

To Catch A Thief II: Computer Forensics in the Classroom

Anna Carlin

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

Steven S. Curl

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

Daniel Manson

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

ABSTRACT

The subject of computer forensics is still new and both challenging and intriguing for students. Cal Poly Pomona has offered this course since September of 2004. The 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 some of the triumphs and pitfalls of including computer forensics as part of an undergraduate information assurance curriculum.

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 may 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, analysis of recovered data, relevance to the crime, 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.

COURSE STRUCTURE

The course was taught over a ten week quarter. The students were primarily undergraduates who were placed into groups and assigned to a case. The course was divided into three parts – each with a corresponding project. The first part 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 two partitions, each with Windows XP Professional Service Pack 2 and

Microsoft Office installed. To facilitate this part of the course, external USB drive enclosures were purchased and attached to existing, surplus hard drives. A 3.5" floppy disk was also provided to store evidence. Excel spreadsheets, temporary internet files, cookies, Word documents, email messages, and images were stored on the hard drive. Windows delete, shredder programs, 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, search warrant, suspect(s) biographical information, crime scene photos, 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 suspect(s) biographical information was important to generate possible passwords to open potential evidence.

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 Guidance Software EnCase Enterprise, AccessData Ultimate Toolkit (UTK) which includes Forensic Toolkit (FTK) Imager, FTK, Registry Viewer, and Password Recovery Toolkit (PRTK). The PRTK software was sensitive since it could provide logon passwords as well as passwords for files. The suspect(s) biographical information was entered into PRTK to create password combinations. If teams used personal suspect(s) information, the software would return the password quickly. If personal information was not used, it took sometimes two to three days for a password to be recovered.

Invisible Secrets and Stegdetect were used on images to detect steganography. Students enjoyed creating steganography making it easy to detect but difficult to separate the two items. For example, if a student saw the same shamrock image on the hard drive, the first thing they would do is compare the file sizes. More often than not, one image was much larger than the others indicating that it was steganography. Experience has shown that the two items that were combined (or one hidden) within the document resided on the drive individually. But due to the large number of files, it is difficult to determine which two items created the one steganography image.

The AccessData and Guidance software were also used to unencrypt files. EnCase worked best when viewing images since the team could view several thumbnails of the images at once. FTK has a feature called Known File Filters (KFF) which contains a dictionary of hash values for harmless files (such as Microsoft Word templates) and illegal files such as pornography. Considering that Microsoft Office alone has over one thousand images, this saved the teams' time and energy.

Students needed guidance on the process of sifting through files on a digital device 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 discussed the evidence found, tools used in the analysis process, time spent on Parts I and II, and the evidence overlooked based on the listing provided by the instructor. Each team then discussed what could have been done better to recover missed evidence. See Figure 1 below for total hours spent on the group project and Figure 2 for Parts I and II. Figure 3 shows the average hours spent per person and per team on the group project. The average per person is necessary because the team size was not always equal.

