May 29th, 9:40 AM

Development and Dissemination of a New Multidisciplinary Undergraduate Curriculum in Digital Forensics

Masooda Bashir
Graduate School of Library and Information Science, Information Trust Institute, University of Illinois at Urbana-Champaign, mnb@illinois.edu

Jenny A. Applequist
Coordinated Science Laboratory, Information Trust Institute, University of Illinois at Urbana-Champaign, japplequ@illinois.edu

Roy H. Campbell
Department of Computer Science, Information Trust Institute, University of Illinois at Urbana-Champaign, rhc@illinois.edu

Lizanne DeStefano
I-STEM Education Initiative, College of Education, Information Trust Institute, University of Illinois at Urbana-Champaign, destefan@illinois.edu

Gabriela L. Garcia
I-STEM Education Initiative, College of Education, Information Trust Institute, University of Illinois at Urbana-Champaign, gjuare3@illinois.edu

See next page for additional authors

DEVELOPMENT AND DISSEMINATION OF A NEW MULTIDISCIPLINARY UNDERGRADUATE CURRICULUM IN DIGITAL FORENSICS

Masooda Bashir (mnb@illinois.edu)
Graduate School of Library and Information Science

Jenny A. Applequist (japplequ@illinois.edu)
Coordinated Science Laboratory

Roy H. Campbell (rhc@illinois.edu)
Department of Computer Science

Lizanne DeStefano (destefan@illinois.edu)
I-STEM Education Initiative, College of Education

Gabriela L. Garcia (gjuare3@illinois.edu)
I-STEM Education Initiative, College of Education

Anthony Lang (ajlang2@illinois.edu)
Department of Computer Science

Information Trust Institute
University of Illinois at Urbana-Champaign
Urbana, Illinois

ABSTRACT

The Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign is developing an entirely new multidisciplinary undergraduate curriculum on the topic of digital forensics, and this paper presents the findings of the development process, including initial results and evaluation of a pilot offering of the coursework to students. The curriculum consists of a four-course sequence, including introductory and advanced lecture courses with parallel laboratory courses, followed by an advanced course. The content has been designed to reflect both the emerging national standards and the strong multidisciplinary character of the profession of digital forensics, and includes modules developed collaboratively by faculty experts in multiple fields of computer science, law, psychology, social sciences, and accountancy. A preliminary plan for the introductory course was presented to a workshop of digital forensics experts in May 2013 and received their strong approval. Pilot versions of the introductory and introductory lab courses were taught to a mixture of computer science and law students at the University of Illinois in the fall of 2013, and were very positively received by the students, who made it clear that they appreciated the multidisciplinary approach. The curriculum, which is designed to obviate the need for expensive labs or team-teaching by specialized faculty, will be made available to other colleges and universities in order to improve the content and quality of existing digital forensics programs, to inspire and greatly facilitate the creation of new programs, and, ultimately, to increase the number of educated practitioners. The developed resources can be used as the basis for future academic programs, distance learning, and multidisciplinary, multi-institutional programs that meet evolving digital forensics educational standards. Much of the material, including a virtual laboratory, will be provided on-line. Introductory course materials will be distributed to other institutions beginning in the summer of 2014; advanced course materials should be available for distribution in 2015. Related outreach activities have been undertaken and will be continued.

Keywords: Digital forensics, Computer forensics, Curriculum development, Curriculum standards, Education standards, Training standards, Undergraduate education, Interdisciplinary studies

1. INTRODUCTION

The Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign (UIUC) is developing a new multidisciplinary undergraduate curriculum addressing digital forensics. *Digital Forensics* (DF) is a branch of forensics that focuses on the recovery and investigation of data that were found in digital devices and have potential legal significance. Innovative DF education is required in order to build a technical workforce that can address the increasing need to perform DF investigations that is flowing from society's increasing dependence on computer systems and infrastructure. As information technology has become pervasive, instances of digital crime and the need to use digital evidence in both criminal and civil investigations have both grown significantly. DF is now a major part of many criminal and civil investigations; its tools are frequently used by local, state, and federal law enforcement agencies. Despite developments in forensic research, data have become harder to analyze because of growing complexity (Garfinkel, 2010). As a result, the number of DF-related job openings is expected to increase dramatically over the next few years (Ismand, and Hamilton, 2010).

