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

A B S T R A C T

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
1742-2876/

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.