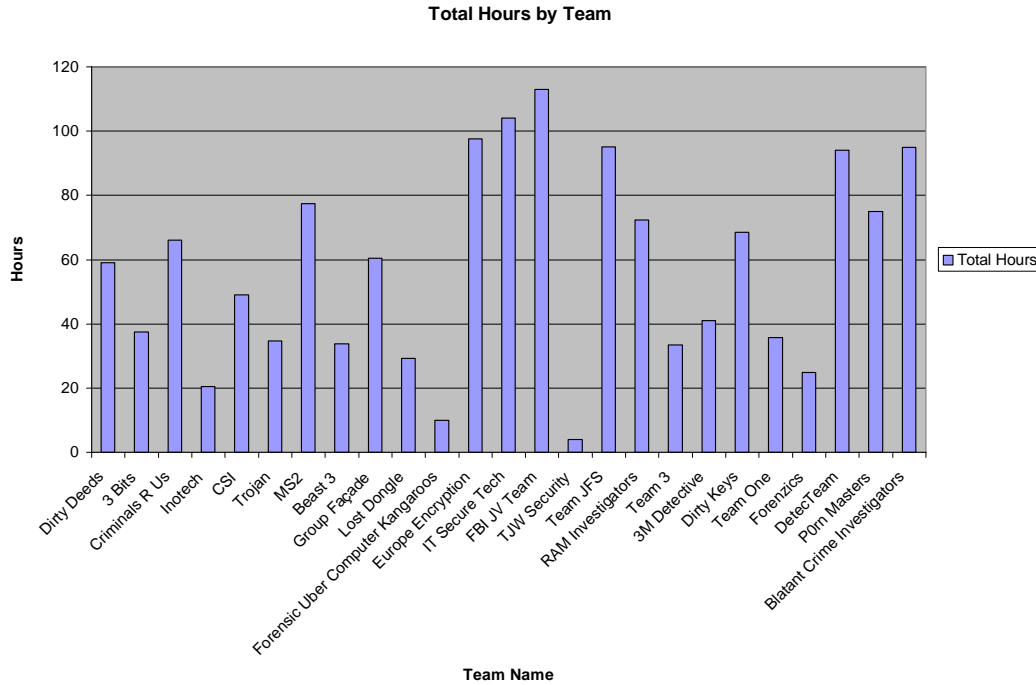


Figure 1: Total Hours Spent on the Group Project From Fall 2005 to Spring 2006.

As shown in Figure 1, the teams averaged approximately 57 hours on the group project. Times ranged from as little as 4 hours to as much as 113 hours. The duration for Part I was approximately 19 calendar days and 28 calendar days for Part II. The final presentation had only two calendar days lapsed.

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.

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

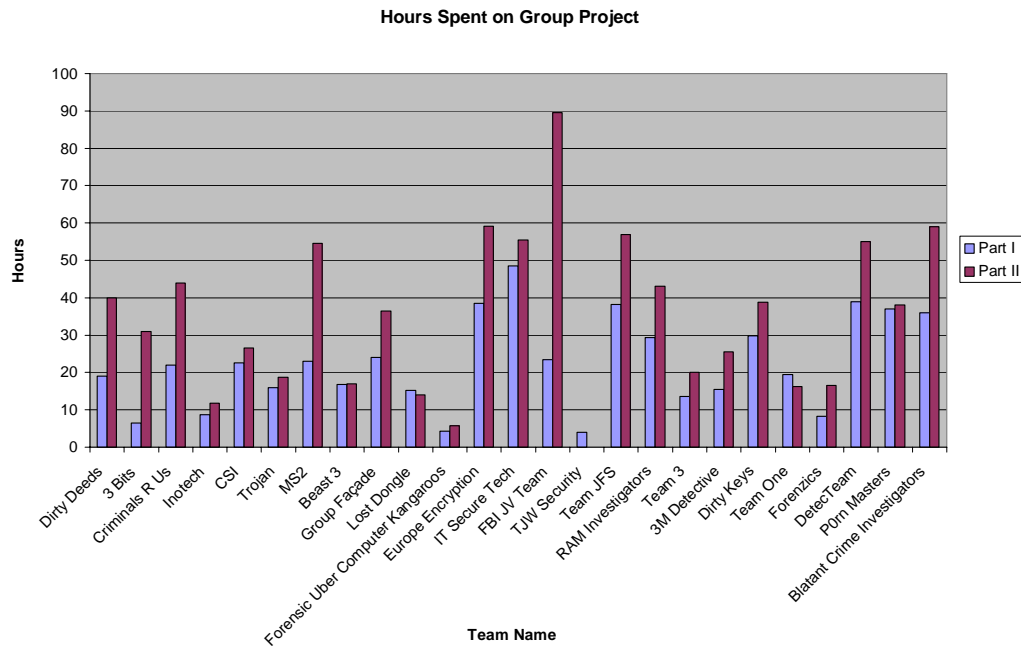


Figure 2: Total Hours Spent on Part I and Part II Group Project from Fall 2005 to Spring 2006.