The purpose of developing a standard undergraduate DF curriculum is to improve the content and quality of universities' current DF programs throughout the nation, inspire and greatly facilitate the creation of additional programs, and, ultimately, increase the number of educated practitioners. To achieve that goal, we are creating resources that can be used as the basis for future academic programs, distance learning, and multidisciplinary, multi-institutional programs that meet the evolving standards. Our program will include a sequence of four courses—an introduction, an advanced course, and accompanying introductory and advanced laboratory courses—with curricula based on emerging national standards. Much of the material, including a virtual laboratory and class notes, will be provided on-line and shared with other institutions. (An alpha version of the introductory course materials will be distributed to other institutions beginning in the summer of 2014; a finalized version, along with an alpha version of the advanced course materials, should be available for distribution in 2015.)

The content of the program has been modeled on the NSA/DHS CAE Digital Forensics Working Group proposal for a standardized DF curriculum (Digital Forensics Working Group, 2010). The content reflects the multidisciplinary nature and breadth of DF and is designed to accommodate the evolving curriculum standards (Rogers and Seigfried, 2004). Our program is unique in that we assembled a large cross-disciplinary team of subject-matter experts to collaboratively develop the curriculum materials. The core curriculum development team includes Illinois faculty members Masooda Bashir (an expert on the psychology of cyber-crime); Roy H. Campbell (a computer security expert); Syed Faisal Hasan (a networking expert); Jay P. Kesan (a law professor with expertise in technology law); Anna-Maria Marshall (an expert on the civil and criminal justice systems, from the Dept. of Sociology); Frank Nekrasz (an expert on fraud investigation from the Dept. of Accountancy in the College of Business); David M. Nicol and William H. Sanders (experts on secure and trustworthy computing and networking, from the Department of Electrical and Computer Engineering); and Jana Sebestik (a K-12 outreach expert from the College of Education). We presented our preliminary design for the introductory course at a workshop of digital forensics experts that we hosted in May 2013 (see Section 4) and received their strong approval. Pilot versions of the introductory lecture and lab courses were taught to a mixture of computer science and law students at the University of Illinois in the fall of 2013, and were very positively received by the students (see Section 6).

In the following, we will discuss the high-level rationale for our new DF curriculum, including the factors we weighed in choosing material to include and the intentions for dissemination to other institutions. In particular, we will discuss why we believe it is critical to approach DF education from a strongly multidisciplinary perspective, instead of concentrating solely on technological aspects. We will also discuss our evaluation of the success of the introductory lecture & lab courses as they were taught in fall 2013.

2. BACKGROUND AND MOTIVATION

A brief look at the history of computer forensics will clarify the need for a new, standardized, and easily distributable educational curriculum. In the late 1980s, DF techniques were developed mostly for data recovery. Investigators sought out people with backgrounds in information technology to unearth evidence found on computers at crime scenes. At that time, there was limited need for DF: evidence could be made visible without the use of recovery tools, so few cases required deep digital analysis. Garfinkel (2010) notes that from 1999 to 2007, digital forensics saw a kind of "Golden Age" characterized by awe at its ability to recover deleted data and peek into a criminal's mind. The dominance of the "WinTel" platform meant that examiners had the relatively easy job of focusing on one type of system, and customers with relatively little training could make use of a variety of DF tools. That initial widespread success resulted in rapid growth of digital forensics research and university adoption.

Evolving computer technology has subsequently led to complications and challenges for DF. The growing size of storage devices, the prevalence of embedded flash storage, and the increasing number of hardware interfaces, operating systems, and file formats are all testing the limits of digital forensics capabilities. The need to analyze multiple devices, pervasive encryption, the use of "cloud" computing, unique malware, and legal challenges all create problems for today's examiners (Garfinkel, 2010). As technology changes and becomes more complex, DF practitioners must expand their knowledge and skill set accordingly (NIST, 2010). DF has great utility, but now requires extensive expertise, and DF as a unique field is not sufficiently stressed in higher education. We are confronted by an urgent need to build a workforce with the ability to "contain, prevent, and prosecute these crimes, frauds, and attacks by efficiently and effectively conducting digital investigations" (Tu et al., 2012). Improvement of the practice of DF requires awareness, the development of better techniques, and a comprehensive forensics education (Tu et al., 2012).

