Digital Forensics Workforce Training for Wounded Warriors

David A. Dampier[1], Kendall Blaylock[2], Robert Wesley McGrew[3]

Abstract – Mississippi State University has a long history of providing digital forensics training to law enforcement through its National Forensics Training Center. Since 2005, the NFTC has trained nearly 5000 law enforcement officers in the tools and techniques used to combat cyber-crimes. This training has been instrumental in the investigation of hundreds of computer crimes in Mississippi and throughout the U.S. In 2008, the NFTC initiated a project to provide digital forensics training to wounded warriors and veterans to facilitate a possible new career as they transition from the military to the civilian workforce. This training has been very well received, and has resulted in the successful training of nearly 500 wounded warriors in the three years of the project. The project continues into 2012 and we hope that we can continue the project into the future.

Keywords: Digital Forensics Training, Wounded Warrior Training

INTRODUCTION

This paper describes an effort at Mississippi State University (MSU) to provide tactical level occupational training to America's wounded warriors. We offer no-cost training at or near military hospitals that have warrior transition units. Often, wounded warriors can no longer work in their chosen career field, and are in need of skill retraining as they make the transition from their current military specialty either into a new military specialty or into a marketable civilian sector job. If they are not qualified to stay on active duty, the Veterans Administration has a number of programs that can assist these warriors, but what they lack are the training resources to get the training in a highly marketable skill. We offer that training in a very successful digital forensics training program targeting America's wounded warriors who may be able to fill critical Department of Defense jobs in the cyber security workforce. These warriors are still on active duty, but are currently undergoing medical processing to determine if they will be allowed to stay on active duty or be required to enter the civilian workforce.

This program builds on the success of a Department of Justice funded forensics training initiative for law enforcement at Mississippi State University [3, 4, 5, 11] and leverages the capability developed there. The USDOJ funding established the National Forensics Training Center in 2005 with the mission to address a training void in the law enforcement community by offering a suite of short, focused tactical level classes in the area of digital forensics at no cost to the law enforcement community. Additionally, to address the lack of a timely investigative capability, MSU worked with the FBI, Secret Service, Mississippi Attorney General, and others to create a *cooperative* Cyber Crime Fusion Center in a state of the art protected facility where Federal, State, and local cyber-crime investigators work together to jointly address investigations in a sharing and supportive manner. The NSF funding provided resources to expand the mission of the NFTC to provide digital forensics workforce training to disabled veterans and wounded warriors. While details of these initiatives are presented later, it is important to note that over the past five years, these programs have produced a meaningful digital forensics curriculum that nearly 5000 law enforcement officers and nearly 500 disabled veterans and wounded warriors have attended.

[1] Department of Computer Science and Engineering, Box 9637, 300 Butler Hall, Mississippi State, MS 39762, dad6@msstate.edu

[2] Department of Computer Science and Engineering, Box 9637, 300 Butler Hall, Mississippi State, MS 39762, kblaylock@cse.msstate.edu

[3] Department of Computer Science and Engineering, Box 9637, 300 Butler Hall, Mississippi State, MS 39762, rwm8@msstate.edu

The non-profit organization, Partnership for Public Service (with sponsorship from Careerbuilder.com), published its 2009 edition of the “Where the Jobs Are” report [9]. This report summarizes the federal government’s most critical hiring needs (by agency, occupation, and skills) through 2012. The Partnership surveyed 35 agencies representing 99 percent of the federal work force about their projected hiring needs. Over the next two years, the largest federal agencies project that they will hire nearly 273,000 new workers for “mission-critical” jobs. The number 2 professional field identified in this report was “security, protection, compliance, and enforcement” with a projection of nearly 53,000 new hires. Veterans have priority (referred to as “veteran’s preference” in the government human resources area) and are an excellent source of talent for these jobs if trained properly. The Department of Defense has a great need for workers skilled in digital forensics to work as cyber warriors in the law enforcement and intelligence fields, and their preference is always for former warriors who understand the environments in which they will operate. In addition to the government needs outlined in [9], there is a commercial industry need for digital forensics talent within corporate information technology organizations. These individuals are used to forensically investigate employee misbehavior or policy violations, to conduct intrusion *post mortem* investigations, and to perform data recovery tasks. Similarly, there is a job market for digital forensics work as a consultant or in private practice. These individuals are often called upon by legal counsel to obtain evidence in civil or criminal cases involving their clients, by private investigators searching for evidence, or by clients that require simple data recovery activities. Finally, we also have seen a documented need for this talent within the law enforcement community to address the rising incidence of computer crime. Our work with the law enforcement community over the last six years has shown a tremendous growth in the number of law enforcement personnel dedicated to working cybercrime issues, and that is exactly what this training is about.