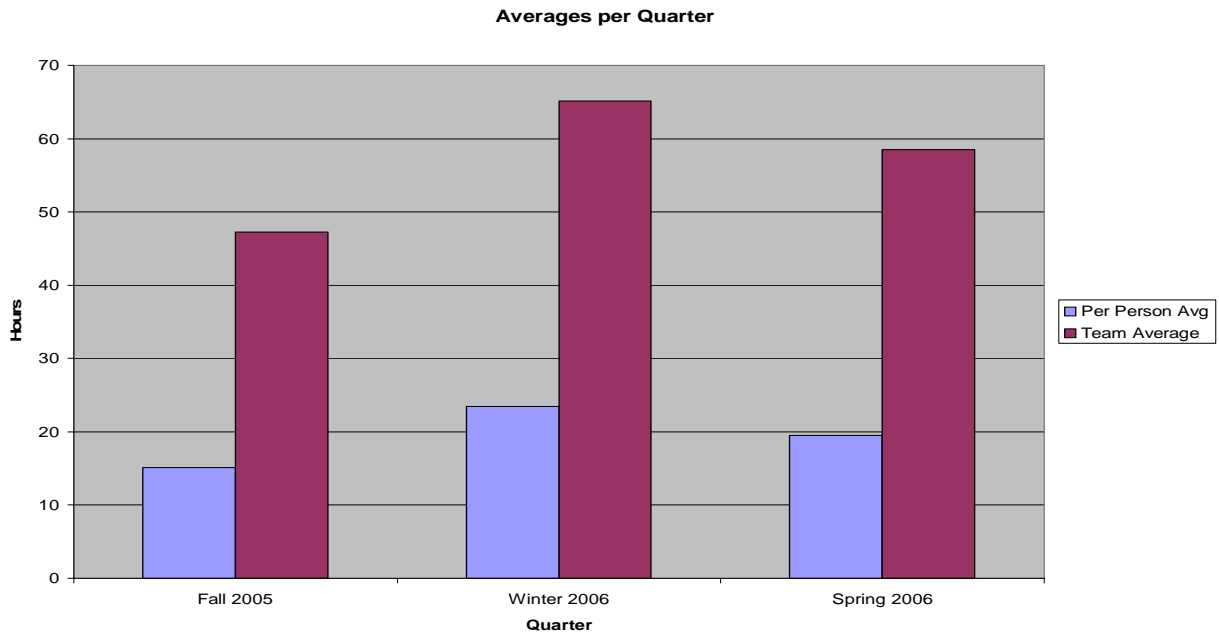


Figure 3: Group Project Average Hours Spent Per Person and Per Team from Fall 2005 to Spring 2006.

and all work is lost. Imaging a 15 GB hard drive required 23 GB on the target image drive and 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.

On May 6, 2006 Cal Poly Pomona hosted the 10th annual Management Information Systems Student Association (MISSA) Information Technology Competition (ITC). Computer Forensics was introduced as a new competition event. Each event models a business problem that must be analyzed, developed, and presented by student teams. All business cases are written by IT professionals. Four student teams from the Cal Poly Pomona computer forensics classes competed with three student teams from Mount San Antonio College. Cal Poly Pomona student teams took first and second place prizes of \$1,000 and \$500, with a student team from Mount San Antonio College taking third prize of \$250.

The case was written by a computer forensics investigator with the Orange County District Attorney's Office, and judged by the investigator and two other industry professionals. Judges were impressed with the winning cases, with one judge asking to interview the entire team for their forensics practice. As the case description below indicates, students were asked to examine and report on a digital forensics crime, similar to the course experience.

ITC 2006: Digital Forensics Case

A large semiconductor manufacturing firm has recently been receiving complaints from internal clients, clients, and vendors regarding reduced throughput and access times to a recently installed web server. Each of these individuals has local access and a World Wide Web access to the secure server. The manufacturer's IT department therefore looks into the problem and notices that a large portion of the server's disk space is being consumed! This is deemed extremely suspicious since the server has plenty of disk space according to the IT department. The IT department suspects that the server has been compromised after finding some suspicious files and immediately reports to upper management.

Since this is a publicly traded firm that abides by all Sarbanes Oxley controls and other protocols, the organization feels that an incident of this nature may have a negative impact on revenues and stock prices if left unattended. Subsequently, your security/digital forensics consulting firm puts forth a request for proposal and wins. Your firm is hired to investigate the incident with a \$5,000 retainer. As a seasoned network security and digital forensics veteran, you realize that the following must be performed immediately:

- Perform forensic analysis on the server image given to you by the IT department
- Create a non-technical report geared toward upper management including all findings
- Create a technical report detailing your forensic process

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.

STUDENT COURSE EVALUATIONS

Our department policy is to conduct an evaluation of teaching performance and effectiveness of the classroom experience. Student opinion is key to improving your teaching performance and the class. The evaluation is conducted by a person other than the faculty member being evaluated and evaluation results are sealed in a closed envelope for delivery to the department office for processing. The results of the evaluation are not provided to the faculty member until after grades for the class have been submitted.