While several academic programs on DF have already been developed, the field and the curriculum standards are still at an early stage and rapidly evolving. Without a standard curriculum, the quality of the courses, content, and faculty varies considerably (Nance et al., 2010), with most universities, in fact, still offering little or nothing in the way of DF coursework. The aim of the current UIUC effort is to develop and implement a model curriculum in digital forensics that balances the various necessary components, and to work for that model's acceptance as a DF educational standard. Given the nation's current shortage of DF learning options, one particular goal is to provide other institutions (including community colleges as well as universities) with a complete set of user-friendly curricular materials that will enable computer science faculty who are not DF experts to set up and teach effective DF courses at their institutions.

3. THE MULTIDISCIPLINARY NATURE OF DIGITAL FORENSICS

To educate competent DF experts, a curriculum must include many in-depth technical topics such as file system analysis, application analysis, network packet analysis, and so forth. It is important for students to understand the underlying technology generating the data they are analyzing, so they understand *why* and *how* the evidence they find is created, and they can reason about it in a wider investigative context.

However, it is critical for educators to recognize that DF is not just a technical discipline, but a multidisciplinary profession that draws on a range of other, very different fields, including law and courtroom procedure, other disciplines of forensic science, and criminal justice. Only through integration of such relevant nontechnical disciplines into the DF curriculum can students develop the comprehensive understanding that they need in order to conduct examinations and analyses whose processes and findings are not just technically sound, but legal, ethical, admissible in court, and otherwise effective in achieving the desired real-world goals.

While there is great variability in the details and types of multidisciplinary content included in previously proposed curriculum standards, there are some key commonalities. In an analysis of training guides, successful academic programs, and the authors' personal experiences, Taylor et al. (2007) outlined areas necessary to excellence in DF education, the major one being "multi-disciplinary content." Again, although digital forensics is largely a technical field concerned with computing, a complete understanding would be impossible without the study of related, nontechnical knowledge areas such as criminal and civil justice, law and courtroom procedure, disk analysis, and evidence handling. The study of criminology gives forensic specialists insight into the behavior and motivations of cyber criminals. Knowledge of relevant laws is critical for people handling digital evidence. DF professionals must understand the legal implications of evidence collection and analysis of data, as well as courtroom procedure. It is important that forensic examiners not only act according to regulation, but also understand their role in investigation and prosecution. An understanding of courtroom procedure would also aid in teaching students how to present technical subjects in an understandable manner. A program that includes these knowledge areas and expert instructors is bound to create a "high-quality learning experience" (Taylor et al., 2007).

Cooper et al. (2010) found that digital forensics relies on a large set of supporting domains, both technical and nontechnical. Computer engineering, computer science, software engineering, information systems, and information technology all play a role in digital forensics education from a technical perspective. The authors noted that the following non-computing-related knowledge areas are also involved: mathematics and statistics, ethics, criminology, forensic science, and law. Statistical analysis and mathematics are required in the analysis of data. An ethics aspect is important, for forensics professionals are likely to be faced with ethical challenges during employment. Criminology is a unique area in digital forensics and helps an investigator understand the causes and motivations for a crime. Topics common to all forensic sciences should also be included in DF education, in addition to law and legal issues; digital forensics professionals should be aware of the rules and regulations involved in their work (Cooper et al., 2010).

Huang et al. (2010) propose a curriculum structure with topics in four categories: evidence collection, evidence preservation, evidence presentation, and forensic preparation. The first three topics deal with evidence, how to recover it, and how to present it for use in the courtroom, while the fourth addresses actions that can be taken before malicious acts occur. All of these skills will "serve the undergraduate well in future classes and in his or her employment upon graduation" (Huang et al. 2010). The authors note that DF also involves many skills-oriented topics and is tool-intensive. However, university educators must take care that they do not go too far towards merely training students to use tools, instead of grounding them in a theoretical understanding of the tools' principles and roles.

