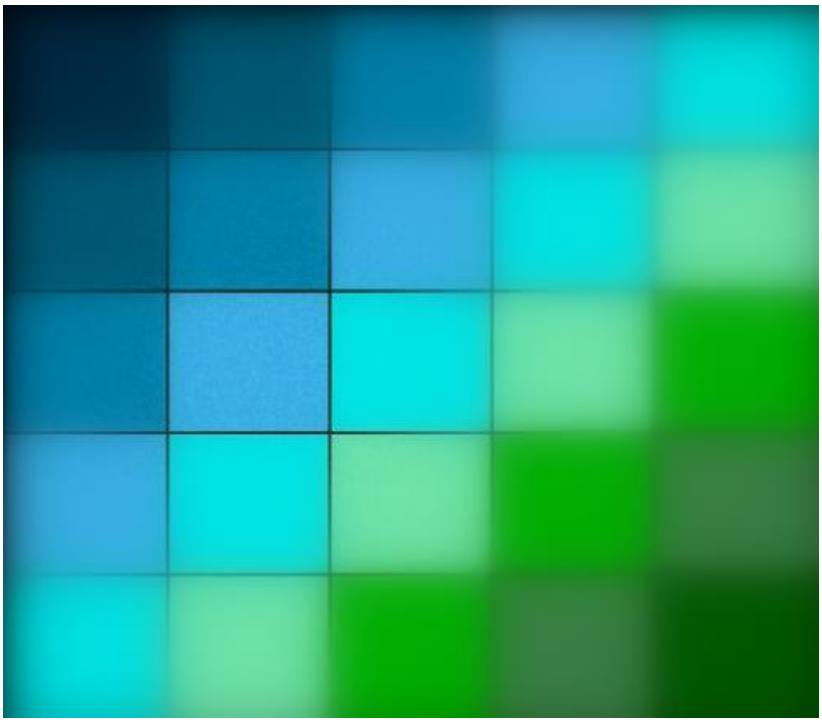

Technical Working Group for Education and Training in Digital Forensics

Funded through National Institute of Justice Award 2001-RC-CX-K003 to West Virginia University Forensic Science Initiative

July 5, 2007

Technical Working Group for Education and Training in Digital Forensics

Table of Contents

TWG Members

Planning Panel:

Abigail Abraham
Assistant Attorney General
Illinois Attorney General's Office

Susan Brenner
Professor
University of Dayton, School of Law

Philip Craiger
Assistant Director for Digital Evidence
Assistant Professor
National Center for Forensic Science
University of Central Florida

Bill Crane
Deputy Head of High Tech Training
The National Centre for Policing Excellence
England

Amber Haqqani
Director Digital Evidence
American Academy of Applied Forensics (AAAF)
Central Piedmont Community College

Erin Kenneally
Forensic Analyst
University of California, San Diego
San Diego Supercomputer Center, Pacific Institute for Computer Security

Scott Patronik
Chief, Division of Technology and Advancement
Erie County Sheriff's Office

Alan Roth
Postal Inspector
Forensic Laboratory Services
U.S. Postal Service

Todd Shipley
Director

Systems Security and High Tech Crime Prevention Training
SEARCH; The National Consortium for Justice Information and Statistics

Sujeet Shenoi
Professor
The University of Tulsa

Chris Stippich
President
Digital Intelligence, Inc.

Mike Weil
Manager
Huron Consulting Group

TWG:

Christopher L. T. Brown
Founder & CTO
Technology Pathways LLC

Walter E. Bruehs
Forensics Examiner
Forensic Audio, Video and Imaging Analysis Unit
Federal Bureau of Investigation

Jeff Cable
San Diego Police Department
Assistant Director
San Diego Regional Computer Forensics Laboratory

Brian Carrier
Research Assistant
CERIAS / Purdue University

Eoghan Casey
Senior Consultant & Computer Forensics Examiner
Stroz Friedberg, LLC

Chris Casto
Sergeant
West Virginia State Police
Bureau of Criminal Investigation

Scott Christensen

Sergeant
Computer Crimes
Internet Crimes Against Children Unit
Nebraska State Patrol

Todd Colvin
Computer Training Specialist
SEARCH

David Dittrich
Senior Security Engineer
University of Washington

Nelson Eby
Federal Bureau of Investigation
FBI CART Training

Don Flynn
Attorney Advisor
Department of Defense Cyber Crime Center

Charles Giglia
Computer Crime Specialist
National White Collar Crime Center

Dave Heslep
Sergeant
Maryland State Police
Computer Forensics Laboratory

Albert Holt
Technical Leader
Department of Defense

Ronnie Jewell
Manager, IT
Marshall University Forensic Science Center

Nigel Jones
Head of High Tech Training
National Centre for Policing Excellence
England

Gary C. Kessler
Associate Professor
Program Director, Computer & Digital Forensics
Champlain College

Keith Lockhart
Director of Training
AccessData

Don Mason
Associate Director
National Center for Justice and the Rule of Law

Sharon Mason
Assistant Professor
Dept. of Information Technology
Rochester Institute of Technology

Mark J. Menz
President
M. J. Menz and Associates

Mike Menz
HP-IT Security Investigator
Detective
Sacramento High Technology Crimes Task Force

Bill Moylan
Detective, Nassau County, New York Police Department
New York Electronic Crimes Task Force

Andrew Murphy
Digital Evidence Training Coordinator
Special Agent
United States Secret Service

Richard S. Murray
Assistant U.S. Attorney
Western District of Michigan

Thomas Musheno
Forensic Examiner
Forensic Audio, Video and Image Analysis
Federal Bureau of Investigation

Glenn J. Nick
Section Chief
Computer Forensics Section
US Immigration & Customs Enforcement, Cyber Crime Center
Department of Homeland Security

Robert O'Leary
Director
Electronic Crime Partnership Initiative

Gary Palmer
Infosec Engineer/Scientist
The MITRE Corporation

Gilbert L. Peterson
Assistant Professor of Computer Engineering/ ENG
Air Force Institute of Technology
Department of Electrical and Computer Engineering

Shari L. Potter
Assistant US Attorney
Northern District of West Virginia

Scott Redmon
Detective
Guilford County S.O.; Special Operations/Computer Crimes

Raemarie Schmidt
Vice President
Digital Intelligence, Inc.

Peter Sommer
Senior Research Fellow, Information Systems Integrity Group
London School of Economics
Joint Lead Assessor, Digital Evidence, Council for the Registration of Forensic Practitioners,
United Kingdom

Preston Thomas
Director
DCITP

Don Tobin
Assistant Professor

Fairmont State University
Computer Science

Shambhu J. Upadhyaya
Associate Professor
Computer Science and Engineering Department
SUNY at Buffalo

Facilitators:

Mary Holloran
Office Administrator
Forensic Science Initiative
West Virginia University

Max M. Houck
Director
Forensic Science Initiative
West Virginia University

Roy S. Nutter, Jr.
Professor
Lane Department of Computer Science and Electrical Engineering
West Virginia University

Anjali R. Swienton
Consultant Program Manager
President & CEO
Sci**Law**Forensics, Ltd.

Preface

This document reflects a new branch of forensic science in the 21st century, what has been termed digital forensics. The ever-increasing complexity of life in the digital age requires that we have scientists who are ready to assist law enforcement with investigations that relate to digital items. To do that, however, we must have educational programs that prepare students for careers in those fields. Much as the NIJ Special Report, *Education and Training in Forensic Science* and the NIJ Research Report, *Curriculum in Forensic Accounting and Fraud Examination*, laid the groundwork for their respective fields, the work of the Technical Working Group on Education and Training in Digital Forensics provides similar foundational work in this new investigative area. Students, colleges, and universities can use this guide to shape the future of digital forensics for academia and the discipline itself.

I am proud of the forensic curriculum development work we have produced here at WVU through the Forensic Science Initiative and I hope you find it useful.