The five questions specific to the class are:

- Question 1 – The instructor encouraged critical thinking in this course
- Question 2 – The instructor helped me understand the concepts covered in the course
- Question 6 – Practical examples were used to help get points across in class
- Question 11 – Class participation was encouraged
- Question 16 – I would recommend this instructor for this course to other students

Question 1 addresses whether the students feel that the course has improved their ability to analyze, assess, and apply the skills learned to the computer forensics process. Figure 4 below shows student evaluations for the last 4 quarters. As evidenced by the chart, the class average for this question is 1.65 compared to the department average of 2.09.

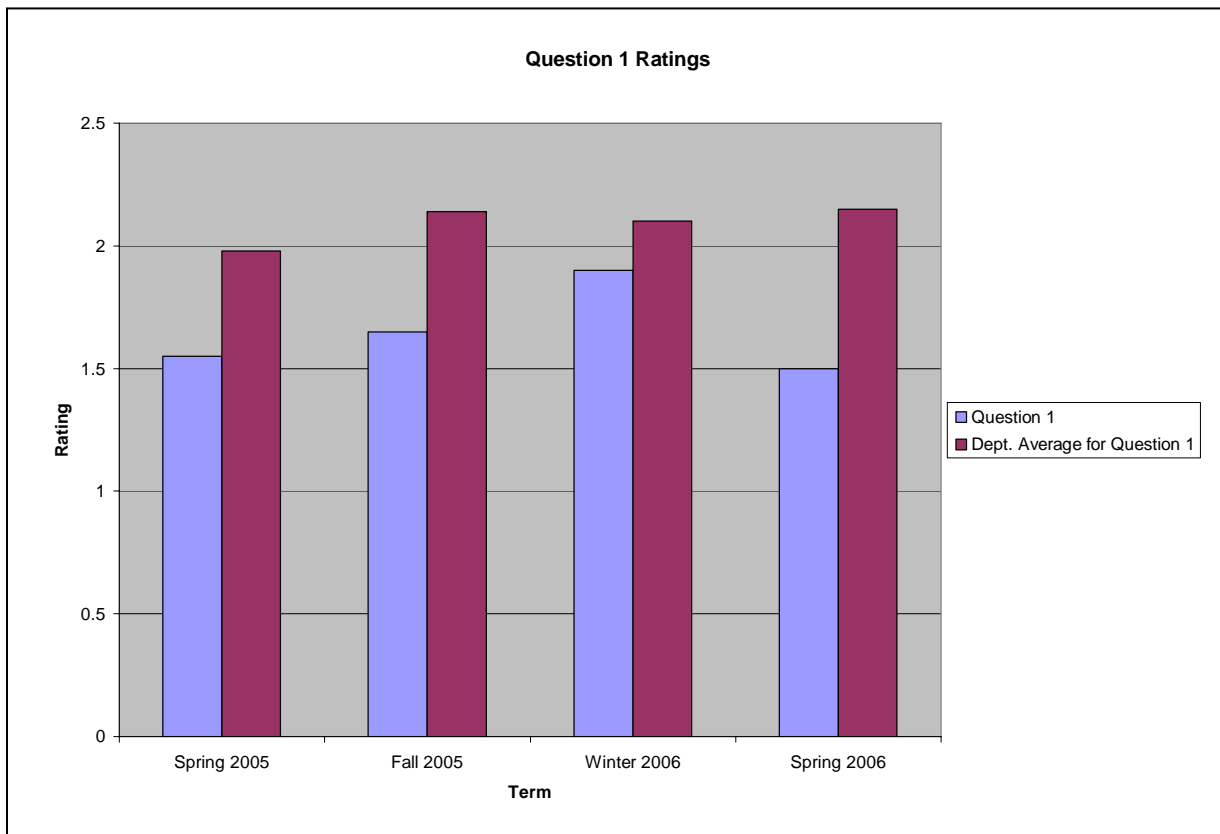


Figure 4: Student Evaluation on Question 1 from Spring 2005 to Spring 2006.
RATING SCALE: 1 for Strongly Agree to 5 for Strongly Disagree

Question 2 addresses whether the instructor helped students understand the concepts covered in the course. Two textbooks were used in the class. Each textbook had a different audience, one was for the person starting in computer forensics and the other for the experienced practitioner. Figure 5 below shows student evaluations for the last 4 quarters. As evidenced by the chart, the class average for this question is 1.73 compared to the department average of 2.29.

