THE JOURNAL OF
DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 14 | Number 1 Article 3

3-31-2019

Digital Forensics, A Need for Credentials and Standards

Nima Zahadat
University of Baltimore, nzahadat@ubalt.edu

Digital Forensics, A Need for Credentials and Standards

Cover Page Footnote
The author acknowledges the kind and professional reviews of the editor and the associated reviewers.

DIGITAL FORENSICS AND CREDENTIALING

Nima Zahadat
University of Baltimore (UB), Universities at Shady Grove (USG)
nzahadat@ubalt.edu

ABSTRACT

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 are several private and mostly for-profit organizations that "sell" training and certifications regarding digital forensics credentials, at the federal and state level in the United States, there seem to be nothing of the kind.

Keywords: Digital forensics, certification(s), computer forensics, digital evidence, quality assurance, licensing requirements, credentials, private investigator (PI), Computer Forensics Innocence Project

1. INTRODUCTION

Despite the wide variety of areas in the medical field and that of the legal field, both requiring credentialing and accreditation at the state and at times the national level, there are no such requirements for digital forensic investigators. It is fair to state that a person caught practicing medicine without a state license or a degree from an accredited institution, would be sued and even prosecuted. It is also fair to state that most people would not trust a doctor or a lawyer who was not a graduate of a properly accredited university with proper credentials from a state or federal government. Even becoming a private investigator (PI) usually requires licensing in most states.

Digital forensic investigation is one of the prominent fields emerging from the broad discipline of forensic science. Though the academic theory and practice of digital forensics has existed since the 1970s, increased interest in the field has been witnessed recently owing to escalated risks of cyber-attacks and computer-related crimes (Altheide & Carvey, 2011). The field of digital forensics is particularly concerned with the evidence found in computers, mobile devices, storage devices, social media and cloud services among other IT related elements that can be used in trials and other forms of inquiries (Mohay, 2005). Data extraction, collation, carving, and the release of forensic expert reports are what encompasses the core of practice in the field.

While there are no national standards for digital forensic credentialing, and for that matter, no state-level ones, some states have attempted to bring about such standards. As will be seen, these efforts have been half-hearted and somewhat disorganized, many times causing more problems on 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, which is quite a peculiar approach. Below are some of the states and localities that have attempted to bring about some consistency to forensics investigations and a brief overview of their attempts and methodologies:

Alabama: Alabama offers no forensic licensing credentials, but the city of Mobile requires a city-issued private investigator (PI) license to do forensic work (Leonardo, White, & Rea, 2012).

Colorado: Colorado is somewhat intriguing as the state does not have any digital forensic requirement, and PI licensing is voluntary. Because Colorado's PI licensing is voluntary, anyone can come to the state and be licensed as a PI, even if they have broken the law elsewhere. According to the Colorado Legislature itself, there have been numerous instances of wrongdoing by licensed PIs from Colorado.

District of Columbia: Washington, DC requires a PI investigator license for digital forensic examiners (Leonardo, White, & Rea, 2012).

Georgia: Georgia has required that digital forensic examiners obtain PI licensing (Leonardo, White, & Rea, 2012).

Indiana: Indiana, as of 2010, has elected not to require any credentialing or licensing for digital forensic examiners (SANS, 2010).

Maine: Maine, like Georgia, has mandated that digital forensic examiners obtain PI licensing (Leonardo, White, & Rea, 2012).

Maryland: Maryland requires a PI license for private investigations, but neither digital forensic licensing or credentialing is addressed.

North Carolina: Like Indiana, North Carolina has elected not to require licensing of any kind for forensic investigators (SANS, 2010).

Oklahoma: Oklahoma is really odd as it 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, they can get one from Colorado first (InfoSec & Forensic Law, 2013).

Texas: 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 (Leonardo, White, & Rea, 2012).

Virginia: Virginia codified in 2011, explicitly stating that PI licensing requirements did not apply to any certified forensic individual employed as an expert witness. Virginia has reciprocity agreements with several states, including Georgia (Leonardo, White, & Rea, 2012).

