Digital Forensics Education: A Multidisciplinary Curriculum Model

Imani Palmer[1], Elaine Wood[2], Stefan Nagy[1], Gabriela Garcia[3], Masooda Bashir[4(✉)], and Roy Campbell[1]

[1] Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL 61801, USA
{ipalmer2,snagy2,rhc}@illinois.edu
[2] Department of English, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL 61801, USA
wood10@illinois.edu
[3] Illinois Science, Technology, Engineering, and Mathematics Education Initiative, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL 61801, USA
gjuare3@illinois.edu
[4] Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL 61801, USA
mnb@illinois.edu

Abstract. This paper reports experiences and lessons learned in the process of developing and implementing an undergraduate curriculum for digital forensics over the last three years at the University of Illinois at Urbana-Champaign. The project addresses the challenges of developing a higher-education standardized curriculum for digital forensics that meets the needs of the digital forensics community. The curriculum provides degree options and considers the growing employability of digital forensics students in an increasing range of jobs. The approach builds on the multidisciplinary nature of the field. The findings include a curriculum model, detailed course content, exams, and an evaluation package for measuring how students respond to the courses. This paper summarizes the model, results, challenges, and opportunities.

Keywords: Digital forensics · Standardization · Higher education · Portable curriculum · Multidisciplinary approach

1 Introduction

Digital forensics involves the investigation of data/evidence from computers, networks, and other electronic devices. It is multidisciplinary in the sense of depending not only on technical aspects of investigation, but on a combination of skills and knowledge of application areas including mathematics, statistics, law and courtroom procedure, government policies, psychology, library science, and finance. Efforts to establish a cohesive body of knowledge and standard curriculum practices remain largely under-developed because digital forensics, and forensics itself, is a new science, quickly

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 3–15, 2015.
DOI: 10.1007/978-3-319-25512-5_1

developing, with applications for all sorts of uses in society. This project argues that computer forensics education is not the same as computer security although it shares many common techniques. The difference lies in the nature and process of digital evidence when it is used by society for social processes, whereas, security concerns information assurance and availability.

Members of the digital forensics community are concerned by the relative absence of digital forensics practitioners training [1–4]. There is a broad need for higher-education standards and curricula. To address the need for a standardized high-quality digital forensics education program, this project, in conjunction with the National Science Foundation (NSF), is developing and piloting a curriculum package in digital forensics suitable for adoption by other institutions. Research by Woods et al. [9, 26], Ismand and Hamilton [27], Al Amro et al. [28], describe a technical foundation for the development of digital forensics education programs. Their scholarly findings provide a basis for this program's development, detailed below.

A Digital Forensics program could be organized in a number of ways. The proposed and adopted approach encourages widespread distribution. Specifically, the Digital Forensics curriculum is offered as a specialization to an existing degree within a department of a university. The project has designed a three-course series of study to prepare students for an increasing number of digital forensics related job openings. The design includes multidisciplinary themes within the curriculum model. The curriculum can be taught as a specialization within just one department or shared between any or all of the multidisciplinary degrees. The project's progress in establishing and implementing a standardized curriculum over the past three years is elaborated in the remainder of this paper. The following sections discuss findings and issues concerning this curriculum.

2 Related Work

Research investigators discuss different approaches to introduce digital forensics in higher education. Chi et al. [6] reported on the challenges of teaching computer forensics at Florida A&M University to students without a strong technical background. To supplement the students' need for technical knowledge, Chi et al. created preparatory courses for students to bolster their prerequisite knowledge of computer forensics before introducing the more technical components of the field. In contrast, Srinivasan [7] described a course on computer forensics at the University of Louisville available only to computer information systems students concentrating in information security. Bashir et al. [5] published research findings on a more multidisciplinary approach.

Other research investigations focus on building a curriculum around industry needs and fortifying the employability of their students in fields related to digital forensics. Liu's baccalaureate program in digital forensics at Metropolitan State University adopted a "practitioner's model," aimed to prepare students for their target industries [20]. This approach failed to recruit the necessary qualified faculty for implementing the model. Wassenaar et al. [8] discusses an approach by Cypress College that prepares students for professional certification. The program required instructors that are digital

forensics practitioners. The program's credibility relied on instructors' abilities to communicate their industry experience.