Max M. Houck
Director, Forensic Science Initiative
West Virginia University

Introduction

Digital forensics is the science of identifying, collecting, preserving, documenting, examining, analyzing and presenting evidence from computers, networks, and other electronic devices. With the proliferation of computers and other electronic devices, it is difficult to imagine a crime that could not potentially involve digital evidence. Due to the paucity of degree programs in digital forensics, practitioners have historically relied on practical training through law enforcement and/or vendor specific programs.

In order to meet the growing needs of the community, a group of educators and practitioners were brought together to outline curricula for different levels of the educational system and prepare this document. It is intended to provide guidance to:

- individuals interested in pursuing academic programs and professional opportunities in digital forensics.
- academic institutions interested in developing digital forensics programs.
- employers seeking information about the educational background of graduates of digital forensics programs and evaluating continuing education opportunities for current employees

This document attempts to improve and advance digital forensics through the development of model curricula consistent with other forensic science programs. Chapter 1 describes the alternative paths by which students may arrive at and move through their professional training. Chapters 2 through 4 cover formal educational programs in order of increasing length: a two year associate's degree, a four year baccalaureate degree and graduate degrees. Chapter 5 provides a framework for academic certificate programs offered by educational institutions. Chapter 6 outlines model criteria and implementation approaches for training and continuing education opportunities provided by professional organizations, vendors, and academic institutions.

In addition to computer forensics, some professional organizations recognize forensic audio, video, and image analysis as sub-disciplines of digital forensics. However, the curricula and specific educational training requirements of these sub-disciplines are beyond the scope of this Guide.

Chapter 1
Qualifications for a Career in Digital Forensics

Introduction

Digital 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 digital forensics must 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 digital forensics and this chapter addresses the qualifications an individual will need to pursue such a career.

As in all forensic disciplines, a combination of personal, technical, and professional criteria will influence a prospective digital forensics practitioner's suitability for employment. Effective written and oral communication skills are essential to digital 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 and/or competency testing as a prerequisite for continued employment.

Career Paths in Digital Forensics

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 digital forensics (or a related field) supported by experience and training.

The discussion of qualifications presents three alternative career paths into digital forensics which are depicted in Figure 1:

- one is for law enforcement personnel who seek to move into digital forensics after they become sworn officers;
- another is for persons with relevant technical and critical thinking skills that are equivalent to a bachelor's degree;
- a third is for persons who have earned the formal degree.

A description of careers in digital forensics is provided in **Appendix A** (page 54)

Regardless of the pathway chosen, the candidate must possess personal integrity, and have the knowledge, skills and abilities (KSAs) that fulfill the requirements of the job.

Personal characteristics

Digital 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 and/or reviewed before an employment offer is made and may be ongoing conditions of employment (this list is not all-inclusive):

- Past work performance
- Drug tests
- History of drug use
- Driving record
- Criminal history
- Citizenship
- Credit history
- History of hacking
- Personal associations
- Psychological screening
- Medical or physical examination
- Polygraph examination

Academic qualifications

Practitioners of digital 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 digital forensics practitioners are discussed in greater detail later in this *Guide* and may include the following knowledge, skills and abilities:

Technical

- Computer hardware and architecture
- Storage media
- Operating systems
- File systems
- Database systems
- Network technologies and infrastructures
- Programming and scripting
- Computer security

- Cryptography
- Software tools
- Validation and testing
- Cross discipline awareness

Professional

- Critical thinking
- Scientific methodology
- Quantitative reasoning and problem solving
- Decision making
- Laboratory practices
- Laboratory safety
- Attention to detail
- Interpersonal skills
- Public speaking
- Oral and written communication
- Time management
- Task prioritization
- Application of digital forensic procedures
- Preservation of evidence
- Interpretation of examination results
- Investigative process
- Legal process

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.

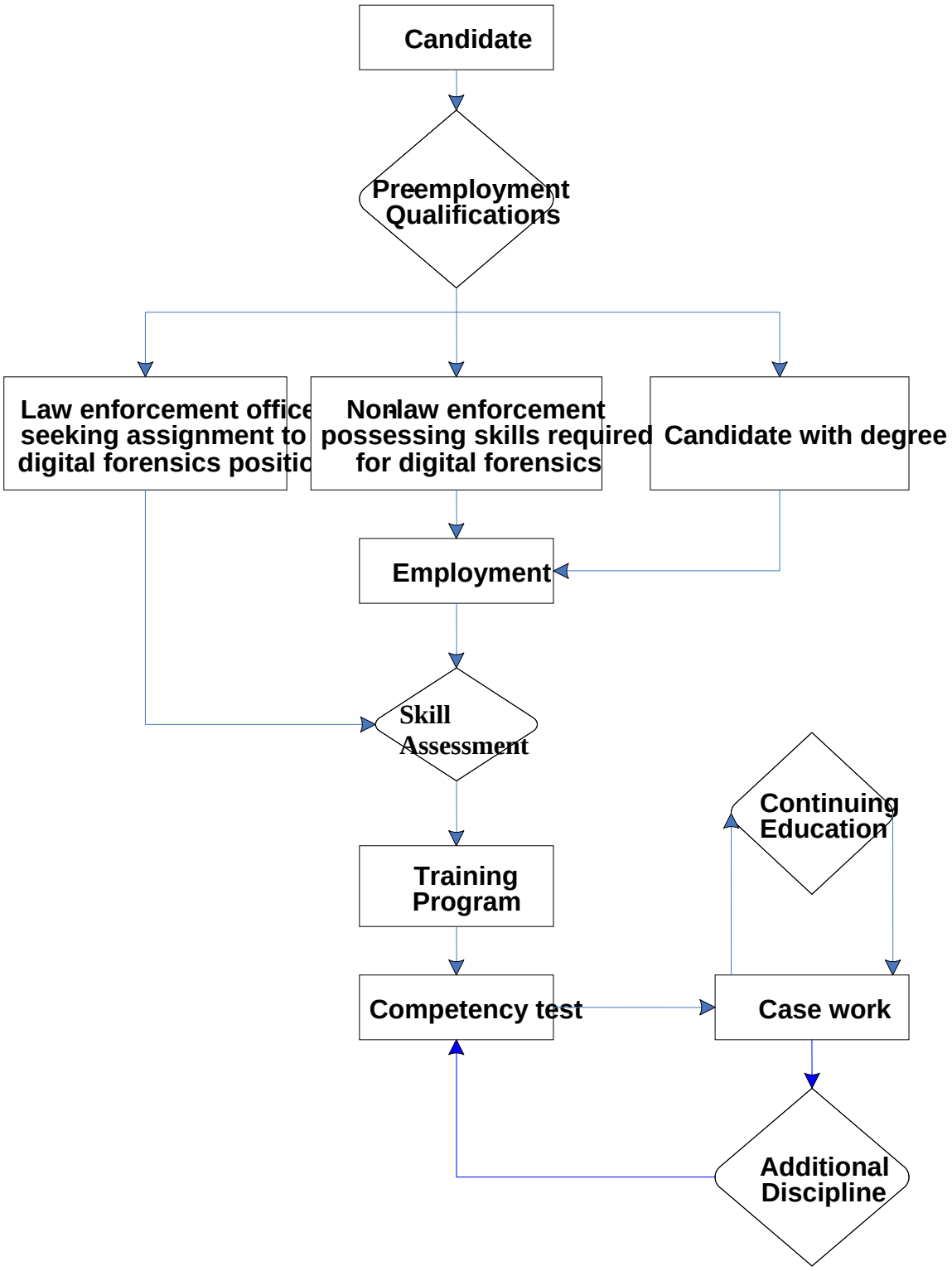

Figure 1: Career Paths for Digital Forensics Practitioners

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 knowledge, skills, and abilities. 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.

Implementation: Keys to a Career in Digital Forensics

Pre-employment preparation

Competitive candidates can demonstrate the interest and aptitude or knowledge, skills, and abilities 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 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.

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.

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 time of this writing, there is no central certifying body for digital forensics in the United States.

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.

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.

Summary

While a strong educational background in science, computer technology, and the law is recommended for a career in digital 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 knowledge, skills and abilities 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.

Chapter 2
Associate Degree Programs in Digital Forensics

Introduction

Forensic science is an applied science that covers an array of disciplines, including the evolving discipline of digital forensics (often called 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 digital forensics.

