Developing a New Digital Forensics Curriculum

By

Anthony Lang, Masooda Bashir, Roy Campbell and Lizanne Destefano

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2014 USA

Denver, CO (Aug 3rd - 6th)

Digital Investigation 11 (2014) S76–S84

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Developing a new digital forensics curriculum☆

Anthony Lang [a], Masooda Bashir [b], *, Roy Campbell [a], Lizanne DeStefano [c]

[a] *Computer Science, University of Illinois at Urbana-Champaign, United States*
[b] *Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign, United States*
[c] *Illinois Science, Technology, Engineering, and Mathematics Education Initiative, University of Illinois at Urbana-Champaign, United States*

Keywords:
Digital forensics
Curriculum
Education
Curriculum standards
Computer forensics
Network forensics

ABSTRACT

We are developing a new undergraduate certificate program in digital forensics at the University of Illinois at Urbana-Champaign. To create a curriculum consistent with the fundamentally multidisciplinary nature of the field of digital forensics, we assembled a curriculum development team that includes domain experts from the fields of computer science, law, social science, psychology, and accounting. To lower the entry barrier preventing institutions from adopting digital forensics programs, we are designing the curriculum with the express intent of distributing it as a self-contained curriculum package with everything needed to teach the course. When complete, our program will consist of an introductory and an advanced course in digital forensics, with accompanying hands-on labs. At the time of writing, we have developed the curriculum for our introductory course and taught a pilot class, and we are in the process of revising the curriculum for distribution to other institutions. This paper describes our program's goals, methodology, and rationale; our experience developing and teaching our new curriculum; and the revisions we are making based on this experience and feedback from our students.

Introduction

As we increasingly rely on digital devices in almost every aspect of our daily lives, these devices are becoming increasingly involved in legal investigations of all kinds. Digital forensics (DF) is the science of identifying, collecting, preserving, documenting, examining, analyzing, and presenting evidence from computers, networks, and other electronic devices. For our purposes, we interpret this to subsume the disciplines of computer forensics, network forensics, and mobile device forensics. DF is now a major part of many criminal and civil investigations; its tools are frequently used by law enforcement agencies and private labs for investigation, data recovery, and diagnostics. Although digital forensics has already assumed such an important role in our society, it is still a new and rapidly developing area of study. This presents a challenging position to the digital forensics education community, that this work proposes to assist with.[1]

Gathering perspectives on curriculum standards

Establishment of a standardized curriculum for digital forensics is important for several reasons. Principally, it provides a means for employers to validate the qualifications of a recent graduate from a digital forensics program. If the student graduated from a program that uses the standard curriculum, employers can immediately assess the minimum skill set that the candidate is likely to have, without the need for additional evaluations. Similarly, as digital forensics graduates may serve as expert witnesses

☆ Parts of this paper appear in the first author's master's thesis under a non-exclusive reproduction copyright (Lang, 2014).

* Corresponding author.
E-mail address: mnb@illinois.edu (M. Bashir).

http://dx.doi.org/10.1016/j.diin.2014.05.008

in legal proceedings, courts would also benefit from the added assurance of their expert's credentials. From the point of view of a prospective student, a standardized curriculum gives the dual benefits of simplifying the evaluation of degree options and of increasing the employability of those degrees, for the aforementioned reasons.

These observations are by no means novel, and there have been concerted efforts from the digital forensics education community to establish standardized curriculum. Most recently, the American Academy of Forensic Sciences' (AAFS) Forensic Science Education Programs Accreditation Commission (FEPAC) published, and offers accreditation based on, a standard that includes digital forensics (Forensic Science Education Programs Accreditation Commission, 2012). However, at the time of writing, only a single university has adopted this standard and received their accreditation for digital forensics (Forensic Science Education Programs Accreditation Commission, 2014).

We organized and hosted a workshop in the spring of 2013 to facilitate a dialog among leaders in the digital forensics research, education, and professional communities about goals for a curriculum standard and roadblocks to widespread adoption of such a standard. Different stakeholders presented their opinions and needs for various aspects of a curriculum standard and gave their perspectives on what is preventing development and adoption of curriculum standards in digital forensics.

The discussions at the workshop generated as many questions as answers. For example, “What prerequisites should be required?” “What department should host the program?” and “What entity should publish the standard?” This may not seem like progress, but the questions themselves are informative. The issues presented and questions asked by the attendees of the workshop indicated that the primary barriers to adoption of curriculum standards are not pedagogical, but practical. In other words, the main problem with previously proposed standards was not the topic coverage, but the fact that they were difficult to implement at most institutions.

