Computer Forensics: Training and Education

Robert F. Erbacher
Department of Computer Science
Utah State University
Logan, UT 84322
robert.erbacher@usu.edu

Richard S. Swart
Department of Business Information Systems
Utah State University
Logan, UT 8433-3515
Richard.swart@usu.edu

Abstract

This paper is an outgrowth of Erbacher's panel presentation at the 2002 Computer Forensic Workshop held in Moscow, ID. The concept behind this paper is to provide a discussion of the needs within the computer forensics curriculum focusing specifically on the need for lab-based experimentation as well as arguing the needs for both an educational component as well as a training component. The discussion looks at the differences between training and education and how these two needs can both conflict and enhance one another. The paper looks at the need to integrate the instruction within the curriculum with effective experiments. Finally, we examine some of the legal and policy issues with running such a course. We take as our basis much of the work that has been done developing security curriculum and examine how this prior knowledge can be used to improve the curriculum development process for computer forensics, as many of the issues are similar.

1 Introduction

In this paper we examine the issues surrounding the development of a computer forensics curriculum. This paper does not cover all aspects of a needed curriculum but rather focuses on a few key components within the purview of the authors, namely: lab-based instructional issues, remediation of the needs for both training and education, identification of the proper positioning and use of both training and education, and finally legal and policy issues. Rather than start from scratch, we rely on many of the concepts and ideas from the development of security curriculums and examine how these issues differ and can be adapted for the computer forensics field.

Computer forensics is generally looked at as having two principal focuses, both of which must be examined. The first focus is that of analyzing an entire hard drive or computer system when suspected of having been used for criminal activity. This often occurs when a computer is found at a crime scene, or a company has cause to believe that an employee has committed a crime. The second focus is the analysis of system log files and associated information to identify the source of an attack or intrusion. In this scenario, the extent to which the company wishes to pursue the intruder will determine the extent of forensic analysis performed. Often the company will wish to maintain the computer system in a running state, but will need assistance in determining how the attack succeeded such that it can be prevented in the future. The dramatic increase in public attention to corporate losses of data has led to an increasing awareness of the need for after-the-fact investigations into computer crimes. Publicly traded corporations are also required to implement effective information security controls under the provisions of the Sarbanes-Oxley Act of 2002. [1] Part of an effective control environment is emergency response to intrusions, and well-trained forensic investigators play a key-role in computer emergency response teams [2]. A key step in meeting the needs of law enforcement, and the corporate community is the development of effective computer forensics education. [3]

When considering the direction and focus of a computer forensics curriculum we must consider its need to be tightly coordinated with the needs of law enforcement, similar to the way that computer security is coordinated with engineering [4]. In the same way that computer systems must be designed from the ground up to be secure using an engineering perspective, computer forensics systems must be designed from the ground up to ensure compliance with applicable laws and standards for preserving evidence from a law enforcement perspective. Ultimately, engineering principles become ever more important with computer forensics to ensure the appropriate legal guidelines are followed stringently. A failure of the engineering design of a tool can lead to a failure in the legal applicability of the tool.

2 Curriculum for Forensics

Computer forensics is still a relatively young field, especially in contrast to other forensic sciences, such as chemistry-based forensics. As chemistry-based forensics has become well established, understood, and accepted by the courts so too must computer forensics. In order for this to take place, we must refine the training and education of forensic computer scientists. Only after the scientists are well trained with well defined tools and processes can we achieve a level similar to that of the other forensic sciences.

In developing a curriculum for computer forensics we must understand that the graduates will not only be employing the tools currently available, but will be developing new tools. That is the ultimate goal of a computer science program. It is proposed by Chin et al. [10] that an information security curriculum is critically dependent on engineering due to the need for said students to be able to correctly develop reliable and secure tools. Only careful adherence to engineering principles will guarantee this result. With computer forensics we must extend this definition as the tools must be defensible in a court of law if they are to be of any value.

