Lack of Oversight and Credentialing Process for Digital Forensic Investigators

Despite the phenomenal growth in the digital world and crimes committed using digital techniques and tools, there are literally no foundational requirements to perform digital forensic investigations. While there is a slew of private and mostly for-profit organizations that sell training and certifications in regard to digital forensic credentials, there seems to be nothing of the kind at the federal and state levels in the United States. To understand the gravity of this, consider if attorneys did not attend law schools and were not required to take the bar exam where they practice and instead could take some private certification from a nonprofit or for-profit organization and then practice law. This is the precise situation when it comes to digital forensics investigators.

Nima Zahadat, Ph.D.
Is a professor of forensics, information systems and data science. He has also held positions as chief security officer, chief information officer, director of security, director of training solutions, dean of computer science, program chair of information systems and director of operations. Zahadat has worked extensively in the public and private sectors throughout the years. He previously taught at George Mason University (Fairfax, Virginia, USA) and The George Washington University (Washington DC, USA) in the fields of information systems, engineering, data science, web development and security. He has developed and taught more than 100 different information systems, security and project management curricula throughout his career. Zahadat's research interests are digital forensics, mobile security, information security, risk management, data mining and information visualization.

The debate among professionals with regard to acceptance of the digital forensic discipline as a scientific area is worth exploring. There have been various US state-level and US federal-level attempts to bring some coherence and credibility to digital forensics as well as several vendor-neutral and vendor-specific certifications. Research has studied the negative implications that the lack of proper credentialing in digital forensic investigation can have on the legal system, legal processes and the public in general.

Any discipline that lacks a properly credentialed and accredited professional license will eventually lead to disaster and become corrupted. In the case of digital forensics, this can mean convicting the innocent or letting go the guilty, which, in fact, has been a considerable problem. Without government oversight, there can be no professional licensing. It is curious that despite the large amount of digital forensics and even crime scene investigation (CSI) forensics, there are no credentialing bodies at the federal and state levels. This article studies this phenomenon in depth and presents recommendations to rectify this situation.

Why are there no national or state-level standards and professional credentialing body guiding forensic investigations and investigators in the United States? Sadly, there are no good answers. There are credentialing requirements for practicing law, becoming and working as a nurse, and even practicing private investigations (PI), but none for digital forensics.[1]

A federal-level licensing examination would establish the field of digital forensic investigators and professionals as a distinct profession. This would mean there would also be no need to leverage their credibility off of another profession such as private investigator licensing. It would also mean that digital forensic investigators would be guided by both the Federal Rules of Civil Procedures as well as state-level judicial statutes. Yet, instead of supporting this approach, some states have taken the approach of lumping private investigators and forensic investigators together. This is generally due to bureaucratic reasons, lack of expertise in digital forensics, or the sheer desire to do something, anything, that would give the field some legitimacy. As such, efforts have been made to bring consensus to the field of digital forensics, including creation of an abundance of process models for digital forensic investigations developed within academia, governments and the private sector. Despite all this, there remains no consensus and there is a lack of a credentialing process and oversight bodies.[2]

> “A FEDERAL-LEVEL LICENSING EXAMINATION WOULD ESTABLISH THE FIELD OF DIGITAL FORENSIC INVESTIGATORS AND PROFESSIONALS AS A DISTINCT PROFESSION.”

Literature Review

According to research, during the early 1990s, the establishment of scientific working groups in the United States guided the movement toward some regulatory improvements in the computer forensics field. These groups met annually and were composed of federal, state and local law enforcement agencies' representatives. The memberships were limited—typically 50, at the most. During the late 1990s, the Scientific Working Group on Digital Evidence was established, with the goal of developing standards for digital evidence gathering and identification. This group published a manual titled "Best Practices for Computer Forensics" in 2000.[3]

During the 2000s, several credentialing bodies were established to enhance digital forensic processes and add some level of quality assurance to gathering of digital forensic evidence. These included the American Society of Laboratory Directors, which established operating standards for forensic laboratories, and the Consortium of Digital Forensic Specialists, an international nonprofit body with the goal of improving the digital forensics profession.