Difficulty of implementing a digital forensics program

Based on input from digital forensics educators at our workshop, our own experience, and a review of the literature, we have identified the principal challenges facing institutions wishing to implement digital forensics programs:

Balancing training and education

Demand for continuing professional education and certification has led to development of training-based courses that teach digital forensics as a stepwise laboratory procedure, and neglect to educate students in the theoretical foundations of what they are learning (Cooper et al., 2010; Gottschalk et al., 2005). The same pressure is put on many applied disciplines, but it is easier to resist in more well-established fields, such as computer science, because there is a tradition of higher education providing a balance of skills and theory, leaving some training to the employer. This pressure poses a significant problem to institutions interested in providing their students with a strong theoretical background in their digital forensics program.

Lack of an adequate textbook on digital forensics

Existing books on digital forensics are mostly written as handbooks for practitioners, containing useful tips and general information about best practice based on the authors' personal experience (Liu, 2006). While these contributions are valuable, they offer very little explanation of the underlying technology or discussion of the theory for the topics, so are insufficient as textbooks for a course in higher education.

Finding qualified faculty

Given the absence of a standard curriculum and adequately detailed textbook resources to teach from, digital forensics training and education must rely heavily on the personal experience of the instructor (Gottschalk et al., 2005; Liu, 2006). This is particularly problematic given the scarcity of qualified digital forensics professionals.

Lab setup

Licenses for proprietary digital forensics software tools and specialized hardware can be prohibitively expensive; even assuming you have lab exercises planned, installing and configuring equipment for a digital forensics lab is no easy task (Gottschalk et al., 2005; Liu, 2006).

Selecting appropriate prerequisites

Since digital forensics is essentially an application area at the intersection of computer science and law, it has natural prerequisite knowledge from those fields. However, since digital forensics students are very unlikely to be double-majoring in Computer Science and Law, the question of which prerequisites to require and which to include in the digital forensics curriculum becomes quite difficult. Most existing programs opt to require substantial technical prerequisites. This enables them to easily focus their curriculum on the topics they see fit, but it restricts their curriculum's target demographics significantly (Liu, 2006; Chi et al., 2010). Where to draw the line on this trade-off was one of the most hotly debated issues at our workshop, and one that we found particularly challenging in our own curriculum development.

Lack of widely accepted curriculum standards

Although proposed curriculum standards exist for digital forensics, there is no generally accepted model (Forensic Science Education Programs Accreditation Commission, 2012; ACM/IEEE-CS Joint Task Force on Computing Curricula, 2013; West Virginia University Forensic Science Initiative, 2007; Scientific Working Group on Digital Evidence, 2010). This directly contributes to institutions' problems in adopting a digital forensics program, by increasing the uncertainty of decision makers and the difficulty of curriculum development. It also contributes indirectly by exacerbating the other difficulties as described above.

The rest of this paper is organized as follows. In Section Related work, we discuss related work; in Section Our digital forensics program, we present our initiative's goals and design; in Section Introductory course curriculum development, we describe our methods for developing the curriculum for our introductory course; in Section Lessons learned from pilot class, we present the lessons we learned teaching our pilot introductory course; in Section Evaluation methodology, we describe how we gathered feedback from our students during and after the pilot class; in Section Student feedback summary, we present highlights from the feedback we received from students in our pilot class; in Section Revisions, we describe the revisions we have made and plan to make to our curriculum, based on the lessons learned and student feedback from the pilot class; and in Section Conclusions and future work, we give our concluding remarks and a roadmap for our future work.

Related work

While many programs have curriculum descriptions available online, and these were considered in developing our own curriculum, such brief listings does not provide the information required to understand the state of the field, such as the important challenges and design decisions of the curriculum development process. Consequently, the current inquiry was restricted to those programs with a published description of their curriculum development in the literature.

Wassenaar et al. (Wassenaar et al., 2009) describe the certificate program in digital forensics at Cypress College. They put a clear focus on training students in practical skills to prepare them for professional certification. They also require their instructors to be digital forensics practitioners, and rely heavily on their personal experience to lend the program credibility, since there is no generally accepted curriculum model at the college level.

