Educating the Next Generation of Cyberforensic Professionals

Mark Pollitt, Philip Craiger

Chapter 22

EDUCATING THE NEXT GENERATION OF CYBERFORENSIC PROFESSIONALS

Mark Pollitt and Philip Craiger

Abstract This paper provides a historical overview of the development of cyberforensics as a scientific discipline, along with a description of the current state of training, educational programs, certification and accreditation. The paper traces the origins of cyberforensics, the acceptance of cyberforensics as forensic science and its recognition as a component of information security. It also discusses the development of professional certifications and standardized bodies of knowledge that have had a substantial impact on the discipline. Finally, it discusses the accreditation of cyberforensic educational programs, its linkage with the bodies of knowledge and its effect on cyberforensic educational programs.

Keywords: Digital forensics, education, certification, accreditation

1. Introduction

Cyberforensics, also referred to as digital forensics, computer forensics and multimedia forensics, has a relatively short history. A new science, it has displayed rapid growth for several reasons, perhaps the most important of which is the world's increasing reliance on technology for computing and communications. The field changes rapidly due to advances in technology. The most illustrative example is the smartphone, which, unlike cellular phones of the past, is essentially a small, but powerful, personal computer. Although smartphones were introduced about a decade ago, a recent study has found that nearly 60% of American adults own a smartphone [18]. Other new technologies, such as wearable computers (e.g., Google Glass [10]) and life-enhancing technologies (e.g., driverless cars [16]) will drive the need for educated, trained and certified cyberforensic professionals. This paper explores where the dis-

cipline of cyberforensics has been, its current state and what the future may hold.

The first question is: Is cyberforensics a scientific discipline? The best way to answer this question is to observe how other sciences are defined. We suggest the use of Thomas Kuhn's framework. In his book *The Structure of Scientific Revolutions* [15], Kuhn says that "normal science" is defined by a common paradigm. The paradigm is a shared set of theories, practices and models that are acknowledged by the community. The paradigm serves both a research purpose and an educational purpose. The former allows scientists the luxury of relying on a foundation of acknowledged principles, freeing them from having to build a foundation for every new research effort and having to re-articulate the basis of every single element of research. It also serves an important purpose in defining the things that a student must know in order to become a researcher or a practitioner. Ultimately, according to Kuhn, it is the combination of shared models, educational experience and discipline-specific language that define a mature science.

We posit that cyberforensics is a mature scientific discipline, notwithstanding the fact that as technology changes, so must the discipline. To support this argument, we offer brief histories of the practice of cyberforensics, the accreditation of cyberforensic laboratories and educational programs, and the certification of cyberforensic practitioners. Note that the term "accreditation" describes the process by which an external body determines that a particular, unit, laboratory or educational program meets the requirements of the education and/or practitioner communities, and "certification" is the attestation that an individual meets the standards of a competent practitioner.

2. Cyberforensics

It is difficult to identify the precise moment that the discipline of cyberforensics started. Perhaps it was shortly after the very first digital computer was invented. But the term "computer forensics" did not come into its own until the 1980s, when the Federal Bureau of Investigation (FBI) and the U.S. Internal Revenue Service (IRS) created small teams of agents to conduct searches of mainframe computers in connection with criminal cases. By the early 1990s, personal computers had become commonplace. Criminal investigators realized that computers were potentially a rich source of evidence. Local, state and federal agencies launched programs to exploit this potential source of evidence. The first training programs for what would be called "computer foren-

sic examiners" began at the Federal Law Enforcement Training Center (FLETC) in Glenco, Georgia [19].

During the mid 1990s, the explosion of the Internet facilitated many new computer-based crimes. In addition to computer and telecommunications fraud, child pornography became a law enforcement problem of unprecedented size. Online undercover operations, which sought to identify and prosecute subjects who were creating and exchanging child pornography, drove a massive need for cyberforensic examinations. Child pornography and all the other Internet-based crimes accelerated through the millennium and into the current era of global cloud computing [19].

Today, with the reality of ubiquitous mobile computing, cloud computing, social networks and other technologies, vast quantities of potential digital evidence are being produced at a phenomenal rate. The use of digital evidence in civil litigation has likewise exploded. Cyberforensic techniques and methodologies have become essential tools in information security and incident response. Cyberforensic examiners require broad and deep technical knowledge as well strong investigative skills.

