Engineering Outreach to Law Enforcement

David A. Dampier[1] and Rayford B. Vaughn, Jr.[2]

Abstract – This paper describes an innovative classroom 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 4 PhD students, more than a dozen Master's level students, and several undergraduates who are focusing on the computer security/digital forensics area of interest.

Computer crime is a rapidly growing problem today in the U.S. and the rest of the world. Not only are computer crimes becoming more numerous and commonplace, but the sophistication of computer criminals is also increasing. When law enforcement officers first started investigating computer crimes in the 1980's, any police officer with a general knowledge of computers could investigate the crimes. Criminals had not yet developed the level of sophistication in place today, and the size of any digital media used to store data, actually potential evidence, was relatively small, and did not require sophisticated tools to investigate. Today's computers with potentially hundreds of gigabytes of storage space, and the availability of fairly sophisticated programs on the internet to hide that data, has forced computer crime investigators to look for extensive training in understanding and exploiting this technology. This trend has also necessitated 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 attend this training free of charge, but are also provided room and meals free of charge as well. The reception of this program has been tremendous, resulting in over 1000 law enforcement officers from over 200 departments in 12 states taking advantage of the training. The training has also resulted in increased convictions. At least seven criminal convictions can be traced directly to support received from the Mississippi State center.

Keywords: Digital Forensics, Cyber Crime, Law Enforcement Training

---

[1] Department of Computer Science and Engineering, PO Box 9637, Mississippi State, MS 39762, Dampier@cse.msstate.edu

[2] Department of Computer Science and Engineering, PO Box 9637, Mississippi State, MS 39762, vaughn@cse.msstate.edu

INTRODUCTION

As the world becomes both more dependent on computers and technology and more comfortable with computers and technology, computer usage by criminals is also increasing. Identity Theft is one of the fastest growing crimes in the United States [1], and although identity theft is not necessarily committed using a computer, the popularity of electronic commerce has certainly increased the opportunities for internet savvy criminals to take advantage of unsuspecting computer users. Computer examination for evidence of criminal activity 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. Early computer crime investigators were self-taught and mostly ad hoc. They used what they knew as computer users, and built home-grown tools for their investigations. As they gained experience, they built more sophisticated tools. This capability continued to grow from the bottom up until very recently. In 1995, a Secret Service survey estimated that approximately one half of all federal law enforcement agencies had some computer forensics capability, and those agencies handled over two-thirds of the computer evidence seized. [7]

The world is now very different. Most households in the United States have computers, and children are more capable of using computers at a very early age than most adults. It is rare to find a business in the U.S. that does not at least use a computer for record keeping. It is essential that law enforcement agencies understand computer crime, and have technically capable people available to investigate computer crimes and perform forensic examinations on computer evidence. Computer forensics has become a necessary skill in modern law enforcement. Federal, state and local agencies have all recognized its importance. However, having sufficient capability to train law enforcement officers to investigate and prosecute computer crimes is still an unsolved problem for most local agencies.

The federal government has been able to develop and maintain excellent facilities for training law enforcement to combat 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 many charge for those classes. Even if they do not charge for the training, it usually requires travel, including lodging and meals that local agencies cannot afford.

Training is not the only issue. Investigating computer crimes takes sophisticated equipment and resources. State and local agencies for the most part cannot possibly provide the resources needed to equip a computer forensics laboratory. Even if the money was available, the local leadership in these agencies will not likely understand the need or be able to justify the expenditure of limited funds for these labs. Many state agencies have developed their own capabilities, incorporating cyber crime investigation into an existing office or agency. Laboratories are then created using equipment that becomes available, or is seized from computer criminals convicted and sent to prison. Local agencies have started their own programs to deal with computer crime. Forming multi-jurisdictional teams or squads is prevalent among smaller agencies. Local agencies ban together across counties and cities to pool their resources to combat the rising incidence of computer crime.

Agencies at all levels that have dealt with computer related crime understand the amount of effort that is required for training, investigating and prosecuting. They understand the amount of

resources needed to maintain the proper technological capability. Software and hardware tools become obsolete and must be updated periodically. Case data must be preserved and archived. The technological edge must be maintained, because criminals are becoming more sophisticated. The bleeding edge of technology can bleed law enforcement agencies dry. Some of the same problems are present in the prosecutorial offices as well. In the state of Mississippi, the only agency with any real capability has been the state Attorney General's Cyber Crime Task Force. As a result, they have always suffered under a lengthy backlog of crimes to be investigated and computers to be analyzed. The need for additional capability in the state of Mississippi is apparent and definite, and it will only get more acute as time goes on. Mississippi is not the only state to be in this predicament.

