AC 2008-129: BUILDING AN EDUCATION PROGRAM FOR ENGINEERS IN DIGITAL FORENSICS

David Dampier, Mississippi State University

Building an Education Program for Engineers in Digital Forensics

David A. Dampier
Jansen Cohoon
Department of Computer Science and Engineering
Mississippi State University
dampier@cse.msstate.edu; jec9@msstate.edu

Abstract

This paper describes an innovative laboratory based program that offers life-long learning activities to working professionals in the law enforcement community while simultaneously including students at the undergraduate and graduate levels in digital forensics service, learning and research. The program has been highly successful with involvement of PhD students, Master's level students, and undergraduates who are focusing on the computer security/digital forensics area of interest. Computer crime is a rapidly growing problem throughout the connected world. Not only are computer crimes becoming more numerous and commonplace, the sophistication of computer criminals is also increasing. As technology has increased in sophistication, and criminals have exploited new technologies, computer forensics investigators trying to solve those crimes have had to learn new techniques. This trend has necessitated the inclusion of new classes in computer science and criminal justice programs.

At Mississippi State University, the Center for Computer Security Research, with the assistance of the Mississippi Attorney General's Office and others developed a digital forensics training program that provides no-cost training to law enforcement officers throughout the Southeast United States in subjects ranging from basic computer skills and introductory courses in cyber crime to very advanced commercial training in using the most sophisticated investigative and analysis software available. Law enforcement officers have been very receptive to this program, with over 1400 law enforcement officers from over 200 departments in 18 states taking advantage of the training. Students in computer science, software engineering and computer engineering programs at Mississippi State University have also benefited from this program. An introductory course in computer forensics has been standing room only for the last several years, and advanced graduate classes in digital forensics are also very popular.

Funding for this center is provided by the United States Department of Justice, and has not only supported the forensics training center, but has also helped to establish a one-of-a-kind Cyber Crime Fusion Center in Jackson, Mississippi, where law enforcement agents from Federal, State, and local law enforcement agencies as well as students and staff from Mississippi State University work together to solve computer crimes. Additionally, the support has enabled Mississippi State University to build a world-class digital forensics laboratory that can be used by researchers, law enforcement agencies, and students alike to experiment with new technologies and build a foundation for pursuing digital forensics as a profession. This paper describes the center, as well as provides evidence of the proven value of such work for the university and the nation.

Introduction

As the world becomes increasingly more dependent on automation and the internet, and computer users are increasingly more comfortable with advanced technology, computer usage by criminals is increasing. One of the fastest growing crimes in the United States is Identity Theft[1], and although identity theft is not necessarily committed using a computer, the increase in electronic commerce has certainly increased the opportunities for internet savvy criminals to take advantage of unsuspecting computer users. As computer related crime increases, the need for investigators and evidence analysts who understand computer evidence must grow to meet the demand. Computer investigation is a relatively young field in law enforcement. The FBI first began to look at computer evidence around 1984[10], about the same time that personal computer usage began to become more commonplace. In the beginning, the techniques used by computer crime investigators were home grown and mostly ad hoc. They used what they knew, and as they gained experience, they built more sophisticated tools. In many cases, because an investigator happened to know something about computers, they were tasked to examine any computer evidence that came in. This capability continued to grow from the bottom up until very recently. Universities in the last five or six years have begun to look at digital forensics as a rich new source of education and research opportunities. Students love the field, and as a result classes offered are always full or overfull and research programs are growing with new ideas coming very rapidly.

The federal government has been able to develop and maintain excellent facilities for training federal agents in computer related crime. Facilities such as the FBI academy in Virginia and the Federal Law Enforcement Training Center in Georgia provide free training for law enforcement, but their capacity is insufficient to make a real impact at the local level across the United States. Regional Computer Forensics Laboratories (RCFL) provide some free training for local and state law enforcement, but require a commitment of time to the RCFL in exchange. Additionally, there are a number of government sponsored and commercial training organizations, like the National White Collar Crime Center that provide excellent training opportunities for law enforcement investigators. These organizations provide excellent training, but training is not education. What is needed is a commitment to education in the field of digital forensics that encourages innovation and creativity, and embraces life-long learning. Academia is able to help in the digital forensics field by providing more sophisticated tools and equipment. Even commercially available equipment has addressed the need but further innovation could be spurred from the academic community. For example, a research project at Mississippi State University using Field Programmable Gate Arrays was able to produce a tool that will image a hard drive, nearly, twice as fast as any commercial hard drive duplicator, and will perform some limited analysis as it images.[7] Academia's vast instructional and research resources should be used in any way possible to combat digital crime.