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

Despite being well established in recent times, the discipline of digital forensics continues to face several core problems. A needs analysis survey by Rogers & Seigfried (2004) indicated training and certification as the main challenges, a claim collaborated by several stakeholders in the field including the National Institute of Justice. There are concerns that the field is largely fragmented, lacking a national framework for curricula training and development. Pollitt (2010) in his paper "A History of Digital Forensics" starts his work by apologizing to his audience, admitting there is little reliable data and rigorous logic that he can bring them regarding digital forensics. He gives a history of digital forensics based on his 20+ years as a criminal investigator, then proceeds to make some bold predictions, acknowledging he will probably be wrong in many of them. In addition,

the field as currently constituted has no gold standard for certification, a central challenge in instilling consistency and professionalism in the field. The National Institute of Standards and Technology (NIST) published special publication 800-181, a National Initiative for Cybersecurity Education or NICE as a reference structure describing the interdisciplinary nature of cybersecurity work. NICE attempts to provide a common lexicon, foundational frameworks, workforce categories, specialty areas, roles, knowledge descriptions, skills descriptions, abilities descriptions and a host of other well-thought-out guidelines, complete with example systems. This special publication would serve as part of an excellent starting point for digital forensics framework development and digital forensics academic development though, by itself, it would not be sufficient as it is too broadly focused on cybersecurity. It is designed as a starting point to be applied in the public, private, and academic sectors but does not focus entirely on forensic training, credentialing, or accreditation. NICE framework is comprised of the following components (NIST 800-181):

1. Categories – a high-level grouping of common cybersecurity functions
2. Specialty Areas – distinct areas of cybersecurity work (includes digital forensic)
3. Work roles – detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities required to perform tasks in a work role

While NICE can be one of the solid starting points, there is still the egregious issue of credentialing and certification in digital forensics, which this paper explores, drawing from relevant academic literature.

It must be pointed out that various agencies such as NSA and DHS have developed programs that institutions can apply for and be designated as meeting the bar set by these agencies. For example, NSA and DHS have jointly developed the Centers of Academic Excellence in Cyber Defense (CAE-CD) program. Regionally accredited colleges and universities can apply to this program and if approved, have their curricula be designated as such, receiving formal recognition from the US government. This is certainly an appealing program for many universities, including the author's university which has applied for this exact program, but it is still a fragmented solution and a voluntary one, and one that does not address digital forensics credentialing and accreditation at a high level; it focuses primarily on what the NSA and DHS consider necessary security processes and controls.

2. RESEARCH METHODOLOGY

The research was qualitative and descriptive in nature, utilizing published research in the field of digital forensic investigation. A search was conducted in major academic databases including Google Scholar and ProQuest, isolating articles from reputed journals on the subject of the federal, state, private, profit and non-profit credentialing of digital forensic investigators in the United States. Additionally, private recommendations and practices of private organizations such as ISC^2, Guidance Software, and AccessData were studied. Each study was evaluated for the relevance of content and timeliness, with the inclusion criteria only featuring articles within roughly 15 years of publication.

A review of literature focused on the general fundamental theories in the domain, the problematic issue of credentialing and possible solutions. Thematic reflections on the findings on various issues were noted and forwarded as recommendations and conclusions on the present state of the identified problem.

3. LITERATURE REVIEW

Though many studies in digital forensic investigations have identified the bias in available research towards applied aspects of the domain as opposed to the development of fundamental theories, prejudice is justified. This is because of the largely practical nature of forensic science at large and the pressure mounting from external events such as cyber-terrorism and cyber-crimes, necessitating more applied research (Nelson, Phillips & Steuart, 2014). As it emerges, the issue of credentialing of digital forensic investigators at various levels falls under applied research and continues the implied bias. However, there is credence in the fact that several studies identify the lack of a proper credentialing standard as one of the main challenges facing the profession today. For instance, a study by Flory (2015) indicated that though the state of Indiana's law enforcement agencies was deliberate about digital forensic training with half of their staff trained, their ability could only be rated from low to mid-range. As such, there was still an overwhelming need to create a standard and comprehensive framework for locating experts, obtain a forensic insight with the help of standard operating procedures, and finance career advancement in the domain. The above study shows the longstanding nature of the challenge of credentialing and locating competent experts in digital forensics and thus justifies the focus of research towards that direction (as opposed to fundamental theories).

