3-2009

A University-based Forensics Training Center as a Regional Outreach, Education, and Research activity

Rayford B. Vaughn

David A. Dampier
Marshall University, dampierd@marshall.edu

Recommended Citation
Vaughn, R. and D. Dampier, "A University-based Forensics Training Center as a Regional Outreach, Education, and Research activity," Journal of Systemics, Cybernetics, and Informatics, Vol. 7, Num. 2, 2009, pp. 23-28.

A University-based Forensics Training Center as a Regional Outreach, Education, and Research activity

Rayford B. Vaughn, PhD
Center for Computer Security Research
Department of Computer Science and Engineering
Mississippi State University
vaughn@cse.msstate.edu

and

David A. Dampier, PhD
Southeast Region Forensics Training Center
Department of Computer Science and Engineering
Mississippi State University
dampier@cse.msstate.edu

Abstract

This paper describes a university-based Forensics Training Center (FTC) established by a Department of Justice grant for the purpose of improving the ability of state and local law enforcement in the Southeastern part of the United States to address the rising incidence of computer based crime. The FTC effort is described along with supporting evidence of its need. The program is not only a service activity, but also contributes to the Mississippi State University (MSU) security program pedagogy, and research effort.

Keywords: Digital Forensics Training

1. Introduction

In 2003, the computer security program at Mississippi State University (MSU) expanded and introduced a digital forensics and computer crime class to meet a growing need for that talent base in government and industry. It quickly became apparent that such a program was also needed by law enforcement practitioners and members of the judiciary in our State and those surrounding. This was made clear to the authors by discussions initiated by our State Attorney General and later by the FBI Special Agent in Charge for Mississippi. Simultaneously, graduate students taking challenged to address this concern and is hampered by a lack of training, tools, and critical facilities necessary to counter this form of criminal activity. For example, in our own State in 2004, the Attorney General had a small Cyber Crime Center with one Forensics examiner who had a 15 month backlog in cases to be worked. The office was funding challenged, located in substandard facilities, and had very little opportunity for training. The head of this Center visited the authors and offered to partner in an effort to improve both our instruction and the ability of the State to address computer crime. The State of Mississippi has seen a rising incidence of computer based criminal activity and a the semester long digital forensics course began to find ideas for research projects and had a strong desire to complete their Masters or PhD research in that area. While most universities value research, service and teaching (albeit with different weights attached to each), our forensics program began to show that one could have a single thread through all three objectives. This paper overviews how our program made substantial progress in service to our state and region, introduced an exceptionally popular course offering (taken by undergraduates and graduates from two different colleges), and developed a strong research focus.

It was apparent to us that the Federal government had excellent training facilities but these were directed toward federal agencies for the purpose of training their employees in the tools and techniques needed to address the rising incidence of computer crime. These facilities included the National White Collar Crime Center (NW3C), the Department of Defense Cyber Crime Center, the FBI Regional Computer Forensics Laboratories, the Internal Revenue Service (IRS) forensics training program, Federal Law Enforcement Training Center, and others. To a lesser extent, some state law enforcement organizations had limited training available to them such as the Regional Computer Forensics Group (RCFG) headquartered in the Fairfax, Virginia area. While there is growing concern with computer crime activity, law enforcement at the state and local levels (particularly in many rural areas) remains shortfall in trained law enforcement officials to address this increase. There are several contributing factors to this shortfall, which include a lack of funding for training, a lack of facilities and equipment, the rural nature of the State and its communities, and the lack of technical expertise within its State and local law enforcement and judicial organizations. This combination of events – the development of a forensics training program, the population of our labs with substantial equipment and software, the needs expressed by our state judicial officials, and our own indications that State and local law enforcement was in need of specialized training in digital forensics led us to embark on a path

to set up a specialized "center" in cooperation with others that would be dedicated to providing no-cost, easily accessible digital forensics and computer crime law training to the judicial and law enforcement communities in our state and region. In planning for the center that we envisioned, we chose to follow the model of training used by the Regional Counter-drug Training Academies (see http://www.rcta.org) where the training, room, and board are provided at no charge to the students and the only cost incurred is transportation to and from the training site. To accommodate this plan, we developed a strategy that involved first acquiring evidence of need followed by presenting that need to funding sources that might be helpful in getting such a program started. The remainder of this paper describes these activities and the program as it exists today – the MSU Southeast Region Forensics Training Center. The SE FTC has today trained over 1000 students from the law enforcement community in 12 states across the southeast U.S.

