Proceedings of the 8th Colloquium for
Information Systems Security Education
West Point, NY June 2004

Designing a Computer Forensics Course for an Information Assurance Track

Barbara Endicott-Popovsky, V. M. Popovsky, and Deb Frincke, *IEEE Member*

Abstract - At the 7th Annual CISSE conference, 2003, a case study was presented regarding adding information assurance to the curriculum of a small private university in the Pacific Northwest with only a moderate budget and without hiring additional permanent faculty. In this paper, we continue to describe the evolution of that curriculum, this time describing the challenges of finding the best way to teach computer forensics, a cross-discipline subject that requires not only technical expertise, but an understanding of the relevant legal and evidence-collecting guidelines that govern a computer forensics investigation. This paper discusses strategies used to design a computer forensics course that combines all of the necessary elements in a way that actively engages students in their own learning. Using resources available within the community and building the course around a business game, the school was able to launch an enthusiastically received course. Central to the curriculum, the business game allowed students to learn while simulating a real world criminal investigation culminating in an actual courtroom where students used the products of their investigations to testify as "expert witnesses." The original stimulus to create this course came from an NSA Center of Excellence (University of Idaho) sponsored Computer Forensics Workshop that encouraged universities with an information assurance track to introduce courses in Computer Forensics. The lessons learned from this effort could prove useful to other universities contemplating similar attempts.

Index terms – Information Assurance, Infrastructure Assurance

I. Introduction

Responding to demand, Seattle University developed an information assurance program during academic year 2003-2004 designed to meet demands of students seeking new skills and businesses (many of which are major software developers and e-commerce institutions located in the greater Puget Sound area) seeking skilled computer security specialists. The program targets senior, undergraduate, computer science students and graduate students in a Masters of Science program in Software Engineering. Courses in the program are offered as electives for undergraduates and a specialty track within the Masters program for graduate students.

Barbara Endicott-Popovsky, Lecturer, Seattle University;
V. M. Popovsky, Affiliate Professor, School of Education, Department of HPERD, University of Idaho;
Deb Frincke, Associate Professor, Computer Science Department, University of Idaho

Pre-requisites for the Computer Forensics course were either an Introduction to Computer Security course, which maps to NSTISSI Standard 4011, or considerable experience with networks.

Seattle University's information assurance program is unique in the Puget Sound area where nothing similar currently exists. With this new program, the school anticipates attracting new students, in addition to serving former alumni. Through the development of a business advisory committee for the program, the school also expects to attract a new pool of students drawn from companies represented on the committee.

In addition, the program is consistent with the educational mission of Seattle University and the school's commitments to education for values and service learning. It provides a natural synergy with Seattle University's Law School and the Ethics Program in the Albers Business School. The first attempt at collaboration among the schools was the initial course in Computer Forensics offered in spring of 2003.

The balance of this paper deals with how that course was conceived and developed, using resources from a variety of disciplines and walks of life to deliver a realistic and meaningful learning experience.

II. Pedagogical Basis

Conventional pedagogy involves delivering information in the stand-up lecture mode accompanied by forced learning techniques such as "cramming" for exams. A more effective approach seeks to inspire active student learning through academic simulations known as "business games." This approach has been implemented in education relatively recently. Fifty years ago, it was introduced in military schools and has since become one of the learning forms of education in leading colleges and universities around the world. [1, 2]

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

A. Business Games

Business games are designed to bring students into the circumstances that they will face in the future as professionals. Effective games meet educational objectives for developing creative thinking skills about a subject, as well as practical knowledge. A successful game inspires students to do independent research into the subject in question. It prepares graduates for the dynamic and intensive experience of modern business, getting them ready to solve the kind of ongoing and unpredictable professional problems they will inevitably face. [2, 3]

B. Planning a Business Game

A pedagogical business game should imitate real professional situations that demand immediate problem solving and allow students to model real business practices. In creating an appropriate game, instructors should follow these steps [3, 4]:

1) Develop the game script and business conditions being emulated.
2) Establish competition among participants to achieve a common objective while working from their assigned business roles.
3) Draw on specific knowledge and skills students are expected to learn.
4) Find a practical problem to solve.
5) Manage the game using experienced instructors to analyze/correct participants' actions/decisions in the dynamic situations that arise during its execution.
6) Evaluate game success on the degree of preparedness and interest of the students.