The issue of credentialing, though vast, seems to be overshadowed by the looming challenge of lack of a proper, consistent curriculum in the first place. As such, a good deal of research is currently dedicated to advancing training and ensuring that there is a teaching framework that can be followed successfully by most universities and colleges. As noted by Lang et al. (2014), the development of a digital forensics curriculum should provide a self-contained and comprehensive tool for teaching the discipline in universities given the failure of many institutions to offer such courses for missing certain aspects of the entry barrier. In their proposed curricula, Lang et al. (2014) offered an introductory and an advanced course and hands-on laboratory programs. They, however, failed to focus or mention at any point, the essence of credentialing and its role in developing the digital forensics investigator. This seems to be consistent with most curricula and reports on the status of digital forensics investigation and related disciplines throughout. For instance, a report by West Virginia University Forensic Science Initiative (2007) submitted to the Department of Justice (DoJ) on training and education of digital forensics investigators highlights the antecedent qualifications and a detailed career path but omits otherwise essential information on credentialing. The report is comprehensive on other aspects of training and career path, highlighting the qualifications, skills, and knowledge needed, the Associate, Baccalaureate, and advanced levels of learning in the discipline, but makes a major omission on certifications and credentials needed in the profession. This sums the whole credentialing challenge in available studies- that most of it loom in the shadow of a clear training and education framework for digital forensic investigators.

The literature on building accreditation and credentialing in digital forensics is quite unappealing. This is primarily due to the confusion surrounding digital forensics in the first place. Losavio et al. (2016) make the bold allegation that digital forensics is not yet a profession and attempts justification of the claim on several grounds. According to the paper, a profession entails specialized knowledge, specialized training, highly valuable work, self-regulation, a code of ethics,

high levels of autonomy, and many other significant elements. Certification and credentialing are what offer code of ethics, autonomy of practice, and evidence of specialized training, but lack in the discipline as per the arguments of Losavio et al. (2016). This has hindered the development of digital forensics as a profession. A large number of studies indeed recommend that proper standardized frameworks are brought into the frame for credentialing of digital forensic investigators. Butler (2015) highlights some of these recommendations offered by the National Academy of Sciences (NAS). They include creating a standardized accreditation model for digital forensic investigators to achieve recognition, consistency, and the "expert" label.

From the reading, it appears that there is a robust framework for providing oversight to various accreditation bodies in digital forensics. These include the National Institute of Standards and Technology (NIST), the Department of Justice (DoJ) and the Organization of Scientific Area Committees (OSAC) which came together to carry out research and chart a framework that can operationalize accreditation bodies. The national commission on forensic science on its part acts as an advisory body to the DoJ and carries out various roles that form the framework for accreditation. These include advice on training on science and law, testimony and reporting, provision of interim solutions, and above all, accreditation and proficiency testing (Garfinkel et al., 2009). Therefore, though there are no consistent accreditation frameworks, the framework to regulate bodies that offer credentialing exists and operates with a clear mandate.

The development of accreditation oversight in digital forensics has since been reported at the national level. Coordinated by the DoJ and with the advice of NIST, such frameworks have emerged as a product of OSAC's efforts. According to Butler (2017), OSAC has been involved in the development and promulgation of technically-appropriate and universally accepted documentary standards that are used by accrediting bodies to audit forensic laboratories and carry out credentialing of forensic investigators. OSAC has since developed to include a Forensic Science Standards Board and various committees and subcommittees that are responsible for offering oversight in the approval process for forensic sciences standards as provided by various scientific area committees.