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 personal 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]

INCREASING TRAINING CAPACITY

After receiving the results of the survey, it was obvious that we had a serious cyber crime problem in Mississippi. Since Mississippi State University had a capability to help, and is the Land-Grant school for the state, there was an implicit obligation to try to provide a remedy. The Center for Computer Security Research (CCSR) at Mississippi State University developed a proposal to receive funding 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 coast 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 1200 law enforcement officers from well over 200 different departments in 12 different states. In addition to free training, we provide lodging and food to law enforcement officers attending the training.

The FTC currently maintains two fixed location training rooms 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 is maintained. This includes hardware imagers (ImageMasster, Logicube MD5 and Talon Devices), write blocking devices, and fully functional, portable forensics workstations. Additionally, two 16-seat mobile instruction laboratories are available for taking the classes on the road.

These portable laboratories enable training to sometimes be brought to the students. The FTC has provided training to numerous agencies across the southeast United States in their facilities for their students. Agencies that are willing to recruit a classroom full of law enforcement students and provide the training facility are eligible to request a training team be sent on-site. On-site training has been provided in Alabama, Mississippi, Arkansas, and West Virginia. Additional training is already scheduled in Texas, Idaho, and Minnesota, and additional classes in California have been requested.

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 have increased five-fold. The following is a current list of courses, 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 only 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 One Day Seminar on Special Topics*

The FTC is continually looking for additional training opportunities that will provide an increased investigative capability among local law enforcement officers.

INCREASING LABORATORY CAPACITY

In addition to the training capability, the FTC has also attempted to increase examination and investigation capacity in Mississippi. A collaborative law enforcement investigative facility called the Cyber Crime Fusion Center has been built in Jackson, MS, and houses federal, state, and local law enforcement agencies cooperating in a cyber crime task force. This facility not only has an investigative capability, but also contains forensic laboratories that allow digital forensic examiners to examine digital evidence. The primary examination capability resides in the Attorney General's

Cyber Crime unit, but the Secret Service has a full time examiner in the facility and local forensic examiners have a workstation in the facility where they can come and work their own cases.

Additionally, through funds provided by the Department of Justice, the FTC has built seven smaller laboratories around the state. Two of these laboratories are nearly full capacity laboratories equivalent to the lab in the Cyber Crime Fusion Center, and five are strategically located miniature laboratories that provide local departments with the capability to examine their own digital evidence on site. These laboratories are also available to investigators and examiners from surrounding jurisdictions to use for their investigations.

SUMMARY

We have discussed a program of support and outreach to law enforcement through skills developed in the laboratory. In addition to training law enforcement officers to solve computer crimes, the training capacity that we have developed also benefits students at Mississippi State University. The expanded capability built to train cops has enabled us to enhance computer forensics education for our students. 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 five 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 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 also 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, 5], resulting in our first successful PhD graduation in 2006. Additional research has been published in data hiding. [6] As we learn more, we expand our ability to provide training to law enforcement and enhanced education for our students.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the support of the Center for Computer Security Research and the Department of Justice Office of Justice Programs.

REFERENCES

[1] K. Baum, "National Crime Victimization Survey: Identity Theft, 2005", *Bureau of Justice Special Report*, November 2007.

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

[3] M. Noblett, M. Pollitt, and L. Presley, "Recovering and Examining Computer Forensic Evidence", *Forensic Science Communications*, Vol. 2, Num. 4, October 2000.

[4] R. Vaughn 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.

[5] R. Vaughn, 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.

[6] A. Bogen 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.

[7] A. Bogen 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.

[8] A. Bogen 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.

[9] A. Bogen, 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.

[10] 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.

David A. Dampier

Dr. David Dampier is an Associate Professor of Computer Science and Engineering at Mississippi State University. He received his PhD in Computer Science from the Naval Postgraduate School in 1994. He currently serves as Director of the Southeast Region Forensics Training Center, responsible for teaching state and local law enforcement officers across the southeastern United States to solve computer crimes. He is a retired Army officer and 2003 winner of the ASEE-SE New Teacher of the Year Award. He served as President of the Software Engineering Division of the ASEE-SE and Secretary of the Instructional Division. His research interests are in Digital Forensics and Software Engineering.

Rayford B. Vaughn, Jr.

Dr. Vaughn received his Ph.D. from Kansas State University in 1988. He is a William L. Giles Distinguished Professor and the Billie J. Ball Professor of Computer Science and Engineering at Mississippi State University and teaches and conducts research in the areas of Software Engineering and Information Security. Prior to joining the University, he completed a twenty-six year career in the US Army retiring as a Colonel and three years as a Vice President of DISA Integration Services, EDS Government Systems. Dr. Vaughn has over 100 publications to his credit and is an active contributor to software engineering and information security conferences and journals. In 2004, Dr. Vaughn was named a Mississippi State University Eminent Scholar. He is the current Director of the MSU Center for Critical Infrastructure Protection and the Center for Computer Security Research.