To Catch a Thief: Computer Forensics in the Classroom

Anna Carlin
acarlin@csupomona.edu

Steven S. Curl
scurl@csupomona.edu

Daniel Manson
dmanson@csupomona.edu
Computer Information Systems Department
California State Polytechnic University
Pomona, CA 91768, USA

Abstract

The subject of computer forensics can be challenging and intriguing for students. Teaching this course involves both the technical and legal aspects of investigative procedures as applied to digital evidence. For the instructor, it can involve challenges not found in other areas of information systems. This paper discusses the triumphs and pitfalls of including computer forensics as part of an undergraduate information assurance curriculum.

Keywords: curriculum, forensics, security

1. OVERVIEW

Computer forensics is the collection and study of computerized evidence as part of a larger investigation. The purpose can be either civil or criminal in nature. Teaching a computer forensics course can be quite an endeavor and can involve challenges not found in other areas of information systems. Furthermore, this course was taught as part of a College of Business Administration curriculum. In addition to relevant information technology, topics covered include the law, seizure of evidence, extraction of evidence, chain of custody, and presentation of relevant findings in court. The course involves specialized hardware and software and puts students on the trail of an imaginary thief. Studies have shown that conducting computer forensics classes in a well-equipped lab helps to ensure a successful and effective learning experience (Logan, 2005 and Whitman, 2004). Labs allow access to specialized tools and provide a hands-on learning experience that textbooks and lectures could never provide.

2. COURSE STRUCTURE

The course was taught over a ten week quarter and divided into three parts – each with a corresponding project. The students were primarily undergraduates who were placed into groups and assigned to a case. The first part of the course involved the creation of evidence for a particular crime. The second part involved the seizing of digital evidence, maintaining a chain of custody, and analysis of the evidence created by a different group. The last part involved presentation of findings. The crime did not need to be a computer crime but did have to involve evidence stored on digital media. One example of a possible crime would be identity theft.

Creation of Evidence: For part one, each student had to identify a crime and create supporting evidence of criminal activity. Each team was given a 15 GB hard drive with Windows XP Professional and Microsoft Office installed. To facilitate this part of the course, external USB drive enclosures were purchased and attached to existing, surplus hard drives. The hard drives were connected to the lab computers and students created a second partition. Excel spreadsheets, Word documents, email messages, and images were stored on the hard drive. Steganography, password protection, and encryption were used to hide evidence. Some evidence was placed on the second partition and that partition subsequently deleted. The deliverable from this phase was the hard drive, an evidence list, and a case summary. The case summary detailed the laws broken and the events leading up to the seizure of evidence, including the persons (or suspects) involved and exactly what media was seized.

The process was also followed, to a lesser degree, for a secondary crime on the same hard drive. The purpose for the secondary crime was to emphasize the Fourth Amendment protection against unreasonable searches and to understand that the search warrant did not encompass the secondary crime. A new warrant would have to be issued to analyze the secondary evidence.

The Search for Clues: Hard drives were collected for assignment to a different team. All evidence was secured in evidence bags along with the case summary. The bags were assigned code numbers and sealed. The team analyzing the evidence did not know which team created the evidence and was prohibited from discussing their project with other teams. Each team was assigned an evidence locker to protect the evidence and maintain a chain of custody.

In order to ensure that the evidence did not become tainted, each team created an image of the original hard drive and a backup image for contingency purposes. All original evidence was then secured in evidence lockers. Hash totals (or numbers) were generated on the original evidence and the image to ensure that the image file was an exact duplicate of the original. Matching hash totals are important so that the evidence can be presented in court. Analysis was always performed on the duplicate drive.

Several tools were used to analyze the evidence, such as EnCase, Access Data Forensic Imaging, Forensic Toolkit, and Password Recovery. The Password Recovery software was sensitive since it could provide logon passwords as well as passwords for files. It took sometimes two to three days for a password to be recovered. Invisible Secrets and Stegdetect were used on images to detect steganography. The Access Data software was also used to unencrypt files. EnCase worked best when viewing images. The team could view thumbnails of the images with several thumbnails viewed at once. Considering that Microsoft Office alone has over one thousand images, this saved teams time and energy.

Students needed guidance on the process of sifting through files on a hard drive and identifying evidence. Most evidence was in pieces and appeared at different locations. Emails could contain passwords for other files. At times, the primary crime was too similar to the secondary crime and caused some confusion.

Students were required to document their process, list tools used, identify any evidence recovered and its relationship to the crime. A report was prepared summarizing this information. Once the report was submitted, the instructor gave the team the evidence inventory list from the original team.

Presentation of Findings: All teams were required to present their findings to the class. As a part of this presentation, students also discussed what evidence was overlooked based on the listing provided by the instructor. Each team then discussed what could have been done better to recover missed evidence.

Instructors who have taught this type of class noted that students experience difficulty presenting the evidence in a coherent, logical manner (Harrison, 2005). The teams had to show how all the artifacts either supported or denied that a crime had been committed. Again this requires the student teams to determine what elements of the crime should be present to support the charges against the suspect or suspects.

3. TRIUMPHS AND PITFALLS

The class was a good learning experience and the students discovered the majority of the evidence created for them. Their final presentations indicated they had developed a solid understanding of the principles of computer forensics and the criminal investigative procedures related to digital evidence. To a lesser extent, the students also learned the meaning of good detective work.

The class experienced one or two false starts at the beginning of the search for clues. When imaging the evidence drive, it was possible to exceed the capacity of the destination drive. The seized drive was 15 GB and the image drive was only 8 GB. If the destination hard drive for the image is not large enough, then the software terminates and all work is lost. Imaging a 15 GB hard drive took approximately 55 minutes. The students needed to free up disk space and then recreate the image.