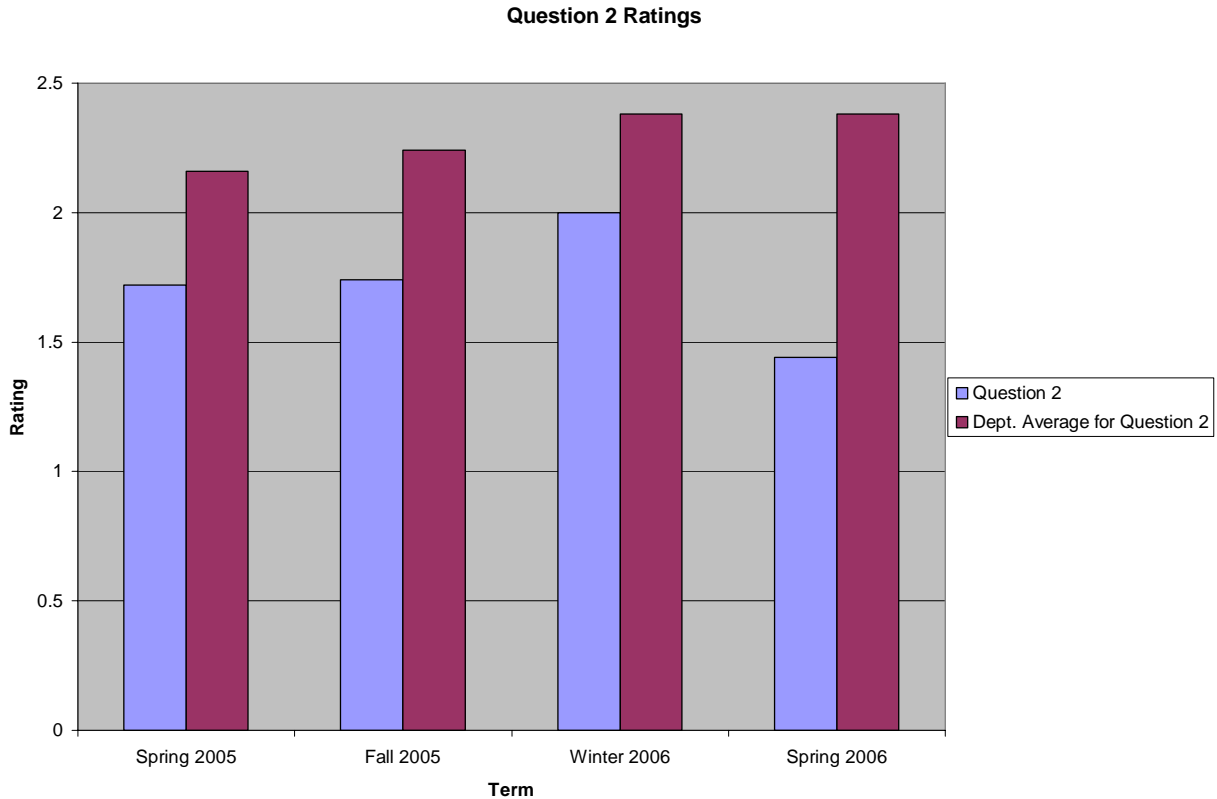


Figure 5: Student Evaluation on Question 6 from Spring 2005 to Spring 2006.
RATING SCALE: 1 for Strongly Agree to 5 for Strongly Disagree

Question 6 addresses whether practical examples were used to help get points across in class. Students’ hands-on labs were developed to help students trace emails, recover passwords, and uncover relevant evidence. Figure 6 below shows student evaluations for the last 4 quarters. As evidenced by the chart, the class average for this question is 1.74 compared to the department average of 2.13.

Question 11 addresses whether class participation was encouraged. Each of the labs were conducted individually but the results were discussed as a class. Also, in Part III of the group project, it usually became an interactive presentation. Students would ask questions on other products used or how the team was able to discover relevant evidence. Figure 7 below shows student evaluations for the last 4 quarters. As evidenced by the chart, the class average for this question is 1.69 compared to the department average of 2.04.

Question 16 addresses whether a student would recommend this instructor for this course to other students. We would like to think that we are completely responsible for a student’s learning but the reality of it is that in this class we introduce concepts, expose them to tools to assist in the group project, and act more as a facilitator. Figure 8 below shows student evaluations for the last 4 quarters. As evidenced by the chart, the class average for this question is 1.56 compared to the department average of 2.2.