There are several credentialing bodies, many of which are international that are apparent in the field of digital forensics. Gladyshev, Marrington, & Baggili (2014) note that the bulk of these organizations are either for profit or privately owned, with the government only providing the business operational framework that such bodies can use in carrying out certification and accreditation. They include companies like Mile2 and ISC^2. Other entities include the EC-Council, the American Board of Information Security and Computer Forensics (ABISCF), International Association of Computer Investigative Specialists (IACS) and International Society of Forensic Computer Examiners (ISFCE) (Freiling & Schwittay, 2007). Some of these bodies, in particular, ISC^2, use the standards and frameworks issued by bodies like NIST to offer certifications such as Certified Information System Security Professional (CISSP), Certified Authorization Professional (CAP), and Certified Cyber Forensics Professional (CCFP). For instance, the CAP certification, which includes Digital Forensics Incident Handling, Risk Management, Continuous Monitoring, Auditing, and Assessment, is based almost entirely on the NIST guidelines, in particular the 800 series and more specifically, 800-86 (Guide to Integrating Forensic Techniques into Incident Response), 800-37 (Risk Management Framework), 800-30 (Risk Management Guide), 800-39 (Managing In-

formation Security Risks), 800-53 (Security Controls), 800-53A (Security Control Assessments), and 800-137 (Continuous Monitoring) among others. Other organizations such as EC-Council have had certifications for years in the field and continue to add more and revise already existing ones to make them more attractive to government agencies and private organizations. These certifications are updated every 3-5 years with more material added, some outdated material removed, and most are touted as skills that government and industry look for in today's forensic and security professionals. The fact that there are so many private organizations offering so many certifications, many in digital forensics, is testament to the need for having a credentialing and accreditation process as well as a testament to how private organizations are utilizing this opportunity to advance their own goals, primarily financial, even if they are labeled as non-profit.

4. CASE STUDIES

The National Academy of Sciences stresses the importance of quality assurance procedures in the practice of forensic science to "identify mistakes, scientific fraud, examiner bias, and to confirm the continued validity and reliability of forensic processes and to improve on processes that need to be improved" (Jordaan, 2012). In digital forensics specifically, a comprehensive quality assurance/quality management plan is required to ensure the credibility of digital forensic laboratories. Quality assurance in the digital forensics process is also seen as a critical issue in the practice of forensic science by both the National Research Council in Washington, DC and the Association of Chief Police Officers in London. As the public have seen in recent years, failure to implement quality assurance procedures in digital forensics can lead to innocent persons being convicted of crimes (Jordaan, 2012).

One particular case which resulted in a wrongful conviction was that of Connecticut school teacher Julie Amero (Jordaan, 2012). According to Alva & Endicott-Popovsky (2012), the case of State of Connecticut v. Julie Amero provides an understanding of how a general lack of knowledge of digital forensic evidence can lead to the wrongful conviction of an innocent person. In 2004, Connecticut substitute teacher Julie Amero was monitoring a seventh-grade classroom. Having had to step out into the hallway for a moment, upon her return, Amero found two students browsing a website about hair styling (Alva & Endicott-Popovsky, 2012). Soon after that, the web browser began opening pop-up advertisements depicting pornographic images. Amero did not turn off the computer, as she was instructed not to and was unaware that the monitor itself could be turned off. Several of the students in the classroom were exposed to the pornographic content. During Amero's trial, the primary evidence presented by the state was the forensic copy of the hard drive of the computer in question. Though the digital forensic investigator, in this case, did not utilize industry standards to make a copy of the hard drive, the evidence was still admitted into court by the judge. The prosecution claimed that digital evidence would show an Internet history of pornographic links, indicating that Amero deliberately visited pornographic websites (Alva & Endicott-Popovsky, 2012).

Later during the ordeal, a computer forensics expert for the defense discovered that the school's antivirus software was not regularly updated nor maintained; also, no antispyware, firewall, or current content filtering tool was found on the school's computer (Alva & Endicott-Popovsky, 2012). The defense computer forensics expert was Herb Horner, a self-employed computer consultant.

