protocol (TCP/IP) network.

2.1.38 *wide-area network (WAN), n*—computer network covering a wide geographical area.

2.2 *Acronyms:*

2.2.1 *FDA, n*—Food and Drug Administration

2.2.2 *FTC, n*—Federal Trade Commission

2.2.3 *IP, n*—internet protocol

2.2.4 *IRS, n*—Internal Revenue Service

2.2.5 *KSA, n*—knowledge, skill, and ability

2.2.6 *SEC, n*—Securities and Exchange Commission

2.2.7 *TCP, n*—transmission control protocol

3. Significance and Use

3.1 With the proliferation of computers and other electronic devices, it is difficult to imagine a crime that could not potentially involve digital evidence. Because of the paucity of degree programs in computer forensics, practitioners have historically relied on practical training through law enforcement or vendor-specific programs or both.

3.2 In this guide, curricula for different levels of the educational system are outlined. It is intended to provide guidance to:

3.2.1 Individuals interested in pursuing academic programs and professional opportunities in computer forensics,

3.2.2 Academic institutions interested in developing computer forensics programs, and

3.2.3 Employers seeking information about the educational background of graduates of computer forensics programs and evaluating continuing education opportunities for current employees.

4. Qualifications for a Career in Computer Forensics

4.1 *Introduction:*

4.1.1 Computer forensics plays a fundamental role in the investigation and prosecution of crimes. Since any type of criminal activity may involve the seizure and examination of digital evidence, the percentage of cases that involves digital evidence will continue to increase. The preservation, examination, and analysis of digital evidence require a foundation in the practical application of science, computer technology, and the law. A practitioner of computer forensics shall be capable of integrating knowledge, skills, and abilities in the identification, preservation, documentation, examination, analysis, interpretation, reporting, and testimonial support of digital evidence. A combination of education and practical training can prepare an individual for a career in computer forensics, and this section addresses the qualifications an individual will need to pursue such a career.

4.1.2 As in all forensic disciplines, a combination of personal, technical, and professional criteria will influence a

prospective computer forensics practitioner's suitability for employment. Effective written and oral communication skills are essential to computer forensics practitioners because they may have to testify to their examination results in court. New employees may be hired provisionally or go through a probationary period that requires successful completion of additional training or competency testing or both as a prerequisite for continued employment.

4.2 *Career Paths in Computer Forensics:*

4.2.1 Numerous competent, accurate, and admissible digital forensic examinations are performed every year by qualified and experienced examiners who have no college education. In fact, much of the expertise in this field is represented by professionals whose practical experience, on-the-job training, and work credentials qualify them in this discipline. Few institutions offer degrees in the discipline because the field is relatively new. As academic programs are developed and made available, it will become preferable for forensic examinations to be performed by individuals who have a degree in computer forensics (or a related field) supported by experience and training.

4.2.2 The discussion of qualifications presents three alternative career paths into computer forensics which are depicted in Fig. 1:

4.2.2.1 One is for law enforcement personnel who seek to move into computer forensics after they become sworn officers,

4.2.2.2 Another is for persons with relevant technical and critical thinking skills that are equivalent to a bachelor's degree, and

4.2.2.3 A third is for persons who have earned the formal degree.

4.2.3 A description of careers in computer forensics is provided in Appendix X1.

4.2.4 *Personal Characteristics*—Computer forensics, like other forensic disciplines, requires personal honesty, integrity, and scientific objectivity. Those seeking careers in this field should be aware that background checks similar to those required for law enforcement officers are likely to be a condition of employment. The following may be conducted or reviewed or both before an employment offer is made and may be ongoing conditions of employment (this list is not all-inclusive):

(1) Past work performance
(2) Drug tests
(3) History of drug use
(4) Driving record
(5) Criminal history
(6) Citizenship
(7) Credit history
(8) History of hacking
(9) Personal associations
(10) Psychological screening
(11) Medical or physical examination
(12) Polygraph examination

4.2.5 *Academic Qualifications*—Practitioners of computer forensics historically have not been required to have a degree. However, the trend within some areas of the field is to strengthen the academic requirements for this discipline and require a baccalaureate degree, preferably in a science. The academic qualifications for computer forensics practitioners are discussed in greater detail later in this guide and may include the following knowledge, skills, and abilities:

4.2.5.1 *Technical:*

(1) Computer hardware and architecture
(2) Storage media
(3) Operating systems
(4) File systems
(5) Database systems
(6) Network technologies and infrastructures
(7) Programming and scripting
(8) Computer security
(9) Cryptography
(10) Software tools
(11) Validation and testing
(12) Cross-discipline awareness