In a 2012 survey, Tu et al. identified the topics that participants in the 2008 Digital Forensics Research Workshop desired in digital forensic courses, and how digital forensics education could be improved. Survey results showed that the "most prevalent tools in use are commercial tools, such as Encase and FTK, and most cases deal with Windows operating systems, followed by Unix/Linux and Macintosh" (Tu et al., 2012). Practitioners responded that most digital forensics cases deal with single personal computers, followed by mobile media and networks, hacking, and multimedia. Also, most digital forensics professionals are willing to collaborate to develop educational programs; in fact, "more than 75% of digital forensics educators and digital forensics investigators agreed to cooperate in the development of a digital forensics program at universities or colleges." The authors recommend courses that simulate real-world digital forensics investigation and are designed to support collaboration with industry and law enforcement agents. They propose six courses covering core DF topics: Digital Forensics Fundamentals, Advanced Computer Forensics, Network/Internet Forensics, Mobile Digital Forensics, Digital Forensics Professional Project, and Courtroom Experience.

4. CHALLENGES IN DIGITAL FORENSICS CURRICULUM STANDARDIZATION

Digital forensics has evolved primarily in response to specific issues, which has made it challenging to pull developments together into a cohesive body of common knowledge. There is very little standardization in the DF community, let alone the DF educational community.

The computer forensics community has been very concerned with the lack of education and training standards for digital forensics (Huebner et al., 2008; Kessler and Schirling, 2006; Rogers and Seigfried, 2004; Yasinsac et al., 2003). Until now, only a few efforts have been devoted to the development of digital forensics program guidelines (FEPAC, 2012; Huebner et al., 2008; Rogers and Seigfried, 2004; West Virginia, 2007; Yasinsac et al., 2003). The American Academy of Forensics Science (AAFS) has provided guidelines for forensic science education and training that was developed by the Forensic Science Education Programs Accreditation Commission in 2008 (FEPAC, 2012). Those efforts only give general guidelines on digital forensic education and training, such as the number of credits needed and the core forensics topics that should be taught. The National Institute of Justice also funded development of guidelines for forensic science education and training by the West Virginia University Forensics Science Initiative (West Virginia, 2007). That effort generated general guidelines for program development as well as detailed topics for digital forensics curriculum design. However, although there are some key principles that forensics educators and practitioners agree a curriculum must contain, an accepted set of standards has remained elusive.

Currently, higher education programs mostly cover DF topics via general and survey courses or, more commonly, through brief mention in broader computer science courses; few have full digital forensics programs. Yasinsac et al. (2003) recognized that some form of computer forensics education will be pursued by students with a variety of needs and skill-level goals. Within the justice system, law enforcement officers as well as judges, prosecutors, and defense attorneys need some level of DF training. Industry requires its forensic examiners to be trained in the event of an incident, and academia focuses on education and training for students, faculty, and researchers (Yasinsac et al., 2003). A standard academic curriculum should be general enough to cover all aspects of the field, and not be too specific in any direction. Students can learn general concepts, theories, and practical application, but it is not realistic to expect them to be fully trained for a job after completing the program without having practical experience (Beebe & Clark, 2006).

Reflecting DF education's lack of standardization, there have been a wide range of solutions to the problem of placing digital forensics curricula within university settings. A study done by Gottschalk et al. (2005) surveyed various computer forensic programs in North America and found them to be located in units as diverse as computing departments, an economic crime institute, a division of account and computer systems, and a criminal justice program.

To help us develop an effective set of DF education standards, we began by doing extensive research on both existing proposed DF curriculum standards and existing digital forensics courses and programs at other institutions, such as (for example) the high-quality offerings at Iowa State University (Guan, 2013) and the University of New Orleans. We then compared the existing standards to the existing courses, and found that existing courses do not closely resemble the theoretical "ideals" described by the standards. We hypothesized that the reason for that disconnect is a gap between industry expectations and the capabilities and standard practices of academia.

To help us develop an initial working list of topics for our own first-semester introductory course, we started by compiling a list of all the topics from all the courses and recommended curriculum lists we could find, de-duplicated them, and then organized them into categories. Within each category we selected what we believed were the most important key concepts that could fit into the time slots available across a semester. (We will cover many of the "rejected" topics in our second, advanced, course, which is now under active development.) We then filled in gaps and also removed material to keep the amount of content realistic within time constraints. For example, we decided that Windows

would be the only operating system covered in the introductory course, as an example OS that DF investigators are most likely to encounter in real life. Other than that, among the technical topics, we tried to include quick introductions to the main elements of network forensics (protocol, packet, and flow analysis), as well as mobile device forensics and malware forensics. Our multidisciplinary subject-matter expert faculty selected and developed the content for introductory modules in law, criminal and civil justice, accounting fraud, and the psychology of cyber-crime. (See the next section for more detail on the finalized list of topics we covered.)