In his examination of the hard drive, imaged from the school's computer, Horner found evidence that spyware had been installed on the computer, thus causing pornographic pop-up images to continuously appear on the monitor (Alva & Endicott-Popovsky, 2012). Despite the evidence found by Horner, the judge, in this case, refused to allow the full testimony of defense expert witness, Herb Horner, into evidence, claiming that the information to be presented by Horner was not made available during discovery prior to the trial proceedings (Alva & Endicott-Popovsky, 2012). 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. Fortunately, the 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 (Alva & Endicott-Popovsky, 2012). The events leading up to and during Amero's trial caused great emotional, social, and financial stress on her and her family. Amero and her family have also experienced several health problems due to the stress caused by the events leading up to and during her trial (Alva & Endicott-Popovsky, 2012).

While the case detailed above shows that digital forensics is not foolproof and can lead to the conviction of innocent persons, digital forensics handled poorly has also led to guilty persons being acquitted in court. One example of this is the case of Aaron Caffrey. On September 20, 2011, less than two weeks after the September 11, 2001 (9/11) terrorist attacks, Aaron Caffrey was charged with "carryout of a denial of service attack on the computers of the port of Houston, Texas" (Brenner, Carrier and Henninger, 2004). During trial proceedings, 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 DDoS attack. A forensic examination of his computer by prosecution's expert witness, Professor Neil Barrett, found tools that could be used to launch an attack, but no trace that a Trojan horse had been planted, despite Caffrey's claim (George, 2003).

Nevertheless, Aaron Caffrey was acquitted of launching a distributed denial-of-service (DDoS) attack in the United States, even though both prosecutorial and defense attorneys confirmed that Caffrey's computer was responsible for the DDoS attack (Brenner et al., 2004). It is assumed that 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 trace of the Trojan; the prosecution claimed that no technology existed that could perform such sophisticated tasks but without success. Caffrey's case is part of the phenomenon commonly known as the "Trojan horse defense," which became popular in the UK during the early 2000s (Brenner et al., 2004).

5. KEY FINDINGS

There were a number of findings from the research conducted on digital forensics investigation. First, it became apparent that credentialing was a major issue in digital forensics and featured some of the main issues that were on the radar of major stakeholders such as the National Academy of Sciences and NIST (Casey, 2009; 2011). It, therefore, qualified to extend the bias on applied research over fundamental theorizing in the general domain of forensic science. In addition, the field in the broader scope was fragmented and lacking in proper curricula,

which was the preoccupation of various stakeholders and educators, rather than the formation of credentialing frameworks (Nance, Hay, & Bishop, 2009). As such, the issue of credentialing while important, had been overshadowed by the lack of proper, standardized curricula in the domain.

It was also apparent that the state and federal levels of governments were largely non-actors in the credentialing of digital forensic investigators. According to Garfinkel (2010), the majority of the bodies involved in accreditation and certification were private companies, including non-profit and for-profit organizations. They included Mile2, EC-Council, and ISC^2 among others, offering a number of accreditations such as the Certified Computer Examiner (CCE) to digital forensic experts. The scarcity of literature on accreditation and credentialing makes it difficult to determine the repute and ratings of these organizations (Lillard, 2010). However, they appeared to be the main players in the credentialing in the absence of state and federal governments actors. Instead, at least in part, the federal government offered guidelines which these bodies used for their curricula and certification development, giving frameworks and standards to be applied in the operationalization of the credentialing bodies. These guidelines were carried out by the DoJ, National Academy of Sciences and other affiliates working closely with the DoJ such as OSAC and NIST.

According to Lundquist (2016), there are several instances where private digital forensics have failed in assisting DoJ investigations, leading to the incarceration of the innocent and mistrials in some cases. These include the case of State of North Carolina vs. Bradley Cooper and the previously mentioned case of State of Connecticut vs. Julie Amero among others. In each of the highlighted cases, there were anomalies in the process of collection, collation, submission, and reporting of evidence. Oversight bodies can improve this by coming up with a standardized framework for digital forensics that can be applied in all cases. This entails credentialing of experts that the court can rely upon as experts in cases requiring digital forensic evidence (Kessler, 2007). At the moment, oversight appears fragmented due to the lack of a singular, unifying, and standardized curriculum to build on at the national or even at the state level.