This project's design and development was influenced by challenges to digital forensics education already identified, discussed, and published by Bashir [5], Lang et al. [10], Woods [9], Walls et al. [11], Beebe [12], Kwan et al. [13], Bishop [14], Craiger et al. [15], Nance et al. [16], and Burnett [17]. Further, this project identified challenges faced by institutions involved with implementing digital forensics programs. These include: balancing training and education [18, 19], lack of an adequate textbook on digital forensics [20], finding qualified faculty [19, 20], lab setup [19, 20], selecting appropriate prerequisites [6, 20], and absence of widely accepted curriculum standards [21–24].

3 Background

To help address the need for qualified digital forensics professionals, this project develops an adoptable curriculum. The goal is to distribute it as a self-contained curriculum package. This includes an instructor handbook, a lab instructor handbook, lecture slides, and question sets. This will be a significant contribution to the digital forensics education community [2]. When complete, the program will consist of an introductory, an advanced course in digital forensics with accompanying hands-on laboratory sessions, and a special topics course. The introductory course is accessible to a wide range of students from many disciplines and valuable as a stand-alone offering. The second course is more technically intensive, but it is intended to be accessible and valuable to students from non-technical disciplines. The third course is a purely technical course, and it focuses on new relevant topics of digital forensics [2].

This DF program is not necessarily a job-track training program intended to prepare students to directly enter the job market as digital forensic examiners and analysts. Instead, it provides a broadly applicable education in the field of digital forensics that will be valuable for students going into many disciplines related to digital forensics, such as law, in addition to forensic analysts. It is expected that these students will receive additional education training specific to their career paths and some on-the-job training specific to their eventual professional roles. At the time of writing, this project developed curriculum for the introductory and advanced course. The pilot courses of both were taught and in the process of curriculum revision for distribution to other institutions [2]. The content includes modules developed collaboratively by faculty experts in multiple fields of computer science, law, psychology, social sciences, and accountancy.

4 Methodology

The vision and strategy for this standardized Digital Forensics education curriculum proposes that digital forensics would be best suited as a *specialization* within a technical domain. The curriculum design envisioned a three-course sequence. The hallmarks of the program include a multidisciplinary approach to digital forensics education. Also, domain experts from multiple fields related to digital forensics develop and teach the curriculum. The course work is modular and portable. Also, live evaluation feedback of the curriculum and teaching was part of the entire design for this project from the beginning.

The modules are combined to form a coherent narrative and introduce students to the complex and multiple dynamics of digital forensics. The laboratory assignments from the project's introductory course solely use open source content (detailed below). Further, the modular course content is designed with the intention of being easily adaptable and integrated at various educational institutions.

Digital Forensics is essentially multidisciplinary – encompassing evidence collection, evidence preservation, evidence presentation, forensic preparation [2] – the research team for this project is also multidisciplinary and includes computer science, electrical and computer engineering, criminal justice, law, psychology, and educational assessment experts. The proposed curriculum introduces students to various application areas of digital forensics, including topics such as fraud investigation and digital archives, with the aim of demonstrating the breadth of application for diverse knowledge in the field. The sections below will detail the specifics for Digital Forensics 1, Digital Forensics 2, and Digital Forensics 3.

To satisfy the multidisciplinary aims of this three-course curriculum sequence, professors and experts in digital forensics and related fields deliver subject-specific course material during lectures. The fields of study mentioned above, including technical and non-technical topics, were carefully chosen as the result of an extensive review of literature that outlined relevant intersecting topics in the expansive field of digital forensics. Experts, who attended the Digital Forensics Research Workshop (DFRWS 2011 – 2013), confirmed the accuracy of structuring the course to include these specific fields.