The US National Academy of Science (NAS) published a report in 2009 titled "Strengthening Forensic Science in the United States: A Path Forward" in which it identified needed improvements to the forensic science disciplines.[4] More precisely, the report advanced the idea of compulsory accreditation of forensic science service providers (including digital forensics) such as forensic laboratories and crime labs. During the same year, in response to the NAS report, the White House Office of Science and Technology established the Subcommittee on Forensic Science. This subcommittee was chartered in 2009 and completed its mission in 2012. During this period, members of the subcommittee, which included more than 200 subject matter experts across 23 US federal agencies, conducted research and examination of relevant issues in order to formulate a proper response to the NAS report.

During 2013, another movement involved the US Department of Justice (DOJ) in collaboration with the US National Institute for Standards and Technology (NIST) to form the Organization of Scientific Area Committees, with the goal of strengthening forensic sciences in the United States.[5] This organization consists of more than 500 forensic science professionals along with other experts representing local, state and federal government agencies, academic institutions and other organizations. The mission of the organization is the “development and propagation of forensic science consensus documentary standards and guidelines and to ensure that a sufficient scientific basis exists for each discipline.”[6] The organization also includes digital evidence as a component of the Digital/Multimedia Committee.

More recently, a variety of professional programs offering certifications have arisen in academia.[7] Many universities, colleges, professional organizations and even federal agencies have facilitated training and continuing education programs in the field of digital forensics. These programs are presumably designed to assist practitioners in qualifying for forensics expertise. For example, the US National Security Agency (NSA) has 85 National Centers of Academic Excellence in Information Assurance Education, where 30 professional certification programs are offered. Additionally, the American Academy of Forensic Sciences (AAFS) is currently working on the development of a standard curriculum for digital forensics.

> “DESPITE THE FACT THAT THE NUMBER OF DIGITAL FORENSIC EXAMINERS AND CERTIFICATIONS HAVE RAPIDLY INCREASED, THERE ARE STILL NO STANDARDS FOR A DIGITAL FORENSIC EXAMINER CERTIFICATION.”

Private enterprises have also jumped on the bandwagon, offering training and certifications specific to their individual products or even those applying to digital forensics in general.[8] Despite the fact that the number of digital forensic examiners and certifications have rapidly increased, there are still no standards for a digital forensic examiner certification. This means the investigators responsible for collecting, examining and analyzing digital evidence have no standardized qualifications. Some other private organizations that offer certifications for digital forensic investigators or examiners include: (ISC)^2, the Digital Forensics Certification Board, the SANS Institute, the International Association of Computer Investigative Specialists, the International Society of Forensic Computer Examiners, EC-Council, EnCase, and various forensics software/hardware suppliers. As one author points out, “…it is important to understand that certification does not mean mastery…. In fact, certification doesn’t necessarily even mean professional competency.”[9]

Computer Forensic Licensing at the State Level

While there are no US national standards for digital forensic credentialing and, for that matter, no state-level ones, some US states have attempted to bring about such standards. These efforts have been half-hearted and rather disorganized, many times causing more problems in the legal realm than offering solutions. Many of these states lump private investigator (PI) licensing and forensic credentialing into one in an attempt to add legitimacy to forensic investigators. State credentials include:

- **Alabama**—Offers no forensic licensing credentials, but the city of Mobile requires a city-issued PI license to do forensic work[10]
- **Colorado**—Does not have any digital forensic requirement and PI licensing is voluntary, which is somewhat intriguing. Because Colorado’s PI licensing is voluntary, anyone can come to the state and be licensed as a PI, even if the individual has broken the law elsewhere. According to the Colorado legislature, there have been numerous instances of wrongdoing by licensed PIs from Colorado.
- **District of Columbia**—Requires a PI investigator license for digital forensic examiners [11]
- **Georgia**—Has required that digital forensic examiners obtain PI licensing[12]
- **Indiana**—As of 2010, elected not to require any credentialing or licensing for digital forensic examiners[13]