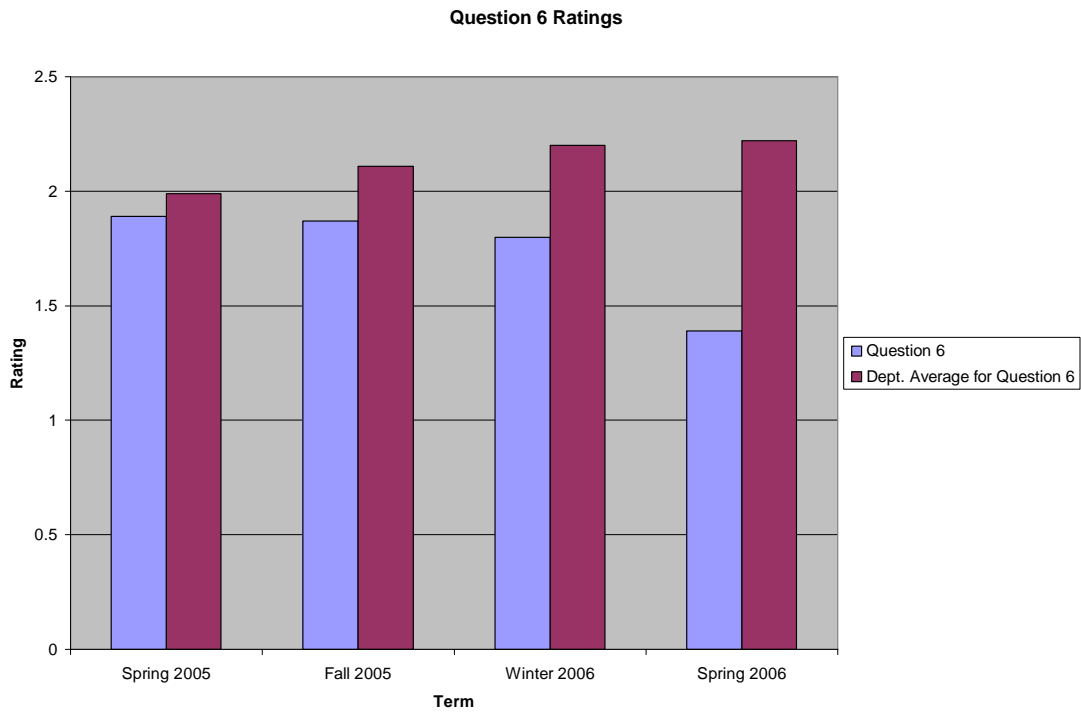


Figure 6: Student Evaluation on Question 6 from Spring 2005 to Spring 2006.
RATING SCALE: 1 for Strongly Agree to 5 for Strongly Disagree