4.1 Digital Forensics 1

Digital Forensics 1 is an introductory course designed to offer an initial overview of the field to students from a broad range of disciplines. Designing a digital forensics curriculum that is appropriate for a large target audience creates particular problems and challenges. It is difficult for a single class to offer a comprehensive introduction to a field as complex as digital forensics; however, the pilot course covered the major forensics-related fields – computer, network, and mobile device – precisely because its pedagogical strategy focuses on education rather than training.

The introductory course was taught in 2013 and 2014. The classes consisted of two 75-min lecture sessions and an hour-long laboratory session each week for a 16-week term. To create a multidisciplinary and modular-based curriculum to correspond with the multidisciplinary nature of the field, the project assembled a development team to include domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. This approach allows the content developers to receive feedback from student interactions and more efficiently revise their materials. Various modules were combined to form a coherent narrative and introduce students to various perspectives of the field.

The learning objectives that guided the curriculum development were that students should understand: (a) Common terminology, techniques, and investigative procedures of digital forensics, including the related disciplines of computer forensics, network forensics, and mobile device forensics; (b) Applications of the scientific method to digital forensics investigation and its importance; (c) Various types of digital forensics evidence acquired and the limitations of current techniques; (d) Basic operations of the

U.S. justice system and court proceedings; (e) Areas related to digital forensics, such as data recovery, psychology, cyber crime, and fraud examination.

4.2 Digital Forensics 2

Digital Forensics 2 (DF2) is an advanced lecture and lab course designed to offer students an in-depth look at particular multidisciplinary topics related to digital forensics. The class consists of two 50-min lecture sessions and two hour-long laboratory sessions each week for a 16-week term. The learning objectives that guided the curriculum development were that students: (a) Should be familiar with the known barriers and challenges in digital forensics research; (b) Should be able to use their investigative skills in real-world scenarios; and (c) Should be able to contribute research to the digital forensics community. DF2 includes greater focus on technical topics and more rigorous laboratory assignments than the introductory course. It also requires students to complete a research project. Notably, despite recent consumer trends, research continues to neglect the forensics of non-Windows operating systems, file systems, and user applications. The course aims to encourage students to research Linux, Mac, and iOS operating systems as they become increasingly prominent in our daily lives. Students' understanding of multiple operating systems contributes to their ability to adapt the digital forensics investigative process for use in different systems.

Another design decision that is important to the curriculum and this advanced course is the inclusion and option for students to learn in a virtual laboratory environment. The program established a virtualized laboratory called ISLET. ISLET allows professors to demonstrate various digital forensics tools and students to complete their laboratory exercises remotely. ISLET is a container-based virtualization system for teaching Linux-based software with minimal participation and configuration effort. The participation barrier is set very low, and students need only a Secure Shell (SSH) client in order to participate [25].

Inspired by the extensive range of open research questions in the field of digital forensics, this curriculum requires students to contribute to solutions rather than only learn about the issues. To achieve this end students chose a topic for a semester-long research project. Students were guided to design manageable and relevant research topics and were provided with a list of research project ideas. Students formed groups and submitted a project proposal. Each proposal was scrutinized to establish feasibility and likelihood of contributing to digital forensics research and/or education community. The midterm progress report indicates whether students are on-track for the semester. Significantly, the report reveals any particular challenges experienced by the students at that point in the semester. This offers an opportunity for instructors to help students develop strategies for addressing challenges as they continue working on their projects. Near the end of the semester, students present their research projects in the form of oral presentations to their peers and instructors. Ultimately, they submit final project reports.

4.3 Digital Forensics 3

Digital Forensics 3 (DF3) is an advanced topics course specifically designed to include a substantial research component, challenging students to investigate, develop, and design a research project that focuses on a particular aspect related to the multidisciplinary field of

digital forensics. This course aims to enroll advanced undergraduate and graduate students to develop topic-specific research that is related to their fields of study. Students will read and examine the latest research in the area of digital forensics. They will be asked to analyze and critique an array of papers, and from this analysis, they will choose a research topic. The strategies for DF3 curriculum design are in development and will focus primarily on enhancing digital forensics research.