6. RECOMMENDATIONS

Based on the research presented, clearly, more attention needs be paid to credentialing, which entails research, funding, and advocacy at the national and state levels. A national framework for developing and teaching digital forensics in order to bring standardization to the field is a necessity. This needs to be followed by a complementary credentialing system which would set the base for professionalism in digital forensics investigation methodology, processes, and techniques. Finally, state and federal governments must assume active roles in the oversight and accreditation of credentialing bodies with measurable results.

Meyers and Rogers (2004) identify the following three areas where the computer forensics field needs improvement: 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.

The second area identified by the authors as needing improvement is the qualification of expert witnesses. Because computer forensics is still considered to be in its infancy, it does not have any formal credentialing bodies, nor 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, Meyers and Rogers (2004) anticipate that in the future, expert witnesses' qualifications will be more commonly challenged.

The final area identified by the authors as needing improvement is standards regarding the analysis, preservation, and presentation of digital evidence. Meyers and Rogers (2004) 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; the authors challenge that relying solely on the 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.

Finally, Meyers and Rogers (2004) stress the importance of the implementation of a universal system for certifying those who claims 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 (Meyers & Rogers, 2004).

7. POSSIBLE OUTLINES FOR A FRAMEWORK

The topic of presenting a potential full solution and/or framework for digital forensics can arguably be a doctorate dissertation in its own right. It is a large undertaking and requires a great deal of research. One can argue that even then it truly requires the efforts of governments, law enforcement, and academics to put forth a viable solution. Nevertheless, the following possible outlines are intended to present the reader with some possibilities that are currently lacking in the field and could serve as starting points.

Abdalla, Hazem, and Hashem (2007) offer a guideline model for digital forensic investigation in their paper presented at the annual ADFSL Conference on Digital Forensics, Security and Law (Abdalla, Hazem, Hashem, 2007). In it they first present several existing models to include:

1. US Department of Justice's Electronic Crime Scene Investigation: A guide to first responders
2. An Abstract Digital Forensic Model (Reith & Gunsch, 2002)
3. The Integrated Digital Investigation Model consisting of 5 groups of 17 phases total (Carrier & Spafford, 2003)
4. A Hierarchical, Objectives-Based Framework for the Digital Investigation Process (Beebe & Clarke, 2004)

The authors then proceed to offer their own model which includes the following:

1. Preparation phase which includes pre-preparation, case evaluation, preparation of detailed design for the case, and determination of required resources.

2. Physical forensic and investigation phase which has the goal of collecting, preserving, and analyzing the physical evidence with an attempt to try and reconstruct the crime scene.

3. Digital forensic phase which needs to identify and collect electronic events that may have occurred and proceed with analyses.

4. Reporting and presentation phase which needs to be based entirely on the policy and laws of each jurisdiction (e.g., state, county, country) and presents the conclusions and corresponding evidence from the investigation.

5. Closure phase which requires reviewing the whole investigation process, determining whether the evidence found and collected solve the case in a forensically sound manner.

The model presented by Abdalla, Hazem, and Hashem (2007), can be considered to be universal, meaning that the authors try to have a model that is applicable in every possible locality. The model does not address issues when dealing with national security and intelligence systems that require higher sensitivity. Nevertheless, it, together with NICE from NIST mentioned previously as well as the other models mentioned can form a solid starting point for the development of a digital forensic investigation framework that once formulated, should be sophisticated and flexible enough to apply to a wide range of localities and entities. Part of the framework would need to discuss how to properly educate and credential would-be investigators.

At its heart, a digital forensic framework must address the following areas:

1. Preparation phase

2. Acquisition phase

3. Analysis phase

4. Reporting phase

5. Legal phase

6. Education phase

7. Credentialing phase

8. Accreditation phase

This means that digital forensic investigators must be trained in these 8 main phases. At the state and/or federal level, interested investigators must be required to register and take rigorous exams. These exams must address the phases of digital investigation and evaluate would-be investigators understanding of the ideals and processes involved in doing digital investigations. These exams must focus on assessing a test taker's ability to understand the digital forensic processes with the realization of its legal and ethical importance. The passing of these exams must be made necessary to receive a state or federal license to practice digital forensic investigation. This would form the backbone of the credentialing process of investigators. Given that such frameworks would have to be turned into curricula at the academic level in order to prepare interested applicants in digital forensics, that, in turn, would bring about the accreditation phase required for digital forensics as all reputable universities teaching the field must be appropriately accredited. Existing private sector certifications must be made moot and removed as they generally serve the financial interest of the organization and not that of the general public.

