



Textbooks for Computer Forensic Courses: A Preliminary Study

Jigang Liu

Department of Information and Computer Sciences, Metropolitan State University, St. Paul, Minnesota USA, jigang.liu@metrostate.edu

Larry Gottschalk

Department of Information and Computer Sciences, Metropolitan State University, St. Paul, Minnesota USA, larry.gottschalk@metrostate.edu

Kuodi Jian

Department of Information and Computer Sciences, Metropolitan State University, St. Paul, Minnesota USA, kuodi.jian@metrostate.edu

Follow this and additional works at: <https://commons.erau.edu/adfsl>



Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Liu, Jigang; Gottschalk, Larry; and Jian, Kuodi, "Textbooks for Computer Forensic Courses: A Preliminary Study" (2007). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3.

<https://commons.erau.edu/adfsl/2007/session-10/3>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



Textbooks for Computer Forensic Courses: A Preliminary Study

**Jigang Liu,
Larry Gottschalk,
Kuodi Jian**

Department of Information and Computer Sciences
Metropolitan State University
St. Paul, Minnesota USA
Jigang.liu@metrostate.edu
Larry.Gottschalk@metrostate.edu
Kuodi.Jian@metrostate.edu

ABSTRACT

As computer forensics develops into one of the fastest-growing areas in the computer related fields, many universities and colleges are offering or are planning to offer a course in computer forensics. When instructors begin to develop a new course in the area, one of critical questions they would ask is what textbook should be used. To better answer the question, we conducted a study in which we tried to find which textbooks are being used in computer forensic courses. We believe that the results and analysis of our study will help instructors in choosing adequate textbooks for their new course in computer forensics.

1. INTRODUCTION

With a loss of more than hundred millions dollars due to computer related crimes [3], the prosecution of criminal activities in cyberspace has become a critical issue. As a result, the demand for the professionals with the expertise in collecting, identifying, reconstructing, preserving, analyzing, and presenting digital evidence in a court of law has been increasing radically. In addition, as stated in [2] the number of incoming freshmen in computer science dropped significantly between 2000 and 2004 by an alarming 60%, the authors suggest recenter or revamp computer science programs through updating the curriculum. According to their recommendation, computer forensics is one of the innovative themes in freshman-sophomore courses.

In responding to this demand and also re-energizing the computer science education, many universities and colleges have recently begun or are planning to offer a curriculum or a course in computer forensics as predicted by the authors of [11] and surveyed by the authors of [5]. The experience from the curriculum design for an undergraduate program were introduced in [6, 7] and for a graduate program was discussed in [8]. The issues on course development were presented in [9,10]. To know how to design labs one can find some suggestions in [4, 9]. Although designing a course in computer forensics is a primary task, choosing an adequate textbook also plays a significant role in developing and then teaching the course.

In this paper, we will first present the method used in the study and then illustrate the results found over the Internet. The analysis and discussion over the finding is provided next. Finally, the conclusion of the study is given.

2. GUIDELINES AND METHODS

Although computer forensics is a new area of study, there are more than 50 books published on the topic. To find one or two books suitable for a computer forensics course is not an easy task due to many concerns, such as the topics covered in the book, the background of the instructor, the prerequisites for taking the course, and the availability of hardware and software.

In order to setup a solid foundation for the analysis of the selection of a textbook for a computer

forensics course, we decided to collect information from two ends. One is to gather information on all the books on computer forensics so that a pool of the books is available for the selection. The other is to examine all the online syllabi on computer forensics so that the current selections of the textbooks are available for the analysis.

Two sources were mainly used to collect computer forensics books. One is Amazon.com (www.amazon.com) and the other is E-Evidence.com (www.e-evidence.com). Both websites have a sound collection of computer forensic books while Amazon.com has more updated information. In addition to the titles of the books, other information has been recorded as well, such as when it was published, if a CD is included, and the cost. To help us to look up the data, we have created an E-Card, as shown in Figure 1, for each book we found.