Graduates of a two-year program should possess a:

- Basic understanding of the justice system
- Basic understanding of forensic processes
- Substantial familiarity with common computer systems, including the hands-on ability to manipulate computer hardware components, common operating systems and digital devices
- Substantial understanding of the electronic crime scene and how to identify, document and protect potential evidence found at the scene
- Substantial understanding of the principles of forensic acquisition, documentation and duplication of digital evidence
- Basic understanding of the forensic analysis of digital data

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:

- Identify and protect digital devices at a crime scene
- Document a crime scene and sources of digital evidence
- Handle evidence properly and maintain chain of custody
- Acquire and validate a forensic image of a digital device
- Restore a forensic image or boot an image within a virtual environment
- Locate potential evidence in a variety of digital media

Model Curriculum: Associate's Degree Programs in Digital Forensics

This section of the guide provides recommendations for an Associate's degree program in digital forensics. This degree provides an educational and practical foundation intended

to meet the minimum hiring requirements for an entry level position as a digital forensics practitioner. Additionally, an Associate degree program in digital 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.

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, etc. 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.

Specific Education Requirements

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

The minimum specific course requirements for Associate degree programs (~27 total credit hours) include:

- Introduction to Computers and Storage Media (3 credit hours)
- Applied File Systems and Operating Systems (3 credit hours)
- Basic Computer Networking and Network Security (3 credit hours)
- Introduction to Forensics (3 credit hours)
- Basic Computer Forensics (3 credit hours + 1 hour lab)
- File System and Operating System Evidence Recovery and Examination (3 credit hours + 1 hour lab)
- Analysis of Digital Media, Devices and Applications (3 credit hours + 1 hour lab)
- Basic Legal Issues (3 credit hours)

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 (e.g., Physics I and II). These courses may also be used to fulfill the institution's general education requirements.

Table 1: Model Curriculum: Associate Degree Programs in Digital Forensics	
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) which 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 credit 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)

Table 2. Recommended Course Content: Associate Degree Programs in Digital 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 World Wide 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 (e.g., 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 (e.g., 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 internetworking 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, etc

	- role of firewalls - attack and defense strategies (e.g., 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, etc. - implications of time constraints for search warrants - 4th amendment exceptions (e.g., warrantless searches) - the ECPA and relevant federal and state statutes - fundamentals of preparing for and providing testimony - civil law issues related to digital 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, etc.
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 digital forensics examinations to examinations performed by other forensic science disciplines (e.g., 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	- Demonstration of crime scene search and seizure

Lab (1 Credit hour)	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
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 (e.g., Windows, Linux, Mac, etc.) and locations of log audit data, configuration files, user profiles, etc - details of common file systems (e.g., 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 - Email - 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

NOTE: For students intending to pursue a four year degree subsequent to the Associate's degree, it is recommended that Programming I be taken as an elective.

Implementation: Keys to Ensuring Curriculum Success

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.

Institutional Support

This curriculum should enjoy a level of institutional support equal to other courses of study in an Associate's degree program. Existing digital forensics programs that are under-supported 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.

Faculty

An adequate number of full-time faculty members ensures continuity and stability to cover the curriculum and to 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, to have knowledge and experience appropriate for the courses they teach, and to recognize advisory duties as a valued part of their workload.

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

Facilities

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 when problem scenarios need to be installed for student assignments.

Each computer should be reasonably state-of-the-art, in terms of CPU, RAM, hard-disk capacity, optical (DVD, etc.) 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, etc.) 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.

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.

Student support

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

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

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:

- Encouragement of scholarly activities
- Sponsorship of research
- Opportunities to attend professional meetings
- Release time and resources for administrative duties
- Technical assistance
- Clerical assistance

Collaboration with Digital Forensics Practitioners

Academic digital 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 digital forensics. Such collaboration can provide meaningful internships, employment opportunities, guest lecturers, adjunct faculty and cooperative research.

Accreditation

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

At the time of this writing, there is no mechanism for accrediting digital forensics Associate's degree programs. When this mechanism is implemented, it is strongly recommended that all such programs seek accreditation. Accreditation provides many benefits, including:

- An external means of program validation
- A tool to help students select a program
- A means for digital forensics practitioners and potential employers to judge graduates' credentials
- An improvement of program quality

Summary

Digital 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.

This section provides recommendations for implementing a successful digital 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.

Chapter 3
Baccalaureate Degree Programs in Digital Forensics

Introduction

Forensic science is an applied science that covers an array of disciplines, including the evolving discipline of digital forensics (often called 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 digital 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.

A baccalaureate degree program in digital forensics should provide:

- Preparation for becoming a digital forensics professional
- Opportunities to establish a network of digital forensics contacts
- An educational background directly linked to the work in a digital forensics laboratory
- Exposure to the breadth of forensic science disciplines
- Acculturation into the digital forensics and justice communities
- Provision of a foundation for professional certification
- Emphasis on a wide range of courses (e.g., public speaking, technical writing, ethics, and statistics) that may not be required in the curricula of natural science majors

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

- Identify, preserve and collect digital devices in the field including networked and/or other advanced components
- Handle evidence properly and maintain chain of custody
- Document crime scene and sources of digital evidence
- Acquire, validate and restore forensic images from a variety of digital devices
- Locate potential evidence in a variety of digital media devices
- Develop/validate new techniques and solve problems using the scientific method
- Identify, analyze and solve both technical and investigative problems
- Demonstrate an understanding of computer and network components and their interactions
- Effectively communicate technical findings both verbally and in writing

Model Curriculum

This section of the *Guide* provides recommended guidelines for a model baccalaureate degree program in digital forensics. This curriculum emphasizes the strong computing foundation as well as the non-technical skills essential to prepare a student for a successful career in digital forensics. Refer to **Table 3** for an overview of the model curriculum.

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

Peer-based working groups have created specific education requirements (see Appendix E). Digital forensics laboratories and graduate programs may require more than the recommended credit hours of specific coursework.

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 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.

Computing and information science core

A digital forensics practitioner must 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.

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 digital 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 (e.g., certain chemicals used in latent print recovery may render the data on digital media unreadable). There are also concepts that are unique to digital forensics that must be included in the curriculum (see **Table 3**).

Internship

It is strongly recommended that students participate in an internship prior to graduation. Such an internship can provide hands-on training and experience in digital forensics to prepare students to be casework-ready upon completion of the program.

Table 3. Model Curriculum: Baccalaureate Degree Programs in Digital Forensics

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) which 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[a]
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 Digital Forensics (1 credit hour Seminar)
Digital Forensics Laboratory Core (12 credit hours)	Basic Computer Forensics (3 credit hours + 1 hour lab) File System and Operating System Evidence Recovery and Examination (3 credit hours + 1 hour lab) Analysis of Digital Media, Storage Devices and Applications (3 credit hours + 1 hour lab)
Upper Division Forensics Courses	
Advanced Digital Forensics Core (required: 11 credit hours)	Advanced Computer Forensics (3 hours + 1 hour lab) Network Forensics (3 hours + 1 hour lab) Storage Systems (3 credit hours)

Technical Electives[b]: (required: 9 hours from the list)	Personal Electronic Device (PED) Forensics (3 credit hours + 1 hour lab) Embedded Device Forensics (3 credit hours + 1 hour lab) Incident Response (3 credit hours) Reverse Engineering Techniques and Countermeasures (3 credit hours) Multimedia Forensics (3 credit hours) Statistics (3 credit hours) Independent Study (3 credit hours) Advanced Legal Issues in Digital Forensics (3 credit hours) Civil Legal Issues (3 credit hours)
Open University Electives (6 hours)	Free electives (may include internship)

a. This course includes ethics, testimony, evidence, chain of custody, safety, etc.
b. Electives listed here are not exhaustive, and students may wish to tailor courses according to their areas of concentration