2. Establishing the Need

While we have published this data before [1], we include it here for the sake of explanation and completeness. Given the dearth of information on the issue of how well state and local law enforcement is prepared to deal with computer crime, in October 2003, the Center for Computer Security Research (CCSR) developed a mail survey which was sent to 82 county sheriff's offices , 22 district attorney's offices, and 20 of the largest municipal police departments in Mississippi. 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. A total of 16 (80%) of the municipal police departments responded, 38 (46%) of County Sheriff's offices responded, and 10 (45%) of DA's offices responded. 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. In addition, the project 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. We were also interested in any protocols local law enforcement agencies have developed for responding to computer-related crimes, and the degree to which they necessarily involved state or federal agencies due to a lack of experience, expertise, and/or resources necessary to investigate and prosecute these crimes.

The survey provided a unique 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% have been involved in the investigation, arrest, prosecution or conviction of a computer related crime.

Agencies saw themselves as not well prepared and having little experience in dealing with computer-related crime. Table 1 shows only 10.9% (seven agencies) felt they were "very well prepared" to deal with CC, and that 56.2% of the sample was not well prepared or totally unprepared to deal with computer-related crime. As the majority of local law enforcement agencies had only encountered a few cases involving computer crimes, it is not surprising that Table 2 shows that 87.5% of the sample has a little to no experience in dealing with computer-related crime, only two agencies claim to have "a great deal of experience", and six agencies claimed "quite a bit of experience" with computer-related crimes.

Table 1. How well is the agency prepared to deal with CC?

Variables	Very well prepared (4)		Somewhat prepared (3)		Not well prepared (2)		Totally unprepared (1)	
	N	%	N	%	N	%	N	%
how well agency prepared to deal with CC	7	10.9	21	32.8	26	40.6	10	15.6

Table 2. How much experience does your agency have in dealing with CC?

Variables	A great deal of experience (4)		Quite a bit of experience (3)		A little experience (2)		No experience (1)	
	N	%	N	%	N	%	N	%
how much experience does your agency have in dealing with CC	2	3.1	6	9.4	43	67.2	13	20.3

Table 3. Frequency of computer-related crimes

Variables	Strongly agree (4)		Somewhat agree (3)		Somewhat disagree (2)		Strongly disagree (1)	
	N	%	N	%	N	%	N	%
CC are one of the fastest growing categories of crime in our jurisdiction	10	15.6	28	43.8	18	28.1	8	12.5

Table 3 shows that nearly 60% of the sample somewhat or strongly agreed that computer related crimes were one of the fastest growing categories of crime in their jurisdiction. Agencies' self-assessments of how they dealt with issues related to computer crimes were not encouraging (see Table 4). In general, law enforcement agencies in Mississippi were ill prepared to deal with computer-related crimes. Nearly 80% somewhat or strongly disagreed that their agency had sufficient personnel trained to deal with computer-related crimes, and nearly 60% disagreed that they had procedures or practices to deal with computer-related crimes. Less than one-third regularly send personnel to receive training in the area of computer-related crimes, and over half disagreed that they make computer-related crime investigation a priority. One should observe that over 90% of responding agencies at the county and local levels disagreed that Mississippi law enforcement was prepared to investigate computer crimes. Among the responding agencies, it appeared that state-level agencies (DA's offices) were better prepared to investigate and prosecute computer-related crimes than were local agencies.