Students in Information Technology or Management of Information Systems Programs must be trained to accurately use these tools and to prepare and present their findings. While these students are less likely to develop new tools, they are likely to work closely with law enforcement, corporate investigators and corporate management to develop effective policies, procedures and training requirements for computer forensics. It is crucial that all students entering the information security field are adequately trained in computer and network forensics.

Target Audience

Identification of the target audience will provide substantial direction as to the direction and focus of the developed curriculum. The audience can consist of computer science undergraduates, computer science graduates, law enforcement, business, information systems, information technology, other majors, and mixed environments. Computer forensics can clearly be seen to be of interest to and an appropriate curricular element for this diverse range of students. Computer forensics has implications for each of these majors. Additionally, each major must gain experience in the other domains so as to understand, at least in part, when they are outside their purview. For example, a computer scientist must know when to consult with the legal department with respect to an attack or questionable computer activity. An information technology or information systems major may need to consult with a computer scientist regarding application code or hardware issues beyond their training. Along these lines, it is very beneficial for individuals to gain experience interacting with other majors. This will aid in their understanding of the point of view of the other domains and to understand the concerns of the other domains. This also helps prepare students to enter a workforce composed of multi-disciplinary teams.

More specifically, Computer Science undergraduates would be expected to learn lower level specifics of deployable technology, their advantages and disadvantages. Computer Science graduates would be expected to learn state of the art techniques and methodologies being researched. Law enforcement would be expected to learn how to use consumer off the shelf (COTS) products, as well as forensics applications restricted to law enforcement. Business majors would focus on policy and legal issues as well as deployment strategies. All majors would cover aspects of legal and privacy issues, as well as COTS products though the extent to which the areas are covered will vary substantially.

2.1 Training vs. Education

There are principally two opposing pedagogues which may be applied in the type of computer forensics class we have discussed. The first pedagogue has the goal of training students for an occupation within the computer forensics field, principally in conjunction with law enforcement or a computer emergency response team. This direction focuses on an application-based curriculum. The second pedagogue educates students on the needed capabilities, but goes a step further and attempts to teach the students a greater level of detail about the applications and tools; particularly the techniques and algorithms used behind the scenes within the tools. Teaching students how to perform a forensic analysis is critical for an immediate position, but likely is not best for them in the long run as the tools and techniques change over time. We must not only teach the student how to perform the analysis but also why it is done the specified way and how the tool performs the analysis [6].

Training is also limited in that it focuses students' attention on current techniques and methods rather than processes. As computer criminals continue to adapt they will most certainly advance their techniques for hiding information. As these illicit techniques progress, students *trained* on particular methods will be at a loss while students educated on processes and more advanced abstract concepts will be able to adapt [7].

In addition to the traditional comparison of training versus education, we must also consider the comparison of practice versus research. While a certain amount of training in conjunction with education makes for a well rounded undergraduate, what about a graduate student? How must the curriculum be adjusted for these students? Clearly, for graduate students the practical aspects of the curriculum must be reduced and they must endeavor to take on a much greater challenge with respect to the educational component, understanding the tools sufficiently to be able to propose enhancements.

Training: Needs and Pedagogy

Training is critical for law enforcement at all levels. Such agencies are in separate need of additional personnel to aid in the analysis process and to assist with criminal investigations within computers. With the ubiquity of computer systems, many such systems are constantly enmeshed in criminal activity. This type of curriculum will focus on the tools available for such forensic analysis, their advantages and disadvantages. Further, the curriculum will cover the correct use of the given tools and the appropriate legal and ethical issues.

Such a curriculum would stop short of covering the inner workings of such tools and focus on the ability of the students to use the given tools correctly and legally. These students would be expected to assist law enforcement but would not be expected to improve upon the capabilities provided to law enforcement. Their ability to troubleshoot the tools would also be greatly limited.

The students would be trained in the proper collection of and preservation of computer forensic evidence. They would understand chain of custody issues, admissibility requirements, and be able to maintain the evidence lifecycle from collection to presentation in court. These students would also receive basic training in the documentation required in effective investigations. They would understand the need to create forensically sterile workstations, be able to maintain these workstations, and use them to create forensic bit-stream images of target drives for use in the forensic investigation.