The above steps were followed in designing a business game for a Computer Forensics course offered at Seattle University during the Spring of 2003. The game threaded through the entire ten-week course culminating in a dramatic end-of-course role play. The course is described next, beginning with a discussion of how the game was conceived and designed.

III. Computer Forensics Course

The course drew on multi-disciplinary resources unique to the school--a law school, an ethics track in the business school, a computer science program and the Jesuit tradition of the university. The course was designed to inspire student involvement and independent study. Using a business game as the basis for the learning process emerged as the best way to gain this kind of student response.

A. Computer Forensics Game

Working with a volunteer who was a retired Federal prosecutor, the game script was devised and resources recruited to support its development. Those activities are described below.

1. Game Script and Business Conditions

The game was built around an actual computer intrusion investigation. Working with professionals in the community, a case was selected that became the backbone for the course.

The following selection criteria were used to identify an appropriate scenario:

1) Is the case in the public domain?
2) Does documentation for the case exist?
3) Is the victim organization willing to permit use of the case in the course?
4) Is the systems administrator, who documented the case, available as a guest lecturer?
5) Does the case involve both disk and network forensic techniques?
6) Was the case developed for criminal prosecution?

The retired federal prosecutor identified an actual case in the public domain that met the above criteria. The systems administrator who documented the intrusion agreed to guest lecture. The case began with "discovering" the intrusion and culminated in a courtroom exercise where students gave "expert testimony" developed from their forensic analyses. The court proceedings were designed to be realistic. The Law School courtroom was reserved and commitments were gained from a sitting Superior Court Judge who agreed to preside, along with two attorneys who agreed to argue the prosecution and defense sides, respectively.

Weekly course topics stepped through the progression of a case. Reading materials, homework assignments and discussion topics aligned with each week's learning objectives. Evidence development for the courtroom exercise built from week to week.

2. Competition

To stimulate excellence, a competition was devised. Students worked in teams of 3 to 5. Each team developed its own forensic investigation and courtroom exhibits and selected one member to be the "expert witness." A "jury" was drawn from the rest who were polled for their opinions on the effectiveness of each witness. A post mortem afterward allowed students to receive feedback from the legal professionals running the mock courtroom. Video cameras recorded the proceedings, providing

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

additional feedback on student performance, which served as an added incentive to do their best.

3. Specific Knowledge and Skills

To participate successfully, students were required to draw on their new knowledge of computer forensics. Readings and hands-on assignments helped students develop skills for analyzing and interpreting network logs and files retrieved from hardware disks.

4. Practical Problem

The game addresses one of the most difficult practical problems faced by computer forensics investigators--explaining what they have done to track a perpetrator in terms a lay jury can understand. The courtroom exercise forces students to grasp becoming an effective expert witness. First, students must master the concepts of the course. Then they must "educate" their assigned prosecuting attorneys and learn how to survive questioning by the defense.

5. Game Management

The instructor, volunteer attorneys and law students guided students' preparation to testify. Testimony summaries and courtroom exhibits were created by each team and scrubbed several times. Practice at fielding questions was conducted before court was held. Every opportunity was taken to prepare students for the experience and coach them through the process.

6. Game Evaluation

Once completed, the game was evaluated based on student preparedness and the results of a student survey at the end of the course.

B. Content

Course content was drawn from computer science, the forensic sciences, law, investigative techniques and ethics. It was organized into three categories: data storage and network fundamentals; security, management and forensics; and law and ethics. Upon successful course completion, students were able to do the following:

Data Storage and Network Fundamentals:
1) Describe the basics of NTFS vs. FAT32 vs. UNIX file systems and data storage
2) Describe wide varieties of data storage devices, how they operate, and how these devices contain and conceal evidence
3) Capture critical system data from computer disks
4) Capture critical information from a network incident.