Justification of Need

Mississippi State University (MSU) and its Center for Computer Security Research (CCSR) developed a survey in 2003 (sent to 82 county sheriff's offices, 22 district

attorney's offices, and the 20 largest municipal police departments in Mississippi) to quantify the State's computer crime problem and to determine state and local law enforcement's ability to address it. Of the 124 surveys distributed, 64 completed surveys were returned for a 52% response rate—quite good given that most mail surveys average well below a 50% response rate. While the primary goal was to generate a baseline and profile of the capability of local and county agencies to respond to computer-related crimes in their respective jurisdictions, the survey examined the degree to which local law enforcement agencies and prosecutors confront instances of cybercrime, what volume and types of cybercrime they have dealt with (if any), and how they went about investigating and prosecuting such crimes. The survey provided a unique quantified snapshot of the degree of experience and readiness to investigate and prosecute computer-related crimes in Mississippi. Of the 64 responding law enforcement agencies and district attorney offices, 79.7% had been involved in the investigation, arrest, prosecution or conviction of a computer related crime (CC). Agencies however, saw themselves as not well prepared and having little experience in dealing with computer-related crime. Only 10.9% (seven agencies) felt they were "very well prepared" to deal with CC, and 56.2% of the sample was not well prepared or totally unprepared to deal with computer-related crime. The data showed that 87.5% of the sample had little to no experience in dealing with computer-related crime. Nearly 60% of the sample somewhat or strongly agreed that computer related crimes are one of the fastest growing categories of crime in their jurisdiction. Agencies' self-assessments of how they deal with issues related to computer crimes were not encouraging. In general, law enforcement agencies in Mississippi were ill prepared to deal with computer-related crimes and nearly 80% somewhat or strongly disagreed that their agency had sufficient personnel trained to deal with computer-related crimes. Nearly 60% disagreed that they had procedures or practices to deal with computer-related crimes. Less than one-third regularly sent personnel to receive training in the area of computer-related crimes, and over half disagreed that they make computer-related crime investigation a priority. Over 90% of responding agencies at the county and local levels disagreed that Mississippi law enforcement was prepared to investigate computer crimes. Finally, we discovered that local law enforcement agencies have very restrictive budgets with little to no funding for training. [9]

Additionally, the federal law enforcement agencies like the Federal Bureau of Investigation and the Secret Service have been increasing their recruiting activities for employees skilled in digital forensics. An education program in digital forensics can not only provide potential state and local law enforcement agents with the proper skills, but many of these graduates can enter the federal service and contribute much faster to the digital forensics mission.

Increasing Training Capacity

After the survey mentioned in the previous section, it was obvious that we had a serious cyber crime problem in Mississippi. The Center for Computer Security Research (CCSR) at Mississippi State University developed a proposal to try and address the problems in the state of Mississippi and the southeast region. With a grant from the Department of

Justice in 2005, the Southeast Region Forensics Training Center (FTC) was established inside the CCSR to provide free training to law enforcement in the investigation and prosecution of computer crimes. The FTC is located on the campus of Mississippi State University in Starkville, Mississippi. It is housed inside the Department of Computer Science and Engineering. Its mission is to provide low or no cost training to the law enforcement community across the southeastern United States. Since the first class was offered in October 2005, the FTC has trained over 1400 law enforcement officers from well over 200 different departments in 18 different states. In addition, FTC facilities are used to teach computer science, computer engineering, software engineering, business information systems, and criminal justice undergraduate and graduate students these same skills.

The FTC currently maintains 18 workstations for interactive training of computer forensics. Students have access to forensics software such as: Access Data's Forensics Toolkit, Guidance Software's Encase Enterprise Edition, Paraben's Small Device Forensics, and many others. Additionally, various hardware devices used in computer crime investigation and forensics are maintained. This includes hardware imagers (ImageMasster, Logicube MD5 and Talon Devices), write blocking devices, Cell Phone Analysis kits (Paraben and Logicube's CellDEK TEK), and fully functional, portable forensics workstations. Additionally, the Mississippi Cyber Crime Fusion Center in Jackson provides a training facility as well as a research facility where graduate students can intern and gather real-time analysis data from a working forensics lab. We will talk more about that in the next section of the paper.

FTC Course offerings have grown over time. Initially, the only courses offered were the Introduction to Cyber Crime and the Forensics Tools and Techniques classes. Since 2005, course offerings available to law enforcement have increased five-fold. The following is a current list of courses offered to law enforcement professionals, including a brief description of each:

- *CF-100 Computer Basics*
  This course was developed by Jackson State University in partnership with the FTC and provides basic computer instruction for those law enforcement officers not comfortable with technology. It focuses on computers using the Windows operating system, and is designed to increase the capability of officers to attend and succeed in the follow on training. This course is optional, and is taught as needed.

- *CF-101 Introduction to Cyber Crime*
  This course provides a basic understanding of computer crime, a detailed breakdown of search and seizure techniques and crime scene "bag and tag" procedures, instruction on and introduction to some of the hardware and software available for computer forensics.