Chi et al. (Chi et al., 2010) describe their efforts to expand the existing computer forensics course at Florida A&M University, which was previously part of the Information Assurance program, into a cross-disciplinary concentration shared with the department of Sociology and Criminal Justice. This paper explains their challenges in teaching computer forensics to students without a strong technical background. Their solution was to create several remedial prep courses to give the Sociology and Criminal Justice students the prerequisite knowledge they need to enter the computer forensics concentration courses; in the process, they shifted the curriculum's focus much more toward training in practical skills to prepare students for professional certification.

Srinivasan (Srinivasan, 2009) describes the computer forensics course at the University of Louisville. They cover a great deal of material, but their target demographics are restricted to students in the Information Security concentration in their Computer Information Systems program.

In Liu (2006 and 2010), Liu describes the development process for Metropolitan State University's baccalaureate program in digital forensics. They employed a “backwards design” or “practitioner's model” to build the topic list for their curriculum. Basically, they looked at the needs of their students' target industry, clustered them into knowledge groups, and derived topic lists from these groups. Since they implemented an entire baccalaureate program in digital forensics, they were able to build the students' required prerequisite knowledge for the digital forensics courses and also cover the theory behind what they were learning. However, one of the most striking things about this work is the author's description of all the difficulties they had to overcome, particularly finding qualified faculty, that illustrate the huge entry barrier facing institutions that want to adopt digital forensics curricula.

These accounts concur with our impression from personal conversations with digital forensics educators and from inspecting online curriculum listings that most digital forensics programs currently have either training-based courses taught by practitioners that teach students how to use a tool and follow a procedure, or courses that cover theory but restrict the student demographics to Computer Science or similar majors.

Our digital forensics program

To help address the needs of the digital forensics research, education, and professional communities detailed in Section Introduction, and the broader social need for qualified digital forensics practitioners, we are developing a new undergraduate certificate program in digital forensics.

To lower the entry barrier facing institutions that wish to adopt a digital forensics program, we are developing our curriculum with the express intent of distributing it as a self-contained curriculum package containing everything a Computer Science professor will need to teach the course, including an instructor handbook detailing the course content, a lab instructor handbook explaining the lab exercises, presentation slides for all lectures, “remedial” resources (such as reading lists) for the benefit of students from less technical backgrounds, and question sets to be drawn from for homeworks and exams. To the best of our knowledge, this will be an unprecedented contribution to the digital forensics educational community.

To create a curriculum in line with the fundamentally interdisciplinary nature of the field of digital forensics, we assembled a curriculum development team that includes domain experts in computer security, computer networks, law, civil and criminal justice, fraud investigation, and psychology. We take a modular approach to curriculum development, with domain experts taking the lead in developing and teaching topical modules focused on their areas of expertise. These modules are combined to form a coherent narrative to expose students to the many important perspectives on digital forensics.

While our curriculum is being developed and revised, these domain experts will serve as instructors for their own modules. This allows the content developers to get live feedback from student interactions and more easily revise their materials. The courses are not intended to require a multi-instructor format, and once the curriculum has been completed, we will transition to a single-instructor format.

In addition to forensic examination, digital forensics knowledge can be useful in a wide range of professions, such as, forensic accounting, accident investigation, e-discovery, and law. Our program is explicitly designed to be accessible to these interdisciplinary demographics.

When complete, our program will consist of an introductory and an advanced course in digital forensics with accompanying hands-on laboratory sessions. The introductory course should be accessible to a wide range of students from many disciplines and valuable as a standalone offering. For example, a lawyer who takes the introductory course will be better able to communicate with digital forensics experts, understand the capabilities and limitations of current digital forensics techniques, and understand what kind of evidence they can furnish. The advanced course will be more technically intensive, but is still intended to be accessible and valuable to students from non-technical disciplines. For example, a lawyer who completes the advanced course can use the more in-depth technical knowledge to critically evaluate digital forensic experts' reports.

This program will not be a job-track training program intended to prepare students to directly enter the job market as digital forensic examiners and analysts. Instead, it will provide 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 examiners and analysts. It is expected that these students will receive additional education specific to their career paths and some on-the-job training specific to their eventual professional roles. For example, a lawyer would naturally be expected to acquire a Law degree before beginning practice, and a student who completes our certificate program would be expected to require additional training (e.g., at a professional workshop) to receive professional and tool-specific certification.

At the time of writing, we have developed the curriculum for our introductory course and taught a pilot class that was cross-listed in Computer Science and Law, and are in the process of revising the curriculum for distribution to other institutions.