Security, Management, and Forensics:
1) Describe threats and vulnerabilities to which a computer system/network may be exposed
2) Describe policies and associated controls that provide appropriate incident response.
3) Identify intellectual property, such as patents, copyrights, critical or confidential information from which a computer incident might arise.

Law and Ethics:
1) Discuss how the 4th Amendment to the U.S. Constitution applies to computer and network search and seizure,
2) Discuss the implications of the Electronic Communications and Privacy Act, the U.S. Patriot Act, U.S. Federal and state guidelines,
3) Identify ethical and legal issues relating to intellectual property, patents, copyright, etc.
4) Apply the rules of evidence to an electronic crime scene and to obtaining computer evidence. (i.e. recognize what can and cannot be seized.)
5) Discuss the methods of ensuring the chain of custody of evidence.

1. Community Resources

Additional professionals were used as guest speakers throughout the course. These included members of local law enforcement, local forensics investigators, as well as the systems administrator who had experienced the break-in used as the case.

2. Textbooks

Two textbooks were adopted:
1) Kruse II, W. G. and Heiser, J. G. (2002*). Computer Forensics/Incident Response Essentials*. New York: Addison-Wesley. ISBN 0-201-70719-5 [5]
2) Marcella, A. J. and Greenfield, R. S. (Ed.). (2002). *Cyber Forensics: A field manual for collecting, examining, and preserving evidence of computer crimes.* Washington, D.C.: Auerbach Publication. ISBN 0-8493-0955-7 [6]

3. Teaching Responsibilities

A full time faculty member from Seattle University's Computer Science Department assumed primary responsibility for teaching the course. However, with the need to teach a significant amount of law, the retired Federal prosecutor participated in teaching those portions of the course and assisted with designing and administering the mock court exercise.

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

C. Lab Exercises

Students were given lab exercises that could be accomplished on their home computers.

Lab Exercise	Description
Social Engineering Project	Students to gathered enough information to impersonate some person on campus in a social engineering exploit, using only open sources—telephone books, dumpsters, wastebaskets, online data.
PC Audit	Students performed and documented a full audit of their home PC's.
Disk Forensics Experiment	Students used open source tools to extract and analyze data from an image of a floppy, obtained from a police search of a suspected drug dealer.
Network Forensics	Students analyzed log evidence seized during an actual investigation to develop summaries and courtroom exhibits.

Table 1. Lab Assignments

1. The Development of the Case

By mastering the skills gained in these exercises, students prepared to develop their testimony. The case progressed week by week, with successive speakers helping to develop it. The systems administrator opened the course, presenting the symptoms of the attack as they first emerged. [7] He discussed the results of the attack and how he recovered the compromised systems in such a way that the evidence was preserved properly in the event the case went to court. This was a good object lesson

The second week the FBI was "called in" to investigate. They presented the case for involving law enforcement and discussed how a criminal investigation would proceed. The following week, students were presented with the laws and legal procedures that constrain an investigation. While students were learning the legal background they conducted their social engineering experiments and audited their own PC's.

The next three weeks were devoted to learning disk and network forensics techniques. Several forensics investigators spoke to the class and students did their forensic assignments. During the remainder of the course, students worked in teams preparing to testify. They were coached on 1) how to become credible expert witnesses and 2) how to develop courtroom exhibits.

2. The Mock Courtroom Exercise

Court was conducted the last day of class, in lieu of a final exam. Each team's "expert witness" testified to the evidence they had prepared. Grading was based on the quality of the materials prepared by the team. The volunteer prosecuting and defense attorneys conducted themselves as in a real courtroom. The presiding judge swore in witnesses and ruled from the bench as he would in a real case.

The experience was effective at mirroring real life. The student teams prepared well, knowing that their grade was determined by the quality of their preparation. Twelve of the remaining students participated as jurors sitting in the jury box, listening to the proceedings. The balance of the class was seated in the courtroom and watched the entire process.