Such a curriculum would consist of a wide variety of students from many disciplines, principally at the bachelor level. The curriculum would be appropriate for students of all levels and abilities and would be particularly applicable to law enforcement officers themselves. The goal is to ensure that law enforcement is aware of how to respond when a computer is found at a crime scene to maintain the admissibility of the computer forensic evidence.

Education: Needs and Pedagogy

It is critical that when we educate students we prepare them for the future, for the unexpected [8]. Thus, educating students requires aspects of both training and education. Educating an individual is no doubt far more demanding of the students than merely training them. This type of rigorous course would be appropriate for both graduate and undergraduate students.

A purely educational curriculum would discuss the tools, techniques, and processes involved in computer forensics. Some level of practicum would be involved; however, the practicum would ultimately be geared towards providing the students with an understanding of how the theory can be put into practice, and how different theoretical aspects build on and impact one another.

Given the level of detail and the challenge of such a course, it must be specialized for a given degree program. Consequently, such a course is less applicable to general students. At the graduate level such a course would focus even more heavily on the theory and the detailed mathematical models for the included techniques. The goal is for the graduate students to be able to direct future research and progress in the field. Undergraduates must be able to implement these future developments without violating any scientific or legal principles.

Integration of Training and Education

Given that education and training have such disparate views of pedagogy, how can they be integrated within a constrained program? The actual integration paradigm will depend on the focus of the curriculum, whether it be graduate or undergraduate, the goals of the students being recruited and their majors, and the level of collaboration with law enforcement taking place. As has been discussed, even a good educational curriculum will benefit from having training to show the students the practical application of their knowledge, and provide them with hands-on experience. Training in and of itself isn't appropriate for a university, which should endeavor to prepare students for a lifelong career, not merely for the here and now.

3 An Academic Forensic Laboratory

One pedagogical technique critical to a successful forensic curriculum is the integration of lab-based instruction. Students show increased learning and motivation when involved with hands-on-practical problem solving. [9] Lab-based instruction provides the hands-on aspect of the curriculum that takes students beyond the theoretical to the practical. How can students be prepared for a computer forensics position or determine if they are truly interested in such a position without hands-on experience? How can a graduate student identify tracks of research and determine what needs to be improved in the forensics process without actually experiencing what current computer forensics experts have to do, and what tools they have available? Do the students understand the "principles enough to apply them..." [10]? Most students do in fact learn through hands-on experience [7, 10].

3.1 Laboratory Requirements

The actual design of the laboratory will vary dependent on its prospective usage. At the very least we do not wish the forensic process to be interfered with, even if only simulated data is being used. Otherwise the students will merely learn a lesson in frustration rather than a lesson on computer forensics. If actual data is to be used then we must be concerned with privacy issues and ensure that access to the sensitive data is strictly controlled. This can go so far as requiring a safe for the sensitive data as the laboratory will likely be used by many individuals throughout the day and the sensitive data should only be available when it can be monitored closely. Additional requirements may include:

- **Lab monitor**. A lab monitor is critical, especially for a lab geared towards educational exercises as such a forensics lab is. First, the lab monitor will assist students and answer questions, especially with the unique software and hardware tools the lab will incorporate. The lab monitor will also ensure the equipment is only used by those authorized to do so and not by random students.
- **System administrator**. System administration support is necessary to maintain the configuration of the analysis workstations, install and configure forensic tools, and to restore the test environment for each group. Some lab exercises will require more involvement by a system administrator than others. Lack of system administration support will likely lead to an inability to incorporate some experiments/exercises that otherwise would prove extremely valuable to the students. Forensic workstations and tools are outside of the expertise of many system administrators, so these individuals will require advanced training in forensics themselves.
- **Physical space**. Physical space is needed in so far as the lab must be physically segregated from other labs/space. Since students can quickly disrupt work in progress on the machines in the lab the systems must be protected from such disruptions.
- **Segregated network**. Having segregated physical space prevents physical intrusions into the systems. A segregated network is required to prevent cyber intrusions into the systems. Such intrusions can cause loss of information and corruption of tasks in progress. An extensive discussion on the needs for an isolated network is found in [8, 9].
- **Hardware requirements**. The environment will require several forensic workstations with hot swappable drive bays for students to experiment on. The hot swappable drive bays will be used for the drives to be forensically analyzed. Several target machines must also be available to explore the feasibility of deriving information from dynamic storage, e.g., main memory and registers. Extensive collections of media and hard drives will also be required in order to maintain the integrity of the data during analysis.
- **Software requirements**. Various software tools are available to aid in forensic analysis. In a research environment this laboratory also provides a unique opportunity to test and compare newly developed tools and techniques. Since some tools are only available to law enforcement, a tight collaboration with law enforcement will greatly aid the educational goals of the environment. Determining which tools to incorporate into such an environment is an open question. Generally, Helix (http://www.e-fense.com/helix/) would be a minimal starting point.