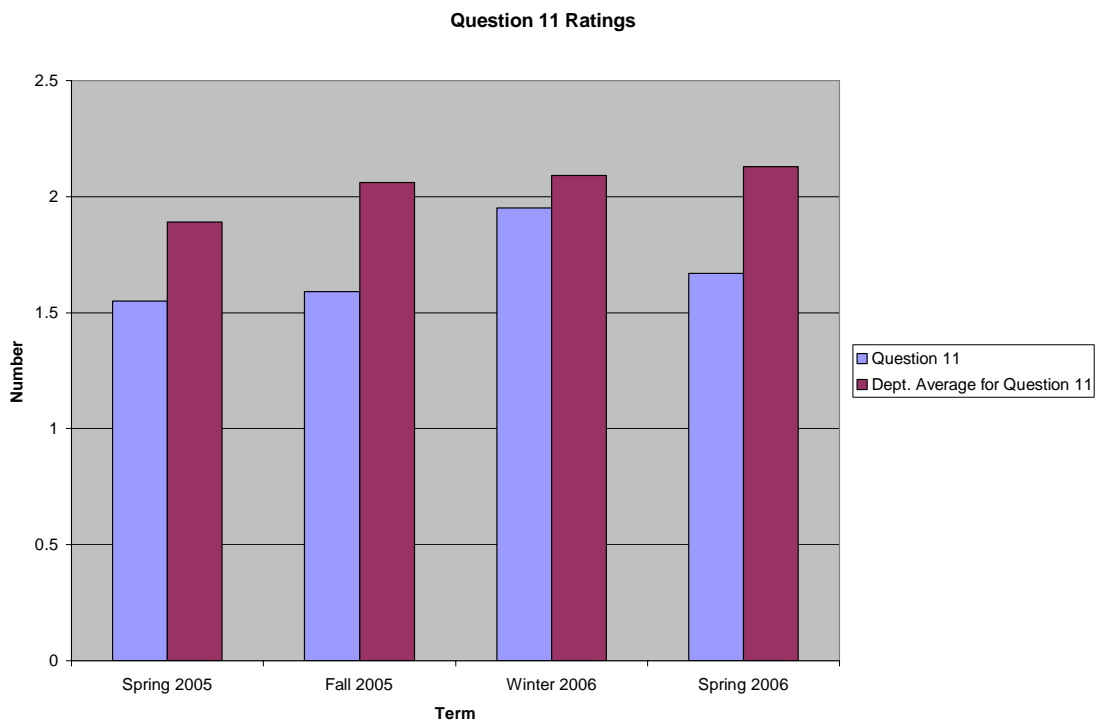


Figure 7: Student Evaluation on Question 11 from Spring 2005 to Spring 2006.
RATING SCALE: 1 for Strongly Agree to 5 for Strongly Disagree

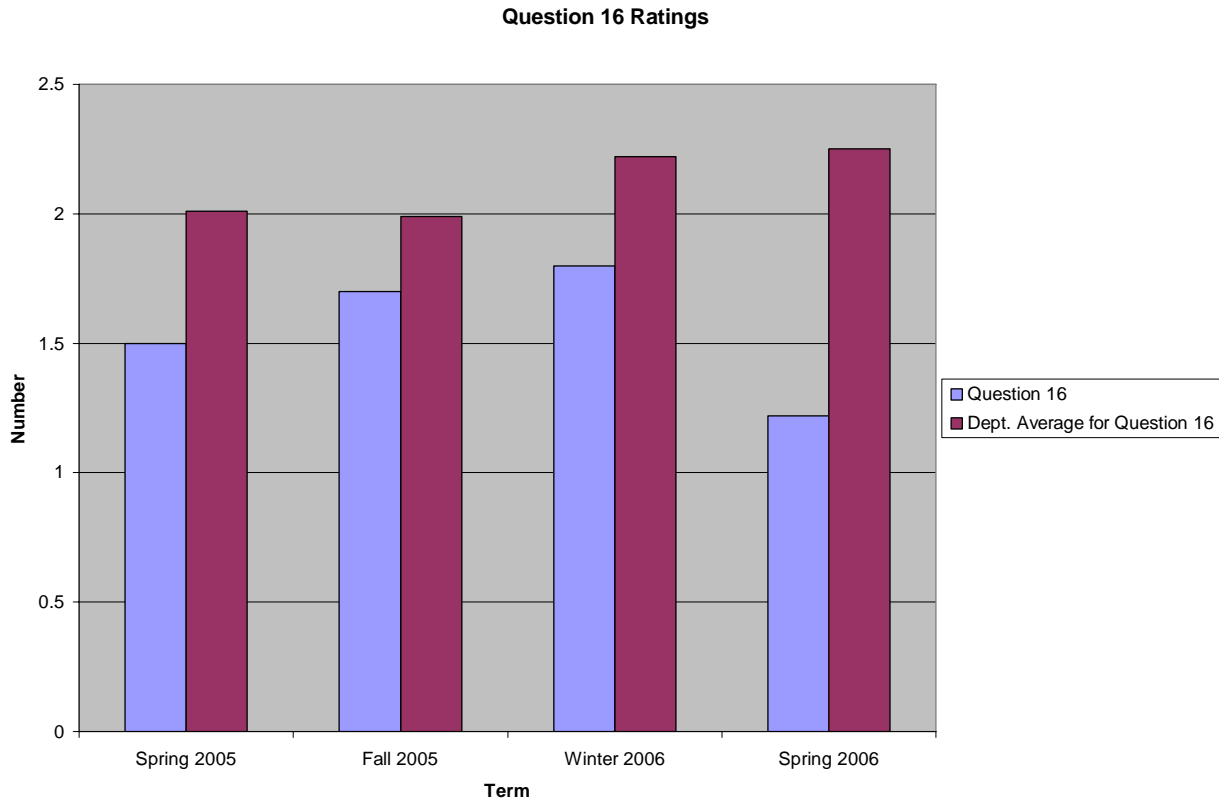


Figure 8: Student Evaluation on Question 16 from Spring 2005 to Spring 2006.
RATING SCALE: 1 for Strongly Agree to 5 for Strongly Disagree

The computer forensics class consistently outperforms other classes in the department. In fact, the student enrollment is holding steady even with the large time commitment for the group project. See Figure 9 below for student enrollment.

