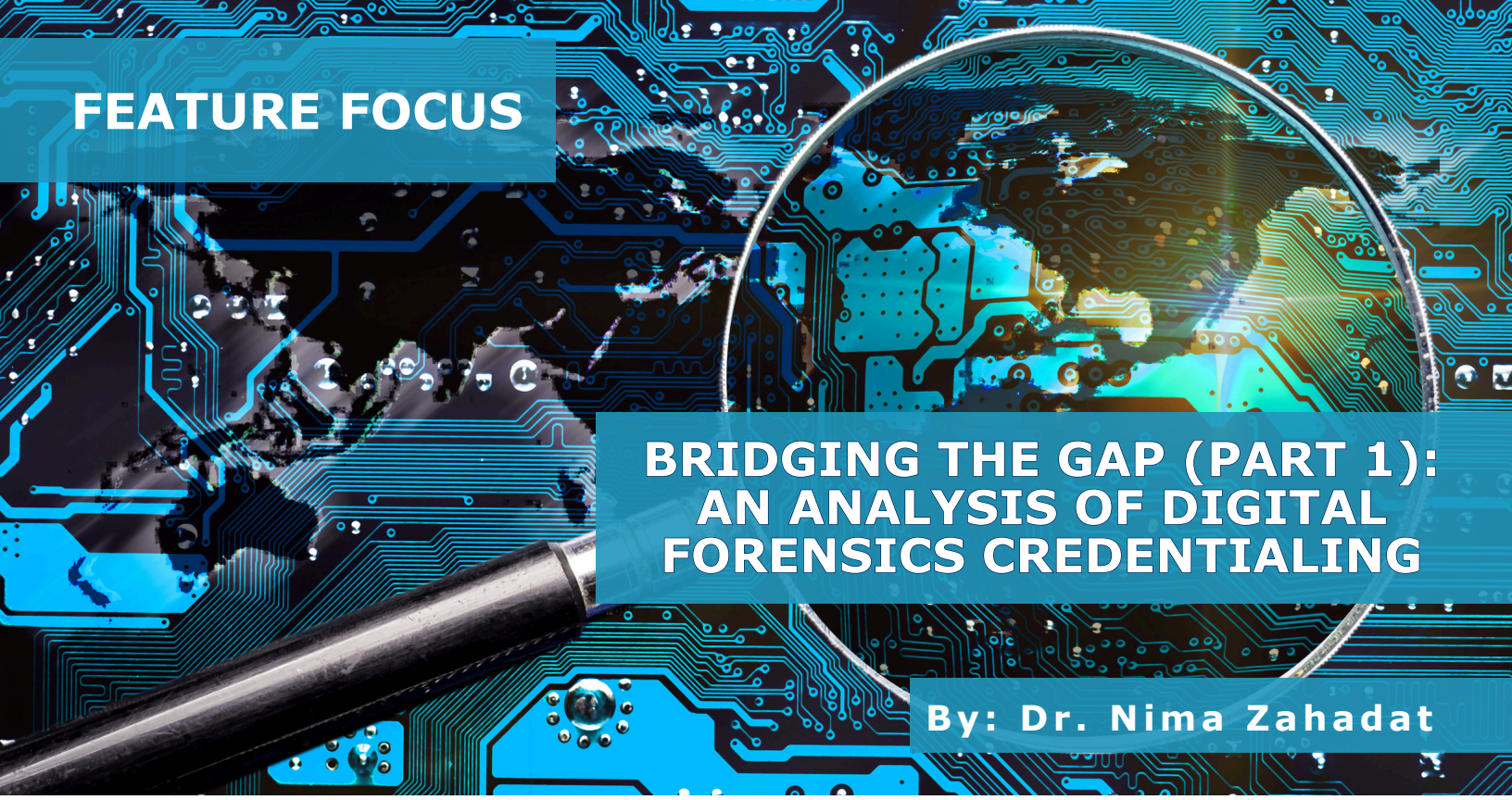

FEATURE FOCUS

BRIDGING THE GAP (PART 1): AN ANALYSIS OF DIGITAL FORENSICS CREDENTIALING

By: Dr. Nima Zahadat

In the medical and legal professions, credentialing and accreditation at the state and sometimes national levels are not merely formalities; they are fundamental requirements that ensure the competence and trustworthiness of practitioners. A doctor practicing medicine without a state license or a degree from an accredited institution would almost certainly face severe legal repercussions, including lawsuits and prosecution. Likewise, the public's trust in a lawyer is heavily contingent upon the lawyer holding proper credentials from an accredited university and certification by state or federal authorities. Even the role of a private investigator typically necessitates state licensing in most jurisdictions.