Total Credit Hours = 120 - 124

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

Table 4: Recommended Course Content: Baccalaureate Degree Programs in Digital Forensics	
Required Courses – Lower Level	**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 World Wide 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 (e.g., 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 (e.g., 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 internetworking 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, etc - role of firewalls - attack and defense strategies (e.g., 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, etc. - implications of time constraints for search warrants - 4th amendment exceptions (e.g., warrantless searches) - the ECPA and relevant federal and state statutes - fundamentals of preparing for and providing testimony - civil law issues related to digital 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, etc.
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 digital forensics examinations to examinations performed by other forensic science disciplines (e.g., 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
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 (e.g., Windows, Linux, Mac, etc.) and locations of log audit data, configuration files, user profiles, etc - details of common file systems (e.g., 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 - Email - 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
Required Courses – Upper Level	**Content**
Advanced Computer Forensics (3 credit hours)	- alternative acquisition methods - interpret common artifacts of system usage - encryption programs and counter-forensic tools - Reconstruct events using timeline analysis

	and correlating logs. - Survey forensic tools - validate results using multiple tools - Demonstrate data carving
Advanced Computer Forensics lab (1 credit hour)	- Reconstruct events using timeline analysis and correlating logs, making necessary adjustments for time zone variations and hardware clock offsets - Validate forensic results using multiple tools - Recover obfuscated and hidden data - Correlate log files from multiple hosts
Network Forensics (3 credit hours)	- network components that may be of evidentiary significance - evidence at OSI layers - evidence recovery techniques for networks - network data reduction and filtering - forensic issues related to advanced networks (P2P, wireless, VoIP) - long-term network data storage issues - common network tools
Network Forensics Lab (1 credit hour)	- Document network architecture - Capture and analyze traffic using network devices (sniffers, IDSs) - Collect volatile network data - Conduct log analyses - Conduct a wireless network analysis - Conduct P2P network analysis - Analyze DDoS attacks
Storage Systems (3 credit hours)	- architecture and implementation of various storage devices - layout and analysis techniques for a common file systems (FAT, NTFS, EXT2/3, HFS+ etc.) - layout and acquisition for various RAID levels - layout and analysis techniques for partitions (DOS, BSD, etc.) - describe low-level steps used by analysis tools to extract data - Manually verify tool results
Elective Courses	**Content**
Personal Electronic Device (PED) Forensics (3 credit	- architecture, functionality, operating systems and implementation of PEDs (e.g.,

hours)	cell phones, PDAs, MP3 music players, GPS devices) - types of evidence recoverable from PEDs (non-volatile and volatile) - procedures for recovering evidence from PEDs - hostile forensic and booby-trapping techniques
Personal Electronic Device Forensics Lab (1 credit hour)	- Image and examine various types of PEDs - Evaluate various PED forensic tools
Embedded Device Forensics (3 credit hours)	- design and implementation of embedded devices (e.g., automobile blackboxes, process control systems (PCSs), consumer electronic devices) - types of evidence recoverable from embedded devices (non-volatile and volatile) - procedures for recovering evidence from embedded devices
Incident Response (3 credit hours)	- Identify, triage, respond, and document incidents - Analyze a live system - Develop an understanding of intrusion techniques - Demonstrate how to deal with large scale systems
Reverse Engineering Techniques and Countermeasures (3 credit hours)	- assembly language - fundamental concepts of compilers - Conduct reverse engineering using binary analysis techniques - Conduct reverse engineering using assembler and debuggers
Multimedia Forensics (3 credit hours)	- Survey of Audio, Video and Image Analysis - Audio: Signal analysis, voice comparison, and authentication - Video: Standards conversion, de-multiplexing, and authentication - Image: Comparison analysis photogrammetry, and authentication
Advanced Legal Issues in Digital Forensics (3 credit	Discussion of contemporary and evolving legal issues related to digital forensics (e.g.,

hours)	computer search and seizure, application of evidentiary standards to digital evidence)
Civil Legal Issues (3 credit hours)	Discussion of contemporary and evolving legal issues related to privacy, compliance and discovery in the civil arena (e.g., HIPAA, Sarbannes-Oxley)

NOTE: For students who have completed an Associate's Degree in digital forensics prior to matriculation, some lower level coursework credits may transfer.

Implementation: Keys to Ensuring Curriculum Success

Many universities will already have a significant number of the courses described in this document. However, significant additional resources may be necessary to create new programs or even to bolster existing baccalaureate degree programs in digital forensics. The following are essential for the proper implementation of a successful baccalaureate degree program in digital forensics.

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 to identify areas for program improvement.

Institutional support

A digital forensics curriculum is expected to enjoy a level of institutional support equal to other computing and information science programs. Baccalaureate degree programs in digital 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.

Faculty

An adequate number of full-time faculty members ensures continuity and stability to cover the curriculum and to 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, to have knowledge and

experience appropriate for the courses they teach, and to recognize advisory duties as a valued part of their workload.

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

Facilities

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 when problem scenarios need to be installed for student assignments.

Each computer should be reasonably state of the art, in terms of CPU, RAM, hard-disk capacity, optical (DVD, etc.) 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, etc.) 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.

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.

Student support

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

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

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:

- Encouragement of scholarly activities
- Sponsorship of research
- Opportunities to attend professional meetings
- Release time and resources for administrative duties
- Technical assistance
- Clerical assistance

Collaboration with Digital Forensics Practitioners

Academic digital 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 digital forensics. Such collaboration can provide meaningful internships, employment opportunities, guest lecturers, adjunct faculty and cooperative research.

Accreditation

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

At the time of this writing, there is no mechanism for accrediting baccalaureate degree programs in digital forensics. When this mechanism is implemented, it is strongly recommended that all such programs seek accreditation. Accreditation provides many benefits, including:

- An external means of program validation
- A tool to help students select a program
- A means for digital forensics practitioners and potential employers to judge graduates' credentials
- An improvement of program quality

Summary

Digital forensics is an applied multidisciplinary profession with a foundation in the practical application of science, computer technology, and the law. Therefore, it is essential that students studying digital forensics have education and training consistent with this foundation. The strengths of a baccalaureate degree program in digital forensics include professional preparation, networking, partnerships with digital forensics laboratories, work-related knowledge, and preparation for professional certification. The

baccalaureate curriculum is designed to prepare students for employment in the digital forensics field, and/or for further graduate-level education and training.

In addition, this section provides recommendations for implementing a successful digital forensics program, including program objectives and assessments, institutional support, faculty qualifications, the role of adjunct faculty, facility requirements, support of students and faculty, collaborations with digital forensics laboratories, and program accreditation.

Chapter 4
Graduate Degree Programs in Digital Forensics

Introduction

The minimum prerequisite for entry into a graduate-level digital forensics program is an undergraduate degree in a relevant field, or an unrelated undergraduate degree in conjunction with relevant experience. The prerequisites for entry into a graduate digital forensics program typically include a background in computers, computer networks, and basic legal issues with respect to digital evidence (refer to Chapter 3, Baccalaureate Degree Programs in Digital Forensics for more information). In addition, grade point average and Graduate Record Examination (GRE) scores may be considered.

A fundamental background in computers, computer networks, and basic legal issues with respect to digital evidence are central to the education of a digital forensic practitioner. A graduate-level digital forensics program is expected to do more than educate students in theoretical concepts. It should provide the student with advanced critical thinking ability, problem-solving skills, and discipline-specific knowledge. It is likely that an increasing number of digital forensics practitioners may seek graduate-level education in digital forensics, computer science, computer engineering and other related areas, which may facilitate career advancement.

Most graduate programs in digital forensics can lead to a Master of Science (M.S.) degree. The graduate curriculum recommendations later in this chapter refer to programs that award an M.S. in digital forensics. Students earning this degree are expected to be prepared for employment in the examination of digital evidence, development of digital forensic products, academia, researchers for leadership roles in public and private laboratories and academic institutions. A full discussion of digital forensics doctoral programs goes beyond the scope of this *Guide*.

An institution's educational objectives and resources govern the nature of any graduate program, and these can vary considerably. The institution is expected to be strongly committed to programs intended to prepare students for a career in digital forensics in accordance with these recommendations.