- *CF-102 Forensics Tools & Techniques*
  This course provides hands on training with tools and techniques used for

investigation and examination of computers in criminal cases.
Prerequisite: CF-101

- *CF-203 Practical Training in Forensic Investigations*
  This training is mentor-based training. It provides one-on-one instruction in a laboratory setting with an experienced computer forensics investigator. It provides an opportunity for an investigator who has been through the basic training classes to gain practical experience working on a real case for their agency. A "coach" is assigned to each student that guides them through a real investigation or examination of evidence for a case they are working.
  Prerequisites: CF-102

- *CF-204 Search and Seizure of Computers and Electronic Evidence: Legal and Testimonial Considerations for Law Enforcement*
  This course covers the legal aspects of search and seizure with respect to computer evidence. Warrant writing procedures and common pitfalls are discussed along with appropriate laws to govern computer crime. This course was developed by and is taught at the National Center for Justice and The Rule of Law at the University of Mississippi. Prosecuting attorneys are eligible to attend this training.

- *CF-205 Search and Seizure of Computers and Electronic Evidence: Legal Considerations for Trial Judges*
  This course will cover the legal aspects of search and seizure with respect to computer evidence, specifically for trial judges. Issues such as case law, legal precedent, and federal and state laws concerning computer crimes are discussed in a forum where judges are free to ask questions and seek advice from national experts on fourth amendment issues for computer related evidence.

- *CF-307 AccessData's BootCamp*
  Mississippi State University and AccessData, Inc. have partnered to provide law enforcement officers with free attendance in AccessData's Ultimate Toolkit BootCamp. This three day course provides detailed instruction on how to install, configure, and use AccessData's Forensic Toolkit (FTK) and Password Recovery Toolkit (PRTK). The training is identical to commercial training provided by Access Data to its corporate and government customers in every respect.
  Prerequisites: CF-102 or the equivalent

- CF-308 Paraben Small Device Forensics
  Mississippi State University and Paraben, Inc. have partnered to provide law enforcement officers with free attendance in Paraben's Small Device Forensics class. This four day course provides detailed instruction on how to recover data from cellphones and Personal Digital Assistants (PDAs) using the Paraben small device forensics software. The training is identical to commercial training provided by Paraben to its corporate and government customers in every respect.
  Prerequisites: CF-102 or the equivalent

- *CF-409 AccessData's Windows Forensics*
  This course is another three day course offered by AccessData, Inc. through the FTC. This class is a follow on course to the CF-307 training and concentrates on using the Ultimate Toolkit software to investigate a Windows system. It provides more detailed instruction on FTK and PRTK, as well as introduction to the Windows Registry Viewer. The training is identical to commercial training provided by Access Data to its corporate and government customers in every respect.
  Prerequisites: CF-307

- *CF-411 AccessData's BootCamp/Windows Forensics Week*
  Combines CF307 and CF409 into a one week course. These two courses are AccessData's ACE certification prerequisites.

- *CF-510 Macintosh Forensics Seminar*
  This course is taught by an expert in performing forensics examinations on Macintosh computers and is intended only for advanced students.
  Prerequisites: CF-307

The capability built by the FTC has also benefitted our academic course offerings. Active learning is an appealing method of instruction in academia. The laboratory facilities available because of the FTC have enabled us to make the university course offerings very active-learning based. Lectures are held right in the lab, and students are provided the opportunity to experiment with the tools immediately upon learning about them in the lecture.

An undergraduate computer forensics course was recently offered for the sixth time, and the number of students interested in taking the class was well more than the capacity of the classroom. A strict limit was required to enable the class to meet in the laboratory. The undergraduate course covers the basic computer forensics principles and offers laboratory assignments to provide hands on learning experience. Recently, Mock trials and seizure have been conducted outside of the university setting to give a real world feel.

Additionally, on three occasions, an advanced topics class in digital forensics has been offered, with the course content being different each time. The most recent offering was dedicated to building tools that could be made available to the law enforcement community that we support. The tools are required to fill a need in the forensics community and explain how the tool would aid in the forensics work flow.

Increasing Laboratory Capacity

In 2007, in partnership with the Mississippi Attorney General's office, the Federal Bureau of Investigation, the United States Secret Service, and others, we opened a one-of-a-kind laboratory facility in Jackson, Mississippi. The Mississippi Cyber Crime Fusion

Center (CCFC) was established to aid in the cooperation and collaboration among different law enforcement agencies investigating computer crimes in Mississippi. The CCFC brings together the FBI, Secret Service, US Postal Inspectors, Attorney General's Cyber Crime Center, as well as several state and local law enforcement agencies in one state of the art facility to investigate and prosecute computer crimes. The CCFC houses the cyber crime investigators, computer forensics examiners, the state and U.S. Attorneys involved in prosecuting computer crimes, as well as a branch of the FTC that conducts training in the facility.