While the field of digital forensics is relatively new within computing sciences and justice programs and has many research challenges associated with it – practitioners are applying the limited tool sets available today in civil, criminal, and private investigations. The field of digital forensics presents a rare opportunity to conduct leading edge research alongside those that practice the science in their daily jobs. This offers researchers the opportunity to perform empirically based research and to validate their proposed tools and techniques in a real environment. Mississippi State University has historically maintained a robust digital forensics research program coupled with its practitioner training program and uses the two efforts synergistically to validate research findings. Over the past five years, MSU and its Center for Computer Security Research (CCSR) (www.security.msstate.edu) has produced research results in digital forensics case modeling [1, 10], techniques to identify *Phishing* attackers [7], honeypot/honeynet techniques [8], forensic tool validation, wireless forensic techniques, Field Programmable Gate Array (FPGA) use in imaging and data capture [2,6], and investigating the use of scientific visualization techniques in digital forensics. The wounded warrior training activities give us a unique testing ground in which to test our new techniques, and introduce new technologies.

The training we offer through DoD warrior transition units gives wounded warriors a chance at a promising future by attempting to assist them in career retraining. Some of these warriors are staying on active duty in the military, while some are being released from active duty and will enter the civilian workforce. As a result of this training and potential follow up training available through the Defense Cyber Crime Center, some of these individuals will be able to enter the Defense Civilian workforce as civilian cyber warriors. Those that do not choose to work in the defense community can take the training provided through this initiative and bolster the capabilities of local, state, and federal law enforcement agencies, as well as civilian corporations employing digital forensics practitioners.[3]

It has been the authors’ intent to broaden the cyber career opportunities available to America’s wounded warriors that have become disabled in service to the nation that are from typically underrepresented groups. In this program, a very high percentage of the students have been from underrepresented groups, and we do not expect this to change.

The overall vision for this project has been to expand a highly successful digital forensics training program [11] and offer it as career transition training for wounded warriors through a cooperative arrangement with the Department of Defense. This permits MSU to enhance participation in cyber-infrastructure science and engineering by diverse groups of people (i.e., America’s veterans) and to address a government skill shortage in cyber-infrastructure talent.

National Forensics Training Center

As described in some of our previous papers [3, 4, 5, 12, 13], the MSU FTC has been offering highly specialized, skill based short courses designed specifically to provide technical skills to law enforcement. These courses are two - five day courses that are intensive, hands on, and tactical in nature. The current offerings can be seen at www.msu-nftc.org. Since 2008, the FTC has also been offering digital forensics training to disabled veterans and wounded warriors through a collaborative project with Auburn and Tuskegee Universities. Law enforcement courses offered by the FTC include:

Computer Forensics Primer: This is an 8 hour course designed to provide an introduction to computer forensics without some of the more technical aspects and exercises in other courses. It is an introductory level course that some law enforcement agencies find helpful in educating their officers in what can be done with digital forensics. This course does not, in itself, impart sufficient skill sets to perform forensics tasks, but teaches first responders how to handle digital evidence.

Introduction to Cyber Crime: This course is structured to provide a basic understanding of the elements of computer crime and contains detailed "bag & tag" legal instruction and an introduction to some of the hardware and software available to the forensics investigator needed in a computer forensics investigation. The course provides sufficient knowledge of the law to prevent the student from rendering the evidence obtained unusable in a court of law.

Forensics Tools & Techniques: This course is a follow on course to CF-101 and provides in-depth instruction on the tools and techniques used for investigation of computers in criminal cases. Actual use of digital forensics hardware (e.g., Logicubes, ImageMassters, and Airlite kits) and software (e.g., Encase, Forensics Toolkit, Coroner’s Tool Kit, and Unix/Linux tools) are taught to students. Hands-on exercises are incorporated to reinforce the skills taught.

Practical Training in Forensic Investigations: This course is a follow on to CF-102 and provides a hands-on experience in a working forensics lab with an active forensics examiner/investigator as a coach and mentor.

Search and Seizure of Computers and Electronic Evidence: Legal and Testimonial Considerations for Law Enforcement: This course covers legal aspects of search and seizure with respect to computer evidence. Warrant writing procedures and common pitfalls are discussed along with appropriate laws that govern the prosecution of computer crime.

