Introduction to Computer Forensics for Non-Majors

Yana Kortsarts
ykortsarts@mail.widener.edu
Computer Science Department

William Harver
weharver@widener.edu
Criminal Justice Department

Widener University
One University Place, Chester, PA 19013, USA

Abstract

In this paper, we present our experience teaching an introductory course in computer forensics for non-majors. The course was taught by an interdisciplinary team of computer science and criminal justice faculty, and was open as a free elective to computer science and information systems students as well. Course curriculum, lecture structure, lab assignments, and hands-on activities are reported and discussed. The paper presents challenges and course results. The proposed approach could be easily adapted to teach an introductory computer forensics course to computer science and information systems majors.

Keywords: computer forensics, pedagogy, introductory computer science and information systems curriculum

1. INTRODUCTION

Computer forensics**,** still a rather new discipline in computer security, focuses on finding digital evidence after a computer security incident has occurred (Computer Forensics, Cybercrime and Steganography Resources website www.forensics.nl).

Computer Forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law (Sammes and Jenkinson, 2000; Pollitt, 1995). Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law. The need for computer forensic services and equipment has emerged from the widespread use of personal computers in both business and the home and the subsequent needs of crime investigators to have access to computer-based information. Computer forensics has a clear interdisciplinary nature. In this paper, we report and discuss our experience and course results teaching an interdisciplinary course, Intro-

duction to Computer Forensics, in Fall 2006. The course was taught by an interdisciplinary team of computer science and criminal justice faculty. The course was designed as a science elective for non-majors and was open as a free elective for computer science (CS) and computer information systems majors (CIS) as well.

2. COURSE DESIGN, GOALS AND CHALLENGES

Computer forensics is a very challenging topic for instructors to teach and for students to learn, but at the same time the topic is very attractive. Recently, many universities and colleges have started to offer courses in computer forensics at different levels and to design computer forensics curricula (Gottschalk, Liu, Dathan, Fitzgerald, Stein, 2005; Carlin, Curl, and Manson, 2005; Desai, Fitzgerald, and Hoanca, 2006; Malinowski, 2004). While there are experiences to learn from, the area is still very young, and designing a computer forensics course takes a lot of effort: the individual features of the department should be taken into account as well as available lab resources and funds, since computer forensics software and hardware can be expensive. Briefly, our department offers an undergraduate program leading to Bachelor of Science degrees in both Computer Information Systems (CIS) and Computer Science (CS). Our department also offers several courses for non-majors and some of these courses are open for majors as free electives. The department constantly updates the existing list of elective courses to stay current in the field and the idea to develop a course in computer forensics was well accepted, but the decision was made first to design an Introduction to Computer Forensics course that primarily would target non-majors and would be open as a free elective to CS and CIS majors. This was done with the idea of fulfilling the departments' long-term plans to develop an upper level technical elective course for majors. The rationale behind this decision was to design a course for non-majors that would not focus on programming, but at the same time would cover computer science and information systems topics that are attractive for non-majors. The goal was to design the course that would bring together undergraduate students from different majors and provide an opportunity for interdisciplinary collaboration in the in-class laboratory assignments and team projects. Mainly, we targeted the course to criminal justice students. We expected that Computer Science and Computer Information Systems students would be more familiar with computers and networks than the Criminal Justice students but less familiar with the legal aspects, and vice versa. Part of the course experience included the blending of such student expertise in the formation of teams.

With all this in mind, the Introduction to Computer Forensics course was designed and offered for the first time in Fall 2006 with enrollment of 14 students, where 9 of the students were non-majors and 5 students were majors. No prerequisites were required for the course. The course was taught by computer science and criminal justice faculty. The course met in the lecture room and in the lab, 3 hours weekly. The lab was equipped with dual bootable PC's that run Windows and Linux OS, and most of the software that we used in the course was free or open source software. Free trial periods for several commercial packages were used for the course, as well.

It is a very challenging task to teach an Introduction to Computer Forensics course for non-majors. Traditionally, this course is an upper level technical elective course in the computer science (CS) and information systems (IS) curriculum and students who are taking this course have all the required knowledge in computer and network security, cryptology, and operating systems. In our course, however, most of the students were non-majors and these students had never been exposed to advanced computer science and information systems topics before. Second, the students who took this course were coming from diverse disciplines some with good technical and mathematical background and some without. Also, in our research, we experienced difficulties finding a comprehensive, pedagogically sound textbook on computer forensics that could be used to teach this subject for non-majors.