Program goals

Several high-level goals have guided the development of our curriculum. In no particular order, these goals are:

Lower entry barrier for institutions to adopt digital forensics programs

As described in Section Introduction, the primary problems facing institutions interested in adopting a digital forensics curriculum are finding a qualified instructor, difficulty and expense of setting up a lab, finding and selecting an appropriate textbook, balancing training and education, selecting prerequisites, and the lack of a widely accepted standard curriculum.

Our curriculum is designed to be easily adoptable by other universities and colleges, so we made two key decisions to address these problems. First, the curriculum package will contain everything a Computer Science professor will need to teach the course. We believe that given sufficiently detailed background material (as provided by our handbook), the instructor will not need to have industry experience practicing digital forensics. Second, the laboratory will not require the purchase of any specialized hardware or software licenses; since the lab exercises in our curriculum require only open-source, freeware tools, the difficulty and expense of setting up a lab are reduced. Our handbook can be distributed to students in place of a textbook, and adoption of a packaged curriculum removes an institution's need to balance training and education or select prerequisites.

Work toward curriculum standardization

Developing a curriculum standard for digital forensics is a challenging problem. As one of several aspects of our program intended to assist with this effort, we believe we can contribute by distributing our curriculum as an easily adoptable option that can be updated from a central source. We presented a draft of the curriculum for our introductory course to the attendees of the 2013 workshop, and received very positive feedback and approval for the course content and modular, interdisciplinary design. We intend to continue revising and improving our curriculum based on feedback from the digital forensics research and education communities, student responses, and future technological developments. Thus we can simultaneously break down the barriers to adoption (by solving additional logistic issues we hear about) and improve our curriculum to more closely match the digital forensics community's requirements for a curriculum standard. We are not proposing our curriculum as a standard, but designing it to be potentially useful in a collaborative effort within the digital forensics community to develop a standard.

Provide students with an education-based introduction to the field of digital forensics

We believe students should understand the theory behind what they are doing, not just how to do it. University graduates are marketable professionals, not because they know how to perform standard techniques better than candidates with training-based education, but because their deeper understanding of the principles and theory underlying those techniques enables them to adapt and innovate when presented with new problems. Such students will contribute to the field of digital forensics, not just by performing sound forensic examination and analysis, but by improving standard practices and finding better solutions to problems. To this end, we designed our curriculum with a focus on knowledge and deeper understanding, rather than memorization of procedures and standard practices.

Develop a curriculum that reflects the fundamentally interdisciplinary nature of digital forensics

Many different disciplines have important perspectives on digital forensics. For example, a lawyer, computer scientist, and psychologist have fundamentally different perspectives on digital forensics. The lawyer sees it as a way to strengthen his or her case; a computer scientist sees it as a way of understanding and manipulating computers; and a psychologist sees it as a way of understanding the criminal mind. Our curriculum is intended to provide students the benefit of those diverse perspectives by having instructors from relevant disciplines develop and teach interdisciplinary modules. Rather than just teach students how to work in a crime lab examining hard drives, we discuss how digital forensics skills can be applied to diverse practices. For example, in network intrusion response, investigations are often focused not on legal recourse, but damage assessment and mitigation and improving defenses for the future. These investigations are then fundamentally different from criminal investigations, because the evidence does not have to be court-admissible, only acceptable to the leaders of the victim organization, and the identity of the attacker is of secondary importance. We also introduce students to other application areas, such as fraud investigation, to demonstrate the breadth of application for digital forensics knowledge.

Make the curriculum accessible and useful to a broad demographic from multiple disciplines

We believe that a course on digital forensics would be a valuable addition to many students' education, even if they do not intend to become digital forensics practitioners. There are many practical topics in our curriculum that are important to everyone. For example, most students have little or no knowledge of the legal justice system or laws related to computer crime. Also, knowing what evidence is left behind by computer and Internet activities can inform better practices (and indeed some of our students enrolled principally for this reason). After Computer Science students, we found that the second largest demographic in our pilot class was Law students, who were interested in digital forensics so they could better understand and utilize digital evidence in their cases.

Design of a digital forensics curriculum that is accessible to such broad demographics is a particularly difficult problem that we have not entirely solved. There are two issues that must be addressed: prerequisites and technical difficulty. The problem is to make the course accessible without reducing the value for Computer Science students. We discuss our efforts in this area in the next section.