Advanced Digital Forensics: This course is an introduction into advanced digital forensics concepts and investigation techniques. This course allows students to broaden their knowledge and expertise in the area of digital forensics. This is done through the combination of lecture and hands on exercises. This course is intended to provide a greater understanding of advanced digital forensics topics.

In addition to the courses offered above, the MSU FTC provides classes for prosecutors and judges, and periodically contracts for highly specialized training courses needed by law enforcement. Since 2008, the FTC has been providing career workforce training for America’s veterans and wounded warriors through the CI-Team program. The training provided in this project evolved from the law enforcement training shown above, and occurs in three tracks:

Track I: This track is structured to provide a basic understanding of computers and the elements of computer crime, and provides sufficient knowledge for the Track II instruction. Experienced computer users can skip this track and move on to Track II.

Track II: This track is a combination of the CF-101 and CF-102 courses taught to law enforcement without the emphasis on legal processes. The instruction is mostly hands-on and focuses primarily on the technical aspects of digital forensics.

Track III: This track is essentially identical to the CF-301 course described above. It provides an advanced look at what tools are available to the digital forensics practitioner, and sufficient hands-on experience with those tools for the student to be able to learn more advanced techniques on their own.

The FTC currently employs three full time staff members (instructors) and a part time administrative assistant. Additionally, the FTC employs graduate students with a research interest in digital forensics to assist with the classes and to gain exposure to practicing forensics investigators. Through the support provided under USDOJ funding, the State of Mississippi created and opened a Cyber Crime Fusion Center in its capital of Jackson MS. This center occupies 10,000 contiguous square feet of modern protected office space specifically designed as a digital forensics facility. Most importantly, it is staffed by Federal, State, and Local forensics investigators working together (includes the FBI, Secret Service, State Attorney General, U.S. Attorneys, Mississippi State University, and local police). It is this facility that offers practical experience training which is coordinated by the MSU FTC, as well as research opportunities for MSU students in a practical setting.

As we move forward with this project, we hope with additional support from the DoD, we understand that the current curriculum will need to be modified and expanded in order to accommodate the DoD's wishes for potential cyber warriors. DC3 has promised to provide the essential elements that must be added to the current three track curriculum, and these elements will include preparation for conducting digital investigations in the field, as well as network essentials that will allow the cyber warrior to conduct forensics over a network. Through this expansion of training offerings, we hope to provide additional opportunities for wounded warriors facing a future where they cannot continue their chosen profession. We hope to offer them the opportunity for careers involving the cyber-infrastructure of the United States. By modifying and leveraging the existing, successful digital forensics training program ongoing at MSU, we are confident that we can provide significant advantages to the government and provide a national capability with an excellent return on investment.

INTEGRATION OF RESEARCH AND LEARNING

Through this project we are developing a cyber-ready workforce at the university and we are increasing the number of practitioners in the digital forensics field through the integration of research and learning. The value of this project was demonstrated earlier in this paper with data provided by the Partnership for Public Service [9] and from our own experience with the National Forensics Training Center (FTC). We realize that such a program offers a unique opportunity to improve science in the field of digital forensics tools and techniques by allowing our researchers to work more closely with current practitioners and future investigators as we train them and develop relationships with the students. In the past, we integrated our graduate students and their research into our law enforcement digital forensics classes in order to validate their work and to gain a greater understanding of the work required. A major example of this was a PhD dissertation titled *"Selecting Keyword Search Terms in Computer Forensics Examinations Using Domain Analysis and Modeling"*, by Dr. Christopher Bogen [1]. In this work, Dr. Bogen developed a method of domain modeling for digital investigation. He validated this work in several case studies performed with students that had participated in the FTC training and by working with the State of Mississippi Attorney General's Cyber Crime Task Force for an extended period of time (an opportunity made available only due to their involvement in the FTC program). As a result of this integrative activity, Dr. Bogen was able to better validate his work. A second dissertation was defended last summer following Dr. Bogen's work in modeling for forensics, and that work was also done in the Cyber Crime Fusion Center. We have also integrated Master's degree student research in our FTC classes – particularly in the areas of wireless forensics and tool effectiveness. In these projects, MS students completed their required graduate level research activity working with FTC resources and students. We also have an ongoing long-term research effort to integrate Field Programmable Gateway Array (FPGA) technology into new and needed digital forensics tools [2, 6]. As we conduct research in the FTC, we can continue to expand the training program and increase the diversity of the student base, and we can continue to provide more validation opportunities for graduate students.