4.4 Evaluation Methodologies

The construction, modifications, and updates to the curriculum are based on workshops, surveys, student evaluations and performance. The construction of the initial curriculum vision is based on summaries of a series of workshops (the proceedings are now in press) that included experts in the field of digital forensics. Findings and guidance gathered from these workshops significantly added to the curriculum development process. An external evaluation team was hired to conduct a formal evaluation of the initiative by providing: (a) Ongoing feedback to inform the implementation and delivery of the curriculum, and (b) Comprehensive assessment of program effectiveness and outcome attainment. Being responsive to the multiple groups of individuals involved with the initiative helps to legitimize a diversity of perspectives and experiences and contribute to a comprehensive understanding of the curriculum being developed. To that end, the evaluation design includes both quantitative and qualitative methods developed in collaboration with the initiative's leadership team.

Three student surveys were developed, which were distributed throughout the academic semester. The initial paper-based survey is administered to registered students during the first week of the course. Its purpose is to gather initial information about enrolled students, including major, technical background, ethnicity, and gender. The second survey is administered mid-course and online after the midterm exam. This survey records how students are experiencing the course. The third survey is an end-course survey administered online during the last week of class. Its aim is to gather information about students' perspectives, experiences, and suggestions. All surveys include multiple-choice questions whereby students indicate their level of agreement with a statement on a scale from 1 to 5. Surveys also included open-ended items, inviting students to include additional comments about specific aspects of the course.

The evaluation team observed most of the lecture and lab sessions. The purpose of these observations was to assess the delivery of the curriculum content, and students' engagement and experience with the course. Information related to the following categories was noted during the observations: (a) Social or interpersonal setting: how groups and individuals were situated; (b) Activities: a systematic description of activities and time-frames; (c) Content: a description of resources and materials used and discussed; and (d) Interactions: a description of student-professor verbal and nonverbal interactions.

Group or individual interviews were conducted in the middle and at the end of the course to explore students' experiences, reactions to, and opinions on the course in detail. Each group or individual interview involved a dialogue between students and one of the evaluators, who prompted conversations about course-related topics. In an effort to maintain student confidentiality and privacy, there were no members of the course's staff or instructors present during the interviews.

5 Results, Opportunities, Challenges

This project found Digital Forensics to be a complex curriculum to teach in a higher-education institution. This curriculum model and course outlines contribute to a stronger basis for a standardized curriculum. The results are based on teaching the first course twice and the second course once and the results are supplemented with evaluations, surveys and exam results. Below is a summary of the project's findings so far, commenting on opportunities to improve the curriculum, and outlining some challenges that remain.

5.1 Findings About Students

The program attracted students from various majors, including law, psychology, math, computer engineering, and computer science. Perhaps unsurprisingly, a major problem with designing a curriculum for multiple majors is that there was a wide difference in students' expectations. Students with a technical background desired to learn more about technical topics, and typically they failed to understand the importance of non-technical topics. Students with a non-technical background and interest tended to appreciate the course overall; however, they struggled with the technical concepts and assignments of the course. The large number of possible careers includes digital forensics analyst, examiner, practitioner, security specialist, expert witness, security researcher, digital archivist, and fraud investigator added to student expectations.

5.2 Team Development of a Course

Lacking any individual with the full range of Digital Forensics expertise, the course sequence is team-taught. The project struggled to present a cohesive course and maintain course integrity related to the differing approaches of the team. Multiple professors did achieve the aim to provide students with a broader understanding of the topics presented. However, many students failed to grasp all of the connections. The intention for the final product is that one instructor will be able to teach all the materials. Part of this project involves providing background material as a teaching aid.