3. COURSE CURRICULUM

The course started with the introductory lecture which provided several definitions of the term "computer forensics" to give students an idea of what this course was about. We

also explained the structure of the course, the tentative list of topics that would be covered, and the level of the technical content, to make sure that CS and CIS students would have right expectations from the course. We also emphasized the interdisciplinary nature of the topic and of the course, as well as the global technical nature of the topic, which means that computer forensics requires knowledge in computer science and information systems as a whole; this justified the structure of the course which compressed of different topics that were all connected under umbrella of applications of these topics in the computer forensics field.

The first two weeks of the course were devoted to the Introduction to Criminal Justice and were taught by the criminal justice faculty. Students learned about the criminal justice system components, structure and conduct of investigations, and collection of evidence. Students got familiar with various laws and regulations dealing with computer forensic analysis. An exam culminated this part of the course to assess students' knowledge. The rest of the course was taught by computer science faculty, even though certain topics were related to criminal justice. The list of the topics, in the order they were taught, with explanation about the specific activities that accompanied the topic and ideas for reading and software resources, is given below.

a. What is computer? What is information? Introduction to History of Computing.

This topic provided a brief introduction the to history of computing (Computing History web resources: www.ComputerHistory.org, www.CompHist.org,www.ieee.org/museum), concepts of computer hardware, software, computer programs and operation systems; binary, octal and hexadecimal number systems; and concept of data storage in the computer memory. This material was mostly familiar to CS and CIS students and we decided that these topics would be taught by majors, which would allow active participation in the teaching process and for the non-majors to learn material from their peers.

b. Introduction to Computer Ethics.

This topic was mostly new for all students and provided an introduction to ethics in information technology, professional codes of ethics, discussion of privacy issues and intellectual property, introduction to computer and internet crime, types of malicious software, and security incidents. All topics were taught with active student's participation. We asked students to form interdisciplinary teams and to prepare short presentations (5-10 minutes) about different malicious software, and computer crimes that were reported and ended in the court. The presentations were conducted at the end of each lecture time.

c. Encryption and Forensics. Part I

In this part of the course, we provided students with a brief history of cryptography (History of cryptography web resources by Ekert, Alves, Gopinathan), definitions of cryptology concepts, simple symmetric (private key) ciphers and we explained the connection between computer forensics and cryptology. The topic of public key cryptology was explained later in the course. The topic of cryptology is not an easy topic to comprehend for non-majors, since the topic requires a solid mathematical background. In order to make this part of the course successful, the class was divided into small interdisciplinary teams and all concepts were practiced within the team with the help of majors. To master the symmetric ciphers, students played "fastest team to encrypt/decrypt the message" games. This was the last topic that was taught in the lecture room. The rest of the course was conducted in the computer lab.

d. Steganography

In this part of the course, students first learned the definition of steganography – the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion (Provos and Honeyman, 2003). The relation of steganography to computer forensics was also explored.

During most of the time devoted to this topic, students worked with the steganography software Invisible Secrets 4 (Invisible Secrets: http://www.invisiblesecrets.com/]) (the company provides 15 days free trial period that was used in the course). The lab assignments included simple hide/unhide tasks with encryption and decryption of the password. Students also worked on team projects where students were required to create a document with multiple hidden files, and for each hidden file the students were required to provide a hint to decrypt or uncover the password, using the encryption techniques learned so far, or/and using the knowledge of the binary/octal/hexadecimal

number systems, or/and using the definitions of the computer science concepts that students learned at the beginning of the course. This was done in an effort to connect all topics under one umbrella. This project was done over two lab meetings; in the first meeting, two teams were created and each team designed the multiple-step hidden assignment for the other team. The number of steps was limited to 10. The second lab was used to unhide the original document. We also timed the teams to find a winner. In this part of the course, students were required to read and participated in the class discussion of articles by Provos and Honeyman (2003) and Wang and Wang (2004). Some technical issues in the articles were not completely clear to non-majors and were explained by majors, which provided an opportunity for students to learn from peers and to be actively involved in the teaching process. Students also were referred to the paper An Overview of Steganography for the Computer Forensics Examiner by Kessler (2004) which we discussed in class as well.

e. Computer examination process.