It is necessary for the lab to be closed, meaning that it is generally not available for general public use. The lab will only be available to students taking appropriate courses, and then only when being monitored. Failing to incorporate this type of protection can result in compromise to the lab and possible civil liability to the university.

Clearly, the costs associated with running an extensive a lab will be substantial. For this reason, collaboration with law enforcement and other groups interested in sharing the burden of such a lab is needed. However, it is possible to develop a basic networking lab without partnering with law enforcement.

3.2 Integration with the Curriculum

Effectively integrating a computer forensics laboratory into the curriculum for a full course requires that the students be actively engaged with lab-based curricular components, that these components generate meaningful results, that the tasks be clearly laid out, and that the assignments be progressive in nature. A lab-based curriculum can take one of several forms:

- **Instructor-directed assignments**. The typical metaphor is that of the instructor assigning tasks based on theoretical and desired expectations. The assignments are generally designed to provide the student with fundamental understanding of the tools and techniques.
- **Law enforcement directed analysis and exploration**. Engaging law enforcement within the pedagogical structure has many benefits. First, it will more greatly engage the students within the process and second it will expose the students to the tasks actually expected to be performed by law enforcement. This will allow the students to better gage whether this is the appropriate career path for them and aid in better training the students for such a position. The disadvantage is that the training may be directed specifically for one agency.
- **Law enforcement collaboration-based analysis**. The most effective way for students to gain the exposure and experience of real computer forensics is for them to participate with law enforcement on actual cases, i.e., case studies. This has the added benefit for law enforcement should they run into a new scenario and require additional insights, perhaps from an academic expert. The difficulty in this scenario results from the sensitive nature of the information and the need to maintain privacy for the individuals involved. Such a course might only be feasible for select students, i.e. law enforcement acquiring additional training, vetted students, etc.
- **Obfuscate versus discovery contest**. This can be considered a derivative of attack/defend scenarios from typical computer security courses [8, 9]. The goal is for one team to attempt to hide information within a computer system and for a second team to locate and decode the information without violating any computer forensic principles, i.e., modifying the system in any way. Only by exploring both sides of the problem can an individual truly become an expert at the process, understand the intricacies involved, and compete with the best criminals who are actively attempting to hide information.
- **Free form exploration**. While the least optimal use of a lab, allowing students with time for free form experimentation and exploration of the facilities and associated tools can have enormous benefits. Namely, it is this free form exploration process that can open up the minds of the students and allow them to arrive at their own methodologies and techniques for the forensic analysis of computer systems. It is this freedom that will lead to new techniques and tools in the future that will progress the nature of computer forensics. Such free form experimentation is of particular necessity for graduate students.

Incorporating such a lab-based curriculum will greatly aid in the training and education of the students and better prepare them for an actual position in computer forensics. Issues of where training belongs in an educational curriculum are discussed above in section 3.2.

