2003

Forensic course development

Luther Troell

Yin Pan

Bill Stackpole

Forensic Course Development

Luther Troell
RIT
102 Lomb Memorial Drive
Rochester, New York 14623
(585) 475-6479
ljt@it.rit.edu

Yin Pan
RIT
102 Lomb Memorial Drive
Rochester, New York 14623
(585) 475-4645
yxp@it.rit.edu

Bill Stackpole
RIT
102 Lomb Memorial Drive
Rochester, New York 14623
(585) 475-5351
wrs@it.rit.edu

ABSTRACT
In recent years, digital technology has experienced dramatic growth. Many of these advances have also provided malicious users with the ability to conceal their activities and destroy evidence of their actions. This has raised the need of developing specialists in computer digital forensics -- the preservation, identification, extraction and documentation of evidence stored in the form of digitally encoded information (data).

In this paper, we present the procedures and rationale used in the development of forensic courses at both the undergraduate and the graduate levels. We also demonstrate our decision making process of selecting topics included in each course.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *security and protection (e.g, firewalls).*

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *curriculum, information systems education.*

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *unauthorized access, invasive software.*

General Terms
Security, Design, Legal Aspects, Experimentation.

Keywords
Computer Forensics, Intrusion Detection, Information Assurance, IT education, Curriculum Development.

1. INTRODUCTION
The use of digital devices such as computers, personal digital assistants (PDAs), cell phones, and cameras, etc., as sources of evidence in fraud, white-collar crime, and other criminal investigations has been steadily increasing in recent years.

With the dramatic expansion of computer use and communication networks, computer crimes such as child pornography, threatening letters, fraud, and theft of intellectual property have been increasing at an alarming rate. Due to the increased sophistication and frequency of remote attacks, the national Computer Emergency and Response Teams (CERT) is not able to investigate all instances of computer crimes. Thus more professionals with appropriate skills and knowledge are needed. Computer forensics, a relatively new field which involves the preservation, identification, extraction, and documentation of computer evidence to a court of law [4], is gaining more and more attention. The professionals in computer digital forensics are in high demand - not only by investigative forces but also by the military, government, and corporations seeking to uncover evidence of illegal activity.

In this paper, we will present the procedures and rationale used in developing curriculum in computer forensics that can be used to train specialists in this field. After taking these courses, students will have obtained basic knowledge in computer forensics, an introduction to computer forensic and intrusion detection tools, and will be able to respond to computer intrusion and forensic incidents promptly and accurately.

CITC4'03, October 16–18, 2003, Lafayette, Indiana, USA.

2. BACKGROUND
Computer forensics involves understanding specific aspects of digital evidence and the general forensic procedures used when analyzing any form of digital evidence. The field utilizes sophisticated technological tools to appropriately preserve, extract and analyze digital evidence.

With such a wide base of prerequisite knowledge, it is impossible to provide a single course to effectively cover all of these materials in-depth. We decided to develop forensic courses at both the undergraduate and the graduate levels to cover the knowledge in breadth and depth.

The undergraduate course is intended for the senior students who are currently pursuing the Applied Networking and Systems Administration Bachelors degree in the Information Technology department (or) as electives to matriculated students in the B.S. in Information Technology program. The B.S. in Applied Networking and Systems Administration is a program designed to teach students how to be the designers, implementers, and operators of computing networks and networked systems (both clients and servers). It is expected that students who enroll in this course already have a theoretical as well as a hands-on understanding of Internet protocol suites and applications including TCP, IP, ICMP, DHCP, DNS etc. The undergraduate course will allow students to gain an understanding of computer forensics essentials. The course will provide the student with the ability to identify and employ tools used for tracking intruders,

gathering and preserving evidence, as well as ensuring admissibility in court.

The graduate course is intended for the graduate students who will take a concentration in security in the department of Information Technology, Computer Science or other programs. It is designed to provide students with advanced techniques and methods for the extraction and preservation of information from digital devices. At the end of the course, the graduate students are expected to be able to not only effectively use, but also to develop new software tools to achieve these ends.