A graduate degree program in digital forensics should provide:

- Exposure to specialized topics in digital forensics
- Opportunities to develop/validate new techniques and solve problems using the scientific method
- Opportunities to conduct research in digital forensics
- Opportunities to obtain teaching experience at the undergraduate level
- Opportunities to participate in internships to enhance professional development
- Opportunities to establish or expand a network of digital forensics contacts
- An educational background directly linked to the work in a digital forensics laboratory

Students should possess specific knowledge, skills and abilities prior to entering a graduate program in digital forensics. Ideally, students should be able to:

- Identify and preserve a myriad of digital devices
- Preserve and collect digital evidence involving a network and/or other advanced components
- Locate potential evidence in a variety of digital media devices
- Acquire, validate and restore forensic images from a variety of digital devices
- Identify, analyze and solve both technical and investigative problems
- Examine digital evidence
- Understand computer and network components and their interactions
- Effectively communicate technical findings both verbally and in writing

If any of the above skills is lacking, additional coursework may be required prior to full admission to the graduate program.

Model Program

The field of digital forensics is quickly evolving. Institutional focus and other considerations may lead to a wide variation in the content and structure of graduate programs in digital forensics.

Curriculum Considerations

Graduate programs in digital forensics can be organized in many ways to reflect the institution's mission, the available facilities, and the interests and capabilities of the students and faculty. Students who enter a graduate digital forensics program with undergraduate coursework or degrees that emphasized forensic science or digital forensics may have their specific coursework adjusted to reflect this background.

An exemplary broad-spectrum graduate digital forensics curriculum will include, at its core, the following topics:

- Digital Forensics Methodology Development
  - Presented with a complex scenario involving a single device or multiple devices or systems, the student will propose, develop and validate a solution
- Advanced Operating Systems Analysis
  - Real-time systems
  - Transaction processing systems
- Digital Forensics Administration
  - Crime Scene Management
  - Laboratory Management
  - Case Management
  - Quality assurance
  - Ethics and professional responsibility

- Preservation of Evidence
  - Control & Verification Procedures
  - Evidence Dynamics: the effect of nature, humans, tools and time on the preservation and recovery of digital evidence
- Criminal and Civil Legal Issues
  - Testimony
  - Presentation of Evidence in Court
  - Advanced legal issues/legislation
  - Computer search and seizure
  - Mock trial
  - Electronic Discovery
  - Rules of Evidence
- Complex Data Analysis
  - Link analysis
  - Linking digital evidence to physical evidence
  - Timeline analysis: correlation of dates and times associated with data
  - Understanding Data Structures
- Complex Case Studies/Simulations
  - Comparison of digital evidence from numerous cases to determine whether they interrelate
  - Examining large data sets
  - Enterprise systems
  - Evidentiary issues of multiple jurisdiction and international investigations
- Data communications and Network Systems
  - Packet and frame analysis
  - Understanding of network security
  - Network traffic reconstruction and tracking

Some institutions may choose to develop specialized programs focusing on one or more of the above topics or other relevant topics.

All digital forensics programs are expected to offer rigorous graduate-level academic coursework in appropriate subjects. Syllabi are expected to be current, describe the content of the course and required textbook(s), and should indicate that the courses are advanced and comprehensive. Advanced courses should be scheduled regularly to enable students to take the courses in proper sequence and with reasonable flexibility. In addition, it is expected that a number of specialized graduate-level courses may be required to suit the students' interests and enhance the research experience. It is recommended that the program offer a graduate seminar that includes presentations by subject matter experts.

Research component

Research in digital forensics advances the body of knowledge and elevates the status of the profession. The student is expected to conduct a research project, prepare a written

report, and present the results of the research in a public forum prior to graduation. The research component of the program may include preparatory coursework in research methods and statistics. The ideal research project is well defined, stands a reasonable chance of completion in the time available, and requires the student to use advanced concepts and a variety of experimental techniques and instruments.

Implementation: Keys to Ensuring Program Success

The institution should ensure the following components are in place to provide an exemplary graduate program in digital forensics:

Institutional Accreditation

The institution granting the degree should be accredited by an accrediting body that is recognized by the U.S. Department of Education.

Faculty Requirements

To ensure continuity and stability to cover the curriculum and to allow an appropriate mix of instruction and research, the majority of the faculty in a graduate digital forensics program should be full-time. 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 have knowledge and experience appropriate for the courses they teach and to recognize advisory duties as a valued part of their workload.

Active digital forensics practitioners, often used as adjunct faculty, provide real-world experience and practical implementation of the topics and techniques being taught. However, it is essential that full-time faculty oversee the curriculum. The faculty-to-student ratio must be sufficient to assure quality research.

Library requirements and information retrieval

A library where faculty and students have access to electronic resources, books, and periodicals is essential to a successful program. An institution with a broad spectrum of research activity may require extensive holdings and is expected to subscribe to appropriate periodicals and journals. Counter-intuitively, it is important to retain legacy documents, software and hardware so that students can be exposed to systems which they may encounter in real-life casework and can perform research.

Classroom and laboratory requirements

Classrooms and laboratories are expected to meet appropriate academic and safety requirements for the number of students in the program. In addition to instructional laboratories capable of hands-on demonstration of the curriculum's chosen concepts,

faculty and students are expected to have access to laboratories with research-appropriate facilities, equipment, and instrumentation. Ideally the laboratory should be dedicated exclusively for digital forensics use to maintain the integrity of the research.

Laboratory experience

The laboratory component is expected to include the use of appropriate instrumentation and give students sufficient hands-on knowledge of digital forensics and competence to:

- Anticipate, recognize, and respond properly to electrical, chemical, and biological hazards
- Keep legible and complete laboratory records
- Conduct qualitative and quantitative analyses
- Use and understand instrumentation and fundamental techniques
- Analyze data and evaluate experimental results
- Assess reliability of results and draw reasonable conclusions
- Communicate effectively through oral and written reports

Interaction with operational laboratories

Academic programs and operational digital forensic programs are encouraged to interact. Cooperative efforts may take the form of internships, adjunct faculty interaction, collaborative research, visiting scientist programs, and seminars.

Such a cooperative effort can provide hands-on training and experience in a forensic specialty and may include discipline-specific simulated casework analysis, oral boards, mock trials, data review and interpretation, and report writing. This option can extend the normal time for completion of a graduate degree.

Funding

Substantial funding is essential for graduate digital forensics education to meet the demonstrated needs of the profession. At the time of this writing, State or Federal funding to support graduate education or research in digital forensics is limited.

In addition to State and private sources, funding may be available from the many Federal agencies including: U.S. Department of Justice (National Institute of Justice, Bureau of Justice Assistance, Federal Bureau of Investigation), U.S. Department of Homeland Security (U.S. Secret Service, Immigration and Customs Enforcement), National Science Foundation, U.S. Department of Energy, U.S. Department of Education, U.S. Department of Commerce (NIST), U.S. Department of Treasury, U.S. Department of Defense, National Aeronautics and Space Administration, and U.S. Department of State.

Support for graduate student education is essential to successful future operations of the graduate programs in digital forensics. Ideally, this support may be provided to educational institutions in the form of competitive training grants. In addition, individual

graduate research fellowships may be available. Programs may also take advantage of existing institutional graduate support mechanisms.

Appropriate legislative bodies can allow programs to forgive student loans for graduates who obtain full-time employment in public digital forensics institutions.

In addition to research and student support, funding may also be needed for the acquisition and maintenance of equipment, research instrumentation, and laboratory renovation. Institutions offering digital forensics programs should provide for ongoing costs associated with the laboratory component of the curriculum and program administration.

Accreditation

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

At the time of this writing, no mechanism exists for accrediting graduate digital forensics programs. It is strongly recommended that all programs seek accreditation when it becomes available. Accreditation provides many benefits, including:

- An external means of program validation
- A valuable tool to help students select a program
- A means for digital forensics practitioners and potential employers to judge the credentials of graduates
- Improvement of program quality

Summary

This chapter provides broad topical guidance for developing a graduate program strongly committed to preparing students for a career in digital forensics. It does not provide a detailed curriculum of course content since graduate programs can vary widely depending on the institution. This approach allows individual institutions the flexibility necessary to design their own program(s).