Expanding Beyond Law Enforcement

In addition to training current law enforcement officers to solve computer crimes, the training capacity developed by the FTC has provided benefits to students at Mississippi State University. The laboratory at MSU, including the equipment and software, as well as the curriculum developed have enabled the sharing of computer forensics education to senior undergraduates and graduate students in computer science, software engineering, computer engineering, management information systems, and criminal justice programs. Courses include the basic Introduction to Computer Forensics course offered for three hours credit every Fall semester, and different special topics classes for graduate students in more advanced forensics technologies and research topics. The Introduction to Computer Forensics class has been offered six times since 2003, and since the law enforcement training was started has been enhanced tremendously by much more active learning activities. During the most recent semester, university students were tasked to create digital evidence, investigate and examine digital evidence, conduct bag and tag drills at a local mock city established for this purpose, and undergo both direct and cross examinations in a mock trial. This mock trial was designed to illustrate how the results of the investigations that they conducted are used to prosecute and convict a computer criminal. The mock trial involved practicing lawyers and a retired judge in the local county courthouse. The students would take the stand and then sweat it out under cross examination. The mock seizure was held at the Regional Counter Drug Training Facility in Meridian, Mississippi. The facility has several buildings that can be used to practice evidence collection. During the time there the students are either directly participating in evidence collection or watching other groups perform. The stress provided by these exercises are hoped to prepare them for future employment in the computer forensics field by giving them a more realistic experience of the practical application of a classroom subject. [8]

Research has benefited from the expanded capacity. Since the forensics program started, more than a dozen graduate students have used the forensics laboratory for experiments and research. The most successful work has been in evidence modeling [2, 3, 4], resulting in our first successful forensics PhD graduation in 2006. Additional research has been published in data hiding. [6]

Successes and Future Work

After our trip to the mock city at the Counter Drug Training Facility in Meridian, Mississippi, one of our undergraduate students said, "the five minutes of awesomeness was well worth the eight hour wait." The student was describing a staged first responder's scenario. The level of student participation was extraordinary. Every student participated in the voluntary event that took place on the weekend.

As the field continues to advance, the need for a more advanced undergraduate course will develop. Topics such as cell phone seizure, wireless network forensics, and Supervisory Control and Data Acquisition (SCADA) forensics will provide the basis for this class. This increased level of education will provide a more accomplished graduate.

In addition to the over 1400 law enforcement students that have gone through training courses at the Southeast Region Forensics Training Center, well over 200 university students have benefited from the training. Our efforts are paying off and should continue to pay off in the future. As the popularity of our program continues to expand, we expect the diversity of our course offerings to continue to expand.

References

1. Baum, K., "National Crime Victimization Survey: Identity Theft, 2005", *Bureau of Justice Special Report*, November 2007.
2. Bogen, A. and D. Dampier, "Knowledge Discovery and Experience Modeling in Computer Forensics Media Analysis," Accepted for publication in the Proceedings of the 3rd International Symposium on Information and Communication Technologies, June 16-18, 2004, Las Vegas, NV.
3. Bogen, A. and D. Dampier, "Preparing for Large-Scale Investigations with Case Domain Modeling," Proceedings of the 2005 Digital Forensics Research Workshop (DFRWS), New Orleans, LA, August 17-19, 2005.
4. Bogen, A. and D. Dampier, "A Software Engineering Modeling Approach to Computer Forensics Examination Planning," Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2005), Taipei, Taiwan, November 7-10, 2005.
5. Bogen, A., D. Dampier, and J. Carver, "Domain Modeling in Computer Forensics Examination: An Empirical Study", Proceedings of the 2007 Hawaii International Conference on the System Sciences, Minitrack on Digital Forensics, Waikoloa, Hawaii, January 3-7, 2007.
6. Cantrell, G. and D. Dampier, "Hiding Data through FAT 32 Boot Sector Manipulation," Proceedings of the 1st Annual IFIP Conference on Digital Forensics, Orlando, FL, February 13-16, 2005.
7. Dandass, Y, "Hardware-assisted Scanning for Signature Patterns in Image File Fragments," *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.
8. Vaughn, R., D. Dampier, and M. Warkentin, "Building an Information Security Education Program," Proceedings of The 2004 Information Security Curriculum Development Conference, Kennesaw, Georgia, September 17- 18, 2004.
9. Vaughn, R. and D. Dampier, "The Development of a University-based Forensics Training Center as a Regional Outreach and Service Activity", Proceedings of the 2007 Hawaii International Conference on the System Sciences, Minitrack on Digital Forensics, Waikoloa, Hawaii, January 3-7, 2007.

10. Whitcomb, C., "An Historical Perspective of Digital Evidence: A Forensic Scientist's View", *International Journal of Digital Evidence*, Vol. 1, Num. 1, Spring 2002.