4.2.5.2 *Professional:*

(1) Critical thinking
(2) Scientific methodology
(3) Quantitative reasoning and problem solving
(4) Decision making
(5) Laboratory practices
(6) Laboratory safety
(7) Attention to detail
(8) Interpersonal skills
(9) Public speaking
(10) Oral and written communication
(11) Time management
(12) Task prioritization
(13) Application of digital forensic procedures
(14) Preservation of evidence
(15) Interpretation of examination results
(16) Investigative process
(17) Legal process

4.2.5.3 Copies of diplomas and formal academic transcripts are generally required as proof of academic qualification. Awards, publications, internships, and student activities may be used to differentiate applicants. Claims in this regard are subject to verification through the background investigation process.

4.2.6 *Credentials*—A digital forensic practitioner should demonstrate continued professional development that is documented by credentials. A credential is a formal recognition of a professional's KSA. Indicators of professional standing include academic credentials, professional credentials, training credentials, and competency tests. Credentials can facilitate the qualification of a witness as an expert.

4.3 *Implementation: Keys to a Career in Computer Forensics:*

4.3.1 *Preemployment Preparation*—Competitive candidates can demonstrate the interest and aptitude or KSAs that establish their readiness for a digital forensic position. These KSAs may include areas important to all potential forensic science practitioners including, but not limited to, quality assurance, ethics, professional standards of behavior, evidence control, report writing, scientific method, inductive and deductive