Chapter Five
Academic Certificate Programs in Digital Forensics

Introduction

This section of the guide is designed to help universities preparing certificate programs, students choosing among institutions offering such programs, and employers assessing certificate programs for their employees. Often universities create certificate programs when limited resources preclude the ability to create a degree program. Sometimes certificate programs are created to gauge interest, to provide an educational alternative, or when the topic material does not justify a degree program.

An academic certificate is earned upon successful completion of a set of courses offered by a college or university focused on a specialty. Academic certificates differ from formal degrees in that the courses alone are insufficient to warrant a degree. In some cases these courses may be credited towards a degree.

Certificates in digital forensics alone may not be sufficient for an entry level position in digital forensics. They should be used to supplement other training and education in computer science, engineering, digital forensics or other related practical or theoretical experience. Trying to identify a typical certificate student is difficult because they come from a variety of backgrounds. Candidates could include a law enforcement officer assigned to a digital forensics position or someone not involved in law enforcement but possessing skills required for digital forensics. Each student will have a specific reason to pursue a certificate program. For example, a computer science student may choose to fulfill elective requirements by taking courses offered in the certificate program, a recent college graduate may enroll in a certificate program to gain credentials for a better position, a practitioner may obtain a certificate to meet the continuing education requirements of his employer.

Model Curriculum

A model certificate program in digital forensics consists of 12-20 credit hours (4-6 courses) specific to the discipline or sub-discipline of interest.

Although there may be no prerequisites for entry into an undergraduate certificate program, individual courses may have requirements that must be satisfied prior to admission.

A sample curriculum for an undergraduate certificate program in digital forensics appears below:

Digital Forensics (4-6 total courses 12-20 credit hours total):

- 2-3 core courses (7-11 total credit hours)
  - Introduction to criminal justice/criminal investigation

    - Basic computer forensics with laboratory (hardware/software/file systems/media)[1]
    - Advanced computer forensics with laboratory (operating system evidence recovery and examination)[2]
- Sample Electives (2-3 additional courses from the below list, 6-9 total credit hours)
    - PDAs, cell phones, personal device forensics
    - Live network forensics
    - LINUX operating systems forensics
    - Macintosh forensics
    - Data mining
    - Analysis of digital media and applications[3]
    - Internet trace evidence analysis

In addition to undergraduate certificates, examples of advanced certificates appear below. Topics covered by coursework for each certificate below may include:

Forensics of Hardware Devices
Mobile data storage devices, software and hardware RAIDs, mobile phones and optical media.

Network Forensics
Wireless, WANs, LANs and PANs.

Multi-media analysis
Video, audio, video surveillance systems, image and video signal processing.

Data concealment
Cryptography, steganography, alternate data streams, and obfuscation.

Software Reverse Engineering
Malware, software protection, and compilers.

Data Analysis
Data reduction, data fusion, and social network correlation.

Unix/Linux forensics
Unix/Linux operating systems and file systems, use of Unix/Linux-based forensic tools, capturing data from a running Unix/Linux system.

[1] Refer to Table 2 for detailed course content information
[2] Refer to Table 4 for detailed course content information
[3] Refer to Table 2 for detailed course content information

Macintosh Forensics
Macintosh operating systems and file systems, use of Macintosh-based forensic tools, capturing data from a running Macintosh system.

Implementation

Regardless of the numerous variables that will influence the certificate program, all certificate programs should be structured, measurable and documented.

Structure

Each course included in the certificate program is expected to include the following predefined components:

- Learning objectives
- Instructor qualifications
- Detailed syllabus or program description
- Assessment
- Documentation

Measurement

Assessment mechanisms may include:

- Oral exams or reports
- Written exams or reports
- Peer-reviewed publications
- Instructor or presenter evaluation
- Scenario-based practical and hands-on exercises
- Observation of technical performance

Documentation

The institution should maintain records that include any certificates awarded in addition to the standard information maintained on a transcript.

Funding

Substantial funding may be necessary to create new programs and to maintain existing digital forensics programs. Funding can create an incentive for programs to provide students with the highest quality education.

Accreditation

At the time of this writing, no mechanism exists for accrediting digital forensics certificates. When this mechanism is implemented, it is strongly recommended that all programs seek accreditation.

Summary

Certificate programs provide specialized training in various areas of digital forensics. They can be taken in conjunction with undergraduate or graduate degrees, as an alternative to a degree, or as a supplement to ongoing practical experience. Academic institutions' certificate programs may provide an expeditious means to meet the growing demand for digital forensics practitioners.

Chapter 6
Training and Continuing Education

Introduction

This section of the Guide outlines model criteria and implementation approaches for the training and continuing professional development of digital forensics practitioners. Model criteria are presented separately for training to attain competency and for continuing professional development.

Training is the formal, structured process through which a digital forensics practitioner reaches a level of scientific knowledge and expertise required to conduct specific digital forensic analyses. Appropriate training and experience is required before an individual is qualified to perform independent casework.

Continuing professional development is the mechanism through which a digital forensics practitioner remains current or advances to a higher level of expertise, specialization, or responsibility. All digital forensics practitioners have an ongoing obligation to remain current in their field through continuing education and other developmental activities noted in **Figure 1**. Similarly, management has an ongoing responsibility to provide support and opportunities for this continuing professional development.

Recognition of any training or continuing professional development requires proper documentation. The agency and the training entity are expected to keep permanent, official training records and to provide the trainee with a copy. The trainee is encouraged to keep a copy of the training record. The training record may include:

- Documentation that entry requirements have been satisfied.
- Detailed description of program structure, content, and assessment.
- Trainee performance documentation.
- Certificate or statement of successful completion of the training program.

Model Criteria: Competency, on-the-job and continued professional development

Model criteria are intended as a guide for formulating training and continuing professional development programs. These model criteria can provide a common framework across digital forensics disciplines and thereby help ensure that programs are consistent and contain essential elements.

Program content can be designed to include both discipline-specific and core elements. Core elements are essential topics that lay the foundation for entry into professional practice regardless of the specialty area. They include the following:

- Standards of conduct—includes professional ethics training
- Safety—includes biological, chemical, and physical hazards

- Policy—includes such administrative and laboratory policies as standard operating procedures, quality assurance, accreditation, and security
- Legal—includes expert testimony, depositions, rules of evidence, criminal and civil substantive and procedural law, and evidence authentication
- Evidence handling—includes recognition, collection, preservation of evidence (e.g., electrostatic discharge protection device), interdisciplinary issues (e.g., prioritization of evidence processing when multiple types of evidence may be present), and chain of custody
- Communication—includes written, verbal, and nonverbal communication skills, report writing, exhibit and pretrial preparation, and trial presentation

Discipline-specific elements guided by recognized peer-defined standards can be incorporated as appropriate. Topics include:

- History of the discipline
- Relevant literature
- Methodologies and validation studies
- Hardware, software and other digital media
- Knowledge of related fields
- Testimony
- Training specific to particular types of crimes
- Knowledge of legal aspects

Training

Model training criteria, whether private sector, agency-provided in-house, or other should include program structure and content, assessment mechanisms, and documentation.

Exemplary program structure includes the following written components:

- Learning objectives
- Instructor qualifications
- Student requirements
- Detailed syllabi
- Performance goals
- Periodic assessments
- Competency testing
- Ongoing proficiency testing

The trainee's progress is expected to be assessed at appropriate intervals. Assessment mechanisms may include:

- Oral exams
- Written exams
- Scenario-based practical exercises

- Mock trials
- Assessment of technical performance by appropriate senior staff

Documentation

An agency is expected to maintain an official record of employees' training activities. Employees are encouraged to keep copies of their records. The agency's record is expected to include a description and format of the activity, and documentation of performance (when available), such as academic credit, continuing education credit, certificates, and/or abstracts of proceedings.