In this part, we discussed the issues of searching and seizing computers for obtaining computer-based evidence and the presentation of the evidence in the court. Students were referred to the resources published on the United States Department of Justice, Computer Crime & Intellectual Property Section webpage, and the paper "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" was discussed in detail. The hands-on activities for this session included practice in writing computer forensics reports. This topic was closely related to the next topic, MD5 algorithm, fingerprints and hashes. Combining these two topics allowed for the creation of more hands-on lab activities.

f. MD5 algorithm, fingerprints and hashes. Application to Computer Forensics.

This part of the course covered the applications of the MD5 algorithm in computer forensics. Students worked with Windows OS and open source software MD5sums 1.2 from pc-tools.net. The explanation of the technical issues, such as the MD5 algorithm, the concept of hash function, and the concept of hash values were partially done by majors, and provided opportunities for active learning. This topic was closely related to the previous one and combining these two topics allowed us to create hands-on lab activities that were done in interdisciplinary teams. Students learned to calculate the MD5sums for files and directories and were required to be capable of answering the question whether the content of the file was altered or not. Also, students explored different manipulations of the files and directories affecting the MD5sums values. In some cases, students worked according to proposed scenarios and used MD5sums for evidence validation.

g. *Introduction to Linux OS and Introduction to FTimes system baselining and evidence collection tool.*

This probably was the most difficult part of the course for all students. None of the non-majors had experience working with Linux prior the course, and the FTImes tool (http://ftimes.sourceforge.net/FTimes/) was a completely new tool for all students. All activities for this part of the course were done in teams. We created five teams that included one major student and one or two non-major students. First, non-majors learned how to use Linux OS at an introductory level. Students learned basic file manipulation operations, EMACS editor, how to read manual pages, and how to use built-in MD5sum command. A few labs were devoted to help gain initial experience working with Linux. The next step was to learn FTimes tool at the introductory level. Students were required to read the paper "System Baselining – Forensics Perspective", by Monroe and Bailey (2006) and to do the simplified version of the first lab exercise Ftimes Mechanics from the Bootcamp session of the FTimes webpage (FTimes bootcamp exercises). This topic provides a lot of opportunities to introduce students to real forensics analysis, but at the same time this is already a very challenging tool to learn for non-major.

h. Encryption and Forensics. Part II: Introduction to Public Key Cryptology and Pretty Good Privacy (PGP) encryption tool.

This topic is a challenging topic as well, and requires a solid mathematical background. All in-class activities were done in the interdisciplinary teams. We introduced the concept of private and public key, explained the difference between symmetric and public key cryptology, discussed the applications of public key cryptology for computer forensics purposes, and explained the RSA algorithm.

The hands-on activities for this part of the topic included encryption and decryption using RSA, finding and presenting information about additional public key cryptology algorithms, and finding information and discussing the weaknesses of the public key cryptology. The second part of this topic was devoted to learning how to use PGP encryption tool (http://www.pgp.com/). We used a 30 day free trial period.

i. Cyber Terrorism

This was the last topic covered in the course. In this part of the course, students were required to read and participate in the in-class discussion of two papers from ACM Journal of Communication Volume 47, Issue 3, March 2004 (John, 2004; Popp, Armour, Senator and Numrych 2004). Students also were referred to the National Cyber Security Division website (www.dhs.gov/xabout/structure/editorial_0839.shtm]. This topic also provided an opportunity to summarize the material that was covered in the course and to finalize the course.