In stark contrast, the field of digital forensic investigation (or for that matter any forensics investigation), despite its critical role within forensic science, lacks such standardized and professional credentialing and accreditation requirements. Digital forensics, which has been evolving since the 1970s, has become increasingly vital as cyber-attacks and computer-related crimes have proliferated (Altheide & Carvey, 2011). This specialized area focuses on analyzing evidence from digital sources such as computers, mobile devices, storage systems, social media platforms, and cloud services, to support legal proceedings and other investigative processes (Mohay, 2005). Core activities in digital forensics include data extraction, collation, carving, and the preparation of detailed forensic expert reports.

However, despite the field's growing importance, there are no universally recognized national or state standards for digital forensic credentialing. While some states have attempted to introduce such standards, these efforts have frequently been inconsistent and disorganized, often leading to more complications than resolutions within the legal system. A common process has been the tendency of states to conflate digital forensic credentialing with private investigator (PI) licensing. This approach is problematic because the skills and expertise required for digital forensics differ significantly from those required for traditional PI work. Such an amalgamation raises concerns about the adequacy and appropriateness of the credentials held by digital forensic investigators.

The absence of standardized credentialing and accreditation in digital forensics poses a significant risk to the field's integrity and the legal processes that rely on it. Without clear and consistent standards, the validity and reliability of digital forensic evidence may be undermined, potentially jeopardizing the outcomes of legal cases. As the reliance on digital forensic evidence continues to grow in addressing cybercrimes and other technology-related offenses, the need for a rigorous and universally recognized system of credentialing and accreditation becomes increasingly urgent. Establishing such a system would not only enhance the professionalism and credibility of digital forensic practitioners but also ensure that the investigations they conduct meet the highest standards of accuracy, impartiality, and technical expertise.

To protect the integrity of the field and the legal outcomes it influences, it is imperative that a robust, nationally recognized framework for digital forensic credentialing be developed and implemented. This framework should be distinct from, yet complementary to, existing licensing requirements for other investigative professions, reflecting the unique challenges and demands of digital forensics.

Here are some examples of how some states and localities have addressed forensic investigation credentialing:

- **Alabama**: The state offers no forensic licensing credentials, but the city of Mobile requires a city-issued PI license for forensic work (Leonardo, White, & Rea, 2012).
- **Colorado**: The state does not mandate digital forensic requirements, and PI licensing is voluntary, allowing individuals to obtain PI licenses even if they have legal issues elsewhere.
- **District of Columbia**: Washington, DC requires a PI license for digital forensic examiners (Leonardo, White, & Rea, 2012).
- **Georgia**: The state requires digital forensic examiners to obtain PI licensing (Leonardo, White, & Rea, 2012).
- **Indiana**: As of 2010, Indiana has no credentialing or licensing requirements for digital forensic examiners (SANS, 2010).
- **Maine**: Similar to Georgia, Maine mandates PI licensing for digital forensic examiners (Leonardo, White, & Rea, 2012).

- **Maryland**: Maryland requires a PI license for private investigations but does not address digital forensic licensing or credentialing.
- **North Carolina**: The state has no licensing requirements for forensic investigators (SANS, 2010).
- **Oklahoma**: Oklahoma permits the use of a PI license from another state for temporary licensing, a practice that can be exploited.
- **Texas**: The state requires digital forensic examiners to be licensed as PIs and even includes computer technicians and repair personnel in this requirement (Leonardo, White, & Rea, 2012).
- **Virginia**: In 2011, Virginia codified that PI licensing requirements do not apply to certified forensic individuals employed as expert witnesses. The state has reciprocity agreements with several others, including Georgia (Leonardo, White, & Rea, 2012).