To clarify the challenge of DF curriculum development and help identify viable solutions, we held the 1st International Workshop on Digital Forensics Curriculum Standards (DFCS, 2013) in Champaign, Illinois, on May 20-21, 2013. The workshop brought together industry, government, and law enforcement practitioners, along with academic experts, in order to discover a common ground of what stakeholders would accept as a curriculum standard, and what roadblocks we face for widespread adoption. We gained a number of useful new insights; for example, we were struck by real-world practitioners' repeated strong emphasis on the urgent need to develop writing and communication skills in DF professionals. As a result of that input we decided to place stress throughout the course on clear, well-organized, general-audience-appropriate writing in homework and lab reports; we also explicitly cover topics such as report writing in the lectures. Other points that emerged clearly in the workshop included the importance of using case studies (including real-life examples) and of focusing on ethics. Participants had a range of opinions on how to present tools alongside theoretical concepts in a course, but generally agreed that some kind of exposure to open-source or commercial tools would be beneficial. Overall, the attendees were very supportive of our planned approach, and offered presentations and comments that confirmed we were on track. Thus, the workshop validated our approach by confirming that a broad range of DF experts felt that our curriculum covered appropriate material and made a good balance among competing priorities for inclusion.

5. INTRODUCTORY COURSE CONTENT: OVERVIEW

At the highest level, we considered the following to be the essential focus of our introductory course curriculum:

- Proper data handling
- Limitations of forensics/techniques/knowledge
- Scientific analysis
- Demonstrated ability to communicate findings (written and oral)
- Understanding of the spectrum of available techniques
- Awareness of the major forensic areas

Those objectives were reflected in 8 topical modules, containing 28 lectures, as follows:

1. **Concept of Forensics (1 week, 2 lectures):** Why study digital forensics?: Course outline/syllabus & introduction. What is digital forensics?: Definition, process of forensic investigation (scientific method).
2. **Psychological Aspects of Digital Forensics (1 week, 2 lectures):** Forensic psychology and cyber-crime. Psychological profiling of the major types of cyber criminals, e.g., hackers and malware distributors.
3. **Computer Forensics (3 weeks, 6 lectures):** Introduction to file systems. NTFS analysis. Deleted file recovery. Windows analysis I. Windows application analysis. Computer forensics scenario.
4. **Sociological Aspects of Digital Forensics (1 week, 2 lectures):** Structure of the legal system. Evidence and decision-makers: Judges and juries.

5. **Network Forensics (3 weeks, 6 lectures):** Networking fundamentals review. Evidence acquisition in network forensics. Packet analysis, part 1. Packet analysis, part 2. Statistical flow analysis. Network intrusion detection and analysis.
6. **Legal Aspects of Digital Forensics (2 weeks, 4 lectures):** The Fourth Amendment and e-discovery. Evidence. Privacy laws. Cyber crimes. Discussion of civil and criminal cases.
7. **Fraud Investigations (1 week, 2 lectures):** Introduction to fraud examination. The nature and extent of fraud; Benford's Law.
8. **Mobile Forensics and Malware (2 weeks, 4 lectures):** Mobile device forensics, part 1. Mobile device forensics, part 2. Mobile network forensics. Malware.

One important issue we grappled with was that of prerequisites. We wanted to ensure that students majoring in (for example) law and business were not excluded from the course, so we tried to minimize the need for technical prerequisites. At the same time, we didn't want the content to be so basic that it would seem trivial and boring to computer science students. We therefore recognized the need to develop "remedial" self-study materials (a "primer") to help students from nontechnical backgrounds get up to speed on basic concepts. We also adjusted the course design to put students with very different backgrounds on, in effect, slightly different tracks. For example, some lab and homework exercises were designed to pair computer science students with law students to address case studies from both perspectives. Finally, we are weighing the possibility of preparing a "quiz" for potential students from nontechnical backgrounds, so that we can assess whether they have adequate basic knowledge—or, indeed, whether they even realize that the course they're considering has considerable technical content—by asking them simple questions (e.g., "What is ASCII?").