On-the-Job Training Programs

For the purposes of this Guide, on-the-job training consists of training conducted after the date of hire in order to ensure competency before performing independent casework. On-the-job training could be conducted off-site, in-house or through a combination of both. Components of an on-the-job training program should include:

- Tool familiarization
- Policies and procedures
- Performance milestones
- Assessments
- Competency testing
- Technical certifications
- Seminars and workshops

Continuing professional development

Continuing professional development encompasses competency maintenance and skill enhancement. It is important that continuing professional development be structured, measurable, and documented.

Structure

Courses for continuing professional development are expected to include the following predefined components:

- Learning objectives
- Instructor qualifications
- Detailed syllabus or program description
- Assessment
- Documentation

Measurement

Assessment mechanisms may include:

- Oral exams or reports
- Written exams or reports
- Peer-reviewed publications
- Instructor or course evaluation
- Scenario-based practical and hands-on exercises
- Observation of technical performance

Documentation

An agency is expected to maintain an official record of employees' continuing professional development activities. Employees are encouraged to keep copies of their records. The agency's record is expected to include a description and format of the activity, and documentation of performance (when available), such as academic credit, continuing education credit, certificates, and/or abstracts of proceedings.

Implementation: Making the Most of Training and Continuing Professional Development

Training and continuing professional development based on the model criteria can be implemented in a variety of ways to maximize opportunities, minimize costs, and ensure high standards of professional practice. The examples below offer guidance for implementation.

- Instructor led training programs
- Professional conferences/seminars
- Distance learning (e.g., webcasts)
- Internship
- Mentoring
- Teaching and presentations by trainee/employee
- Independent learning
- Targeted feedback based on annual proficiency testing
- Listservs
- Participation in professional organizations
- Certificate programs
- Vendor sponsored training
- Professional journals
- Networking with peers

Different disciplines require varying levels and combinations of approaches to training and continuing professional development. The approach depends on the relative degree of academic and experiential learning required to attain and maintain competency.

Administration

It is recommended that digital forensics operations or institutional authorities establish a process to oversee, coordinate, and document all training and continuing professional development. In addition, quality control of the training program could be achieved through external audits.

It is recommended that continuing education and training courses include:

- Qualified instructor(s)
- Written course syllabus/outline
- Written course objectives
- Instructor/course evaluation
- Mechanism for student assessment
- Documentation of student performance
- Quantifiable element, such as continuing education units, academic credits, number of hours, or points

Although seminars, lectures, professional meetings, and in-service training classes may be less structured than a formal course, they also add to the professional development of digital forensics practitioners. Content and attendance are expected to be documented and available for external audits.

Sources

The sources of training and continuing professional development can be internal and/or external to a digital forensics unit. Training partnerships are valuable because they provide broad perspectives and facilitate consistency of professional practice. Sources can include:

- Government agencies
- Academic institutions
- Training academies and institutions
- Private industries and organizations
- Professional societies and associations (local and national)
- Mentors

Funding

Resources are needed to properly support training and continuing professional development. In addition to their regular duties, qualified digital forensics practitioners and supervisors are expected to receive time to continue professional development and to mentor trainees. In addition, the nature of digital forensics and evolving technology may require more ongoing training to remain current compared to other disciplines. Agencies should anticipate and plan for the effects of training on case productivity.

Agencies can partner to develop and provide intensive formal discipline-specific programs for trainees. These programs can relieve operational digital forensics facilities of some of the in-house mentoring needed to qualify individuals to conduct casework. This partnering model also can be extended to continuing professional development, with agencies working together to develop and provide standardized training curricula and materials for use across several agencies. Although these partnerships can significantly reduce costs, funding for student attendance may still be needed.

When considering the costs of continuing professional development, some scientific/technical working groups recommend minimum mandatory continuing education. Continuing education requirements may be imposed by agencies, accrediting bodies, certifying bodies and/or professional organizations. For example, the FBI Computer Analysis Response Team (CART) requires its practitioners to take a minimum of 64 contact hours per year. The American Society of Crime Laboratory Directors Laboratory Accreditation Board (ASCLD-LAB) requires a minimum of 40 contact hours per year for all examiners in the laboratory. The International Association of Computer Investigative Specialists (IACIS) recommends 60 contact hours of continuing education plus a competency examination every three years for individuals to maintain certification.

Some agencies choose to impose their own continuing education requirements which may be based on or exceed the requirements listed in the above paragraph. Agencies may specify a training and continuing professional development budget on a per-examiner basis. Such funds are used to support travel and fees for both outside learning opportunities and implementation of in-house programs. It is recommended that anticipated costs related to travel, equipment (hardware, software) and vendor-sponsored courses be taken into consideration when developing budget allocations for training and continuing professional development. Additionally, the cost of specialty training related to emerging issues should be considered. Examples include new technologies or new operating systems (e.g., PDAs, cellular phones, wireless) or forensic techniques to counter emerging threats (e.g., malicious software, systems vulnerabilities).

The professionalism expected of digital forensics practitioners requires that appropriate resources for training and development be provided by the parent agency. Digital forensics is a labor-intensive undertaking, in which the quality, experience, and technical currency of personnel performing the work are paramount. Neglecting ongoing training and professional development can lead to program failure.

Regardless of the mechanism used, it is essential that a reasonable foundation be put in place to offset the direct and indirect costs of an adequate program of training and continuing professional development.

Summary

Model criteria are presented as a framework for achieving and maintaining professional competency in digital forensics. Implementation of these criteria will extend learning opportunities and promote high standards of professional practice.

Appendices

Appendix A
Digital Forensics Careers

Traditionally, computer forensics examinations were performed by law enforcement officers and crime laboratory personnel to support the investigation and prosecution of crimes. However, the same skills are now being used in many areas in both the public and the private sector. Corporations, government and military organizations frequently employ computer forensics techniques for purposes such as internal investigations, intrusion investigations, preservation of information, and intelligence gathering.

Public Sector

Digital forensics employment opportunities in the public sector include positions in the criminal justice system, forensic crime laboratories, military services and other government agencies. Within the criminal justice system, positions exist in Federal, State and local law enforcement agencies as agents, investigators, detectives and forensic examiners, who specialize in cases involving digital evidence. There are some Federal, State and local prosecutors who specialize in cases involving high-tech crime; their offices may have their own support personnel with digital forensics skills. Opportunities are available within forensic crime laboratories for digital forensics examiners where they may encounter evidence related to homicide, drug investigations, child exploitation, white collar crimes, etc. The military services and intelligence and security agencies have opportunities for digital forensics specialists in investigations, information and intelligence gathering, and counterintelligence. Other government agencies (e.g., IRS, FTC, SEC, FDA) may employ digital forensics personnel to assist in functions such as regulatory and compliance activities.

Private Sector

Digital forensics employment opportunities in the private sector include positions in corporations and other entities involved in litigation, internal investigations, and information security. These may include private forensics laboratories, internal information technology positions, private investigative organizations, accounting firms and other companies that provide digital forensics services. Employment opportunities also exist with companies that design and develop digital forensics hardware and software tools, and provide training and consulting. Note, some states may require licensing in order to conduct independent digital forensics examinations.

Appendix B.

List of Organizations

The following is a list of organizations to which a draft copy of this document was mailed.