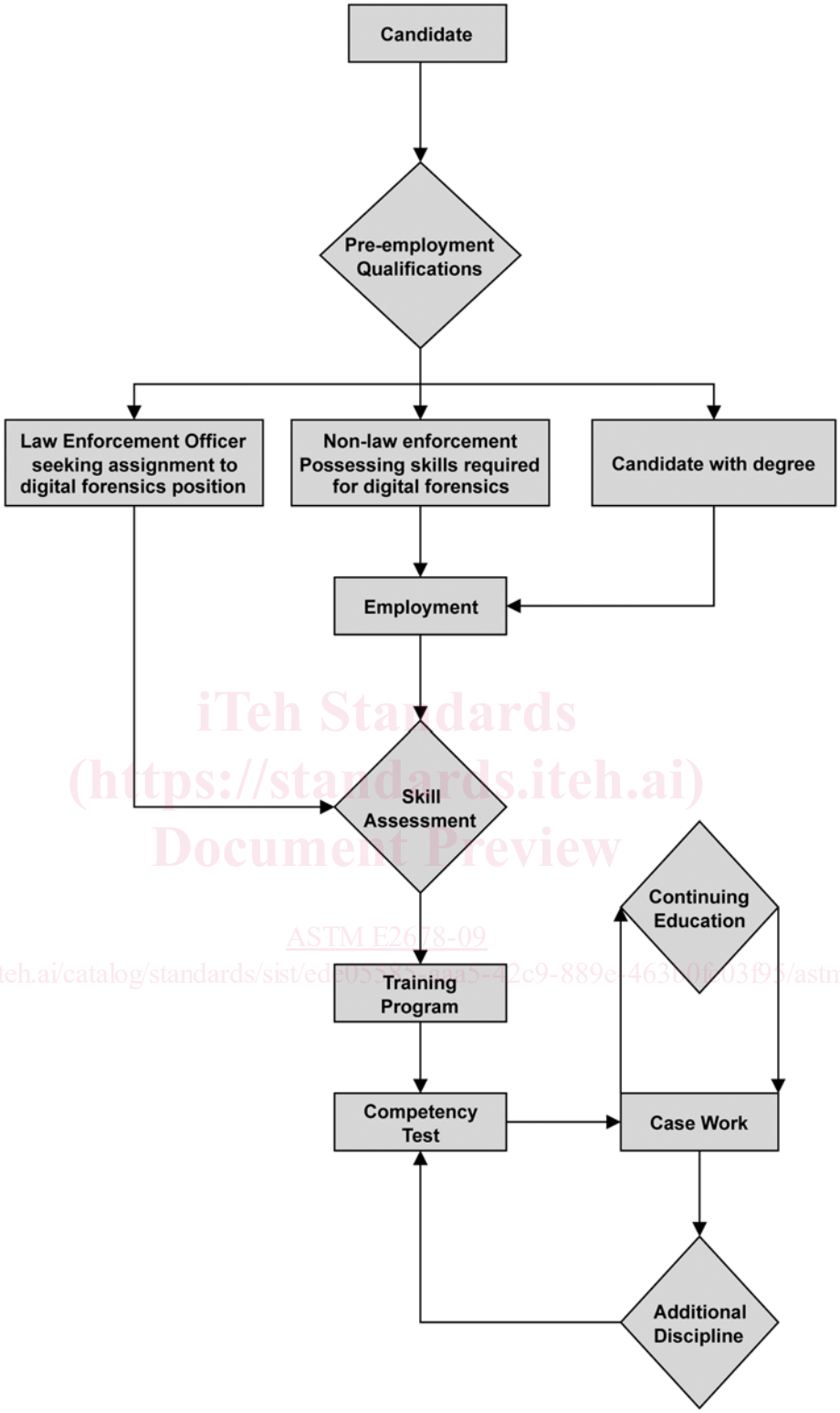

FIG. 1 Career Paths for Digital Forensics Practitioners

reasoning, investigative techniques, statistics, and safety. Documentation of coursework and practical experiences involving these KSAs can significantly enhance the objective information available to an agency evaluating potential new hires.

4.3.2 *On-the-Job Training*—After hire, on-the-job training by the hiring agency is common. The length of this training may depend on the particular responsibilities or job function of the trainee and is typically completed within six months to one year of the date of hire, depending on the trainee and the

agency. During this period, trainees can expect to learn the practical implementation of skills acquired in the classroom.

4.3.3 *Certification and Accreditation*—Accreditation applies to forensic science laboratories, whereas certification applies to practitioners or examiners. Individuals whose competencies have been certified by an independent, peer-based, appropriately credentialed certifying body could be desirable to employers. At the present time, there is no central certifying body for computer forensics in the United States.

4.3.4 *Continuing Education*—As with any forensic science discipline, it is important to remain current with generally accepted best practices, tools and techniques, and changes in technology. The practitioner should select continuing education opportunities that address these needs.

4.3.5 *Professional Involvement*—While casework is the primary focus of a digital forensic practitioner, one can also strive to advance the profession. This may be accomplished through professional involvement such as research, mentoring, teaching, community outreach, publishing, participating in professional organizations, conferences and workshops, and other professional activities.

4.4 *Summary*—While a strong educational background in science, computer technology, and the law is recommended for a career in computer forensics, this emerging field includes practitioners from a variety of educational backgrounds. Regardless of the route taken to become a digital forensic practitioner, all require a common base of KSA in professional and technical areas as well as personal attributes such as honesty and integrity. Implementation of the programs described in this guide will further enhance the professionalism of the digital forensic practitioner.

5. Associate Degree Programs in Computer Forensics

5.1 *Introduction:*

5.1.1 Forensic science is an applied science that covers an array of disciplines, including the evolving discipline of computer forensics. A two- year degree will provide a solid foundation for further study in the field and prepare practitioners seeking an entry level job. A two-year degree program should provide a credible foundation in the fundamentals of the justice system and forensic methodologies, especially as they relate to computer forensics.

5.1.2 Graduates of a two- year program should possess a:

5.1.2.1 Basic understanding of the justice system;

5.1.2.2 Basic understanding of forensic processes;

5.1.2.3 Substantial familiarity with common computer systems, including the hands-on ability to manipulate computer hardware components, common operating systems, and digital devices;

5.1.2.4 Substantial understanding of the electronic crime scene and how to identify, document. and protect potential evidence found at the scene;

5.1.2.5 Substantial understanding of the principles of forensic acquisition, documentation, and duplication of digital evidence; and

5.1.2.6 Basic understanding of the forensic analysis of digital data.

5.1.3 The preservation and documentation of digital evidence are important parts of any investigation involving electronic data. Proper processing of digital evidence provides the foundation for a strong case, and mistakes at the initial stages can undermine all subsequent work by providing the basis for legal challenges to the admissibility of the evidence. Therefore, it is important that practical applications of the knowledge acquired in this degree program be demonstrated by the student. A variety of hands-on laboratory and field exercises should be included in the curriculum to demonstrate the abilities to:

5.1.3.1 Identify and protect digital devices at a crime scene,

5.1.3.2 Document a crime scene and sources of digital evidence,

5.1.3.3 Handle evidence properly and maintain chain of custody,

5.1.3.4 Acquire and validate a forensic image of a digital device,

5.1.3.5 Restore a forensic image or boot an image within a virtual environment, and

5.1.3.6 Locate potential evidence in a variety of digital media.

5.1.4 *Model Curriculum: Associate Degree Programs in Computer Forensics* (Table 1)—This section of the guide provides recommendations for an associate degree program in computer forensics. This degree provides an educational and practical foundation intended to meet the minimum hiring requirements for an entry level position as a computer forensics practitioner. Additionally, an associate degree program in

TABLE 1 Model Curriculum: Associate Degree Programs in Computer Forensics[A]

General Education (~35 credit hours)	Courses required by the institution, which may include language, humanities, social sciences, mathematics, and public speaking. Six credit hours of science courses (plus two credit hours of labs) that expose students to the scientific method and the fundamentals of electricity and magnetism should be taken within these credits. In addition, a course in discrete math should be taken to obtain the necessary foundation in computer mathematics. Some forensic computer science/digital evidence degree coursework may count toward fulfilling these requirements.
Computing and Information Science Core (9 credit hours)	Introduction to Computers and Storage Media Applied File Systems and Operating Systems Basic Computer Networking and Network Security
Forensic Science Core (18 hours)	Introduction to the Forensic Sciences Basic Computer Forensics and Lab File System and Operating System Evidence Recovery and Examination and Lab Analysis of Digital Media, Storage Devices and Applications and Lab Basic Legal Issues (Evidence)

[A] For students intending to pursue a four-year degree subsequent to their Associate Degree, it is recommended that Programming I be taken as an elective.

computer forensics prepares students to pursue a baccalaureate degree in the field. Note that further on-the-job training and academic study may be necessary to meet the needs of individual employers.

5.1.5 *General Education Requirements*—General education requirements are those college courses intended to provide students with a well-rounded education. They may include languages, humanities, social sciences, mathematics, physical sciences, English composition, and so forth. The actual number of credit hours will vary from college to college but is generally around 35 credit hours. Some of the recommended forensic courses may count toward fulfilling this requirement, and carefully selected general education courses, especially with an emphasis on mathematics and laboratory based science, can complement the student's main program of study.

5.1.6 *Specific Education Requirements* (Table 2):

5.1.6.1 Certain specific courses are required for any student of computer forensics. These include broad-based courses in the justice system, forensic processes, and computer and digital media specific studies.

5.1.6.2 The minimum specific course requirements for associate degree programs include:

(1) Introduction to Computers and Storage Media (3 credit hours),

(2) Applied File Systems and Operating Systems (3 credit hours),

(3) Basic Computer Networking and Network Security (3 credit hours),

(4) Introduction to Forensics (3 credit hours),

(5) Basic Computer Forensics (3 credit hours + 1-h lab),

(6) File System and Operating System Evidence Recovery and Examination (3 credit hours + 1-h lab),

(7) Analysis of Digital Media, Devices and Applications (3 credit hours + 1-h lab), and

(8) Basic Legal Issues (3 credit hours).

5.1.6.3 To provide a background in the scientific method, discrete math (3 credit hours) and some combination of science courses with a laboratory component (to total 6 credit hours plus 2 credit hours of lab) should be taken (for example, Physics I and II). These courses may also be used to fulfill the institution's general education requirements.

5.2 *Implementation: Keys to Ensuring Curriculum Success:*

5.2.1 *Assessment*—A program such as this should provide documented, measurable objectives, including expected skill-based outcomes for graduates. It should be regularly assessed to determine if course objectives have been met and to identify areas for program improvement.

5.2.2 *Institutional Support*—This curriculum should enjoy a level of institutional support equal to other courses of study in an associate degree program. Existing computer forensics programs that are undersupported can be upgraded according to these recommendations. Institutions should provide the recommended courses often enough to allow students to complete the program in a reasonable amount of time.

5.2.3 *Faculty:*

5.2.3.1 An adequate number of full- time faculty members ensures continuity and stability to cover the curriculum and allow an appropriate mix of instruction and scholarly activity. The faculty members' interests and qualifications are expected to be sufficient to teach the courses and plan and modify the courses and curriculum as necessary. Faculty members are expected to be current in the discipline, have knowledge and experience appropriate for the courses they teach, and recognize advisory duties as a valued part of their workload.

5.2.3.2 Active computer forensics practitioners, often used as adjunct faculty, provide realworld experience and practical implementation of the topics and techniques being taught. However, it is essential that full-time faculty oversee the curriculum.