Introductory course curriculum development

The introductory course was designed to give students from a wide range of disciplines an introduction to the field of digital forensics, focused particularly on the subdisciplines of computer forensics, network forensics, and mobile device forensics, and providing relevant interdisciplinary perspectives.

It is difficult to give an introduction to a field as broad as digital forensics in a single class, but we were able to cover the major sub-disciplines and introduce many interdisciplinary perspectives in part because of our focus on education rather than training. Memorization of standard practices and procedures would be time-consuming, so by removing it, we were able to increase the breadth of topics in the introductory course. To reduce the computer forensics module to a manageable size, we chose to focus on NTFS and Windows forensics, as these are the systems students will be most familiar with and most likely to encounter in practice.

To help us develop an initial working list of topics for our introductory course, we started by compiling a list of all the topics from all the courses and recommended curriculum lists we could find, de-duplicating them, and then organizing them into modules. Within each module, we selected what we believed were the most important key concepts that could fit into the time slots available across a semester. To develop the curriculum for these topics, we started by referencing various textbooks recommended online or used by other institutions for their digital forensics classes. However, we found (as did Liu (2006)) that most of them were basically handbooks focused only on industry practice based on the authors' personal experience. For those topics for which we were not able to find adequately detailed textbook references, we gathered the required details from research papers, technical reports, and other sources. This had the added benefit of necessitating that we find the most up-to-date source material available. In addition to these resources, we incorporated our interdisciplinary curriculum development team's domain expertise into the relevant modules.

A detailed description of the lecture learning objectives for the introductory course would exceed the scope of this paper, but the high-level student learning objectives that guided our curriculum development can be concisely summarized as follows: Students should be familiar with the common terminology, techniques, and investigative processes of digital forensics, including the sub-disciplines of computer forensics, network forensics, and mobile device forensics. Students should understand how to apply the scientific method to digital forensics investigation and the importance of doing so. Students should be familiar with the different types of digital forensics evidence that can be acquired and the limitations of current techniques. Students should understand the basic operation of the United States legal justice system and court proceedings. Students should be familiar with the important laws relating to digital forensics, and how they affect the practice of digital forensics. Students should be familiar with and understand the importance of related areas such as data recovery, psychology of cyber crime, and fraud examination.

The issue of prerequisites was also difficult to resolve, since, even at an introductory level, digital forensics is a technically challenging topic that a student without a strong technical background would have great difficulty understanding. Simply requiring an operating systems course and a networking course would have been sufficient, but would have shut out the broad interdisciplinary demographics our program targets. Fortunately, the majority of the topics covered in such courses are not necessary background for a digital forensics course. For example, it is unnecessary to know how to design context switching and memory management modules to get started in our computer forensics module. All students need is a high level of computer literacy and some basic familiarity with how an operating system works. Our solution was to require knowledge prerequisites rather than course prerequisites. The course required instructor permission to enroll, and this permission was given only after the instructor had a conversation with the student and was satisfied he or she had the necessary level of prerequisite knowledge.

Lessons learned from pilot class

In the fall of 2013, we taught a pilot class of our introductory course. The class consisted of two 75-min lecture sessions and an hour-long lab session each week for a 16-week term. Table 1 shows a brief topic list for each module in our pilot class.

Teaching the pilot class for our introductory course was a very illuminating experience for our curriculum development team. While it went quite smoothly in general, several unforeseen issues became apparent as the semester progressed.

1. Coordination between instructors/modules was a challenge. We found it difficult to maintain a good narrative flow between modules. In retrospect, it is clear that the modules could have been ordered more efficiently. Some modules had overlapping topics, and the relevance of some topics needed to be made more explicit.
2. We had differing understandings of the knowledge prerequisites among the professors. Consequently, some students enrolled in the course who did not have the necessary technical background to understand the material. There was a very wide range in levels of computer literacy. In fact, several of the students were unaware that they were enrolling in a course that required a high degree of computer literacy. This issue was especially visible during the hands-on lab exercises.
3. Our pilot class enrollment mainly consisted of Computer Science students and Law students. The Computer Science students, and some of the Law students, had little trouble following the technical material. However, most of the Law students had difficulties, even with tutoring. The students' wide range of computer literacy made it difficult to pace the exercises appropriately. Although the students who struggled were a small minority of our pilot class's enrollment, they represented the potential interdisciplinary demographics to which we want our curriculum to be accessible. So as the semester progressed, and these issues became apparent, we reevaluated our curriculum to devise a solution that would not shut out these students. We observed that many of our exercises naturally had both investigative/legal components and technical components. The Law students typically performed better on the investigative components (e.g. not jumping to conclusions about a piece of evidence), and the Computer Science students generally performed better on the technical components. The solution we implemented was twofold. First, we decided to put less focus on technical detail and more on investigative and evidentiary complexities. Second, we reworked some of the labs into group assignments in which Law students were required to partner with Computer Science students. We also wrote a team project for which Law students partnered with Computer Science students and performed different roles; together they submitted a report on a fictitious case. Grouping them together allowed them to learn from each other, and we observed positive results, with students teaching each other their domain knowledge and putting their expertise together to better solve problems. The labs went visibly smoother, and both Computer Science and Law students commented that their experience was enriched by interacting with the other majors.