4 Student and Course Policies

The need to consider legal and policy issues with respect to the administration of the course itself resolves from the fact that it is necessary to discuss security dual-use tools within the class. Essentially, while many of the tools discussed in the class can be applied to help protect and secure a networked infrastructure, and to examine the environment to identify how a break-in occurred, they can also be used to identify weaknesses and how to cover up the typical tracks left behind by a successful intrusion. Tools such as password crackers can be used to ensure all passwords on the system are secure, but can also be used to resolve weak passwords by a potential intruder. Tools such as Ensight are used to analyze a seized hard drive, but understanding how this tool works can provide insight into how to better cover-up the intrusion trail or contained criminal evidence.

Related discussions within the security curriculum community [6, 8] led to the conclusion that it is better to have well trained graduates. These well trained graduates understand the capabilities and issues involved, can deal with the experienced criminal techniques, and advance the science behind computer forensics to deal with new techniques. On the other hand, a poorly trained graduate will be incapable of dealing with the experienced computer criminal and unable to aid in the progress of computer forensic science. This will ultimately lead to missed opportunities. Additionally, given the number of criminals trying to hide information in computer systems versus the

number of researchers and practitioners attempting to locate said information, it is critical that the students be well trained.

4.1 Course Admission Polices

Given the sensitive nature of the course it is critical that students understand the ethical expectations of students entering the course. Again, this is similar in many respects to a computer security curriculum [4] and must be dealt with readily. One consideration is the level of culpability of the professor of such a course should a student go rogue. This can be dealt with in a variety of ways, including:

- **Signed agreement form**. This is likely the most stringent policy and can be considered an extension to the policy of requiring students to agree to a set of pre-specified rules and regulations upon receipt of a university or departmental account. Requiring students to enter into such an agreement provides a measure of protection for the professor and ensures the student is aware of the severity of violating course ethics policies. As this can be construed as a measure for limiting access to the course material it generally would not be found to be acceptable in a public university.
- **Ethics prerequisite requirement**. The need for ethics in a computer science curriculum has often been discussed. In fact, many computer science degree programs do in fact require at least one ethics course. Extending the prerequisites for a computer forensics course to require such an ethics course is easily implemented and managed and provides substantial benefits.
- **Ethics as a required course component**. Integrating ethics tightly into a course such that not only is it discussed throughout the course but appears as a graded component of the course will embed the necessity and impact of ethics on the material.
- **Syllabus stipulated expectations**. Whether alternative mechanisms are employed or not, the course syllabus should incorporate some discussion on the expectations of ethical behavior. This is easily incorporated and used in conjunction with the prior techniques. Used alone this mechanism provides the weakest form of ethical guarantee but provides to the student a limited sense of the necessity for ethics when none other is provided.

As is typical, a combination of these requirements may be most appropriate. It is critical, however, that should a student violate ethics requirements that a severe penalty be imposed and that penalty be acted upon. The consequences of not doing so are far too great. It is also helpful to keep in mind that not acting upon the specified consequences can be construed by the students as to implying they are not meaningful or relevant.

It has been discussed [4] that ethics has not been given sufficient attention in the past. Having ethics as a separate course or discussed intermittently within a few select courses does not indoctrinate students as to the importance of ethics and in fact can be seen by students as a counter indicator. Lidtke called for ethics to be integrated into all courses as intrinsic components and not as add-ons [4]. Only then will students see its true relationship to the material. For the computer forensics course this is a necessity, the ethical discussions must be intermingled with the regular discussions as a single whole rather than being treated as a separate concept. These ethical concepts will then be well served in a computer science curriculum in which all courses appropriately incorporate ethics as a principal discussion in conjunction with the typical discourse.

Many of these course policies are easier implemented at the undergraduate level. At the graduate level it is far more difficult to require an ethics course as a prerequisite or to otherwise limit enrollment. Since it is at the graduate level that students are most likely to be engaged in sensitive activities, i.e., collaborating with law enforcement, the need to maintain a strict ethics doctrine is critical.