Many states, including New York, Nevada, North and South Carolina, Washington, and Virginia, are increasingly directing private investigators (PIs) to handle digital forensic investigations. However, none of these states provide a clear pathway for independent digital forensic licensing and credentialing, leaving a critical gap in the standardization and professionalization of this emerging field.

A needs analysis conducted by Rogers & Seigfried (2004) identified training and certification as major obstacles, a sentiment echoed by the National Institute of Justice and other key stakeholders. The discipline remains fragmented, with no national framework for curriculum development or standardized training. Pollitt (2010), drawing on over 20 years of experience as a criminal investigator, highlighted the lack of reliable data and rigorous standards in his paper, "A History of Digital Forensics." He underscores the urgent need for a universally accepted certification standard to ensure consistency, credibility, and professionalism across the field.

The National Institute of Standards and Technology (NIST) addressed some of these challenges by publishing Special Publication 800-181, known as the National Initiative for Cybersecurity Education (NICE). This framework aims to establish a common lexicon, foundational frameworks, workforce categories, specialty areas, roles, and detailed knowledge, skills, and abilities required in cybersecurity work. While NICE provides a valuable foundation for the development of digital forensics frameworks and academic curricula, its focus is predominantly on cybersecurity, leaving gaps in addressing specific needs for forensic training, credentialing, and accreditation.

Furthermore, agencies like the NSA and DHS have developed programs to recognize institutions that meet certain standards. The Centers of Academic Excellence in Cyber Defense (CAE-CD) program, co-developed by the NSA and DHS, allows regionally accredited colleges and universities to apply for designation. While such programs are attractive, they remain voluntary and fragmented solutions. These programs focus primarily on cybersecurity processes, rather than offering a comprehensive framework for digital forensics credentialing and accreditation.

As digital forensic investigations become increasingly central to addressing cybercrime and related offenses, the establishment of a robust, universally recognized credentialing and accreditation system becomes more and more essential. Such a system would not only enhance the credibility of digital forensic professionals but also ensure that investigations are conducted with the highest standards of accuracy, impartiality, and technical expertise.

LITERATURE REVIEW

Numerous studies in the field of digital forensic investigations have highlighted a prevailing bias in research, which tends to focus more on applied aspects of the domain rather than on the development of fundamental theories. This bias, however, is not without justification, given the practical nature of forensic science and the increasing pressure from external factors such as cyber-terrorism and cyber-crimes, which demand more applied research (Nelson, Phillips & Steuart, 2014). As digital forensic investigations evolve, the issue of credentialing at various levels falls squarely within the realm of applied research, perpetuating this bias. Nevertheless, there is strong evidence to support the claim that the lack of a standardized credentialing process remains one of the primary challenges facing the profession today. For example, a study by Flory (2015) revealed that despite Indiana's law enforcement agencies' deliberate efforts to provide digital forensic training, where half of their staff were trained, their capabilities were still rated from low to mid-range. This underscores the urgent need to establish a standardized and comprehensive framework for identifying experts, developing forensic insights through standard operating procedures, and supporting career advancement in the field. The study also highlights the long-standing challenge of credentialing and locating competent experts in digital forensics, further justifying the focus of research in this direction rather than on fundamental theories.

The challenge of credentialing, while significant, seems to be overshadowed by the even more pressing issue of a lack of consistent curriculum development in digital forensics. Consequently, a substantial amount of research is currently devoted to advancing training and creating a teaching framework that can be widely adopted by universities and colleges. Lang et al. (2014) emphasize that the development of a digital forensics curriculum should result in a comprehensive and self-contained tool for teaching the discipline at the university level, given that many institutions fail to offer such courses due to missing entry requirements. Their proposed curriculum includes introductory and advanced courses, along with hands-on laboratory programs. However, they notably fail to address the critical role of credentialing in the development of digital forensic investigators. This omission is consistent across most curricula and reports on the status of digital forensics and related disciplines. For instance, a report by the West Virginia University Forensic Science Initiative (2007), submitted to the Department of Justice (DoJ) on the training and education of digital forensic investigators, provides detailed qualifications and career paths but omits essential information on credentialing. The report is thorough in its coverage of training and career paths, detailing the qualifications, skills, and knowledge required at the Associate, Baccalaureate, and advanced levels, yet it makes a significant omission by not addressing certifications and credentials. This encapsulates the broader credentialing challenge in existing studies, where the issue is often obscured by the lack of a clear training and education framework for digital forensic investigators.