3. Origins of Cyberforensics Training

A number of watershed events have steered the disorganized practice of forensics into a scientific discipline. Arguably, the creation of formal training and certification programs laid the first foundation for the discipline. In 1991, the International Association of Computer Investigative Specialists (IACIS) [11] was formed and it soon launched formal efforts to train law enforcement officers in conducting forensic examinations of computers. IACIS also created the first certification program for practitioners [19].

The establishment of formal law enforcement units to conduct digital forensic examinations also played a major role in the development of cyberforensics as a discipline. In 1992, the FBI created the Computer Analysis Response Team (CART) at the FBI Laboratory in Quantico, Virginia. This unit, along with similar units in the United States Secret Service (USSS) and the IRS would play important roles in the creation of stakeholder organizations that would develop standards for the nascent discipline. The FBI developed its own training unit and staff at the FBI Academy in Quantico, Virginia, while the USSS, IRS and others developed a robust training facility at FLETC in Glynco, Georgia [19].

In the late 1990s, commercial forensic tools became available. Vendors began to offer courses to train new users in the use of their tools and subsequently offered certifications such as EnCase Certified Examiner

(EnCE) [9] and Access Data Certified Examiner (ACE) [1]. Initially, these vendor certifications were the only certifications available outside of law enforcement agencies and other government organizations [19].

4. Cyberforensic Functional Standards

In 1995, some 20 agencies from countries such as the United States, United Kingdom, France, Australia, The Netherlands and Sweden set up the International Organization on Computer Evidence (IOCE) [13]. This organization would go on to develop and promulgate the principles on which standards would be built. The IOCE Principles were developed from principles originally proposed by the Association of Chief Police Officers (ACPO) from the United Kingdom. While the ACPO principles were important, in and of themselves, it was the international consensus obtained by IOCE that was revolutionary. It marked the first time that disparate organizations publicly acknowledged a shared view of the forensic examination process. In 2000, the Group of Eight (G8) Subgroup on High Technology Crime voted to accept the IOCE Principles, thus gaining political recognition of the consensus view of the digital forensic community [19].

In 1998, the Scientific Working Group on Digital Evidence (SWGDE) [20] was established. The stated goal of this organization was to develop standards for the governance of digital forensics within the United States. SWGDE also sought to have digital forensics identified as a legitimate forensic laboratory discipline. SWGDE worked with the Association of Crime Laboratory Directors – Laboratory Accreditation Board (ASCLD-LAB) [4] to make digital evidence an accreditable discipline for crime laboratories. In 2003, ASCLD-LAB accredited the first digital evidence unit. As of 2013, ASCLD-LAB had accredited 73 digital evidence laboratories.

Meanwhile, the European forensic science community developed its own working group called the European Network of Forensic Science Institutes – Forensic Information Technology Working Group (ENFSI-FITWG) [7]. This group continues to provide a forum for training and standards development [19].

Near the end of the first decade of the 21st century, the United States Government established the National Initiative for Cybersecurity Education (NICE) [17]. This initiative sought to identify the knowledge, skills, experience and academic preparation needed for the cybersecurity workforce. The resulting NICE Framework (Version 1.0) identifies seven functional specialty areas. One of the areas is "Investigative Specialty," which has a sub-area dedicated to cyberforensics. In 2013 and 2014,

NICE utilized focus groups from the stakeholder communities to further develop the core definitions and duties associated with each specialty area and sub-area. The first author of this paper participated in this activity, and he can attest that the functional standards described above were relied upon heavily in the focus group deliberations. Version 2 of the NICE Framework, incorporating the work of the focus groups, is expected to be promulgated in 2014.

5. Educational Program Accreditation

A number of organizations focusing on education, training and certification were established to ensure that practitioners would be knowledgeable in the principles and practice of cyberforensics. In 2006, the Technical Working Group on Education – Digital Evidence (TWGED-DE) was created by the National Institutes of Justice. This working group brought together academics (including the second author of this paper) and practitioners to develop a common understanding of the required knowledge and skills for digital forensic practitioners. TWGED-DE produced a document outlining the best practices for cyberforensics education and training [22]. This document has been the basis of much subsequent work in the discipline [8].