4.2 Course Administration Policies

Computer security differs from many courses in the level of dual use techniques and tools discussed under the auspices of the curriculum. While the course desires to teach issues of computer security and computer forensics, this same knowledge can be applied in attempts to better circumvent the forensic process or more directly attack computer systems. It is for this reason that the curriculum should consist of a strong section on legal and ethical issues. Ignoring the ethical issues can quickly lead to inappropriate behavior. Students must be clearly informed as to the limits and applicability of their newly gained capabilities. It is best when the ethical needs of the material are stressed and reinforced from day one. It has been shown that treating ethics as an add on [4] can lead students to treat ethics as secondary. Rather, it must be tightly integrated and treated as one with the remainder of the course material.

Education is geared principally towards computer science students and at one level will cover the tools available to law enforcement but at another level will cover the details of the tools and their inner workings in great depth. Legal and ethical issues remain critical. Ultimately, these students, while they will be capable of assisting law enforcement directly, will be educated with the ultimate goal of their improving on the capabilities provided to law enforcement. While training is particularly focused on undergraduates, educational initiatives are focused at all levels with particular interest in graduate education. How can the techniques be improved? What capabilities can be integrated to improve the existing facilities. What are the limitations of current tools from a law enforcement perspective? What are the absolute requirements for such tools from the law enforcement point of view?

5 Conclusions

We have presented a discussion on aspects of curriculum development for computer forensics. This discussion is currently very focussed. A more complete discussion is required with regards to actual components of a computer forensics education. Additionally, many of the lab-based components remain untested. A discussion with regards to the effectiveness of the various techniques must be incorporated once students have actually been put through there paces. Finally, we must analyze the effectiveness of the students so trained on the job form the perspective of the law enforcement agencies that would be looking to hire such individuals.

What cannot be denied is that a lab-based component is critical to the success of any curriculum within computer forensics. In order for students to understand what the process truly entails they must experience. This is needed both to prepare students to work in the field and also to perform research in the field and improve the state of the art to make the task more acceptable to the users of the technology. Such a lab-based curriculum has policy issues due to the dual use nature of the knowledge being imparted to the students. As in the computer security field this is a necessary risk in order to improve the ability of law enforcement to combat the criminal element's ever growing reliance on advanced technology.

6 References

[1] Sarbanes_Oxley Act (2002) INSERT FULL LEGAL CITATION HERE

[2] T. Welch, "Computer Crime Investigation and Computer Forensics," in *Information Management Security Handbook, 5(e), Auerbach Publications:Boca Raton, FL 2004.*

[3] A. Yasinsak, R.F. Erbacher, D.G. Marks, M.M Pollitt, and P,M. Sommer, "Computer Forensics Education," IEEE Security and Privacy ???? 2003, pp. 15-23.

[4] C.E. Irvine, S-K. Chin, and D.A. Frincke, "Integrating Security into the Curriculum," *IEEE Computer*, December 1998, pp. 25-30.

[5] G. White, G. Nordstrom, "Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles," *National Infromation Systems Security Conference*, 1996.

[6] C.E. Irvine, "Amplifying Security Education in the Laboratory," *Proceeding of the IFIP TC11 WC 11.8 First World Conference on Information Security Education* , Kista, Sweden, June 1999, pp 139-146.7 D.K.

Lidtke, “Ethical Behavior in the Curriculum,” *IEEE Computer*, November 1997, pp. 51-52.

[5] J.E. Anderson and P.H. Schwager, "Security in the Information Systems Curriculum: Identification & Status of Relevant Issues," *Journal of Computer Information Systems*, Spring 2002, pp. 16-24.

[8] W. Yurcik, D. Doss, "Different Approaches in the Teaching of Information Systems Security," *Proceedings of the Information Systems Education Conference*, November 2001.

[9] J. M. D. Hill, J. W. Humphries, C.A. Carver, Jr., and U. W. Pooch, "Using an Isolated Network Laboratory to Teach Advanced Networks and Security," *Proceedings of the 32nd SIGCSE Technical Symposium on Computer Science Education*, Charlotte, North Carolina, February 21-25, 2001, pp. 36-40.

[10] S-K. Chin, C.E. Irvine, D.A. Frinke, "An Information Security Education Initiative for Engineering and Computer Science," *Naval Postgraduate School Technical Report*, NPSCS-97-003, Naval Postgraduate School, Monterey, CA, December 1997.