3. DEVELOPMENT PROCEDURE

3.1 Undergraduate Forensics Course

3.1.1 Define the goals and expected outcomes

Presenting the right amount of basic knowledge to fit within the broader contexts of forensic science, crime, and the legal system is crucial. Before choosing the materials from various books and literature, we first clearly defined the goals and expected outcomes for the undergraduate students to achieve.

3.1.1.1 Goal

This undergraduate forensics course is designed to provide students with the ability to identify and employ tools used for tracking intruders, gathering, preserving and analyzing evidence of their activities. The course emphasizes both the fundamental computer forensics techniques and the hands-on experience of utilizing the tools needed to uncover illegal activities of computer users. Such evidence might include deleted and hidden files, encrypted information, steganography, illegal software, log files, email traffic, network tables, etc. Students will learn the procedures used to gather and preserve this evidence to ensure admissibility in court.

3.1.1.2 Outcomes

Upon completion of this course, students will be able to

1) Understand the fundamental techniques and procedure of computer forensics, including inherent flaws and limitations.
2) Understand social, legal, and ethical considerations that are encountered when working in this field.
3) Demonstrate their ability to identify and utilize appropriate IDS tools to detect network and system intruders.
4) Describe the basic procedure of incident response.
5) Utilize available forensic tools to discover, collect, preserve, analyze and document digital evidence.
6) Obtain the basic skills to uncover hidden evidence such as deleted and hidden files, cryptographic steganography, illegal software and crack encrypted files.

3.1.2 Information to be conveyed

Once the goals and outcomes were agreed upon, the next step was to determine what information needed to be conveyed to allow the students to reach those goals and outcomes. Computer forensics incorporates many areas, including intrusion detection [6], incident response [9], network security [3], law enforcement and, most importantly, the computer crime investigation [1, 2]. This is a very wide variety of topics.

To pare down the content to a manageable size, everyone involved in the development of this curriculum agreed to work concurrently on different, related tasks. Curriculum reviews were performed, books were ordered, and many materials related to the computer forensics field were read and assimilated. Telephone calls were made to individuals from law enforcement, the legal sector, and industry. Periodic meetings were held to keep all members informed of team progress. A "brainstorming" session allowed a list of topics to be developed. The list was reorganized multiple times. Finally an informal pareto analysis of all items yielded four areas of focus:

1) Collection
2) Preservation
3) Analysis
4) Reporting

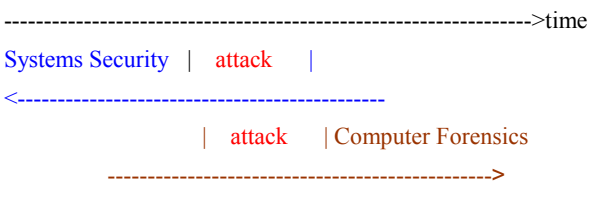
Clearly the techniques and tools involved are largely dependent on the operating system under investigation. We determined that each of these four areas should be examined with respect to Windows, Linux and Networking. It was also determined that some areas relevant to all systems and networks should be examined - these include an introduction to forensic tools and procedures as well as discussions of discovery and policy. Finally, legal issues needed to be examined with regard to computer forensics. The general consensus was that the legal topic should be covered by an 'expert' in this area (likely someone outside of the IT faculty).

3.1.3 Addressing content overlap and conflicting goals

Intrusion Detection concepts and tools, covered in the prerequisite course *Systems Security*, focus on detecting intrusion, halting the attack and rebuilding the system (e.g. getting the machine back online and running as quickly as possible). Computer forensic techniques, on the other hand, focus on preserving the evidence of the attack, which can delay putting a machine back into production. This "rebuild" versus "preserve" issue creates conflict that deserves some attention.

To ensure focus is brought to this issue, intrusion detection systems (IDS's) and IDS tools will be reviewed in this forensics course. However, the focus on the IDS will be shifted from attack detection to review of the generated log files – providing further evidence of the source and timing of an attack. The preservation and analysis of IDS data may be as important to a legal court presentation as that of the victim's and suspect's computers. The conflict between systems security and computer forensics goals will be brought to the attention of the student to promote a better understanding and to ensure the student is prepared to deal with such issues.