7. COURSE RESULTS

To assess the students' experience, we designed a short post-survey that included only open-ended questions and asked students to provide their feedback. We asked students to list their expectations from the course as well as to answer the question of whether the course met their expectations or not. It was interesting to see that most of the students didn't have a clear idea of what this course would be about; some students mentioned that they were not familiar with the term "computer forensics" at all before they actually started the course. But most of the students, about 95%, answered that the course met their expectation after the definition of the concept was provided in the first lecture. No student dropped the course. We asked students to list their three most favorite activities and three least favorite activities. The answers didn't surprise us. Some students, about 50%, probably most of them non-majors, unfortunately, mentioned LINUX as the least favorite topic. As most favorite topics students mentioned steganography, MD5, cryptology and binary system. Some students also mentioned the criminal justice part as their favorite topic, but at the same time some students wrote that they took Introduction to Criminal Justice course prior to our course and criminal justice topic was not their favorite because of this reason. We asked students to list their most favorite and least favorite activities, and for this part we also didn't receive any surprising answers. All students mentioned that working in the lab was their favorite part, and the beginning of the course that was conducted in the lecture room, while provided opportunities for active participation, was the least favorite. Students mentioned that lab assignments helped to gain better understanding of the material. A separate question was devoted to the team work. We asked students to comment on the contribution of the team work to learning course material. We were pleased to receive positive answers from all students, where they mentioned that they liked team work, and that the team work helped them to better understand the course material, and provided an opportunity to share information. Also, students mentioned that team work provided a possibility to practice how to explain material to other students. Students also mentioned that it was beneficial to learn from the instructor and from the peers at the same time. We also asked students' opinion about the best percentage division of the criminal justice and computer science topics. On average, students proposed that 25% should be devoted to criminal justice topics and 75% to computer science. Some students suggested that the topics should be blended together throughout the course. On our request to provide recommendations to improve the course, students proposed to teach the course in the lab for the entire semester, and to teach more in depth some of the technical topics (probably, this request came from majors). We also got requests for a separate course for majors, and some suggestions about the prerequisites for the course. Some students also mentioned that a guest speaker from the computer forensic field would benefit the course. To summarize, students showed satisfaction from the course. To assess the students' learning, several quizzes, tests and graded lab assignments were conducted through the course and the results showed that students successfully learned the challenging topic of computer forensics on the introductory level and showed that it is possible to teach introduction to computer forensics for non-majors by taking into account very careful consideration of the topics, preparing de-

tailed and simplified explanations of the advanced computer science and information systems topics, and creating team projects and hands-on activities. Also, it was a very beneficial experience for the instructors and for the students to be involved in team teaching. Students had an opportunity to see how the computer forensics problem is approached from different perspective- computer science and criminal justice- and instructors had an opportunity to learn from each other and to create a productive collaboration while teaching the course.

8. LESSONS LEARNED AND FUTURE PLANS

Based on the students' post-survey results we could state that the first iteration of the Introduction to Computer Forensics course in Fall 2006 was successful. We are planning to offer this course again in Fall 2007. In its main features, the course will remain the same. But based on our first experience and taking into account some of the students' suggestions, several changes will be introduced. The entire course will be held in the computer lab and will include modification of the lecture style to use in-class activities as a way to build students' understanding of the course material: the lectures will be shortened and the concentration will be on the hands-on activities. This teaching approach will try to generate the students' capabilities of learning through a research-based process. We will try to blend the criminal justice topics with computer science topics throughout the course. We will continue our efforts to bring a guest speaker. We contacted the Regional Computer Forensics Laboratory Guest Speaker program, and we hope that this year we will be more successful in this process. Since some topics were not directly connected to the computer forensics topic and had to be taught since non-majors didn't have any prior computer science background, we will work on making better connections among all topics covered in the course and computer forensics by designing assignments that have a computer forensics nature. Also, we will try to redesign the LINUX topic to make it more attractive to non-majors by designing computer forensics scenarios that require knowledge and understanding of certain LINUX features. Students would have an opportunity to learn LINUX while solving computer forensics mysteries. We also decided to purchase the Invisible Secret steganography tool, since all students mentioned this part of the course as their favorite topic and activity. We will continue to emphasize the interdisciplinary team work through the entire course, and will continue designing more team competition activities to make the course a fun and enjoyable experience. Finally, a special word should be said about the textbook. Based on our research, as we mentioned before, no comprehensive, pedagogically sound textbook on computer forensics that could be used to teach this subject for non-majors was found. Even for majors, the task of choosing the good textbook could be very complicated. For the first iteration of the course we used several textbooks (see References session for the complete list of all textbooks that were used for the course). For the next iterations of the course, we are planning to design our own custom text for the course using several textbooks and our own lecture notes with help of a professional publisher.

While a first iteration of the course was successful all the above-mentioned ideas would definitely help to improve the course, and we are looking forward to the Fall 2007 semester.