As shown in Table 5, agencies felt that Mississippi should train more people to investigate and prosecute computer-related crimes (78.1% strongly agreed), computer-related crimes should be punished much more severely than they are currently (83.6% strongly or somewhat agree), and that special multi-jurisdictional task forces are necessary to investigate and prosecute computer-related crimes (82.3% strongly or somewhat agreed).

Table 4. Assessment of agencies' preparedness for dealing with computer-related crimes

Variables	Strongly agree (4)		Somewhat agree (3)		Somewhat disagree (2)		Strongly disagree (1)	
	N	%	N	%	N	%	N	%
Our agency has sufficient personnel trained in the area of CC to deal with cases of that sort	-	-	13	20.3	17	26.6	34	53.1
Our agency has established cooperative procedures and protocols with other agency to address CC	8	12.5	21	32.8	17	26.6	18	28.1
Our agency regularly sends personnel to receive training in the area of CC	4	6.3	16	25	14	21.9	30	46.9
Our agency is not currently trained or staffed to deal with CC	15	23.4	14	21.9	14	21.9	21	32.8
Our agency has made investigation and/or prosecution of CC a priority	3	4.7	24	37.5	23	35.9	14	21.9
Most local law enforcement agencies in MS are prepared to investigate CC	-	-	5	7.9	31	49.2	27	42.9
Most county-level law enforcement agencies are prepared to investigate CC	-	-	4	6.3	30	47.6	29	46
Most state-level law enforcement agencies are prepared to investigate CC	8	12.5	33	51.6	15	23.4	7	10.9

Table 5. What should be done to handle computer-related crimes?

Variables	Strongly agree (4)		Somewhat agree (3)		Somewhat disagree (2)		Strongly disagree (1)	
	N	%	N	%	N	%	N	%
MS should train more people to investigate and prosecute CC	50	78.1	12	18.8	1	1.6	-	-
CC should be punished much more severely than they are currently	21	34.4	30	49.2	7	11.5	3	4.9
Special multijurisdictional task forces are necessary to investigate and prosecute CC	28	45.2	23	37.1	8	12.9	3	4.8

While nearly 60% of responding agencies agreed that computer-related crimes are one of the fastest growing categories of crime in their respective jurisdictions, and the vast majority (some 80%) of Mississippi agencies in this study confronted computer-related crimes, the majority of these agencies were not prepared to do so. Most agencies have no personnel trained to handle such crimes, do not have established protocols or procedures for addressing them, and have not made the investigation or prosecution of such crimes a priority. In fact, the majority of responding agencies transfer such cases to another agency because they lack the training, expertise, and resources to deal with them in-house.

The survey defined a clear need for training to assist State and local law enforcement in addressing digital crime and provided quantifiable data needed to make the case to funding agencies of the need for digital forensics training and assisted in acquiring the support of the judicial and law enforcement community for such a capability.

3. Creation of the Forensics Training Center (FTC)

Once the need was established with the survey results described in Section 2, the authors then proceeded to develop the necessary partnerships between academia, federal, state, and local authorities that would be necessary for the center to effectively address the computer crime initiative – in terms of organization, capability, training and funding.

3.1. Organization and Mission of the Cyber Crime Fusion Center

After several planning meetings with the FBI Special Agent in Charge for the State of Mississippi and representatives of the State Attorney General's Office it was clear that organizationally we needed to address two distinct areas – the first was the creation of an operational digital forensics investigation capability exceeding that currently available in the State and second was initiating a training program for local and state law enforcement. The primary responsibility for digital forensics investigation in the State was vested in the Attorney General's office – with only one computer forensics investigator on the staff. The FBI, Secret Service, and US Postal Inspectors also had forensics investigators – but all at separate locations. Our sister university, the University of Mississippi School of Law, also had a strong interest in computer crime – albeit from the perspective of search and seizure and the law itself. This interest was manifested in their National Center for Justice and Rule of Law (http://www.ncjrl.org).