Project: Textbooks for Computer Forensics Courses: A Preliminary Study		Metropolitan State University
Project No: R200604		Department of ICS
Book Card No: 001		Minneapolis/St. Paul, MN
Date: Sept. 22, 2006		
Book title: Author(s): Year published: Edition: Publisher Number of pages ISBN: Cost: Major stuff on the CD* Targeted audience* Teaching materials* Learning support* Adopted institutions*:		
Notes: Major stuff on the CD: list three to five items that could be tools included; experimental examples, or exercises. Targeted audience: practioners, IT professionals, managers, law enforcement officers, or students; Teaching materials: whether lecture slides, exercise solutions, or other teaching support materials are provided; Learning support: whether a self-learning CD, a website, or student learing materials are provided; Adopted institutions: whether a two-year, four-year, or research institution. It can be filled up later.		

Figure 1 E-Card for Recording a Computer Forensic Textbook

To locate all the computer forensic course syllabi that are available over the Internet is a bit time consuming. The search is based on the *google* search engine with the key words “computer forensic course syllabus.” Based on the syllabi found over the Internet we can uncover what textbooks have been used and then determine which has the most adoption (?), the “most adoption” phrase is confusing). As for a computer forensic book, we have also created an E-Card for each syllabus we found, as shown in Figure 2. Through a CF-course E-Card, we can obtain all the information we need, such as the category of the institution, research institution vs. teaching institution vs. two-year colleges; the department which offers the course, computer science vs. management information systems vs. or criminal justice; the textbook or textbooks used, a single textbook vs. multiple textbooks; the type of the course, a lecture-based course vs. an online course vs. an independent study course vs. a hands-on course; and the level of the course, graduate-level vs. senior-level vs. junior-level vs. sophomore-level vs. freshmen-level, etc.

Project: Textbooks for Computer Forensics Courses: A Preliminary Study Project No: R200604 Course Card No: 001 Date: Sept. 22, 2006	Metropolitan State University Department of ICS Minneapolis/St. Paul, MN
Title of the course Level of the course*: Offered by (department) Textbook used: Title: Author(s) ISBN: Prerequisites: Targeted audience Type of the course*: Type of the institution*: Length of the course*: Credit of the course*:	
Notes: Level of the course: course number or freshmen, sophomore, junior, or senior. Type of the course: independent study, seminar, or lectured based Type of the institution: community college, technical college, four year college or university, or a research university Length of the course, 14 weeks, 15 weeks, or 16 weeks. Credit of the course: number of credits in semester or quarter	

Figure 2: E-Card for Recording a Computer Forensics Course Syllabus

3. SEARCH RESULTS

Through the two resources mentioned previously, we located 75 books that relates to computer forensics. The google search on computer forensic course syllabus returned 792 hits on Sept. 20, 2006. By checking each of the hits, we found 53 course syllabi among 41 institutions. Out of 53 syllabi, 23 different books have been chosen as the textbooks. Table 1 indicates the categories of institutions which offer at least one course in computer forensics. Table 2 shows how the courses offered through various departments. The distribution among the levels of the courses is presented in Table 3. Table 4 provides the three most frequently used textbooks. The way in which the three most popular books are distributed among the 53 syllabi is given in Table 5.

Table 1 Distribution over Institution Categories (N=53)

Category	# of course	Percentage
Research Institution	19	36
Teaching Institution	31	58
Two-year College	3	6

Table 2 Distribution over Departments (N=53)

Department	# of course	Percentage
Computer Science	32	60
Criminal Justice	3	6
Business	10	19
Other (Interdisciplinary)	8	15

Table 3 Distribution over Level of courses (N=53)

Academic Level	# of course	Percentage
Graduate	16	31
Junior or Senior	28	54
Freshmen or Sophomore	9	18

Table 4 Three most chosen textbooks

Title	Author(s)	Year
Guide to Computer Forensics and Investigation	Phillips, A. et al.	2005
Computer Forensics: Incident Response Essentials	Kruse, W. and Heiser, J.	2001
Incident Response: Computer Forensics	Prosise, C. and Mandia, K.	2003

Table 5 Distribution over three popular books (N=53)

Book	# of course	Percentage
Phillips and et. al.	14	26
Kruse and Heiser	8	15
Prosise and Mandia	5	9

4. ANALYSIS AND DISCUSSION

Based on the search result provided above, we found there has not been a dominate textbook chosen by a majority of the institutions. Although the Phillips's book has the highest rate of adoption, only one in four schools selected this book.