The literature on establishing accreditation and credentialing in digital forensics is relatively sparse and lacks appeal. This is primarily due to the inherent confusion surrounding the field of digital forensics itself. Losavio et al. (2016) make the bold assertion that digital forensics has not yet achieved the status of a profession, and they attempt to justify this claim on several grounds. According to their paper, a profession requires specialized knowledge, training, highly valuable work, self-regulation, a code of ethics, high levels of autonomy, and other significant elements. Certification and credentialing are the means by which a code of ethics, autonomy of practice, and evidence of specialized training are established elements that are currently lacking in digital forensics, according to Losavio et al. (2016). This deficiency has hindered the development of digital forensics as a recognized profession. Several studies have indeed recommended the establishment of standardized frameworks for credentialing digital forensic investigators. Butler (2015) highlights several such recommendations from the National Academy of Sciences (NAS), which include the creation of a standardized accreditation model to achieve recognition, consistency, and the designation of "expert" status for digital forensic investigators.

From the available literature, it appears that a robust framework exists for providing oversight to various accreditation bodies in digital forensics. This includes organizations such as the National Institute of Standards and Technology (NIST), the Department of Justice (DoJ), and the Organization of Scientific Area Committees (OSAC), which have collaborated to conduct research and establish a framework for operationalizing accreditation bodies. The National Commission on Forensic Science, for its part, acts as an advisory body to the DoJ and plays a critical role in the framework for accreditation, which includes advising on training in science and law, testimony and reporting, providing interim solutions, and overseeing accreditation and proficiency testing (Garfinkel et al., 2009). Although a consistent accreditation framework is lacking, there is a clear structure in place to regulate the bodies that offer credentialing.

The development of accreditation oversight in digital forensics has been reported at the national level, coordinated by the DoJ with the advice of NIST. These frameworks have emerged as a product of OSAC's efforts. According to Butler (2017), OSAC has been instrumental in the development and promulgation of technically appropriate and universally accepted documentary standards used by accrediting bodies to audit forensic laboratories and credential forensic investigators. OSAC has since expanded to include a Forensic Science Standards Board, along with various committees and subcommittees responsible for overseeing the approval process for forensic science standards as developed by different scientific area committees.

There are several credentialing bodies, many of which are international, that operate within the field of digital forensics. Gladyshev, Marrington, & Baggili (2014) note that most of these organizations are either for-profit or privately owned, with the government merely providing the operational framework for these bodies to conduct certification and accreditation. These organizations include companies like Mile2 and ISC2, as well as entities such as the EC-Council, the American Board of Information Security and Computer Forensics (ABISCF), the International Association of Computer Investigative Specialists (IACS), and the International Society of Forensic Computer Examiners (ISFCE) (Freiling & Schwittay, 2007). Some of these bodies, particularly ISC2, utilize the standards and frameworks issued by organizations 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 NIST guidelines, specifically the 800 series, including 800-86 (Guide to Integrating Forensic Techniques into Incident Response), 800-37 (Risk Management Framework), 800-30 (Risk Management Guide), 800-39 (Managing Information Security Risks), 800-53 (Security Controls), 800-53A (Security Control Assessments), and 800-137 (Continuous Monitoring), among others. Other organizations, such as the EC-Council, have long offered certifications in the field and continue to update and revise their offerings to appeal to government agencies and private organizations. These certifications are updated every three to five years, with new material added, outdated material removed, and an emphasis on skills sought after by today's forensic and security professionals. The proliferation of private organizations offering a wide range of certifications, many of which focus on digital forensics, underscores the need for a formal credentialing and accreditation process and highlights how these organizations are capitalizing on the opportunity to advance their own, primarily financial, goals, even when labeled as non-profit.