5.2.4 *Facilities:*

5.2.4.1 Computer facilities that are available, accessible, and adequately equipped and supported are essential to enable students to complete their coursework and support the teaching needs and scholarly activities of the faculty. Ideally, these facilities should be separate from other computer-based classrooms and labs since many of the lesson activities are potentially destructive to the host computer-operating systems and data. When separate facilities are not possible, existing facilities should support server-based imaging of the classroom computers so that they can be easily and quickly re-imaged when they are corrupted and problem scenarios need to be installed for student assignments.

5.2.4.2 Each computer should be reasonably state of the art, in terms of CPU, RAM, hard-disk capacity, optical (DVD and so forth) drives, and external connections for peripheral devices. Ideally, each computer should have two internal physical drives, and there should be a supply of external digital media devices (hard drives, thumb drives, and so forth) that students can use in their assignments. Keeping this equipment up to date and functional will require a significant commitment by the institution; however, it may be possible to obtain grants or in-kind donations of equipment from equipment vendors and manufacturers.

5.2.4.3 Such institutional facilities as the library, classrooms, and offices are expected to be adequate to support the program objectives. These should include access to legacy equipment and software since students are likely to encounter them in the field. A library where faculty and students have access to books, periodicals, and electronic resources (with adequate support for database searching) is essential to a successful program. The institution is also expected to subscribe to peer-reviewed computer forensics journals.

5.2.5 *Student Support:*

5.2.5.1 It is essential that each student has adequate and reasonable access to equipment currently being used by computer forensics practitioners and appropriate to the course of instruction.

5.2.5.2 Students should be afforded ample opportunity to interact with their instructors and offered timely and informed guidance about program requirements, course options, and career opportunities.

5.2.6 *Faculty Support*—Sufficient support for faculty enables the program to attract and retain high-quality faculty capable of accomplishing the program's objectives. Support is expected to include:

5.2.6.1 Encouragement of scholarly activities,

TABLE 2 Recommended Course Content: Associate Degree Programs in Computer Forensics

Course	Content
Introduction to Computers and Storage Media (3 credit hours)	the term "computer," its components, and their functionality history of computers and significant milestones purpose and components of a network including hardware, software, and protocols uses of the internet and the worldwide web steps necessary to build a computer using a variety of peripherals, input/output devices, storage, and other components. Students will be given a broad overview of all the hardware necessary to build a functioning system low-level functioning of storage media recognition and configuration of common storage device interfaces (for example, USB, SCSI, IDE, FireWire, SATA) difference between physical and logical storage categories of application software functions of an operating system, and comparison of some of the more widely used operating systems importance of security, and discuss techniques to prevent unauthorized access and use the importance of safeguarding against malware (for example, computer viruses, worms, spyware, and Trojan horses) the importance of computer backup and methods of implementation
Applied File Systems and Operating Systems (3 credit hours)	underlying components and functionality of an operating system, including the historical progression of some of the major operating systems main user features, administrative capabilities, system requirements, and interoperability of the DOS and legacy and current Windows, Macintosh, and Unix/Linux operating systems methods to navigate the file structures in DOS, Windows, Macintosh. and Unix/Linux systems file system concepts and the differences between FAT, NTFS, ext2/ext3, and HPFS/HFS/HFS+
Basic Computer Networking and Network Security (3 credit hours)	transmission media options, protocols, topologies, network devices, network interface cards, and WAN, LAN, PAN, and internet working terminology typical network access technologies in business as well as residential applications structure and operation of the Internet basic network security techniques such as VPN, PKI, and so forth role of firewalls attack and defense strategies (for example, spoofing, port scanning, network sniffing) risk management
Basic Legal Issues (Evidence) (3 credit hours)	basics of the justice system and its relation to digital forensics and digital evidence rules and issues relating to the admissibility of evidence, both constitutional and statutory to include search and seizure, chain of custody, and suppression, and so forth implications of time constraints for search warrants 4th amendment exceptions (for example, warrantless searches) the ECPA and relevant federal and state statutes fundamentals of preparing for and providing testimony civil law issues related to computer forensics and electronic discovery current case law for digital forensics
Introduction to the Forensic Sciences (3 credit hours)	investigative process and the role that forensics plays in this process basics of forensics protocols, the scientific method, and sound reporting practices professional ethics crime scene investigation major forensic disciplines – chemistry, biology, comparative sciences, and so forth
Basic Computer Forensics (3 credit hours)	roles of computers in crime and other misconduct intricacies and volatility of the electronic crime scene analysis procedures: identification, preservation, examination, analysis, and reporting principles of device imaging, restoration, and validation characteristics of physical/logical hard drives common digital storage devices effective and efficient examination techniques for different types of investigations demonstrate application of the scientific method (formulate and test a hypothesis about a digital event) report writing analysis platforms and tools relationship of computer forensics examinations to examinations performed by other forensic science disciplines (for example, using cyanoacrylate (Superglue) fuming to develop latent print evidence on a CD may negatively impact the ability to subsequently recover digital evidence from the CD) preservation of other forms of evidence during the digital forensics process
Basic Computer Forensics Lab (1 credit hour)	demonstration of crime scene search and seizure techniques for digital evidence formal presentation of digital evidence in a mock trial identification and documentation of evidence use of hardware and software write blockers image a physical hard disk and validation of the copy image a logical drive and validation of the copy image a variety of digital storage devices validation of the forensic tools used in imaging demonstration of report writing skills control the boot process of unknown systems