6. EVALUATION METHODOLOGY AND RESULTS

To ensure that we ultimately disseminate a documented, validated, effective model for a multidisciplinary undergraduate curriculum in digital forensics, we are employing a values-engaged, educative evaluation that is designed to provide formative and summative information on benchmark attainment (Greene et al., 2006). The purpose is to guide program improvement by assessing program effectiveness and short- and long-term outcomes. Specifically, the evaluation is designed to determine whether the educational programming is being implemented as planned; whether it is working effectively and/or could be improved in identifiable ways; what outcomes/value are associated with participation; and to what extent the programming is becoming successfully incorporated in the larger mission and culture of the institution. Multiple evaluation methods are being employed, including interviews, observation of classroom and laboratory experiences, expert review of the course materials, direct assessment of student knowledge and skills, and surveys. (Institutional review board (IRB) approval was obtained.)

In the Fall of 2013, we team-taught pilot offerings of the introductory lecture and laboratory DF courses at the University of Illinois at Urbana-Champaign. Enrollees included both computer science majors and law students, some of whom had a limited technical background.

Fall 2013 evaluation data collection techniques employed included (1) three student surveys (pre-course, mid-course, and end-course); (2) course observations by evaluators during both lectures and labs; (3) mid-course and end-course focus groups (including both computer science and law students); and (4) analysis of documents (e.g., student assignments, midterm, lecture presentations, and so forth).

A much fuller analysis of our experiences is currently being prepared for publication, but here we provide some high-level remarks on the success of that initial offering, as established by the evaluation process.

It was clear that the large majority of students enjoyed the course and were satisfied with the material covered. They viewed the interdisciplinary aspect as a major strength of the course; many student comments particularly stressed the excitement of looking at the material from multiple perspectives

and gaining exposure to areas outside their primary fields of study. Survey results also showed that a majority of students said that their own learning was enhanced by the presence of students from other departments in the course. They enjoyed working on group assignments, and, indeed, said they wished the course had offered more opportunities to work together.

The information we gained in the evaluation process is being used to refine and improve the curriculum prior to its dissemination.

7. OUTREACH

Portions of the developed curriculum are also being adapted for K-12 outreach purposes. The main goals are to promote online awareness and safety, but we also hope to generate enthusiasm for cyber security careers while more generally encouraging interest in technology, science, and mathematics. We want to offer young people information about their digital footprints and access to real tools that encourages responsible and ethical use of skills and information without producing inappropriate behavior or anxiety.

Specifically, we are developing project-based curriculum modules for middle school and high school students. The modules integrate concepts of digital forensics and use interactive technologies to explore age-appropriate multidisciplinary topics related to personal privacy, legal and ethical issues, mobile devices, and investigative processes. The curriculum materials provide hands-on activities that improve awareness of digital forensics issues related to losing or sharing of computers, digital tablets, and cell phones. Students will learn about the digital debris left behind by users of Internet browsers, social media, search engines, and online gaming sites. Many students are already aware that they are the recipients of targeted advertising, but may not know how their Internet usage behaviors and habits can be collected and used. Other curriculum topics include legal and ethical concerns related to digital photography and chain of custody for evidence.

We have also been working closely with Girls' Adventures in Mathematics, Engineering, and Science (G.A.M.E.S), a popular annual week-long summer camp program of the University of Illinois. G.A.M.E.S offers several tracks designed to give high-school-aged girls an opportunity to explore exciting engineering and scientific fields through demonstrations, classroom presentations, hands-on activities, and contacts with women in technical fields. In 2013, we developed curriculum and conducted classroom presentations and hands-on activities for the Computer Science Track.

8. CONCLUSIONS AND NEXT STEPS

The curriculum we're developing for the introductory lecture and lab courses includes a detailed instructor handbook providing the entire course content in narrative form; PowerPoint slide decks for all 28 lectures; an instructor's laboratory handbook giving details on how to set up and lead 13 lab exercises; question sets that can be drawn from in preparing tests and homework exercises; "remedial" resources (such as reading lists) for the benefit of students from less technical backgrounds; and lab exercises (which were developed for a conventional computer lab setting, but which will soon be converted to online form). To reduce barriers to adoption of the curriculum, all of the lab exercises have been designed to use open-source, freeware tools.