Over the course of one year, a memorandum of agreement (MOA) was developed for the creation of a Cyber Crime Fusion Center as the needed operational entity and its location was chosen to be in the State capital in 10,000 square feet of recently renovated State office building space. The MOA was initially signed by MSU, the Attorney General's Office, and the FBI and outlined the agreement to work together in a single facility, share equipment and expertise, and to provide for day to day management. Later, the agreement was also accepted by many others to include the Federal Attorneys in Mississippi, the Secret Service, US Postal inspectors, and the Jackson Police Department. This effort resulted in (we believe) the first center of this kind in the US – a combined Federal, State, and Local facility collectively sharing resources to employ digital forensics techniques in computer related crime investigation. The center began operation officially in 2007.

3.2. Forensics Training Center Service Offerings

To get the training program started, two pilot workshops were run in 2004; one on campus at Mississippi State University and the other in Jackson, MS. These workshops were used to gauge interest in the training on the part of law enforcement agencies as well as to determine an appropriate level of training to best meet their needs. As a result of these pilot workshops, a curriculum was developed and a former graduate student was hired with an expertise in digital forensics to be the primary instructor. The first few offerings of the basic classes enabled us to refine the curriculum and provide a more effective introductory capability. Additionally, we learned that "word of mouth" advertising would not be sufficient to get the officers in the seats. A concerted effort after the first quarter of offerings increased attendance significantly, enabling to surpass our first year goal of 200 students within 9 months. By the end of the first year, over 350 students had taken our classes, and now after the first two years, we have served over 1000 law enforcement professionals from over 200 different departments in 12 different states.

All classes and registration procedures for SE FTC training for law enforcement can be found at http://www.security.msstate.edu/ftc. The FTC initially established three primary course offerings: CF 101 *Introduction to Cyber Crime*; CF 102 *Forensics Tools and Techniques;* and, CF 203 *Practical Training in Forensics Investigations***.** During the second year of operation, two additional classes were offered in cooperation with the National Center for Justice and Rule of Law at the University of Mississippi. These classes, CF 204 *Search and Seizure of Computers and Electronic Evidence:*

Legal and Testimonial Considerations for Law Enforcement and CF 205 *Search and Seizure of Computers and Electronic Evidence: Legal Considerations for Trial Judges***,** are directed to not only the law enforcement officer – but also attorneys and justices in the region. Since the initial offerings, classes have been expanded to include a Basic Computer Literacy course, a cell phone/PDA forensics class, specialized training in Forensics Tool Kit and other Access Data software. With about two years of full operation, more than 1000 law enforcement professionals have gone though the training thereby validating the need we established earlier. In fact, the authors were quite surprised to find that request for attendance were not only received from the Southeast Region (our target audience), but also from Texas, Minnesota, Ohio, West Virginia, Idaho, and other states. As a result of this need, we intend to move toward a National Consortium organization in the future and expand our program to other sites. We have also obtained funding from the Department of Homeland Security which will allow us to move this training into the commercial sector as well as offering it to attorneys in general practice.

3.3. Funding for the SE FTC

Obviously, funding for such a program as described in this paper becomes a concern and is substantial. We were able to obtain seed funding through Congressional appropriation based on our demonstrated and quantified need for the service. We elicited the support of the FBI, the Attorney General and our Congressional delegation and (based on the survey results described in section 2 of this paper) we made the case that a digital forensics training capability was at least a regional and perhaps a national need for State and local law enforcement. Funding was then acquired from the Department of Justice, Bureau of Justice Programs to initially develop and prototype the FTC as well as to partially support the creation of the Cyber Crime Fusion Center. Subsequent funding was achieved through competitive grant programs offered by the Department of Justice and from the Department of Homeland Security as part of a Critical Infrastructure Protection grant.