5.2.6.2 Sponsorship of research,

5.2.6.3 Opportunities to attend professional meetings,

TABLE 2 *Continued*

Course	Content
File System and Operating System Evidence Recovery & Examination (3 credit hours)	types of potential digital evidence that can be created by an OS current operating systems (for example, Windows, Linux, Mac, and so forth) and locations of log audit data, configuration files, user profiles, and so forth details of common file systems (for example, FAT, NTFS, ext2/ext3) and partitioning potential OS vulnerabilities and malware OS-specific data-hiding techniques
File System and Operating System Evidence Recovery & Examination Lab (1 credit hour)	identify configuration-based evidence on several images analyze a log to identify event-based evidence manual file system recovery identify hidden data demonstrate report writing skills
Analysis of Digital Media, Storage Devices and Applications (3 credit hours)	engineering aspects of digital media and storage devices file systems usually associated with the most common digital media and storage devices application-level digital evidence for the most common types of applications: internet e-mail documents graphics
Analysis of Digital Media, Storage Devices and Applications Lab (1 credit hour)	analyze and recover potential evidence from several types of digital media and applications in a scenario-based exercise demonstrate report writing skills

5.2.6.4 Release time and resources for administrative duties,

5.2.6.5 Technical assistance, and

5.2.6.6 Clerical assistance.

5.2.7 *Collaboration with Computer Forensics Practitioners*—Academic computer forensics programs are expected to establish working relationships with experienced practitioners, if possible. Recommended partners are state, local, or federal law enforcement agencies or civilian entities engaged in practical computer forensics. Such collaboration can provide meaningful internships, employment opportunities, guest lecturers, adjunct faculty, and cooperative research.

5.2.8 *Accreditation:*

5.2.8.1 The institution granting the degree is expected to be accredited by an accrediting body recognized by the U.S. Department of Education.

5.2.8.2 At the present time, there is no mechanism for accrediting computer forensics associate degree programs. When this mechanism is implemented, it is strongly recommended that all such programs seek accreditation. Accreditation provides many benefits, including:

(1) An external means of program validation,

(2) A tool to help students select a program,

(3) A means for computer forensics practitioners and potential employers to judge graduates' credentials, and

(4) An improvement of program quality.

5.3 *Summary:*

5.3.1 Computer forensics is a relatively new discipline that will be greatly expanded and improved by academic rigor. Future practitioners must have education and training consistent with the other forensic sciences.

5.3.2 This section provides recommendations for implementing a successful computer forensics program at the two-year college level that will turn out entry level practitioners or students with a solid foundation and advantage if they choose to pursue a more advanced degree.

6. Baccalaureate Degree Programs in Computer Forensics

6.1 *Introduction:*

6.1.1 Forensic science is an applied science that covers an array of disciplines, including the evolving discipline of computer forensics. A model program should emphasize the scientific method and the application of problem-solving skills in both classroom and laboratory settings. A baccalaureate degree program in computer forensics should be interdisciplinary, combining a strong foundation in the computing and information sciences with extensive laboratory experience and ancillary courses from criminal justice. In addition, graduates should demonstrate proficiency in technical writing, oral communication, laboratory skills, and safety practices, as well as forensic software applications.