Teaching institutions have been taking the lead in offering courses in computer forensics. Research institutions also represent a good percentage in offering the course. In terms of departments, computer science has led the crowd. But the study might not be 100 percent accurate because many criminal justice departments might not post the syllabi on the Internet. The low percentage attributed to two-year colleges might also be caused by this reason.

More than 80 percent of the courses have been offered at junior or above level, which indicates the subject needs a higher prerequisite than many other courses. More than 30 percent of the courses have been offered as a graduate level course, which indicates that there is a fair number of people who believe the course should be offered at a graduate level.

The major components of the courses we found are lectures, labs, case studies, and guest speakers. Most of courses were offered by a single instructor but some of them were team-taught. Some universities hired adjunct faculty to teach the skill-based and experience-concentrated components while the full-time faculty covered subjects that are more theory and foundation related. A detailed discussion on the design and construction of computer forensics courses will be presented in a future paper.

5. CONCLUSION

In this paper, we did a primary survey over the available websites provided by the instructors. We appreciate their generosity in sharing their teaching materials with everyone so that this study could be conducted. We realize that a few of schools did not make their teaching materials available on the Internet or removed their teaching materials from the Internet after the classes were over.

We concurred with the opinion presented in [1] that "analogies should not be applied too rigidly or rigorously." The new program needs the room and time to be further developed and the standardization will prevent it from being fully and healthily developed. "Most importantly, for the

analogy to gain some validity, the next logical step is to look for evidence of concomitant speciation toward security, assurance and forensics concerns in colleges of business and to digital concerns in criminal justice.”

Computer forensics is a growing field and that requires more attention and more coordination to keep it healthy and growing. It is normal for a young field to not have a dominated textbook. As more studies are conducted and more experience is gathered, a consensus on the textbook as well as the topics in a course will be eventually reached.

6. REFERENCES

- [1] Cooper, P., “Speciation in the Computer Sciences: Digital Forensics as an Emerging Academic Discipline,” Information Security Curriculum Development Conference '05, Sept. 23-24, 2005, Kennesaw, GA.
- [2] Denning, P. and McGettrick, A., “Recentring Computer Science,” Communication of the ACM, Nov. 2005, Vol. 48, No. 11, pp15-19
- [3] Dixon, P. “An Overview of Computer Forensics,” IEEE Potentials, Dec. 2005, pp7-10
- [4] Francia, G., “Digital Forensics Laboratory Projects,” Journal of Computing Sciences in Colleges, Volume 21 Issue 5, May 2006, Information Security Curriculum Development Conference '05, Sept. 23-24, 2005, Kennesaw, GA
- [5] Gottschalk, L., Liu, J., Dathan, B. Fitzgerald, S. and Stein, M., “Computer Forensics Programs in Higher Education: A Preliminary Study,” proceedings of the 36th ACM/SIGCSE Technical Symposium on Computer Science Education, Feb. 23-27, 2005, St. Louis, MO
- [6] Kessler, G. C. and Schirling, M. E., “The Design of an Undergraduate Degree Program in Computer and Digital Forensics,” Journal of Digital Forensics, Security and Law, Vol. 1(3), 2006
- [7] Liu, J. “Developing an Innovative Baccalaureate Program in Computer Forensics,” proceedings of the 36th ASEE/IEEE Frontiers in Education Conference, Oct. 28 – 31, 2006, San Diego, CA
- [8] McGuire, T. and Murff, K., “Issues in the Development of a Digital Forensics Curriculum,” Journal of Computing Sciences in Colleges, Volume 22, Issue 2 (December 2006), pp 274-280
- [9] Troell, L. Pan, Y. and Stackpole, B., “Forensic Course Development,” Proceedings of the 4th Conference on Information Technology Curriculum (CITC4 '03), Oct. 16-18, 2003, Lafayette, IN
- [10] Troell, L. Pan, Y. and Stackpole, B., “Forensic Course Development: One Year Later” Proceedings of the 5th Conference on Information Technology Curriculum (CITC5 '04), Oct. 28-30, 2004, Salt Lake City, Utah
- [11] Yasinsac, A. and et. al., “Computer Forensics Education,” IEEE Security and Privacy, July-August, 2003, pp15-23