Table 1
Pilot class topic list, by module.

Forensics concepts
Course outline and syllabus
Define digital forensics and its subfields
Evidence handling
Psychology
Psychology of cyber crime
Criminal profiling
Computer forensics
Introduction to file systems
NTFS analysis
Deleted file recovery and file carving
Windows Registry, log files, link files, Recycle Bin
Web browser forensics, email forensics, EXIF
U.S. legal system
Disputes, courtroom workgroup, attorneys
Judges, juries, legal process
Network forensics
Networking fundamentals review
Network evidence acquisition
Protocol analysis, packet analysis, flow analysis
Application protocols, statistical flow analysis
Network intrusion detection and analysis
Law
Fourth Amendment: reasonable expectation of privacy
Warrant vs. subpoena, Federal Rules of Evidence
Privacy laws, computer crime laws
Fraud examination
Introduction to fraud examination
Characteristics and skills of a forensic accountant
The nature and extent of fraud, Benford's Law
Mobile device forensics and malware
Mobile device technology fundamentals
Mobile device evidence extraction and analysis
Mobile network evidence
Legal and ethical considerations of interception
Malware taxonomy, detection, and circumvention

Evaluation methodology

The Illinois Science, Technology, Engineering, and Mathematics Education Initiative (I-STEM) office was hired to conduct an evaluation of our digital forensics pilot class (Illinois Science, Technology, Engineering, and Mathematics Education Initiative, 2014).

The evaluation design served both formative and summative purposes; it was intended to provide us with useful feedback on the quality of implementation and delivery of the curriculum and to offer NSF insight into the curriculum's efficacy. The evaluators collected data using three methods:

1. Three student surveys were developed and distributed throughout the Fall 2013 semester. First, a pre-course

online survey was administered to registered students during the first week of the course. The survey inquired about their major, technical background, and course expectations. Second, a mid-course online survey was administered after the midterm exam; it asked students about their experiences and perspectives regarding the course thus far. Third, an end-course online survey was administered during the last week of the course to gather insight into students' overall perspectives, experiences, and suggestions for future course improvements. The surveys included both multiple-choice questions, for which students indicated their level of agreement with a statement on a scale from 1 to 5, and free-form items, prompting them for comments about specific aspects of the course or feedback in general. The first survey response rate was 93%, with 28 of the 30 students completing it. The second survey response rate was 46% (14 of 30 participants completed the survey), and the third survey response rate was 53% (16 of 30 participants completed the survey).

2. Course observations were conducted during the lectures and lab sessions. The purpose of these observations was to assess the delivery of the curriculum content, and students' engagement in and experiences with the course. Information related to the following categories was noted during the observations:
   a. Social or interpersonal setting: who was clustered with whom, and how groups and individuals were arrayed in this context.
   b. Activities: a systematic description of the activities, with time-frames.
   c. Content: a description of the resources and materials used and discussed.
   d. Interactions: a description of verbal and nonverbal interactions between the professors and students.
3. Focus groups were conducted in the middle of the course and at the end of the semester to explore students' experiences, reactions, and opinions on the course. Each focus group involved a dialog between students and one of the evaluators, who prompted the students with topics to get the conversation started. The sessions were conducted without any course staff present. A total of three focus groups (two with Computer Science students and one with non-Computer Science students) were conducted. The focus groups lasted between 30 and 40 min and included seven Computer Science and four non-Computer Science students.