6.1.2 A baccalaureate degree program in computer forensics should provide:

6.1.2.1 Preparation for becoming a computer forensics professional,

6.1.2.2 Opportunities to establish a network of computer forensics contacts,

6.1.2.3 An educational background directly linked to the work in a computer forensics laboratory,

6.1.2.4 Exposure to the breadth of forensic science disciplines,

6.1.2.5 Acculturation into the computer forensics and justice communities,

6.1.2.6 Provision of a foundation for professional certification, and

6.1.2.7 Emphasis on a wide range of courses (for example, public speaking, technical writing, ethics, and statistics) that may not be required in the curricula of natural science majors.

6.1.3 Graduates of a baccalaureate degree program in computer forensics should be able to:

6.1.3.1 Identify, preserve, and collect digital devices in the field including networked or other advanced components or both;

6.1.3.2 Handle evidence properly and maintain chain of custody;

6.1.3.3 Document crime scene and sources of digital evidence;

6.1.3.4 Acquire, validate, and restore forensic images from a variety of digital devices;

6.1.3.5 Locate potential evidence in a variety of digital media devices;

6.1.3.6 Develop/validate new techniques and solve problems using the scientific method;

6.1.3.7 Identify, analyze, and solve both technical and investigative problems;

6.1.3.8 Demonstrate an understanding of computer and network components and their interactions; and

6.1.3.9 Communicate technical findings effectively both verbally and in writing.

6.1.4 *Model Curriculum:*

6.1.4.1 This section of the guide provides recommended guidelines for a model baccalaureate degree program in computer forensics. This curriculum emphasizes the strong computing foundation as well as the nontechnical skills essential to prepare a student for a successful career in computer forensics. Refer to Table 3 for an overview of the model curriculum.

6.1.4.2 Note that additional on-the-job training and possible postgraduate studies may be necessary to meet the specific needs of the individual employer.

6.1.4.3 Peer-based working groups have created specific education requirements. Computer forensics laboratories and graduate programs may require more than the recommended credit hours of specific coursework.

6.1.5 *University General Education*—General education requirements are those college courses intended to provide students with a well-rounded education. They may include language, humanities, social sciences, mathematics, technical writing, natural sciences, and public speaking. The actual

TABLE 3 Model Curriculum: Baccalaureate Degree Programs in Computer Forensics[A]

University General Education (36-40 credit hours)	Courses required by the university, which may include language, humanities, social sciences, mathematics, and public speaking. Six credit hours of science courses (plus two credit hours of labs) that expose students to the scientific method and the fundamentals of electricity and magnetism should be taken within these credits. Some forensic computer science/digital evidence degree coursework may count toward fulfilling these requirements.
Computing and Information Science Core (24 credit hours)	Introduction to Computers and Storage Media Applied File Systems and Operating Systems Basic Computer Networking and Network Security Programming I Computer Architecture Database/Applications Information Security Discrete Math
Forensic Science Core (6 credit hours)	Introduction to the Forensic Sciences Forensic Science Professional Practice[B]
Additional Required Courses (16 credit hours) (Some courses may count toward fulfilling general education requirements)	Basic Legal Issues (Evidence) Criminal Investigation Public Speaking Technical Writing Capstone Project Topics in Computer Forensics (1 credit hour seminar)
Computer Forensics Laboratory Core (12 credit hours)	Basic Computer Forensics (3 credit hours + 1-h lab) File System and Operating System Evidence Recovery and Examination (3 credit hours + 1-h lab) Analysis of Digital Media, Storage Devices, and Applications (3 credit hours + 1-h lab)
Upper Division Forensics Courses	
Advanced Computer Forensics Core (required: 11 credit hours)	Advanced Computer Forensics (3 h + 1-h lab) Network Forensics (3 h + 1- h lab) Storage Systems (3 credit hours)
Technical Electives[C] (required: 9 h from the list)	Personal Electronic Device (PED) Forensics (3 credit hours + 1- h lab) Embedded Device Forensics (3 credit hours + 1-h lab) Incident Response (3 credit hours) Reverse Engineering Techniques and Countermeasures (3 credit hours) Multimedia Forensics Overview (3 credit hours) Statistics (3 credit hours) Independent Study (3 credit hours) Advanced Legal Issues in Computer Forensics (3 credit hours) Civil Legal Issues (3 credit hours)
Open University Electives (6 h)	Free electives (may include internship)

[A] Total credit hours = 120 to 124.
[B] This course includes ethics, testimony, evidence, chain of custody, safety, and so forth.
[C] Electives listed are not exhaustive and students may wish to tailor courses according to their areas of concentration.

number of credit hours required may vary from university to university but generally ranges from 36 to 40. Some forensic degree coursework may count toward fulfilling the general education requirement. Carefully selected general education courses can complement the student's main program of study. A public speaking course should be required of all students in the program because a forensic examiner may have to testify in court.