CASE STUDIES

The National Academy of Sciences emphasizes the critical importance of implementing robust quality assurance procedures in forensic science. These procedures are designed to "identify mistakes, scientific fraud, examiner bias, and to confirm the continued validity and reliability of forensic processes, while also improving processes that require enhancement" (Jordaan, 2012). In the context of digital forensics, a comprehensive quality assurance and management plan is essential to maintaining the credibility of digital forensic laboratories. Both the National Research Council in Washington, DC, and the Association of Chief Police Officers in London recognize quality assurance in digital forensics as a pivotal issue. As recent years have shown, the failure to implement such procedures can lead to grave miscarriages of justice, including the wrongful conviction of innocent individuals (Jordaan, 2012).

A notable case illustrating the dire consequences of inadequate digital forensic practices is that of Connecticut school teacher Julie Amero. In the 2004 case of State of Connecticut v. Julie Amero, Amero was wrongfully convicted due to a lack of understanding and proper handling of digital forensic evidence (Alva & Endicott-Popovsky, 2012). Amero, a substitute teacher, was supervising a seventh-grade classroom when students accessed a website that triggered a series of pornographic pop-up advertisements. Unaware of how to stop the pop-ups, Amero followed school instructions not to shut down the computer, inadvertently exposing students to inappropriate content.

During the trial, the prosecution's case hinged on a forensic copy of the computer's hard drive, which was improperly handled and did not adhere to industry standards. The digital forensic investigator failed to use appropriate methods to copy the hard drive, yet the evidence was still admitted in court. The prosecution argued that the computer's Internet history indicated Amero had intentionally accessed pornographic websites, leading to her conviction for "Risk of Injury to a Child" and a potential 50-year prison sentence (Alva & Endicott-Popovsky, 2012).

However, a defense expert, Herb Horner, later discovered that the school's computer was severely compromised due to outdated antivirus software and the lack of antispyware, a firewall, or a content filtering tool. Horner's analysis revealed that spyware on the computer was responsible for the pornographic pop-ups. Despite this critical evidence, the judge refused to allow Horner's full testimony, citing procedural issues during the discovery phase (Alva & Endicott-Popovsky, 2012). Although Amero's conviction was eventually overturned by the State Court of Appeals, and she accepted a plea to a lesser charge to avoid further legal battles, the case caused significant emotional, social, and financial harm to her and her family.

This case starkly demonstrates the fallibility of digital forensics when quality assurance is neglected. However, poorly executed digital forensics does not only risk convicting the innocent; it can also lead to guilty individuals being acquitted. A case in point is that of Aaron Caffrey, who was charged with launching a denial-of-service (DDoS) attack on the Port of Houston, Texas, shortly after the September 11, 2001, terrorist attacks.

During his trial, Caffrey claimed that malicious actors had installed a Trojan horse on his computer, which then carried out the attack without his knowledge. Although the prosecution's expert, Professor Neil Barrett, found tools on Caffrey's computer that could be used to launch such an attack, no evidence of a Trojan horse was detected. Nevertheless, Caffrey was acquitted, largely due to the defense's argument that the Trojan horse, armed with a sophisticated "wiping tool," had erased all traces of its existence from the system logs (Brenner, Carrier, & Henninger, 2004). This case is a classic example of the "Trojan horse defense," a strategy that became increasingly common in the UK during the early 2000s, where defendants claimed their computers were hijacked by malware to carry out criminal activities without their knowledge (George, 2003).

Perhaps the most egregious of these cases is that of Gene Morrison from Manchester, UK. Gene Morrison was a man who managed to deceive the British legal system for nearly three decades, posing as a forensic expert despite having no formal qualifications in forensic science. His story is a startling example of how one individual's deceit can have far-reaching consequences in the justice system, leading to wrongful convictions, miscarriages of justice, and a significant breach of public trust.