- **Maine**—Like Georgia, mandated that digital forensic examiners obtain PI licensing[14]
- **Maryland**—Requires a PI license for private investigations, but does not address digital forensic licensing nor credentialing
- **North Carolina**—Like Indiana, elected not to require licensing of any kind for forensic investigators[15]
- **Oklahoma**—Permits that a PI license from another state can be used to get a temporary license in Oklahoma. This means if an investigator needs a temporary license in Oklahoma, he or she can get one from Colorado.[16]
- **Texas**—Has implemented the notion that digital forensic examiners/investigators license themselves as PIs in the state. Texas has gone so far as to interpret digital investigation to include computer technicians and repair personnel.[17]
- **Virginia**—In 2011, codified explicitly stating that PI licensing requirements do not apply to any certified forensic individual employed as an expert witness. Virginia has reciprocity agreements with several states, including Georgia.[18]

It is worth pointing out that several states, including New York, Nevada, North and South Carolina, Virginia, and Washington, are pushing to have PIs handle digital forensic investigations. No states were found to be offering any paths toward independent digital forensic licensing and credentialing.

> "DUE TO THE LACK OF AN ACCREDITED PROCESS TO BECOME A DIGITAL FORENSICS EXPERT, THERE ARE NUMEROUS CASES IN WHICH INDIVIDUALS HAVE BEEN CONVICTED AND SENT TO PRISON WRONGFULLY."

Digital Forensics Certifications Obtainable From Private Organizations

According to the InfoSec Institute, popular computer forensic certifications fall into two major categories: vendor-neutral and vendor-specific.[19] The vendor-neutral certifications purportedly advance best practices in particular fields while vendor-specific certifications focus on advancing the vendor's platform, applications and tools.

The following vendor-neutral certifications are listed as best by the InfoSec Institute: Certified Forensic Computer Examiner (CFCE), Certified Computer Examiner (CCE) and Global Information Assurance Certification (GIAC).[20]

The best vendor-specific certifications, according to the InfoSec Institute, are: EnCase Certified Engineer (EnCE) and AccessData Certified Examiner (ACE).[21] The EnCE certification process can be taken by private- and public-sector professionals who use Guidance Software's EnCase computer forensics application to do their work. The EnCE certification tests professionals' knowledge of both computer examination methods and use of the EnCase application in conducting computer forensic analysis. There are advantages to obtaining EnCase's certification, including enhancement of the examiners' marketability. However, unlike some other certifications such as those offered by (ISC)^2, EnCE does not have a standard code of ethics by which professionals holding the certification must abide.[22]

Case Studies of Wrongful Convictions

Due to the lack of an accredited process to become a digital forensics expert, there are numerous cases in which individuals have been convicted and sent to prison wrongfully. It is possible that there are just as many who have gone free who were guilty. According to the Mid-Atlantic Innocence Project website, there are six causes of wrongful convictions.[23] Two of those causes are:

- Unreliable or improper forensic science
- Government misconduct, which usually refers to the government's failure to disclose exculpatory evidence

Two cases that relied on forensic "experts" follow—one that led to a wrongful conviction and one to a possible wrongful acquittal.

Julie Amero, a Connecticut (USA) schoolteacher, was wrongfully convicted of possession of pornographic content on her school computer.[24] The case of State of Connecticut v. Julie Amero provides a dark understanding of how a lack of expertise and knowledge of digital forensic evidence can lead to the wrongful conviction of an innocent person. In 2004, Connecticut substitute teacher Julie Amero was observing a seventh-grade classroom. At one point, Amero stepped out into the hallway for a short moment and found, upon her return, two students browsing a website about hairstyling. Shortly thereafter, the web browser started showing pop-up advertisements depicting pornographic images. Amero had been instructed not to turn off the computer, so she did not. Furthermore, she was not aware that the monitor could be turned off. This meant that some of the students in the classroom were exposed to the pornographic content. Once in court, at Amero's trial, the primary evidence presented by the state was a forensic copy of the hard drive of the computer in question. Fantastic as it may seem, the digital forensic investigator in this case had not applied industry standards to make a copy of the hard drive, yet the evidence was still admitted into court by the judge. The prosecution declared that the digital evidence would show an Internet history of pornographic links, showing that Amero deliberately visited pornographic websites.[25]