In 2008, the American Academy of Forensic Sciences (AAFS), the premier American professional organization for forensic sciences, established its Digital and Multimedia Sciences Section [3]. The section was formed with approximately 40 members. As of 2014, it had nearly 100 members.

Traditional forensic science education programs have existed for many years. However, as a result of the work done by TWGED-DE, AAFS created the Forensic Science Education Program Accreditation Commission (FEPAC) [8] in 2004. FEPAC focuses on the accreditation of digital forensic education programs. In 2012, FEPAC accredited its first master's program in digital evidence at Marshall University.

Recognizing the need for digital forensic practitioners in the U.S. Department of Defense, the Defense Cyber Crime Center (DC3) brought together a number of academics and practitioners to develop a certification and accreditation program for the Department of Defense called the Centers of Digital Forensics Academic Excellence (CDFAE) [5]. The standards, developed by consensus, drew on bodies of knowledge that were previously identified by other organizations, including ASCLD-LAB, TWGED-DE, FEPAC and the Digital Forensics Certification Board (DFCB) [6]. In 2013, CDFAE accredited its first two-year academic program [5].

In 2012, the Advanced Technology Education Program of the National Science Foundation (NSF-ATE) invested nearly $2 million in the Advanced Cyberforensics Education (ACE) Consortium [2] for the express purpose of developing cyberforensic education programs that meet the needs of government and industry. The authors of this paper are the Principal and Co-Principal Investigators, respectively, of the ACE effort. Key ACE initiatives are to develop and disseminate course curricula (including syllabi, course materials and laboratory exercises) and to conduct faculty training programs that will meet the educational accreditation standards of FEPAC and CDFAE. The goals of ACE are to: (i) ensure that faculty know and teach the core knowledge of the field; (ii) ensure that faculty teach courses that meet the needs of employers; (iii) ensure that academic institutions develop programs that are accreditable; (iv) prepare students for professional certifications; and (v) provide education and training opportunities for displaced professionals.

6. Practitioner Certification

Similar to the development of standards and accreditations, the certification of cyberforensic practitioners grew organically. The first certification for professionals was likely created by the International Association of Computer Investigative Specialists (IACIS) in 1991. IACIS hosted *ab initio* training courses that were available only to sworn law enforcement professionals. Since training and certification predated the development of commercial digital forensic software, the courses focused heavily on understanding the operation of computers, operating systems, file systems and applications. Foundational tools such as hex editors were utilized in a methodological way to exploit the practitioner's understanding of the technology for forensic purposes [13, 19]. This instituted the paradigm of requiring professional certifications to cover a foundational set of knowledge, a forensic methodology and tool usage.

In the late 1990s, integrated commercial tools such as EnCase [9] and Forensic Toolkit [1] were sufficiently complex that practitioners required special training to utilize them effectively. Vendors thus began to offer training courses on the use of their tools; the courses were typically two to five days in length. While the vast majority of the training focused on using tools, some basic knowledge was covered to ensure that the participants had a common baseline. At the end of the training courses, the participants were offered the opportunity to take written and practical tests and be "certified" by the vendors. Formal training in these complex tools is necessary and important. Nevertheless, it is abundantly

clear that a short tool-centered class does not provide the full range of knowledge and experience that defines a cyberforensic professional.

Over the past decade or so, a number of organizations in addition to IACIS have developed and fostered "professional certifications" that seek to recognize individuals who have broad foundational knowledge as well as adequate practical experience to demonstrate a professional level of competence in the cyberforensics field [19, 21]. Examples of these professional certifications are the Certified Computer Examiner (CCE) from the International Society of Forensic Computer Examiners (ISFCE) [14], Certified Forensic Computer Examiner (CFCE) from IACIS [11], Digital Forensics Certified Practitioner (DFCP) from DFCB [6] and Certified Cyber Forensics Professional (CCFP) from $(ISC)^2$ [12]. The authors of this paper were actively involved in developing some of these professional certifications and can vouch for the tremendous difficulty in developing such certifications. In 2014, the DC3 in conjunction with the CDFAE Accreditation Program [5] began to issue certifications to individual students who completed CDFAE-approved academic programs and passed written and practical tests.