To illustrate this conflict, we developed a diagram/timeline to define when systems security ends and network/systems forensics begins. Note the overlap in the area labeled "attack". Both the *Systems security* and the *Computer Forensics* classes will address what actions might be taken in this area.



3.1.4 Course Content Scheduling

The next challenge was to fit the topics into the RIT schedule. RIT works on a quarter system, utilizing three ten-week "quarters" to comprise a full academic year. A number of different schedules were suggested until final agreement was reached. Four, two-week blocks would be scheduled focusing on (weeks 1 & 2) a general introduction to computer forensics, (weeks 3 & 4) Unix, (weeks 6 &7) Windows, and (weeks 8 & 9) Networking. The remaining two weeks (weeks 5 & 10) would be used for review and an introduction to the legal issues associated with digital forensics.

3.1.5 Content Development (or "Our New Way")

Faculty at many universities very likely use the techniques outlined above to develop new curriculum. That is: Pick goals and determine desired outcomes, decide what information needs to be conveyed, work it down to a reasonable amount of information while addressing content overlap and finally, determining a workable schedule. Once all of these issues have been addressed there still remains the formidable job of developing the presentation materials. Even more daunting a task is that of developing the faculty to teach this material.

To address this task, rather than having one person develop all the content, we split the workload between the interested faculty and tasked each with developing one "module" for presentation. Each faculty member then presented their module to the other members of the group, allowing for an interactive learning experience for all parties involved.

3.1.5.1 The Benefits

This development technique provided specific and tangible benefits to all parties involved. For example, the faculty member who developed a specific portion of content was able to present the material to a group of their peers for review. The other members of the group were introduced to the material in advance and were able to ask questions of the presenter (who, having developed the materials, was well-versed in that subset of the course content). This allowed kinks in the presentations to be worked out, and holes in the content to be filled prior to the formal presentation of the material to students. All of the faculty who participated in the course development learned something new and were better prepared to teach their upcoming courses. Continued research into new content areas was helpful in keeping research skills in practice and as an added bonus, may be applicable to scholarship. And finally, "the team that works together stays together" - the process helped create a bond between members of the faculty. (After all, working on the same project you're bound to learn more about your peers and share in their joys and disappointments.)

3.1.6. Labs

The lab content has yet to be developed. However we expect it to be created in much the same way – with each participating faculty member developing lab exercises based on their selected content area. The unassigned labs will be developed as a team exercise by the group and all lab exercises will be presented and supervised by the person that developed them. (Again, the benefit of working out the kinks and bugs ahead of time is a worthwhile endeavor in itself.)

Labs provide more than a reinforcement of lecture material – they also allow for student discovery. Each of the topics introduced in the lecture materials will be further explored with lab experiences. The outline of the lecture plan lends itself well to introducing tools and techniques specific to certain operating systems. For example, during the 2 weeks of lecture covering Unix forensic tools and techniques, students will be presented with labs whose content is geared to that operating system.

Furthermore, students will be expected to conduct their lab exercises as if they were working in the field. Log books and detailed notes for each lab exercise will be required. Written reports generated from this data may be used by faculty for student evaluations. Students can use these documents in a portfolio – providing typical examples of their work.

3.2 Graduate Forensics Course

3.2.1 Define the goals and expected outcomes

Similar to the development procedure for the undergraduate course, the first step to develop our graduate course is to define the goals and expected outcomes. At the graduate level, we assume that the students are familiar with computer forensics techniques that are covered in the undergraduate course. We expect the graduate students to reach for a higher goal.

3.2.1.1 Goals for the graduate student

This course is designed to provide students with the advanced techniques and methods needed for extracting information from digital devices. It emphasizes the experience of *developing* tools to further extract and preserve information from digital devices rather than simply using tools developed by others. Students will also be expected to develop sound procedures to ensure evidence integrity. Admissibility of the collected evidence in a court of law will be an item of utmost importance. At the end of the course, the students should be better prepared to become computer forensics investigators as well as active researchers at the forefront of the subject.

3.2.1.2 Outcomes

Upon completion of this course, students will be able to

1. Identify, analyze, and discuss tools used in computer forensics for examining file systems, file recovery and malicious code discovery.
2. Describe court admissibility investigative procedures – evaluated through a research report and an in-class presentation.
3. Completely understand basic function and forensic implications of the boot process such as cold boot, reset, warm boot, windows boot and Unix boot, and processes of starting and maintaining Windows, Unix and Mac.