8. CONCLUSION

The present research brings to light obstinate issues in the credentialing of digital forensic investigators. The status quo reveals a troubling scenario of governments' lack of full

participation, lack of proper certification bodies, and oversight. This has, however, been overshadowed by the apparent lack of a consistent curriculum at the national and state levels to guide the teaching of digital forensics at the university level and other institutions of higher learning. The findings at a glance show that there is a lot to do to instill professionalism and inspire further development of digital forensics not only as a branch of forensic science but as an independent domain emerging in contemporary scholarship. If the recommendations issued are to be followed, there shall not only be a solution at the academic level of digital forensics but also at the professional level, which remains a cause for concern. The governments should spearhead curricular reinvention and development and take their active roles in the promotion of a unified credentialing framework to guide other bodies in the same direction.

To be sure, federal agencies such as FBI, Secret Service, IRS, and DoD have their own certification and accreditation processes. NIST also offers excellent certification and accreditation guidelines in its 800 series Special Publications. External certification and accreditation processes supported and approved by governments are desirable as they bring consistency and professionalism to the profession of digital forensics. Programs developed by DoD, NIST, DHS, etc. are certainly useful and at times quite necessary, but these efforts are not coordinated and often target the specific needs of the agency developing it. Many times, they are too broad, attempting to address too much. What is needed is a collective and coordinated effort by the governments, and this cannot come soon enough. The recent breaches of the federal Office of Personnel Management (OPM) which leaked over 22 million classified personnel records and Equifax's breach resulting in over 146 million private records of Americans being stolen show the tremendous need for proper education, credentialing, and accreditation of professionals in digital forensics investigations.

Finally, there will never be perfect solutions to digital forensics, and any attempt at designing a framework with perfection in mind would be futile. This is because it is impossible to plan out every imaginable scenario. The framework should create the needed structure, academics would provide the proper education and lab skills lumped up as credentialing, and accrediting bodies would provide oversight of the whole thing. With that in place, there is still the professional outlook and behavior of the investigator, along with how much creativity he or she brings to the job. Consider the simple case of whether during an investigation, a computer that is running should be left on while it is being triaged or be turned off and taken to a laboratory first.

There cannot be a single answer or a simple answer to such situations. Part of the education and design has to be teaching would-be investigators that each situation is unique and while requiring proper and professional steps to be taught and to be followed, cases also need the proper application of judicial prudence on the part of the examiner. Another situation that is a major issue is the application of encryption to devices. It is still the case that most devices are not encrypted and can be analyzed without the worry of dealing with encryption. That being the case, investigators will come across devices that may be encrypted and then would have to make decisions as to what to do. For instance, if coming across a Windows machine that "might" be encrypted but is currently on and running, a professional investigator should have the skills to take a memory dump of the running system since memory is never encrypted. Given the large memories of today's computers, a wealth of information may be available just from the memory dump alone.

Having properly dumped the memory, the investigator can then determine from the memory whether the computer is using encryption at all and then make a proper assessment on how to take the next steps. Skills such as this are taught in proper accredited curricula and also come by with some experience and creativity. It should go without saying that such skills are best taught and tried in the academic and laboratories, in a structured and controlled environment, instead of rogue investigators botching up investigations while they learn on the job!

REFERENCES

[1] Abdalla, S., Hazem, S., & Hashem S. (2007).Guideline Model for Digital Forensic Investigation. Conference on Digital Forensics, Security and Law, 200

[2] Alva, A. & Endicott-Popovsky, B. (2012).Digital evidence education in schools of law.The Journal of Digital Forensics, Security, and Law, 7.