Student feedback summary

Feedback from the students in our pilot course was generally quite positive, with 80% of survey respondents agreeing or strongly agreeing that course objectives and content were thoroughly covered, and 93% agreeing or strongly agreeing that they were satisfied with what they learned, for the amount of time they invested in the course. In particular, students viewed the interdisciplinary aspect as a strength of the course, and said that having multiple instructors teach the course was useful, helpful, and exciting. This is apparent from their responses in free-form feedback and focus groups, and from the 70% of survey respondents who agreed or strongly agreed that having multiple instructors teach the course was helpful. The students also gave positive feedback for the group work and interactions with students from other disciplines. Their free-form survey responses and focus group comments show that they enjoyed the cross-disciplinary engagement, and they felt they learned from the other students. Specifically, 88% of survey respondents agreed or strongly agreed that the group assignment contributed to their learning.

In the free-form feedback, students also reported issues with several aspects of the course. Students felt that there was a lack of communication among the instructors, and that the topics felt out of place and did not fit with one another. They suggested using a single, long-term case study to connect the lectures from the beginning to the end of the semester. In addition, some Law students had difficulty with the technical terminology. They suggested that instructors provide a sort of glossary of terms for quick reference.

Revisions

At the time of writing, we are revising the curriculum based on what we learned teaching the pilot class and feedback from the students. We are making several significant changes.

To improve the flow of the course between modules and make the relevance of topics more explicit, we are incorporating a fictitious case study that will run through the entire course. The story in the case study will advance as the semester progresses; new examples and assignments will be tied into the story to maintain students' interest and make the "big picture" clear.

We will be changing the module ordering. Specifically, we will put the legal justice system and law modules before any of the technical material, as those modules present the wider social impact of digital forensics and how it is used in court respectively. This will make it clear to students *why* digital forensics is practiced before they learn *how* it is practiced. Other modules will be ordered to best fit the overall fictitious case study.

We will be making four substantial changes to address the problem of varying computer literacy in students, without shutting out the interdisciplinary demographics.

First, we will extend the increased focus on investigative issues, analysis of evidence, and group activities that we successfully applied to the later portion of the course to the earlier portions as well. These group activities are not intended to *require* a legal background for any of the students, as we understand that it is likely that many institutions will not have students with such a background in their class. Rather, the activities will encourage students to look at the problems from a different perspective. Thus, students from diverse backgrounds will be more valuable to the group, and all the students will gain a broader understanding of the issues they are learning about.

Second, we have decided to compile a primer on technical fundamentals, to be made available to students before the first day of class. It will contain very brief explanations of fundamental concepts that are important as knowledge prerequisites, to refresh the memory of students who may have taken the relevant background classes some time ago, and will also contain references to more in-depth readings for students who are missing specific topics.

Third, we will provide a glossary of terminology for quick reference. This will be useful for students from diverse backgrounds who may be familiar with the concepts, but under different names.

Fourth, we will include a short prerequisite “quiz” that must be completed before students can receive the required instructor permission to enroll in the course. Considering the wide range of technical literacy we saw in our pilot course, a couple simple questions that would seem trivial to someone with a technical background, but very challenging to a typical layperson would suffice (e.g., “What is ASCII?”). The quiz should take no more than a couple of minutes to complete, with the answers written or given verbally to the instructor, and would have two primary purposes. First, it would let students know what sort of course they are enrolling in from the start. Second, it would deny enrollment to students who simply do not have the background to understand even the primer material we will make available to them.

Conclusions and future work

In order to address the growing need for more high-quality digital forensics education programs, we are developing a curriculum package in digital forensics suitable for easy adoption by other institutions. This curriculum is designed to reflect the interdisciplinary nature of the field of digital forensics and provide a strong theoretical foundation for the techniques the students learn. We have completed the curriculum for the introductory course and taught a pilot class using it. Based on our experience developing and teaching this class and feedback from the students, we are revising the introductory course curriculum for distribution.

An alpha version of our curriculum package for the introductory course will be available in the summer of 2014. We are very excited to share it with universities and colleges looking to adopt a digital forensics curriculum; we encourage interested readers to contact us. We would also be grateful for any feedback from the digital forensics education, research, and professional communities. Based on this feedback, and our future experiences teaching the curriculum, we will continue to revise and improve our curriculum package.

We are also developing the curriculum for our advanced course in digital forensics, to be piloted here in Spring 2015. We plan to include the advanced course and a further-updated introductory course in our curriculum package by sometime in 2015, and we intend to offer an online version of both courses in the future.

Acknowledgments

We would like to acknowledge the attendees of the 2013 Digital Forensics Curriculum Standards workshop for their engaging discussions and invaluable feedback. This work was 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.

Appendix A. Student survey responses

Table A.1
Student survey responses.