5.3 Digital Forensics Theory and Practice

Approaching Digital Forensics education using a scientific approach requires evaluation of methods and experimental results. However, scientifically evaluating Digital Forensics methods and reasoning about that evidence using logic is immature in theory and in practice. The project introduced a module in Digital Forensics 2 on "Reasoning about Evidence" with the intention of promoting a more scientific approach to digital forensics research than was offered in the introductory course. The following challenges resulted from this approach. First, the time limitations of a 16-week course limited covering several topics in depth. Second, digital forensics practitioners, educators, and researchers identified that a robust scientific basis for the evaluative methods involved with digital forensics investigations was ongoing research. The Scientific Working Group on Digital Evidence (SWGDE), for instance, have released several documents since 1999 concerning digital forensics standards, best practices, testing, and validation

processes, and these were considered in the development of our curriculum. Additionally, in 2001, the U.S. National Institute of Standards and Technology (NIST) began the Computer Forensic Tool Testing (CFTT) Project. It subsequently established and implemented validation test protocols for several digital forensics tools. Moreover, DF2 includes a module entitled tool validation but remains challenging because tool evaluation technologies are unavailable.

The first Digital Forensics Research Workshop (DFRWS 2011) initiated a gathering of over 50 researchers, investigators, and analysts. It aimed to establish a research community that would apply the scientific method in finding focused near-term solutions that were based on practitioner requirements. The community addressed future aims for developing the field of digital forensics. The related curriculum emphasizes the need to bring rigorous scientific methodological approaches to evidence evaluation. One example is "fuzzy logic," a particular form of reasoning about digital evidence. Fuzzy logic allows elements to be identified as true or false *to some degree*. A "fuzzy engine" provides a solution to human errors (such as word misspellings) that might skew the results of analysis by selecting an acceptable degree of "fuzziness." A fuzzy expert system regards a misspelled or mistaken word as input and then finds relationships for it with other similar words.

5.4 Project Opportunities

The Digital Forensics 2 advanced course implements a semester-long research project. This provided the students with opportunities to explore different concerns of Digital Forensics. For example, several students decided to develop a case study as their research project that will be available to other institutions to be used in future work and may also be incorporated into the next iteration of the introductory course, Digital Forensics 1. A group interested in social media investigated the amount of shared information by considering application programming interfaces that could potentially be used to extract data about individuals. The project involves the creation of a correlation engine that would be able to demonstrate a connection between application programming interfaces and the ability to extract information about an individual from an online environment. Another group of students introduced digital forensics to high school students. Modeled on their own abbreviated curriculum they also created challenge exercises for the high school students. The goal of the students is to produce outcomes of their project that will contribute to outreach programs that engage students of all ages in digital forensics education. Yet another research group designed a lab for students to examine Mac operating system malware and relevant legal aspects of an investigation.

5.5 The Laboratory Environment: Results and Challenges

The collaborative virtual lab environment also led to some challenges. It requires students to be knowledgeable about the Linux command-line, which is a challenge for many non-technical students. This will hopefully be overcome in the future by designing a laboratory assignment based on an introduction to the Linux command-line.

5.6 Evaluation Methodology Challenges

The evaluation progressed with some challenges. As the aim of the evaluation is to provide ongoing feedback to the initiative's leadership team, a mid-course survey is administered to students during each course. Much of the feedback provided by students is related to the structural organization of the course, which is not feasible to change in the middle of the semester. Another challenge is the variability in student participation. Encouraging students to participate in surveys and interviews was difficult as students' participation declines closer to the end of the semester. Different strategies are being explored to maintain and encourage student participation. Another challenge is that the data gathered are representative of the perspectives and experiences of students enrolled at a particular university. As an alpha version of the curriculum is in the process of being distributed, the goal is to also gather data from institutions adopting the curriculum. Gathering a broad range of data will potentially provide support for the initiative's goal of the curriculum's acceptance as a national standard.

The course enrolls students from various majors, including law, psychology, math, computer engineering, and computer science. Conducting course and lab session observations yielded a significant amount of insight about the curriculum being implemented. First, these observations offered an immediate impression of how the courses are progressing, which informs and further enlightens data gathered from surveys and interviews. For instance, during the evaluation of the introductory course in the fall of 2014, it was observed that students struggled with answering and finishing lab assignments. Students were asked in an open-ended question format about the pace and structure of the lab, especially if they were dissatisfied with the lab section. Second, conducting observations allowed for the evaluation team to further understand the curriculum because it was situated within a classroom environment. Observing the curriculum's implementation and development progress revealed how it was being structured, delivered and received by students. Third, classroom presence, for the purposes of observation, helped to build rapport between the evaluation team and enrolled students. Conducting observations is time consuming, but it is an important method as it helps to situate the program overall.