SUMMARY

In this paper, we have described a highly successful effort to provide workforce transition training to America's wounded warriors. This effort evolved from a highly successful law enforcement training program at Mississippi State University's National Forensics Training Center, and is continuing into the next year with existing funding. We are hoping that additional funding requested through the National Institutes for Standards and Technology will support the effort even further into the future. The hands-on, practical, tactical level training provided in this project is uniquely suited to wounded warriors and has been well received thus far. The warriors are learning and discovering that a career in digital forensics may provide them with a future, where the military may not be able to. This effort is good for the country, good for the wounded warriors, and good for Mississippi State University.

REFERENCES

[1] Bogen, C., *"Selecting Keyword Search Terms In Computer Forensics Examinations Using Domain Analysis and Modeling"*, PhD dissertation, Mississippi State University, December 2006. Available at http://library.msstate.edu/content/templates/?a=73.

[2] Condi, S. and Dandass, Y., "Scanning workstation memory for malicious codes using dedicated coprocessors", Proceedings of the 44th ACM Annual Southeast regional conference, 2006, ISBN:1-59593-315-8, pp. 661 – 666.

[3] Dampier, D. and J. Cohoon, "Educating Tomorrow's Digital Forensics Examiners", Innovations 2008, INEER, July 2008, pp. 273-282.

[4] Dampier, D. and R. Vaughn, "Hands-On Discovery Learning in Computer Security and Forensics," Proceedings of the 2009 International Conference on Engineering Education and Research (ICEER), Seoul, Korea, August 25-28, 2009.

[5] Dampier, D., "Building an Education Program for Engineers in Digital Forensics," Proceedings of the 2008 ASEE Conference, Pittsburgh, PA, June 22-25, 2008.

[6] Dandass, Y. "Hardware-Assisted Scanning for Signature Patterns in Image File Fragments", Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences (HICSS-40), P. 268, Waikoloa, Hawaii, January 3-7, 2007.

[7] McRae, C. and Vaughn, R., "Phighting the Phisher: Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks", Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences (HICSS-40), Waikoloa, Hawaii, January 3-7, 2007.

[8] McRae, C., McGrew, R. and Vaughn, R., "Honey Tokens And Web Bugs: Developing Reactive Techniques For Investigating Phishing Scams", Journal of Digital Forensic Practice 1 (03), September 2006, pp. 193-199.

[9] Partnership for Public Service, "Where the Jobs Are – Mission Critical Opportunities for America", 3d ed, 2009, available at: http://data.wherethejobsare.org/wtja/home

[10] Tanner, A. and D. Dampier, "Concept Mapping for Digital Forensics Investigations," *Advances in Digital Forensics V*, **2009**.

[11] Vaughn, R. and D. Dampier, "The Development of a University-Based Forensics Training Center as a Regional Outreach and Service Activity", Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences (HICSS-40), Waikoloa, Hawaii, January 3-7, 2007.

[12] Vaughn, R. and D. Dampier, "A Discovery Learning Approach to Information Assurance Education", Proceedings of the 2009 Hawaii International Conference on the System Sciences, Minitrack on Digital Forensics, Waikoloa, Hawaii, January 5-9, 2009.

[13] Vaughn, R. and D. Dampier, "Outreach, Teaching and Research Facilitated by a Forensics Training Center in Direct Support of Public Safety and Criminal Justice," International Journal of Computers and their Applications (IJCA), Vol.16, Num. 2, June 2009.

David A. Dampier

Dr. Dave Dampier is a veteran of 20 years in the U.S. Army, and currently serves as Associate Professor of Computer Science and Engineering at Mississippi State University. He also directs the university's Center for Computer Security Research and the National Forensics Training Center. He teaches information security and digital forensics courses, and his research interests are in the areas of digital forensics and the application of software engineering to the development of tools for digital forensics.

Kendall Blaylock

Kendall Blaylock received his Masters and Bachelors degrees from Mississippi State University. After graduating from MSU he then went on to work for the National Forensic Training Center at MSU. At the NFTC Kendall is currently serving as a Research Associate III. As an instructor for the NFTC Kendall provides training for law enforcement officers and Military Veterans. In addition to being an instructor for the NFTC, he also oversees and conducts research projects at the NFTC.

Robert Wesley McGrew

Robert Wesley McGrew is a full-time instructor at the National Forensics Training Center and Ph.D. student at Mississippi State University. He teaches digital forensics to law enforcement and armed-services veterans at the NFTC, performs and directs research on new computer security and forensics techniques, and develops new tools for practitioners in these fields.