Once the image was created and a hash total generated, a different software package was used to create a hash total that should have matched the first hash total. Some students chose to use a software product that was an evaluation version and did not perform the hash total calculation properly. The hash total verification took about 20 minutes to complete. The teams had to use a different software package with full capabilities.

The forensics software used to analyze the evidence required a dongle, or electronic key, to access its full capability. A dongle resembles a USB flash drive and works to authorize the use of the software. To operate correctly, the dongle needs to be inserted into the USB drive the entire time the forensics software is running. In one instance, when trying to obtain a password, students inadvertently removed the dongle and all work performed to crack the password was lost.

While the forensics software can be installed on many computers, the dongle is the key that allows use of the application. Each team was given a dongle whenever it was necessary to use the forensics software. Since the images were stored on hard drives in the lab, this required time outside of class for working on the group project. Over five weeks of study, four to six hours were needed each week to complete the project.

4. INSTRUCTOR PREPARATION

Specific instructor skills are needed to teach digital forensics. These skills include practical aspects of the software, hands-on conduct of an investigation, and theoretical, procedural, and legal material that the students should learn in the class. All faculty members who have taught Computer Forensics at our school have taken digital forensics training courses, and have been involved with the Digital Forensics Educators Working Group.

5. CONCLUSION

The computer forensics field will continue to grow since computers are being used to commit numerous crimes. Students in our program will be experienced in the laws surrounding internal and external investigations, acquiring digital media, analyzing the digital media, and presenting their findings.

Conducting an exhaustive search for clues is time-consuming. A careful and deliberate analysis cannot be done in a timely manner without the use of appropriate software tools. This class used tools from Guidance Software's EnCase and AccessData's FTK, among others. Students were exposed to a variety of software tools that verified their findings. Verification solidifies the authenticity of evidence presented in court.

The analysis itself is of little use without a well written report that presents the evidence in a coherent and logical manner. Reports are relied upon to document what digital evidence was seized and what items were found related to the crime. Expert witnesses will use these reports to familiarize themselves again with the case since it is not unusual for several months or even years go by before the evidence is presented in court.

Our class experienced some success and difficulties. Students had a firm grasp on the principles of computer forensics and the criminal investigation process. The difficulties were more hardware and software related issues. Between hard drives full to capacity, trial software with partial functionality, and missing dongles, we experienced several false starts that required more lab time spent repeating analysis work.

Checklists and software tools should not be solely relied on when conducting an investigation. Each piece of evidence recovered requires evaluation by an experienced examiner. Consequently the need for experienced examiners is growing. Programs like ours will expose students to the computer forensics field and help fill the growing industry need for knowledgeable computer forensic examiners.

6. FUTURE IMPROVEMENTS

While the course was well received by the students, there is always room for improvement. For this session, the search warrants were provided by the instructor. To better teach the meaning of the Fourth Amendment, we would have students write their own search warrants for the primary crime. We would also put more emphasis on the legal significance and handling of evidence related to secondary crimes. The tools worked well from a technical perspective but do nothing to determine whether or not any evidence discovered is covered by the search warrant. The team performing the analysis needs to exercise judgment and prudence when interpreting evidence of crimes and should then go back and write appropriate warrants whenever evidence is discovered for other crimes. These crimes would not fall under the authority of the search warrant and that a new warrant is needed for that evidence to be admissible in court.

We also believe that checklists for the seizing, analyzing, and reporting of evidence would be helpful for those not experienced in computer forensics. Our hesitation in using checklists is that the students would blindly follow the steps listed and not consider other avenues of investigative thought. When analyzing evidence, one clue can lead the investigator in a different direction. If the checklist does not include that additional analysis, the evidence may be overlooked.

The evidence seized should include more than one type of media. The student teams were provided USB hard drives but it would be helpful to include a flash or floppy drive, cell phones, and a PDA. In addition, photographs from the crime scene would add a creative touch to the exercise.

Some evidence created by the students was too good. For example, one team created fake drivers' licenses for an identity theft case. Photoshop was used and the resulting licenses were very convincing. It was only apparent that the images were faked due to the fact that fictitious names and supporting data were used along with faculty photos. In the future, we would require evidence banners to be placed on any images related to fictitious crimes.

A forensics software usage policy should be required for the class. Since the software involved in the course can be used for recovering passwords, a usage policy restricting use to class projects seems appropriate. The policy should also describe consequences for failure to comply with this rule.

7. ACKNOWLEDGEMENTS

We would like to acknowledge the Digital Forensics Educators Working Group. They provide a forum for educators to discuss changes in the field and ways to share program information and digital forensics curriculum.

We would also like to thank Warren Harrison, Professor of Computer Science at Portland State University and a Police Reserve Specialist in Digital Forensics with the Hillsboro (Oregon) Police Department. Sharing his experience in teaching computer forensics was instrumental to how we structured our group project.

8. REFERENCES

Harrison, Warren (2005) "Forensics Course Project Development", Digital Forensic Working Group, University of Central Florida, February 12-13.

Logan, Patricia and Allen Clarkson (2005) "Teaching Students to Hack: Curriculum

Issues in Information Security", ACM Special Interest Group on Computer Science Education, St. Louis, Missouri, February 23-27.

Soe, Louise, Marcy Wright, and Dan Manson (2004) "Establishing Network Computer Forensics Classes", Annual Conference on Information Systems Security Curriculum Development, Kennesaw State University, October 8.

Whitman, Michael and Herbert Mattord (2004) "An Introduction to Teaching & Developing Information Security Curriculum", Annual Conference on Information Systems Security Curriculum Development, Kennesaw State University, October 8.