Sometime later, a computer forensics expert for the defense discovered that the school's antivirus software had not been regularly updated nor had it been maintained; no antispyware, firewall or current content filtering tool was found on the school's computer. The computer forensics expert hired for the defense was Herb Horner, a self-employed computer consultant. During his examination of the suspected hard disk, imaged from the school's computer, Horner found convincing evidence that spyware had, in fact, been installed on the computer, thus causing pornographic pop-up images to continuously appear on the monitor. Despite the evidence found by Horner, the judge in the case refused to allow Horner's full testimony into evidence, claiming that Horner's information was not made available during discovery prior to the trial proceedings, a clear case of misconduct by the government. Ultimately, Amero was found guilty of "risk of injury to a child" and, at one point, faced the possible fate of a 50-year prison sentence. However, the Connecticut State Court of Appeals reversed the decision made by the lower court, and a motion for a new trial was accepted. In an effort to put the events behind her, Amero eventually pled guilty to a misdemeanor and agreed to have her teaching license terminated.[26]

While the Amero case shows that digital forensics is not foolproof and can lead to the conviction of innocent persons, improper digital forensics has also led to allegedly guilty persons being acquitted in court. One example of this is the case of Aaron Caffrey. On 20 September 2011, less than two weeks after the 11 September 2001 attacks in the United States, Caffrey was charged with carrying out a "denial of service attack on the computers of the Port of Houston, Texas."[27] During the trial, Caffrey claimed that the evidence brought against him had been installed on his computer without his knowledge by malicious actors installing a Trojan horse program to gain control of his computer and launch the distributed denial-of-service (DDoS) attack. Despite Caffrey's claims, a forensic examination of his computer by the prosecution's expert witness, Neil Barrett, found tools that could be used to launch a DDoS attack but no trace that a Trojan horse had been planted.[28]

Eventually, Caffrey was acquitted of launching a DDoS attack, despite the fact that both prosecutorial and defense attorneys confirmed that Caffrey's computer was responsible for the attack. Apparently Caffrey's defense was able to convince the jury that a Trojan horse armed with a "wiping tool" was responsible for the attack, which resulted in the editing of the system's log files and deletion of all traces of the aforementioned Trojan; the prosecution claimed that no technology existed that could perform such sophisticated tasks. Caffrey's case is part of the phenomenon commonly known as the "Trojan horse defense," which became popular in the United Kingdom during the early 2000s.[29]

Recommendations for Improving the Digital Forensics Process

The following three areas where the computer forensics field needs improvement have been identified:[30]

1. The creation of a flexible standard; qualification of expert witnesses; and standards regarding the analysis, preservation and presentation of digital evidence. Any standard(s) developed for use in the computer forensics discipline must allow for flexibility, so that the standard may adapt to the continuous changes in technology and the forensic process. It is also important that computer forensic standards cover all aspects of the forensic process, from the search and seizure of digital evidence to the analysis and examination of the evidence.
2. The qualification of expert witnesses. Because computer forensics is still considered to be in its infancy, it lacks any formal credentialing bodies and a formal educational process. Therefore, in adjudication processes, the courts accept persons as expert witnesses based on their skills and previous professional work experience. While this process has not been challenged thus far, researchers anticipate that, in the future, expert witnesses' qualifications will be more commonly challenged.
3. Standards regarding the analysis, preservation and presentation of digital evidence. Researchers also state that there should be "rigorous" standards and requirements along with continuous updates to the forensic process. Currently, the common method used to analyze digital evidence relies mostly on the software and/or hardware an expert uses in the analysis of the evidence. It has been asserted that relying solely on software/hardware does not allow experts to fully understand the digital forensics process so that they may articulate the process to a judge in court proceedings.

> “ANY STANDARD(S) DEVELOPED FOR USE IN THE COMPUTER FORENSICS DISCIPLINE MUST ALLOW FOR FLEXIBILITY, SO THAT THE STANDARD MAY ADAPT TO THE CONTINUOUS CHANGES IN TECHNOLOGY AND THE FORENSIC PROCESS.”

Additionally, researchers have emphasized the importance of the implementation of a universal system for certifying those claiming to be computer forensic professionals, as a continuous lack of professional certification, investigative standards and peer-review process may eventually result in computer forensics being labeled as "junk science" instead of an accepted scientific discipline.[31]

Lack of High-Level Oversight for Forensic Investigators

One study noted that, unlike many other professional fields, there is no universally accepted digital forensic oversight body or accrediting board to ensure the consistency of digital forensic education programs.[32] The reasons for this can be speculated upon and, perhaps, one reason is that there has not been any research conducted to identify needs and current challenges faced by digital forensic professionals. Further, there is no research agenda that identifies the improvements that are needed in digital forensic education programs to properly inform members of the industry.