6 Conclusion

This proposed project offers a standardized multidisciplinary curriculum model for digital forensics education. It is being made available to institutions for adoption. This project transformed the multidisciplinary undergraduate education at a Midwest university in the United States by institutionalizing this program and the collaborations upon which it is built. In accordance with the multidisciplinary nature of the field of digital forensics, the curriculum development team included domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. The modular approach to curriculum development is organized by a three-course digital forensics education sequence, and the modules are combined to form a coherent narrative, thus exposing students to multiple perspectives on digital forensics. The curriculum package provides a strong theoretical foundation for the techniques learned by the students as well as an array of studies in fields related to digital forensics. Hopefully this paper will initiate

a conversation with the international community, note that standards need to continue to be developed for digital forensics curriculum, and recognize the multidisciplinary need for this field of study. This project, curriculum, and course outline are available on the website http://publish.illinois.edu/digital-forensics/ and a content package containing all of these materials will be posted there in the near future.

Appendix A. Digital Forensics Curriculum Topics

See Tables 1 and 2.

Table 1. Topics for digital forensics 1

Introductory course topic list by module
Introduction and Concepts of Forensics
Define digital forensics
Process of forensics investigation
Review of case studies
Sociological Aspects of Digital Forensics
Legal Aspects of Digital Forensics
Fourth Amendment
Evidence
Privacy laws
Cyber crimes
Computer Forensics
Introduction to computer forensics
Introduction to file system forensics
NTFS analysis
File carving
Windows analysis and application
Psychological Aspects of Digital Forensics
Forensics psychology and cyber crime
Psychological profiling of cyber criminals
Network Forensics
Network fundamentals
Evidence acquisition
Packet analysis
Fraud Investigations
Introduction to fraud examination
Nature and extent of fraud; Benford's Law
Mobile Forensics and Malware
Mobile device forensics
Mobile network forensics
Malware

Table 2. Topics for digital forensics 2

Advanced course topic list by module
Sociological Perspectives on DF-related Cases Computer Fraud and Abuse Act Privacy
Incident Response
Reasoning about Digital Evidence
File System Forensics Timeline analysis
Tool Validation and Anti-Forensics Linux/Mac operating system analysis Mobile (Android/iOS) OS analysis
Network Forensics Network log analysis Traffic pattern analysis Network protocol analysis Unknown network protocol analysis Wireless traffic analysis
Psychology of Cyber Crime Understanding hackers Human heuristics and biases
Digital Archives Basics of archival perspective Digital forensics hardware and software in archives
Reverse-Engineering Malware Overview of malware analysis Case Study

References

1. Meyers, M., Rogers, M.: CF: the need for standardization and certification. Int. J. Digital Evid. **3**(2), 1–11 (2004)
2. Yasinsac, A., Erbacher, R.F., Marks, D.G., Pollitt, M.M., Sommer, P.M.: Computer forensics education. IEEE Secur. Priv. **1**(4), 15–23 (2003)
3. Bem, D., Huebner, E.: Computer forensics workshop for undergraduate students. In: Proceedings of the Tenth Conference on Australian Computing Education, vol. 78, pp. 29–33. Australian Computer Society, Inc., January 2008
4. Kessler, G.C., Schirling, M.E.: The design of an undergraduate degree program in computer and digital forensics. J. Digital Forensics Secur. Law **1**(3), 37–50 (2006)