Alaska Criminal Laboratory
America Online
American Society of Law Enforcement Trainers
Bank of America, Corporate Information Security
Bureau of Alcohol, Tobacco, Firearms and Explosives
California Department of Justice Advanced Training Center
Chicago-Kent College of Law, Illinois Institute of Technology; Center for Law and Computers
Chicago RCFL Office
Computer Forensics Branch
Computer Forensics Inc.
Criminal Division (CCIPS), U.S. Department of Justice
Defense Computer Investigator Training Program
DEA Digital Evidence Laboratory
Federal Bureau of Investigation National Infrastructure Protection Unit
Federal Law Enforcement Training Center (FLETC) Legal Division
Financial Fraud Institute
Guidance Software
Hawaii Police Department
Mares and Company
Missouri Southern State University
The MITRE Corporation
The National Academies, Computer Science and Telecommunications Board National Law Enforcement and Corrections Technology Center–West; c/o The Aerospace Corporation
Naval Criminal Investigative Service Headquarters
Norcross Group
Ohio Bureau of Criminal ID and Investigation
Purdue University
RCFL, Heart of America Office
RCFL, Intermountain West Office
RCFL, Miami Valley Office
RCFL, National Program Office
RCFL, North Texas
RCFL, Northwest Office
RCFL, Rocky Mountain Office
RCFL, San Diego Office

RCFL, Silicon Valley Office
Regional Electronics and Computer Investigation Section; Hamilton County Sheriff's Office
School of Public Safety & Professional Studies University of New Haven
U.S. Department of Defense Cyber Crime Center
U.S. Postal Service Office of Inspector General

Appendix C
Professional Organizations and Associations

American Academy of Forensic Sciences (AAFS)
American Society of Crime Laboratory Directors (ASCLD)
Digital Detective Forum (DDF)
Electronic Crime Partnership Initiative (ECPI)
Forensic Association of Computer Technologists (FACT)
High Technology Crime Consortium (HTCC)
High Technology Crime Investigation Association (HTCIA)
International Association of Computer Investigative Specialists (IACIS)
International Organization on Computer Evidence (IOCE)
International Police Organization (Interpol)

Appendix D
Technical and Scientific Working Groups

Digital Forensics Research Workshop (DFRWS)
Digital Forensics Working Group (DFWG)
International Federation of Information Processing Working Group 11.9 on Digital Forensics (IFIP WG 11.9)
Scientific Working Group on Digital Evidence (SWGDE)
Scientific Working Group on Imaging Technologies (SWGIT)

Appendix E
Technical and Scientific Working Groups Educational Criteria

Scientific Working Group on Digital Evidence (SWGDE) – www.swgde.org

Scientific Working Group on Imaging Technologies (SWGIT) – www.theiai.org/swgit

Appendix F
Supplemental Resources

TWG member organizations

Access Data
Air Force Institute of Technology; Department of Electrical and Computer Engineering
American Academy of Applied Forensics (AAAF); Central Piedmont Community College
Assured Information Security Cyberforensics Science and Technology Center
AFRL/IFGB
CERIAS / Purdue University
Champlain College
DCITP
Department of Defense
Department of Defense Cyber Crime Center
Digital Intelligence, Inc.
Electronic Crime Partnership Initiative (ECPI)
Fairmont State University
Federal Bureau of Investigation CART Training
Federal Bureau of Investigation; Forensic Audio, Video and Imaging Analysis Unit
Guilford County S.O.; Special Operations/Computer Crimes
Hewlett Packard
Huron Consulting Group
Illinois Attorney General's Office
Information Systems Integrity Group; London School of Economics (England)
Infosec
M. J. Menz and Associates
Maryland State Police; Computer Forensics Laboratory
Marshall University Forensic Science Center
Nassau County, New York Police Department; NewYork Electronic Crimes Task Force
National Center for Forensic Science (NCFS), University of Central Florida (UCF)
National Center for Justice and the Rule of Law
The National Centre for Policing Excellence (England)
The National Consortium for Justice Information and Statistics
National White Collar Crime Center (NW3C)
Nebraska State Patrol - Omaha; Internet Crimes Against Children Unit
Northern District of West Virginia US Attorney's Office
Rochester Institute of Technology
Sacramento High Technology Crimes Task Force
San Diego Regional Computer Forensics Laboratory
Sci**Law**Forensics, Ltd.
SEARCH, the National Consortium for Justice Information and Statistics
Stroz Friedberg, LLC Technology Pathways LLC
SUNY at Buffalo; Computer Science and Engineering Department

United States Secret Service
University of California, San Diego; San Diego Supercomputer Center, Pacific Institute for Computer Security
University of Dayton, School of Law Division of Technology and Advancement; Erie County Sheriff's Office
The University of Tulsa
University of Washington
US Immigration & Customs Enforcement, Cyber Crime Center; Department of Homeland Security
U.S. Postal Service; Forensic and Technical Services
Western District of Michigan U.S. Attorney's Office
West Virginia State Police; Bureau of Criminal Investigation
West Virginia University

Generic statement on federal agency assistance or resources

Appendix G
Glossary

The below definitions are meant to explain the included terms as they are used in this Guide.

Assembler
Software that translates a low level program into a form that can be executed by a computer

Capstone Project
A 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

Compiler
Software that translates a high level program into a form that can be executed by a computer

Computer Forensics
The science of identifying, collecting, preserving, documenting, examining and analyzing evidence from computer systems, the results of which may be relied upon in court.

CPU: (Central Processing Unit)
The computer chip that interprets commands and runs programs.

Cryptography
Using the sciences of encryption to transform data to hide its information content and decryption to restore the information to its original form.

DDoS: (Distributed Denial of Service)
The intentional paralyzing of a computer or a computer network by flooding it with data sent simultaneously from many locations**.**

Data Fusion
The process of associating, correlating, and combining data and information from single and multiple sources.

Debugger
Software that is used to find faults in programs

De-Multiplexing
The process of isolating individual images from a video flow

Digital Evidence
Information of probative value that is stored or transmitted in binary form that may be relied upon in court

Digital Forensics
The 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.

ECPA (Electronic Communications Privacy Act)
The ECPA 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.)
www.cybercrime.gov/cclaws.html

Embedded Device
A special-purpose computer system, which is completely encapsulated by the device it controls. An embedded system has specific requirements and typically performs pre-defined tasks, unlike a general-purpose personal computer.
http://en.wikipedia.org/wiki/Embedded_device

Enterprise System
Computer systems and/or networks integral to the operation of a company or a large entity, possibly global in scope.

ext2/ext3 (Linux-Extended 2/Linux-Extended 3) **File System**
A file system typically used with Linux-based operating systems

FAT (File Allocation Table) **File System**
The original file system used with Microsoft and IBM-compatible operating systems - still in common use.

FDA (Food and Drug Administration)

FTC (Federal Trade Commission)

Graduate Seminar
Seminar usually required of graduate students with presentations in a technical area

IDS (Intrusion Detection System)
Software or hardware that is used to identify attacks or anomalies on computers and/or networks

IRS (Internal Revenue Service)

In-Service Training

Periodic training provided for those actively engaged in a profession or activity.

LAN (Local Area Network)
A computer network covering a local area, like a home, office or small group of buildings such as a college.

Link Analysis
A 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

Malware
Malicious software designed to cause unexpected and frequently undesirable actions on a system (e.g., viruses, worms, spyware or Trojan horses)

Mock Trial
Often referred to as "moot court," role playing court proceedings intended to prepare students for courtroom testimony

NTFS (New Technology File System)
An advanced file system with security features commonly used with the Windows NT, Windows 2000, Windows 2003 and Windows XP operating systems.

P2P (Peer to Peer)
A communications network that allows multiple computers to share files

PAN (Personal Area Network)
A networking scheme that enables computers and other electronic devices to communicate with each other over short distances either with or without wires.

Partitioning
Software method of dividing a physical hard drive into logical containers that will appear as multiple logical drives

PED (Personal Electronic Device)
Consumer electronic devices that are typically mobile or handheld (e.g. PDA, cell phone, iPOD)

Photogrammetry
Science of obtaining dimensional information of items depicted in photographs

PKI (Public Key Infrastructure)
A system that uses encryption to verify and authenticate network transactions

OSI (Open System Interconnect)
A layered model that describes the way computers communicate on a network

RAID (Redundant Array of Inexpensive/Independent Disks)
A system that uses two or more drives in combination for fault tolerance or performance.

RAM (Random Access Memory)
A computer's read/write memory, it provides temporary memory space for the computer to process data.

SEC (Securities and Exchange Commission)

Steganography
A 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

Thumb Drive
A small digital storage device that uses flash memory and a USB connection to interface with a computer

Topology
The physical layout or logical operation of a network

VoIP (Voice over Internet Protocol)
A technique for transmitting real-time voice communications over the Internet or other TCP/IP network

VPN (Virtual Private Network)
A computer network that uses encryption to transmit data in a secure fashion over a public network

WAN (Wide Area Network)
A computer network covering a wide geographical area.

Updated March 6, 2006