9. REFERENCES

Barr, Thomas H (2002) Invitation to Cryptology, Prentice Hall

Carlin, A, Curl, S.S and Manson, D. (2005) "To Catch a Thief: Computer Forensics in the Classroom", In The Proceedings of ISECON 2005, v 22 (Columbus OH): §3574. ISSN: 1542-7382

Carrier, Brian (2005), File System Forensic Analysis, Addison – Wesley

Computer Crime & Intellectual Property Section, United States Department of Justice www.usdoj.gov/criminal/cybercrime

Computer Forensics, Cybercrime and Steganography Resources website (2007) http://www.forensics.nl/

Computing History web resources: www.ComputerHistory.org, www.CompHist.org, www.ieee.org/museum

Desai, A M, Fitzgerald, D and Hoanca, B

(2006) "Offering a Digital Forensics Course in Anchorage", In The Proceedings of ISECON 2006, v 23 (Dallas TX): §5114. ISSN: 1542-7382

Ekert, Artur, Alves, Carolina Moura and Gopinathan, Ajay (2007) The history of cryptography web resources cam.qubit.org/articles/crypto/intro.php

Farmer, Dan and Venema, Wietse (2004) Forensic Discovery, Addison – Wesley

FTimes Project page http://ftimes.sourceforge.net/FTimes/

FTimes bootcamp exercises, http://ftimes.sourceforge.net/FTimes/Bootcamp/Exercises/index.shtml

Gottschalk, Larry, Liu, Jigang, Dathan, Brahma, Fitzgerald, Sue and Stein, Michael (2005) "Computer forensics programs in higher education: a preliminary study", Proceedings of the 36th SIGCSE technical symposium on Computer science education SIGCSE' 05, Volume 37, Issue 1

Invisible Secrets software website (2007) http://www.invisiblesecrets.com/

Jones, Keith J., Bejtlich, Richard and Rose, Curtis W. (2006), Real Digital Forensics, Computer Security and Incident Response, Addison – Wesley

Kessler, Gary C. (2004) "An Overview of Steganography for the Computer Forensics Examiner", Forensic Science Communications, July 2004, Volume 6, Number 3.

Kruse II, Warren G. and Heiser, Jay G. (2005) Computer Forensics, Incident Response Essentials, Addison-Wesley

Malinowski, C. (2004) "Information Systems Forensics: A Practitioner's Approach, In The Proceedings of ISECON 2004, v 21 (Newport): §3232. ISSN: 1542-7382

Mandia, Kevin, Prosise, Chris and Pepe, Matt (2003) Incident Response and Computer Forensics McGraw-Hill

MD5sums 1.2. for Windows http://www.pc-tools.net/win32/md5sums/

Monroe, Klayton and Bailey, Dave (2006) "System Baselining – Forensics Perspective" http://ftimes.sourceforge.net/Files/Papers/baselining.pdf

National Cyber Security Division www.dhs.gov/xabout/structure/editorial_0839.shtm

PGP website http://www.pgp.com/

Pollitt, Mark (1995) "Computer Forensics: An Approach to Evidence in Cyberspace", National Information Systems Security Conference www.digitalevidencepro.com/Resources/Approach.pdf

Popp, Robert, Armour, Thomas, Senator, Ted and Numrych, Kristen (2004) "Countering terrorism through information technology" Communications of the ACM, Volume 47 , Issue 3 (March 2004)

Provos, Niels and Honeyman, Peter (2003) "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy Magazine

Regional Computer Forensics Laboratory Speaker Bureau, http://www.rcfl.gov/index.cfm?fuseAction=Public.top3

Reynolds, George (2007) Ethics in Information Technology, Second Edition, Thomson Course Technology

Sammes, Tony and Jenkinson, Brian (2000) Forensic Computing, A Practitioner's Springer

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf#search=%22seizing%20comp uters%22

Vacca, John R. and River, Charles (2002), Computer Forensics, Computer Crime Scene Investigation, Media Inc

Wang, Huaiqing and Wang, Shuozhong (2004) "Cyber Warfare: Steganography vs. Steganalysis Communication of the ACM, October 2004, Vol. 47, No. 10

Yen, John, (2004) "Emerging Technologies for Homeland Security", Communications of the ACM, Volume 47, Issue 3 (March 2004)