5. Bashir, M., Applequist, J., Campbell, R., DeStefano, L., Garcia, G., Lang, A.: Development and dissemination of a new multidisciplinary undergraduate curriculum in digital forensics. In: ADFSL, Richmond, Virginia, 28–29 May 2014
6. Chi, H., Dix-Richardson, F., Evans, D.: Designing a computer forensics concentration for cross-disciplinary undergraduate students. In: Information Security Curriculum Development Conference, pp. 52–57. ACM (2010)
7. Srinivasan, S.: Computer forensics curriculum in security education. In: Information Security Curriculum Development Conference, pp. 32–36. ACM (2009)
8. Wassenaar, D., Woo, D., Wu, P.: A certificate program in computer forensics. J. Comput. Sci. Coll. **24**(4), 158–167 (2009)
9. Woods, K., Lee, C.A., Garfinkel, S., Dittrich, D., Russel, A., Kearton, K.: Creating realistic corpora for forensic and security education. In: Proceedings of the ADFSL Conference on Digital Forensics Security and Law, pp. 123–134 (2011)
10. Lang, A., Bashir, M., Campbell, R., DeStefano, L.: Developing a new digital forensics curriculum. In: DFWRS, Denver, CO, 3–6 August 2014
11. Walls, R.J., Levine, B.N., Liberatore, M., Shields, C.: Effective digital forensic research is investigator-centric. In: HotSec (2011)
12. Beebe, N.: Digital forensic research: the good, the bad and the unaddressed. In: Peterson, G., Shenoi, S. (eds.) IFIP WG. IFIP AICT, vol. 306, pp. 17–36. Springer, Heidelberg (2009)
13. Kwan, M., Chow, K.-P., Law, F., Lai, P.: Reasoning about evidence using bayesian networks. In: Ray, I., Shenoi, S. (eds.) Advances in Digital Forensics IV. IFIP, vol. 285, pp. 275–289. Springer, Heidelberg (2008)
14. Bishop, M.: Education in information security. IEEE Concurrency **8**(4), 4–8 (2000)
15. Craiger, P., Ponte, L., Whitcomb, C., Pollitt, M., Eaglin, R.: Master's degree in digital forensics. In: System Sciences, HICSS 2007, 40th AHIC, pp. 264b. IEEE (2007)
16. Nance, K., Armstrong, H., Armstrong, C.: Digital forensics: defining an education agenda. In: System Sciences, HICSS 2010, 43rd AHIC, pp. 1–10. IEEE (2010)
17. Burnett, S.F.: Computer security training and education: a needs analysis. In: 2012 IEEE Symposium on Security and Privacy, p. 0026. IEEE Computer Society (1996)
18. Cooper, P., Finley, G.T., Kaskenpalo, P.: Towards standards in digital forensics education. In: Proceedings of the 2010 ITiCSE Working Group Reports, New York, pp. 87–95. ACM (2010)
19. Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M.: Computer forensics programs in higher education: a preliminary study. In: SIGCSE Bulletin, vol. 37, pp. 147–151 (2005)
20. Liu, J.: Implementing a baccalaureate program in computer forensics. J. Comput. Sci. Coll. **25**(3), 101–109 (2010)
21. FEPAC Accreditation standards Technical report. AAFS (2012)
22. Curricula, C.: Report of ACM/IEEE-CS Joint Curriculum Task Force (1991)
23. WVUFSI: Technical working group for education and training in digital forensics technical report. U.S. Department of Justice, August 2007
24. Scientific Working Group on Digital Forensics. SWGDE/SWGIT guidelines and recommendations for training in digital and multimedia evidence technology (2010). https://www.swgde.org/documents/CurrentDocuments
25. Schipp, J., Dopheide, J., Slagell, A.: ISLET: an isolated, scalable and lightweight environment for training. In: The Proceedings of XSEDE 2015, St. Louis, MO, July 2015
26. Woods, K., Lee, C., Garfinkel, S., Dittrich, D., Russel, A., Kearton, K.: Creating realistic corpora for forensic and security education. In: ADFSL Conference on Digital Forensics, Security and Law (2011)

27. Ismand, E.S., Hamilton, J.A. Jr.: A digital forensics program to retrain America's veterans. In: 5th ASIA, pp. 62–66 (2010)
28. Al Amro, S., Chiclana, F., Elizondo, D.A.: Application of fuzzy logic in computer security and forensics. In: Elizondo, D.A., Solanas, A., Martinez, A. (eds.) Computational Intelligence for Privacy and Security. SCI, vol. 394, pp. 35–49. Springer, Heidelberg (2012)