6.1.6 *Computing and Information Science Core*—A computer forensics practitioner shall have a foundation in the computing and information sciences and mathematics. This foundation allows the practitioner to understand computer technology and how digital information is generated, stored, and transmitted.

6.1.7 *Forensic Science Core*—Knowledge of forensic science practices provides a foundation for meeting criminal justice requirements such as the preservation of evidence, maintaining chain of custody, and courtroom testimony. It is also essential to have an understanding of the interaction between computer forensics and other forensic disciplines. This allows the practitioner to recognize how the examination of digital media may impact the recovery of other types of physical evidence and also how other forensic examinations may impact the recovery of data (for example, certain chemicals used in latent print recovery may render the data on digital media unreadable). There are also concepts that are unique to computer forensics that must be included in the curriculum (see Table 3).

6.1.8 *Internship*-—It is strongly recommended that students participate in an internship before graduation. Such an internship can provide hands-on training and experience in computer forensics to prepare students for casework upon completion of the program.

6.1.9 Table 4 outlines sample course content for the core courses and electives in a baccalaureate degree program in computer forensics.

6.2 *Implementation: Keys to Ensuring Curriculum Success*—Many universities will already have a significant number of the courses described in this guide. However, significant additional resources may be necessary to create new programs or even bolster existing baccalaureate degree programs in computer forensics. The following items are essential for the proper implementation of a successful baccalaureate degree program in computer forensics.

6.2.1 *Objectives and Assessments of Institutional Effectiveness*—A program such as this should provide documented, measurable objectives, including expected outcomes for graduates. It should be regularly assessed to determine if course objectives have been met and identify areas for program improvement.

6.2.2 *Institutional Support*—A computer forensics curriculum is expected to enjoy a level of institutional support equal to other computing and information science programs. Baccalaureate degree programs in computer forensics that are under-supported can be upgraded according to these recommendations. If proper facilities and operating budgets are not provided, the programs may not succeed. Funding sources could include competitive federal funding, other public and private sources, in addition to internal funding. Institutions should provide the recommended courses often enough to allow students to complete the program in a reasonable amount of time.

6.2.3 *Faculty:*

6.2.3.1 An adequate number of full- time faculty members ensures continuity and stability to cover the curriculum and allow an appropriate mix of instruction and scholarly activity. The faculty members' interests and qualifications are expected to be sufficient to teach the courses and plan and modify the courses and curriculum as necessary. Faculty members are expected to be current in the discipline, have knowledge and experience appropriate for the courses they teach, and recognize advisory duties as a valued part of their workload.

6.2.3.2 Active computer forensics practitioners, often used as adjunct faculty, provide realworld experience and practical implementation of the topics and techniques being taught. However, it is essential that full-time faculty oversee the curriculum.

6.2.4 *Facilities:*

6.2.4.1 Computer facilities that are available, accessible, and adequately equipped and supported are essential to enable students to complete their coursework and support the teaching needs and scholarly activities of the faculty. Ideally, these facilities should be separate from other computer-based classrooms and labs since many of the lesson activities are potentially destructive to the host computer operating systems and data. When separate facilities are not possible, existing facilities should support server-based imaging of the classroom computers so that they can be easily and quickly re-imaged when they are corrupted and problem scenarios need to be installed for student assignments.

6.2.4.2 Each computer should be reasonably state of the art in terms of CPU, RAM, hard-disk capacity, optical (DVD and so forth) drives, and external connections for peripheral devices. Ideally, each computer should have two internal physical drives, and there should be a supply of external digital media devices (hard drives, thumb drives, SD memory devices, and so forth) that students can check out for use in their assignments. Keeping this equipment up to date and functional will require a significant commitment by the institution; however, it may be possible to obtain grants or in-kind donations of equipment from equipment vendors and manufacturers.

6.2.4.3 Such institutional facilities as the library, classrooms, and offices are expected to be adequate to support the program objectives. These should include access to legacy equipment and software since students are likely to encounter them in the field. A library where faculty and students have access to books, periodicals, and electronic resources (with adequate support for database searching) is essential to a successful program. The institution is also expected to subscribe to peer-reviewed digital forensics journals.

6.2.5 *Student Support:*

6.2.5.1 It is essential that each student has adequate and reasonable access to equipment currently being used by computer forensics practitioners and appropriate to the course of instruction.