We are actively revising the entire set of materials in response to our experiences with the Fall 2013 pilot offering, with the particular goal of knitting the various disciplines' modules together more closely, such as by incorporating a substantial fictitious case study that draws together the multiple perspectives.

An alpha version of the introductory course materials will be available in the summer of 2014, and we are actively seeking opportunities to distribute them to other institutions. Interested educators are strongly encouraged to contact us, and we encourage scholars from other institutions to offer comments on our work and potentially contribute additional material. We expect that a revised and

updated package of introductory course materials, and an alpha set of materials for the advanced courses, will be available by sometime in 2015. We anticipate that online lab modules will also be available in 2015.

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. DUE-1241773. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

Beebe, N. L., & Clark, G. J. (2006). Digital forensics curriculum development: Identification of knowledge domains, learning objectives, and core concepts. Twelfth Americas Conference on Information Systems (AMCIS), August 4-6, 2006, Acapulco, Mexico.

Cooper, P., Finley, G. T., & Kaskenpalo, P. (2010). Towards standards in digital forensics education. 2010 ITiCSE Working Group Reports, June 26-30, 2010, Bilkent, Ankara, Turkey, 87-95.

Digital Forensics Working Group. (2010). NSA/DHS CAE Principals Meeting [private wiki], November 14-17, 2010, St. Louis, Missouri, USA. Retrieved from http://digitalforensicswg.wikispaces.com/

FEPAC: Forensic Science Education Programs Accreditation Commission. (2012). Accreditation standards. American Academy of Forensic Sciences. Retrieved from http://fepac- edu.org/sites/default/files/FEPAC_Standards_11092012.pdf

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7(sup.), S64-S73.

Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., & Stein, M. (2005). Computer forensics programs in higher education: A preliminary study. 36th SIGCSE Technical Symposium on Computer Science Education, February 23-27, 2005, St. Louis, MO, USA. 147-151.

Greene, J. C., DeStefano, L., Burgon, H., & Hall, J. (2006). An educative, values-engaged approach to evaluating STEM educational programs. In D. Huffman & F. Lawrenz (Eds.), *Critical Issues in STEM Evaluation (special issue). New Directions for Evaluation*, *109*, 53-71.

Guan, Y. (2013). CprE 536: Computer and network forensics [course website]. Retrieved from http://home.eng.iastate.edu/~guan/course/CprE-536/index.html#Course%20Description

Huang, J., Yasinsac, A., & Hayes, P. J. (2010). Knowledge sharing and reuse in digital forensics. Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '10), May 20, 2010, Oakland, CA, USA, 73-78.

Huebner, E., Bem, D., & Ruan, C. (2008). Computer forensics tertiary education in Australia. International Conference on Computer Science and Software Engineering, December 12-14, 2008, Wuhan, Hubei, China, 1383-1387.

Ismand, E. S., & Hamilton, J. A., Jr. (2010). A digital forensics program to retrain America's veterans. 5th Annual Symposium on Information Assurance (ASIA '10), June 16-17, 2010, Albany, NY, USA. 62-66.

Kessler, G. C., & Schirling, M. E. (2006). The design of an undergraduate degree program in computer & digital forensics. *Journal of Digital Forensics, Security and Law*, *1*(3), 37-50.

Nance, K., Armstrong, H., & Armstrong, Colin. (2010). Digital forensics: Defining an education agenda. 43rd Hawaii International Conference on System Sciences, January 5-8, 2010, Honolulu, Hawaii, USA.

NIST: National Institute of Standards and Technology. (2010). Computer forensics. Retrieved from http://www.nist.gov/itl/ssd/computerforensics.cfm

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security*, *23*(1), 12-16.

Taylor, C., Endicott-Popovsky, B., & Phillips, A. (2007). Forensics education: Assessment and measures of excellence. Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '07), April 10-12, 2007, Bell Harbor, WA, USA, 155-165.

Tu, M., Xu, D., Wira, S., Balan, C., & Cronin, K. (2012). On the development of digital forensics curriculum. *Journal of Digital Forensics, Security and Law*, *7*(3), 13-32.

West Virginia University Forensic Science Initiative. (2007). Technical working group for education and training in digital forensics. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/219380.pdf

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., & Sommer, P. M. (2003). Computer forensics education. *IEEE Security & Privacy*, *1*(4), 15-23.