An information technology and cybersecurity expert indicates that the reason for the lack of proper oversight of the work conducted in the digital forensics field is not intentional, but is instead due to the hefty backlogs of evidence often faced by digital forensic examiners. He asserts that the backlog of evidence leads examiners to place a low priority on working to develop policies and procedures.[33]

A real-life example of an attempt to formalize and oversee the credentialing of a digital forensic process occurred in 2008, when the US Treasury Inspector General for Tax Administration (TIGTA) published an audit report that revealed the lack of program-level processing controls for digital forensic examinations that were creating risk that could potentially compromise investigations.[34] At

TIGTA, digital forensic examinations are conducted within the Electronic Crimes Program (E-Crimes) Field Services Program. The E-Crimes program provided technical expertise and digital examination of evidence to special agents. Due to the continuous increase in digital evidence, the US Internal Revenue Service (IRS) conducted an audit to ensure that the digital forensics processes ran efficiently. Additionally, TIGTA's Criminal Investigation (CI) division had developed an initiative known as the Information Technology Executive Steering Committee and Governance Process. The mission of the initiative was to provide information technology oversight both for the technologies and processes used by the division, and the employees responsible for conducting examinations of digital evidence. Ultimately, TIGTA recommended that the division take steps to protect digital evidence by developing effective quality assurance and documentation procedures to be followed throughout the digital forensic processes.[35]

Key Findings

It is fascinating to see the many cases leading to wrongful conviction of individuals in which digital evidence was involved. This should not be surprising due to the lack of availability of digital forensic accreditation processes and the clear lack of oversight. The phenomenon of the "Trojan horse defense" is also interesting, albeit disturbing, as it allows for potentially guilty persons to simply claim that their computer was infected with a Trojan, thereby absolving them of any wrongdoing. It must become the responsibility of lawmakers and legal and IT industry professionals to conduct substantive research to determine the merits of such a defense.

There has been some movement toward strengthening digital forensics accreditation, as noted throughout this article. In August 2008, the American Bar Association stated in Resolution No. 301 a recommendation discouraging states from requiring PI licenses for digital forensic investigation and instead recommending an effort to establish a professional certification of competency based on science and technology.[36] The US National Academy of Science proposed methods to strengthen forensic science in general in 2009, in a study authorized by Congress.[37] Still, the testimonies of most forensic examiners are not properly monitored for accuracy and, in fact, it is rare even in cases of misconduct (as opposed to error) to have any oversight and even any process to correct and prevent such issues from occurring in the future. So it appears that lawyers, judges, prosecutors and jurors tend to believe anyone who is labeled as an expert, especially if that "expert" holds some certification from some private organization.

> SO IT APPEARS THAT LAWYERS, JUDGES, PROSECUTORS AND JURORS TEND TO BELIEVE ANYONE WHO IS LABELED AS AN EXPERT, ESPECIALLY IF THAT "EXPERT" HOLDS SOME CERTIFICATION FROM SOME PRIVATE ORGANIZATION.

Conclusion

While there are private certifications in digital forensics, many of them are vendor-specific. There are no federal-level or state-level digital forensics certification standards, procedures or accreditation processes. Furthermore, there is not even any independent research to determine which of the available certifications are best in qualifying a digital forensic individual. As technology continues to advance and cybercrimes become more commonplace, it is vital for governments and industry to collaborate in implementing policies, procedures, and a certification and accreditation process that offers quality assurance of a digital forensic investigation and properly credentialed individuals certified as such. Certainly, the Amero and Caffrey cases prove that error and doubt are still contributing factors in the use and acceptance of digital forensic evidence. The technology and processes that reduce and, in some cases, eliminate these errors and doubts are in place. What is lacking are the proper standards, oversight and professional processes for conducting digital forensics. Further, the legal system must demand professional and high-quality examination results and experts based on those professional codes of ethics, procedures, investigations and witnesses.

Endnotes

1 Vincze, E. A.; "Challenges in Digital Forensics," *Police Practice and Research*, vol. 17, iss. 2, 2016, p. 183-194

2 *Ibid*.