4. Write/modify programs to enhance the retrieval of computer forensic evidence from different types of media storage.
5. Be able to utilize advanced intrusion detection tools such as SNORT. Combine SNORT with Apache, MySQL, ACID, and other such tools to log intrusion detection data and analyze it using a web interface [8].

3.2.2 Information to be conveyed

Again, interested faculty members helped determine the necessary content for inclusion while keeping the defined goals and objectives in mind. With the goal to prepare our students with the ability to creating new tools to enhance intrusion detection and the retrieval of computer forensic evidence, it was agreed that focus needed to be on the following areas:

1. Acquire the fundamental knowledge of hard disks and different file systems; Understand how different operating systems work, the boot procedures and processes.
2. Obtain implementation skill such as basic I/O and simple OS versions.
3. Analyze the current forensic tools.
4. Develop new forensics tools.
5. Explore SNORT (a network intrusion detection tool) at a high level so that students are able to develop programs to interface with SNORT and other network intrusion detection tools.

3.2.3 Making the transition to the graduate course

The prerequisite Undergraduate computer forensics course covered fundamental computer forensic techniques as well as hands-on utilization of forensic tools. The first issue during the development process was determining how to balance the amount of time spent on review. It was decided that one week was sufficient to overview the principles of computer forensic investigations. An initial student project might be to survey currently-existing forensics investigation and intrusion detection tools – discussing the merits and liabilities of each. Through such an initial project, students should quickly become aware of the current state of tools in the field, and be prepared to do research in the area. The network intrusion detection tool SNORT, introduced in the prerequisite *Systems Security* course, might be recapped at a high level. These types of activities should work to help the student in their own review process as well.

3.2.4 Course Content Scheduling

Our next step was to determine a proper schedule that would allow focus to be drawn onto all areas mentioned in Step 2. Discussion of various scheduling options yielded a split at the five week point as the most viable option. The first five weeks could be spent covering the fundamentals with more focused implementations being addressed during the second five weeks.

Content during that first half of the quarter might include study of basic boot procedures, operating systems concepts, file systems, and drives. Students would learn the details of how computer components including disk drives, memory, cache, kernel, peripherals and hard drives integrate and what might be the implications to forensic evaluation. This may also include how operating systems cooperate with other components to function effectively. The network intrusion detection tool, SNORT, would also be reviewed at the first half quarter. During the second half of the quarter, students will learn how to implement tools to deal with data I/O and data searching. Advanced feature of SNORT would be introduced and practiced.

3.2.5 Content Development

The faculty members divided into two separate groups. One group focused on developing presentation materials for classes; the other group investigated implementation and research issues of the subject. These two groups met periodically to discuss the progress and synchronize the contents of presentations with the implementation details. The first group provided directions and requirements to the second group, while the second group shared new research discoveries and implementation progresses with the first group.

3.2.5.1 Possible Exercises and Implementations

1. Students start to work on simple C programs to make a bit-stream dump to an external storage.
2. Write a simple disk wiping program to write both fixed and randomized data to each and every sector of a hard drive.
3. Write a simple tool to capture data from allocated, unallocated, and slack space on the disk.
4. Write scripts to glean desired information from IDS log files.
5. Combine Snort with Apache, MySQL and ACID to log the intrusion detection data into a database, and then view and analyze it using a web interface [8].
6. Final project: Develop programs to possibly improve and incorporate with existing forensics tools or IDS tools such as SNORT.

While working on these implementations, students are learning how to do research on the subjects. Their final projects will help lead them to their master degree capstone projects.

3.2.5.2 Research Ideas

- Extract digital evidences from RAM to an external device.

  When investigating a computer related crime, one has to make a decision whether or not to turn off the computer. If you turn off the computer, you may destroy potential evidences in the RAM memory of the computer. For example, in many Internet intrusion related cases, much of the evidence existed only in the RAM memory of the computer. Thus, we need tools extract digital evidences from RAM in a running operating system environment. What tools might allow one to capture certain states of memory? So far we have not found many available tools to help us accomplish this task.