The results were riveting. Although each student team was investigating the same case, the presentations were different, reflecting the creativity with which each team rendered the material intelligible for a lay jury. Examples and metaphors were well thought out. At the post mortem, students expressed their enthusiasm. More than one said this was the best class they had taken during their studies at the university. They learned a great deal and enjoyed the process at the same time.

IV. Course Outcomes

37 undergraduate and 6 graduate students completed the course. Students were required to complete a student survey; the results follow. Answers range from a high of 5 to a low of 1.

Questions	Score
1. Course as a whole was well organized	4.3
2. Instructor's use of class time was effective	4.5
3. Instructor's attitude/teaching style encouraged my learning	4.7
4. Overall impression is that the instructor was effective	4.7
5. Instructor appropriately assessed learning skills	4.3
6. Best effort was given to achieve course objectives (Compared to other courses)	4.4
7. Hours spent per week on the course	7.5
8. Overall Evaluation	4.5

Table 2 Undergraduate Student Survey Results

Questions	Score
1. Course as a whole was well organized	4.5
2. Instructor's use of class time was effective	5.0
3. Instructor's attitude/teaching style encouraged my learning	5.0
4. Overall impression is that the instructor was effective	5.0
5. Instructor appropriately assessed learning skills	5.0
6. Best effort was given to achieve course objectives (Compared to other courses)	5.0
7. Hours spent per week on the course	8.0

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

8. Overall Evaluation	4.9

Table 3 Graduate Student Survey Results

The most significant score to Seattle University is the one given for overall evaluation of a course. Undergraduates rated the course a 4.5 out of 5, while graduates rated the course at 4.9 out of 5. This is high compared to other department courses, which usually range from 3.0 to 4.0.

Based on the scores and student comments, the course was considered a success and has become a permanent part of the curriculum. As part of the permanent curriculum, additional measures of course success will be applied to future course evaluations. These include mappings of course objectives to course outcomes such as test scores and student assignments. Additional data will be collected during follow up surveys, post graduation, to determine if graduated students have found this course and/or the information assurance track valuable in finding good jobs or in advancing their careers.

V. Lessons Learned

The successful outcome for Seattle University's Computer Forensics course relied on resources provided by a variety of sources both inside and outside the university. Table 4 summarizes these resources and identifies their source and the contributions they provided the course.

Source	Resources Provided	Contribution
Community experts	• Guest lecturers –Systems analyst –FBI agent –Federal Prosecutor, ret –Forensics investigators • Mock court volunteers –Superior Court Judge –Experienced trial attys	Provided guest lectures & moral support for launching the course. Provided volunteer support for conducting moot court
Law School	• Court facilities • Law students • Video taping	Provided the ability to conduct a moot court as the culmination of the course.
Conference	• Forensics Workshop CSDS, U of Idaho 9/23/02 • Computer Security & Cyber Crime II K. Co. Bar Asso. 10/ 24/02 Seattle	Provided course content material as well as a network of resources for advice on building the program.
Publication	• Textbooks • Journal articles • Magazines • Online sources • Newspapers	Provided updated info. on computer forensics advances.

Table 4: Sources/Resources Contributing to Course Success

Developing a business game that threaded through the entire course presented coordination challenges to the curriculum developer. Assembling the resources required orchestration and a project management effort throughout the term to ensure that everything went smoothly.

Looking back, the volunteer commitment of the retired Federal prosecutor was significant, about 10 hours a week during much of the course. This goes beyond the typical guest lecturer who might be asked to participate once or twice a quarter. As a result, it was determined that the next time the course was offered, a half time adjunct faculty stipend would be offered as compensation to anyone assuming responsibility for conveying the legal perspective.

Course results were excellent, but anyone attempting to repeat this effort would be advised to develop a similar resource set. Careful project planning and management are then required to keep the entire process on track.

In addition, team work-products created in support of the final courtroom exercise proved an effective replacement for a final exam. It is not uncommon for computer science courses to substitute a substantive end-of-term team project for the final exam. The amount of work required in this instance was considerable. Teams spent a minimum of 40 hours to develop testimony summaries, courtroom exhibits and prepare their attorneys. They were graded on the substance and quality of their work-products, rather than the presentation of their selected witness on the witness stand. The former was deemed a fairer assessment of individual student performance.