3 *Ibid*.

4 Butler, J. M.; *Proceedings of the International Symposium on Human Identification,* The National Commission on Forensic Science and the Organization of Scientific Area Committees, 2014

5 *Op cit* Vincze

6 *Ibid*.

7 *Ibid*.

8 *Ibid*.

9 Huber, E.; "Certification, Licensing and Accreditation in Digital Forensics," A Fistful of Dongles Blog, 13 November 2010, *http://www.afodblog.com/2010/11/certification-licensing-and.html*

10 Leonardo, T.; D. White; A. Rea; "To License or Not to License Updated: An Examination of State Statutes Regarding Private Investigators and Digital Examiners," *Journal of Digital Forensics, Security and Law,* vol. 7, no. 3, article 5, 2012

11 *Ibid*.

12 *Ibid*.

13 Garnett, B.; "Computer Forensic Examiners: PI Licensing Requirement Revisited," SANS Digital Forensics and Incident Response Blog, 21 June 2010, *https://digital-forensics.sans.org/blog/2010/06/21/computer-forensic-examiners-pi-licensing-requirement-revisited*

14 *Op cit* Leonardo *et al*.

15 SANS Digital Forensics (2010), *https://digital-forensics.sans.org/blog/2010/06/21/computer-forensic-examiners-pi-licensing-requirement-revisited*

16 Wright, B.; "Should a Computer Forensics Expert Get a Private Investigator License," InfoSec & Forensics Law Blog, 2013, *https://hack-igations.blogspot.com/2013/10/regulation.html*

17 *Op cit* Leonardo *et al*.

18 *Ibid*.

19 Imam, F.; "The Best Computer Forensics Certifications," InfoSec Institute, 2017, *https://resources.infosecinstitute.com/category/computerforensics/introduction/computer-forensics-certifications/#gref*

20 *Ibid*.

21 *Ibid*.

22 *Ibid*.

23 Mid-Atlantic Innocence Project, "Causes of Wrongful Convictions," *https://exonerate.org/causes-wrongful-convictions/*

24 Jordaan, J.; "A Sample of Digital Forensic Quality Assurance in the South African Criminal Justice System," *Information Security for South Africa (ISSA)*, 2012

25 Alva, A.; B. Endicott-Popovsky; "Digital Evidence Education in Schools of Law," *The Journal of Digital Forensics, Security, and Law*, vol. 7, iss. 2, 2012

26 *Ibid*.

27 Brenner, S. W.; B. Carrier; J. Henninger; "The Trojan Horse Defense in Cybercrime Cases," *Santa Clara High Technology Law Journal*, vol. 21, iss. 1, 2004, *http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1370&context=chtlj*

28 George, E.; "UK Computer Misuse Act, The Trojan Virus Defence: Regina v Aaron Caffrey, Southwark Crown Court, 17 October 2003," *Digital Investigation*, vol. 1, iss. 89, May 2004

29 *Op cit* Brenner *et al*.

30 Meyers, M.; M. Rogers; "Computer Forensics: The Need for Standardization and Certification," *International Journal of Digital Evidence*, vol. 3, iss. 2, p. 1-11, 2004

31 *Ibid*.

32 Nance, K.; H. Armstrong; C. Armstrong; "Digital Forensics: Defining an Education Agenda," *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 2010, *https://www.computer.org/csdl/proceedings/hicss/2010/3869/00/10-06-03.pdf*

[33] Moulin, J.; “Digital Forensics/Incident Response Forms, Policies, and Procedures,” JoshMoulin.com, 2015, *https://www.joshmoulin.com/digital-forensics-incident-response-forms-policies-and-procedures/*

[34] Phillips, M. R.; “While Renowned for Its Forensic Capabilities, the Digital Evidence Program Faces Challenges and Needs More Controls,” *Treasury Inspector General for Tax Administration*, 30 April 2008, *https://www.treasury.gov/tigta/auditreports/2008reports/200810106fr.html*

[35] *Ibid*.

[36] Whittemore, G.; Resolution to the American Bar Association, 11-12 August 2008

[37] National Science and Technology Council Committee on Science: Subcommittee on Forensic Science, *Strengthening the Forensic Sciences*, May 2014, *https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/NSTC/forensic_science_may_2014.pdf*