  One idea is to write a simple OS that requires very small memory, whose only job is to dump all of data in RAM, including deleted and slack space, to an external device.

Perhaps this OS might be stored and invoked from a floppy disk.

Another idea may be to write a program that will dump all free blocks from the storage media to an external device prior to putting the machine in hibernation mode. This should allow preservation of forensically-interesting file slack space as well as the cached data from RAM.

- Apply Fuzzy Logic to SNORT

  SNORT's detection system is based on rules. We can apply fuzzy logic techniques to fuzzify detection rules used in SNORT. Linguistic variables can be used to specify more human readable rules that are more flexible and realistic than the current rules in SNORT.

  With these new rules, artificial intelligence can then be used to detect potential attacks in a network environment.

3.2.6 A Different Approach to Lab Component of Grad Course

The lab experience for the graduate curriculum is expected to be more self-directed than that of the undergraduate lab experience. Where the undergraduates will be provided with something of a "cookbook" approach – provided with a general outline and expected outcomes, the graduate labs will be open to student interpretation.

In keeping with the different goal of the Graduate course, the programming component of the lab experience will provide a deeper understanding of the complexities of forensic evaluation. Rather than being expected to use and rely on tools developed by others, the graduate lab work will involve the development of new digital forensic evaluation tools. This change in focus, from tool *use* to tool *development* will more deeply involve graduate students in a research role. It will also provide for personal development and an opportunity to learn much more about whichever portion of digital forensics piques their interest. Research areas are self-selected by the students.

4. CONCLUSION

In this paper, we presented our procedures and rationale in developing graduate and undergraduate computer forensics courses. The undergraduate course will be offered in the spring of 2004 with the graduate course soon to follow. After taking both the undergraduate and the graduate courses, students will be at the forefront of computer forensics investigations. They will be able to apply commercially available tools along with their own investigative techniques to forensic evaluations of digital data. They will also be capable of develop their own tools to handle new, unique, or peculiar cases. The Graduate course will be included in the curriculum of a future Master degree program in the department concentrating on computer security.

We know that forensics courses have been developed and are currently being offered in many universities. To the best of our knowledge these courses are still covering computer forensics technologies and utilizing available tools. We hope that our Graduate course, with it's tool development focus, will initiate a new direction in the forensics education area.

5. ACKNOWLEDGMENTS

The authors would like to acknowledge both Professor Sharon Mason, the course development leader, and Professor Peter Lutz, who has contributed to the development of the graduate course.

6. REFERENCES

[1] Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, NY, 2000.

[2] Casey, E. Handbook of Computer Crime Investigation: Forensic Tools and Technology. Academic Press, NY, 2002.

[3] Kaufman, C., Perlman, R., and Speciner, M. Network Security: Private Communication in Public World. 2nd Edition. Prentice Hall, NJ, 2002.

[4] Kruse, W., and Heiser, J. Computer Forensics: Incident Response Essentials. Addison-Wesley, Boston, 2002.

[5] Marcella, A., and Greenfield, R. Cyber Forensics: A Field for Collecting, Examining, and Preserving Evidence of Computer Crimes. Auerbach Pub, New York, 2002.

[6] Northcutt, S., and Novak, J. Network Intrusion Detection. 3rd Edition. New Riders, Boston, 2003.

[7] Pipkin, D. Halting the Hacker: a practical guide to computer security. 2nd Edition. Prentice Hall, NJ, 2002.

[8] Rehman, R. Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID. Prentice Hall, NJ, 2003.

[9] Schultz, E. and Shumway, R. Incident Response: A Strategic Guide to Handling System and Network Security Breaches. New Riders, Boston, 2002.

[10] Shinder, D., and Tittel E. Scene of the Cybercrime: Computer Forensics Handbook. Syngress Publishing, MA, 2003.

[11] Skoudis, E. Counter Hack: A Sep-by-Step Guide to Computer Attacks and Effective Defenses. Prentice Hall, NJ, 2002.

[12] Wolfe, H. Encountering Encrypted Evidence (potential). In Proceedings of the Informing Science + IT Education Conference (June 19-21), 1601-1607.