Mid-course student survey responses to question “Having multiple instructors teach the course is helpful.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	1 (7%)	1 (7%)	10 (71%)	2 (14%)
Post-course student survey responses to question “Having multiple instructors teach the course was helpful.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	2 (13%)	5 (31%)	4 (25%)	5 (31%)
Mid-course student survey responses to question “Course objectives/content are thoroughly covered.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	–	2 (14%)	11 (79%)	1 (7%)
Post-course student survey responses to question “Course objectives/content were thoroughly covered.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	–	4 (25%)	12 (75%)	–
Mid-course student survey responses to question “For the amount of time I invest in this course, I'm satisfied with what I learned.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	1 (7%)	–	10 (71%)	3 (21%)
Post-course student survey responses to question “For the amount of time I invested in this course, I'm satisfied with what I learned.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	1 (6%)	–	10 (63%)	5 (31%)
Post-course student survey responses to question “The group assignment contributed to my learning.”				
Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
–	–	2 (13%)	12 (75%)	2 (13%)

References

ACM/IEEE-CS Joint Task Force on Computing Curricula. Computer Science Curricula 2013 [Tech. rep.]. ACM Press and IEEE Computer Society Press; December 2013. http://dx.doi.org/10.1145/2534860. URL, http://dx.doi.org/10.1145/2534860.

Chi H, Dix-Richardson F, Evans D. Designing a computer forensics concentration for cross-disciplinary undergraduate students. In: Proceedings of the 2010 Information Security Curriculum Development Conference. New York, NY, USA: ACM; 2010. pp. 52–7. http://dx.doi.org/10.1145/1940941.1940956. URL, http://doi.acm.org/10.1145/1940941.1940956.

Cooper P, Finley GT, Kaskenpalo P. Towards standards in digital forensics education. In: Proceedings of the 2010 ITiCSE Working Group Reports. New York, NY, USA: ACM; 2010. pp. 87–95. http://dx.doi.org/10.1145/1971681.1971688. URL, http://doi.acm.org/10.1145/1971681.1971688.

Forensic Science Education Programs Accreditation Commission. FEPAC accreditation standards [Tech. rep.]. American Academy of Forensic Sciences; 2012.

Forensic Science Education Programs Accreditation Commission. Accredited universities. URL, http://fepac-edu.org/accredited-universities; 2014.

Gottschalk L, Liu J, Dathan B, Fitzgerald S, Stein M. Computer forensics programs in higher education: a preliminary study. SIGCSE Bull Feb. 2005;37:147–51. http://dx.doi.org/10.1145/1047124.1047403. URL, http://doi.acm.org/10.1145/1047124.1047403.

Illinois Science, Technology, Engineering, and Mathematics Education Initiative. Digital forensics course evaluation report [Tech. rep.]. University of Illinois at Urbana Champaign; January 2014.

Lang A. A new portable digital forensics curriculum [Master's thesis]. University of Illinois at Urbana-Champaign; 2014.

Liu J. Developing an innovative baccalaureate program in computer forensics. In: Proceedings of the 36th Annual Frontiers in Education Conference; 2006. pp. 1–6. http://dx.doi.org/10.1109/FIE.2006.322593.

Liu J. Implementing a baccalaureate program in computer forensics. J Comput Sci Coll 2010;25(3):101–9. URL, http://dl.acm.org/citation.cfm?id=1629116.1629134.

Scientific Working Group on Digital Evidence. SWGDE/SWGIT guidelines and recommendations for training in digital and multimedia evidence [Tech. rep.]. Scientific Working Group on Digital Evidence; January 2010. URL, https://www.swgde.org/documents/Current Documents.

Srinivasan S. Computer forensics curriculum in security education. In: Proceedings of the 2009 Information Security Curriculum Development Conference. New York, NY, USA: ACM; 2009. pp. 32–6. http://dx.doi.org/10.1145/1940976.1940985. URL, http://doi.acm.org/10.1145/1940976.1940985.

Wassenaar D, Woo D, Wu P. A certificate program in computer forensics. J Comput Sci Coll Apr. 2009;24:158–67. URL, http://dl.acm.org/citation.cfm?id=1516546.1516575.

West Virginia University Forensic Science Initiative, August. Technical Working Group for Education and Training in Digital Forensics [Tech. rep.]. United States Department of Justice; 2007. URL, https://www.ncjrs.gov/pdffiles1/nij/grants/219380.pdf.