4. Implications for Student Instruction

Our first computer forensics class was offered as a trial course in 2003 and on a regular basis beginning in 2004. Initially considered mostly a lecture course with a few homework assignments, it quickly became apparent that a strong lab component was essential to student learning. As the SE FTC was built with external funding, we were able to populate our student lab with the same equipment we used for law enforcement students and simply shared facilities. This excited the students when they realized they were using the same software and hardware devices that actual practitioners were being trained on and our SE FTC students seemed to realize that they were receiving strong academic based training since our students were sharing there facility. Soon the class actually moved out of the classroom and into the lab facility shown in Figure 1 below.

Figure 1: Computer Forensics Training Facility

In addition, state of the practice tools were used with MSU students and with our SE FTC students. A sample of these tools is shown in Figure 2 below along with students exposed to this equipment.

Figure 2: Tool sets used for Forensics Training

Eventually, the academic version of the course became so popular that we considered offering it every semester and every time it was offered, it was oversubscribed. Over time we built substantial lab exercises for the students to give them challenging cases to work on, we involved real judicial authorities (lawyers and judges) in real courtrooms so the students could present their cases and be exposed to cross examination. A side effect of this training was that a certain amount of "expert witness" training resulted for our students. Lastly, we integrated a live fire exercise conducted at the Regional Counterdrug Training Academy (www.rcta.org) mock village where our students actually enter a mock crime scene and acquire evidence before criminals can delete it or hide it. The students are taught how to do this in a legal manner such that evidence is admissible in court. The key point here is that such training would not be possible without the strong cooperation of judicial authorities and law enforcement and that cooperation willingly comes because of the relationships developed through the SE FTC.

5. Impact on Research

Given the excitement generated by the class itself and the involvement of graduate students, we soon began to experience students bringing good research ideas to the authors and asking for guidance and direction in that research. The majority of this

research resulted in Master's degree projects, thesis, and one PhD dissertation.

One of the earliest efforts was performed by a Masters student who acquired several used hard drives from the popular online auction site eBay and explored each disk with commonly available forensics tools. After finding a significant amount of privacy related data, he reported on this in a project form. His findings were significant and demonstrated shortfalls in industrial practices to protect employee privacy as old hard drives are discarded. Interest in the results of this research was widespread and resulted in several presentations to major organizations and commercial companies.

Another Masters degree student became interested in hard drive wiping tools – both shareware and commercial products. She acquired several tools and examined disks with low level forensics exploration techniques after wiping the disk. She reported on shortfalls of each product – discovering that in every case, some residual data was left after wiping. She also reported that the best tool was a shareware product. This project had obvious useful data for practitioners in SE FTC classes.

Three faculty members teamed with one of the authors on a successful NSF Cyber Trust grant proposal to use scientific visualization techniques to aide in discovery of evidentiary data on a disk. This project is underway at the present and involves several graduate student research projects. It is expected that results of their work may have product potential.

A successful PhD student did his dissertation work on creating a model framework for forensics investigators. He validated his work through a cooperative effort with investigators in the Cyber Crime Fusion Center – an advantage that was made available through our outreach efforts and partnerships with the FBI and State Attorney General's Office. [2]

Last, a faculty member became interested in using FPGA devices as a method of performing line speed evidence identification while a disk is being imaged. By building an evidence pattern recognition capability into an onboard database – the FPGA device can check for specific patterns at line speed while the suspect disk is being imaged. This work is supported by an NSF grant and successful results have been reported. [3,4]

6. References

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

[2] Bogen, A., Selecting Keyword Search Terms in Computer Forensics Examinations with Domain Analysis and Modeling, PhD Dissertation, Mississippi State University, December 2006.

[3] Dandass, Y. S., "Hardware-Assisted Scanning for Signature Patterns in Image File Fragments," in Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS 2007), Waikoloa, Big Island, Hawaii, 2007.

[4] Dandass, Y.S., "Using FPGAs to Parallelize Dictionary Attacks for Password Cracking," to appear in Proceedings of the 41st Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa, Big Island, Hawaii, 2008.