These are lessons learned from this experience:

1) Designing a computer forensics course around an actual criminal investigation provides a powerful learning experience.
2) A high level of planning and coordination is required to successfully execute such a course.
3) Partnering with a legal professional ensures that aspect of computer forensics is taught credibly.
4) Recruiting someone familiar with prosecuting cybercrime adds value to the instruction.
5) Community resources are eager to help. Information security professionals in the Seattle community proved to be a close knit, helpful group—interested in seeing knowledgeable students graduate with skills that can be immediately put to use in their field.
6) Be prepared for a lot of student interest. The choice to turn down students was not considered an option since there was a desire to promote student enthusiasm. The class size was large and required

ISBN 0-87145-192-1/04/$15.00 © 2004 CISSE

extra help from law school students to manage the many witness teams that resulted.

7) Seek feedback to improve the course. Mid-course evaluations kept the course on track. End-of-course feedback helped with modifications for next year.

VI. Conclusions and Future Work

The results of this experiment at introducing a computer forensics course into the information assurance curriculum at Seattle University were excellent as judged by student survey results. Students exceeded instructor expectations in terms of preparing themselves for class, and the department expanded its information assurance course offerings. In unsolicited emails, students expressed their enjoyment and appreciation for a powerful learning experience. Several were inspired to pursue information assurance careers and related internships.

The University now offers a concentration in information assurance in its Software Engineering Master's program; its courses are NSA certified against NSTISSI standards 4011 and 4012. In addition, the school has received NSF funding for a computer forensics certificate program in collaboration with the University of Washington and Highline Community College. Three additional courses are planned--Advanced Disk Forensics, Host Forensics and Network Forensics. The experience and feedback from the course discussed in this paper will be used to design these additional courses.

VII. References

[1] Achmetov, N.K., and Haidorov, J.C. (1985). *The Game as an Educational Process*. Alma-Ata, Kazakhstan.

[2] Petrovsky, A.M. (Ed.). (1986). *Fundamentals of Pedagogy and Psychology in Schools of Higher Education*. Moscow, Russia.

[3] Roginsky, V.M. (1990). *Alphabet of Pedagogical Work*. Moscow, Russia: School of Higher Education.

[4] Simonov, V.P. (1981). *The Emotional Brain.* Moscow, Russia: Science.

[5] Kruse II, W. G. and Heiser, J. G. (2002*). Computer Forensics/ Incident Response.* New York: Addison-Wesley.

[6] Marcella, A. J. and Greenfield, R. S. (Ed.). (2002). Cyber Forensics: A field manual for collecting, examining, and preserving evidence of computer crimes. Washington, D.C.: Auerbach Publication.

[7] Dittrich, D. "*The Honeynet Project*." http://staff.washington.edu/dittrich/pnw-honeynet/reading/ .

[8] Ryan, D.Sc., J. J. C. H. and Ryan, J. D., D. J. (2002). "Institutional and Professional Liability in Information Assurance Education." George Washington University web site.

[9] Endicott-Popovsky, B.E. and Frincke, D. (June, 2003). " A Case Study In Rapid Introduction of Computer Security Curricula," *CISSE 7th Colloquiam*. Washington, D.C.

[10] Endicott-Popovsky, B.E. (July, 2003). "Ethics and Teaching Information Assurance," *IEEE Journal of Security and Privacy*, pp.6-8.

[11] Endicott-Popovsky, B.E. and Frincke, D. (December, 2003). " A Case Study In Rapid Introduction of Computer Security Curricula," *Journal of End-User Computing* (spec. ed.). Boise, Idaho. (derivative of [9])

[12] Endicott-Popovsky, B.E. and Frincke, D. (March, 2004). " A Case Study in Rapid Introduction of an Information Assurance Track into a Software Engineering Curriculum," *IEEE Computer Society Press 17th Conference on Software Engineering and Training* . Norfolk, Virginia.