[3] Altheide, C., & Carvey, H. (2011). Digital forensics with open source tools. Elsevier.

[4] Beebe, N. & Clark, J. (2004), "A hierarchical, objectives-based framework for the digital investigations process", Paper presented at the DFRWS, June 2004, Baltimore, MD.

[5] Bradshaw, K. & Jordaan, J. (2015). The current state of digital forensic practitioners in South Africa: Examining the qualifications,certifications, training and experience of South African digital forensic practitioners. 2015 Information Security for South Africa (ISSA).

[6] Brenner, S.W., Carrier, B. & Henninger, J. (2004). The Trojan horse defense in cybercrime cases. Santa Clara High Technology Law Journal 21. Retrieved `http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1370\&context=chtlj`.

[7] Butler, J. M. (2015). US initiatives to strengthen forensic science & international standards in forensic DNA.Forensic Science International: Genetics, 18, 4-20.

[8] Butler, J. M. (2017). Recent activities in the United States involving the National Commission on Forensic Science and the Organization of Scientific Area Committees for Forensic Science. Australian Journal of Forensic Sciences, 49, 526-540.

[9] Carrier Brian & Spafford (2003), "Getting Physical with the Digital Investigation Process", International Journal of Digital Evidence, Volume 2 (Issue 2):3.

[10] Casey, E. (2009). Handbook of digital forensics and investigation. Academic Press.

[11] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press.

[12] Flory, T. A. C. (2015). Digital forensics in law enforcement: A need based analysis of Indiana agencies, (Doctoral dissertation, Purdue University).

[13] Freiling, F., & Schwittay, B. (2007). A common process model for incident response and digital forensics. Proceedings of the IMF2007.

[14] Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital investigation, 7, S64-S73.

[15] Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. digital investigation, 6, S2-S11.

[16] George, E. (2004). UK Computer Misuse Act – the Trojan virus defence: Regina v Aaron Caffrey, Southwark Crown Court. Digital Investigation.

[17] Gladyshev, P., Marrington, A., & Baggili, I. (Eds.). (2014). Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013, Moscow, Russia, September 26-27, 2013, Revised Selected Papers, (Vol. 132). Springer.

[18] Jordaan, J. (2012). A sample of digital forensic quality assurance in the South African criminal justice system. Information Security for South Africa (ISSA) 1-9.

[19] Kessler, G. C. (2007, March). Anti-forensics and the digital investigator. In Australian Digital Forensics Conference,(p. 1).

[20] Lang, A., Bashir, M., Campbell, R., DeStefano, L. (2014). Developing a new digital forensics curriculum. Digital Investigation, 11, S76-S84.

[21] Leonardo, Thomas; White, Doug; and Rea, Alan (2012) "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.

[22] Lillard, T. V. (2010). Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Syngress Publishing.

[23] Losavio, M., Seigfried-Spellar, K. C., Sloan III, J. J. (2016). Why digital forensics is not a profession and how it can become one.Criminal Justice Studies,29, 143-162.

[24] Lundquist, R. (2016). An Examination of Failed Digital Forensics and the Criminal Justice System (Doctoral dissertation, Utica College).

[25] Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. International Journal of Digital Evidence. 3, 1-11.

[26] Mohay, G. (2005, November). Technical challenges and directions for digital forensics. In Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on (pp. 155-161). IEEE.

[27] Nance, K., Hay, B., & Bishop, M. (2009, January). Digital forensics: defining a research agenda. In System Sciences, 2009. HICSS'09.42nd Hawaii International Conference on (pp. 1-6). IEEE.

[28] Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.

[29] Pollitt, M. (2010, January). A history of digital forensics. In IFIP International Conference on Digital Forensics (pp. 3-15). Springer, Berlin,Heidelberg.

[30] Reith, M., Carr, C., & Gunsch, G. (2002), "An Examination of Digital Forensic Models", International Journal of Digital Evidence, Volume 1(Issue 3):6.

[31] Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. Computers & Security, 23,

12-16.

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

[32] West Virginia University Forensic Science Initiative. (2007). Technical working group for education and training in digital forensics. US Department of justice.