While the certifications differ, they share a common set of requirements. All of them require demonstrated mastery of a core set of knowledge coupled with demonstrated skill and experience. Especially interesting is the fact that the core knowledge required by each of the certifications is remarkably similar. This should not be surprising because many of the individuals who contributed to the development of these certifications also helped set the functional and academic standards that were discussed previously.

7. Conclusions

Training, education, professional certifications and organizational accreditation have made substantial inroads in the cyberforensics field during the past decade. One might surmise that this is merely a "happy coincidence." However, we posit that, given the wide range of educators, practitioners, managers and government officials involved, the events described in this paper are evidence of the development of a paradigm that corresponds to the concept of "normal science" according to Kuhn [15]. Indeed, what has emerged is a common view of the fundamentals that form the basis of cyberforensics, an acknowledged set of processes that constitute the practice of cyberforensics, and an agreed set of norms that define the ethical conduct of cyberforensics.

The future is bright. The cyberforensics community is engaged in an active dialog involving government and industry, academics and prac-

titioners, investigators and forensic examiners, as well as certification and accreditation bodies. This collaboration will enable standards to evolve quickly in the dynamic world of technology. No doubt, there will be bumps in the road. But the constant challenges and evolution that characterize "normal science" will continue to strengthen cyberforensics as a scientific discipline.

References

[1] AccessData, AccessData, Lindon, Utah (www.accessdata.com).

[2] Advanced Cyberforensics Education Consortium, Advanced Cyberforensics Education (ACE), Daytona State College, Daytona, Florida (cyberace.org).

[3] American Academy of Forensic Sciences, Digital and Multimedia Sciences, Colorado Springs, Colorado (aafs.org/about/sections/digital-multimedia-sciences).

[4] American Society of Crime Laboratory Directors/Laboratory Accreditation Board, Accredited Laboratory Index, Garner, North Carolina (www.ascld-lab.org/accredited-laboratory-index).

[5] Defense Cyber Crime Center, CDFAE, Linthicum, Maryland (www.dc3.mil/cyber-training/cdfae).

[6] Digital Forensics Certification Board, Digital Forensics Certification Board (DFCB) (dfcb.org).

[7] European Network of Forensic Science Institutes, Structure, Warsaw, Poland (www.enfsi.eu/about-enfsi/structure).

[8] Forensic Science Education Program Accreditation Commission, Forensic Science Education Program Accreditation Commission (FEPAC), Colorado Springs, Colorado (fepac-edu.org).

[9] Guidance Software, Guidance Software, Pasadena, California (www.guidancesoftware.com).

[10] M. Honan, I, Glasshole: My year with Google Glass, *Wired* (www.wired.com/2013/12/glasshole), December 30, 2013.

[11] International Association of Computer Investigative Specialists, About IACIS, Leesburg, Virginia (www.iacis.com/about/overview).

[12] International Information Systems Security Certification Consortium, $(ISC)^2$, Clearwater, Florida (www.isc2.org//default.aspx).

[13] International Organization on Computer Evidence, Guidelines for Best Practice in the Forensic Examination of Digital Technology (www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html).

[14] International Society of Forensic Computer Examiners, International Society of Forensic Computer Examiners (ISFCE), Brentwood, Tennessee (www.isfce.com/index.html).

[15] T. Kuhn, *The Structure of Scientific Revolutions*, University of Chicago Press, Chicago, Illinois, 1996.

[16] J. Markoff, Google cars drive themselves, in traffic, *New York Times*, October 9, 2010.

[17] National Institute of Standards and Technology, National Initiative for Cybersecurity Education (NICE), Gaithersburg, Maryland (csrc.nist.gov/nice).

[18] Pew Research Internet Project, Mobile Technology Fact Sheet, Pew Research Center, Washington, DC (www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet), 2014.

[19] M. Pollitt, A history of digital forensics, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 3–15, 2010.

[20] Scientific Working Group on Digital Evidence, Scientific Working Group on Digital Evidence (www.swgde.org).

[21] E. Tittel, Best computer forensics certifications for 2014, *Tom's IT Pro* (www.tomsitpro.com/articles/computer-forensics-certifications,2-650.html), November 15, 2013.

[22] West Virginia University Forensic Science Initiative, Technical Working Group for Education and Training in Digital Forensics, Morgantown, West Virginia (www.ncjrs.gov/pdffiles1/nij/grants/219380.pdf), 2007.