FUTURE IMPROVEMENTS

While the course was well received by the students, there is always room for improvement. To better teach the meaning of the Fourth Amendment, students wrote their own search warrants for the primary crime but not the secondary 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. Since teaching this class in the last year, typically only one team would highlight that evidence related to the secondary crime did not fall under the purview of the search warrant and would not be admissible into 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 over-looked.

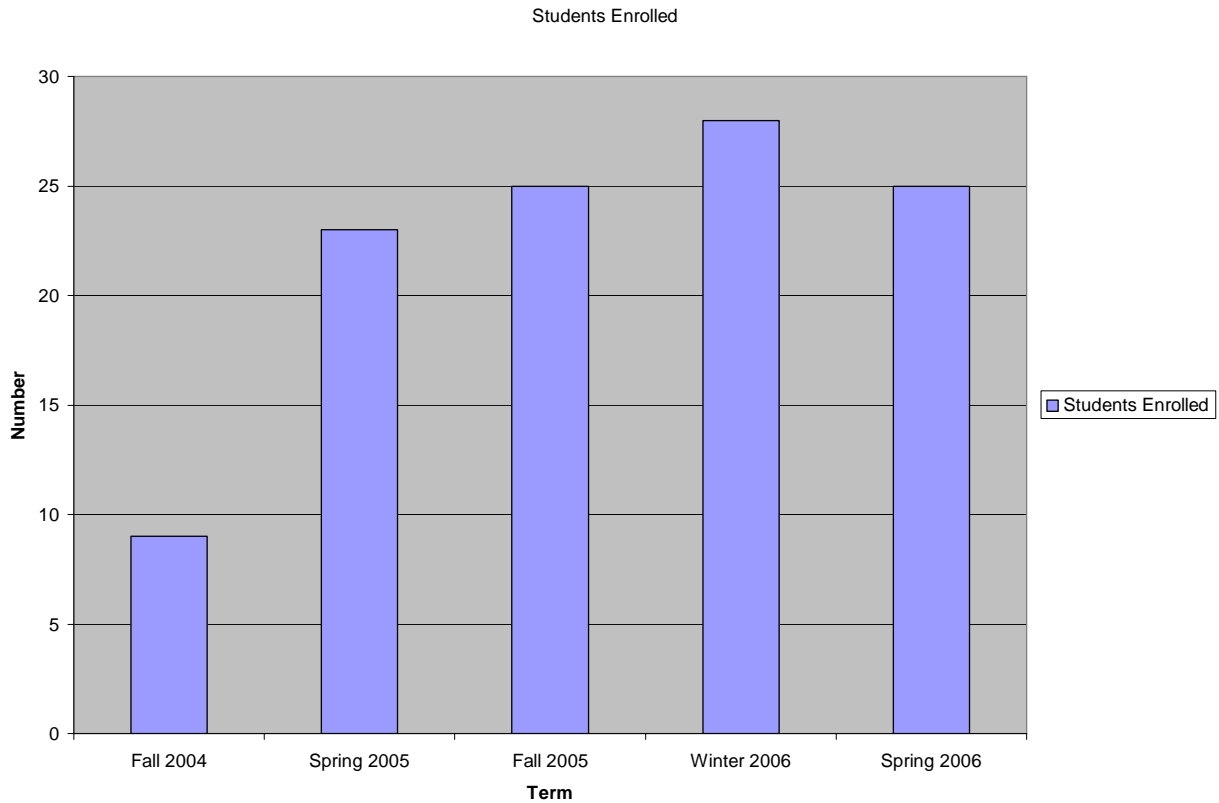


Figure 9: Student enrollment

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.

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 UTK, 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 to lapse 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.

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.

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.

Student Evaluations for CIS481 Computer Forensics class (2005 to 2006), California State Polytechnic University, Pomona.

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.