Gene Morrison, originally from Hyde, near Manchester, began his fraudulent career in the 1970s. With no formal education or training in forensic science or for that matter in anything else, Morrison nonetheless established himself as a forensic expert, creating a business under the name "Criminal & Forensic Investigations Bureau" (CFIB). He claimed to hold advanced degrees and multiple qualifications in forensic science, psychology, and criminology, all of which he entirely fabricated.

Morrison was a master of deception. He produced impressive-looking reports filled with scientific jargon, which he used to present himself as a credible expert witness in court. His reports and testimonies were accepted in more than 700 cases, including criminal trials, civil disputes, and family court proceedings. Over the years, Morrison's "expertise" was trusted by law enforcement agencies, solicitors, and judges across the UK, as he built a reputation for being a reliable and knowledgeable forensic consultant.

For over 26 years, Gene Morrison's fake credentials went unquestioned, allowing him to operate with impunity. The consequences of his fraud were severe. His testimonies and reports were instrumental in numerous legal decisions, some of which led to wrongful convictions or acquittals. Innocent people were sentenced based on his flawed and often completely fabricated testimonies and/or evidence, while the guilty were sometimes exonerated. The lives of many individuals and families were irreparably damaged by the trust placed in Morrison's false expertise.

One of the most alarming aspects of Morrison's deception was the breadth of cases he influenced. From criminal trials involving serious charges like murder and sexual assault to sensitive family court cases, Morrison's fraudulent testimony factored in a wide array of legal outcomes. His ability to evade detection for so long was a testament to the lack of rigorous vetting of expert witnesses at the time in the United Kingdom.

Gene Morrison's downfall began in 2005 when suspicions arose about the authenticity of his qualifications. Up until then, Morrison had relied primarily on the process of taking court forensics cases and contracting them out to third party professionals. It appears that after such a long streak of good luck, his confidence had gone to his head, and he truly believed that he had been the real investigator. For one of his 2005 cases, he decided to handle the case by himself which arose the suspicious of the police. A police investigation was launched after one of his reports was found to be suspiciously lacking in basic forensic details and professionalism. As investigators delved deeper into Morrison's background, they discovered that he had no legitimate qualifications in forensic science or any related field. His entire career was built on lies and forged documents, including his degrees all of which had been forged.

In 2007, Morrison was brought to trial at Minshull Street Crown Court in Manchester. During the trial, it was revealed that Morrison had never received any formal education beyond basic schooling. He had purchased his fake doctorate from a bogus university in the United States and had been fabricating investigations, evidence, and testimonies for decades. The court heard how Morrison had copied information from textbooks and later, Internet sources to create his reports. It was revealed how Morrison had contracted outside experts, and then presented such works as original forensic analyses of his own doing.

Morrison was found guilty of 22 charges, including perjury, obtaining money by deception, and perverting the course of justice. He was sentenced to five years in prison. The case sent shockwaves through the legal community, leading to the reopening of numerous cases in which Morrison had been involved. Many of these cases had to be reviewed, and in some instances, convictions were overturned. It was further found out later that Morrison had been a child molester all these years and many young girls had been sexually molested by him. His sentence was updated to be indefinite.

The exposure of Gene Morrison's fraud highlighted significant flaws in the UK's legal system, particularly in the process of vetting and accrediting expert witnesses. The case underscored the need for more stringent checks on the qualifications and credentials of those who present themselves as experts in court.

In response to the scandal, there were calls for reforms in how forensic experts are vetted and accredited. The case served as a catalyst for discussions about the need for a national registry of accredited forensic experts, as well as the implementation of more rigorous standards for expert testimony in court. Although Morrison's case was particularly egregious, it drew attention to the broader issue of ensuring that forensic science in the UK, the US, and elsewhere to be conducted with integrity, professionalism, and accountability.

Gene Morrison's story is a cautionary tale of how one individual's deceit can infiltrate and corrupt the justice system, leading to profound consequences for countless lives. It is a reminder of the importance of due diligence in the legal process and the need for ongoing vigilance to protect the integrity of forensic science. A documentary was created about Gene Morrison, his rise to fame, his deception, and his eventual downfall. It can be watched online on YouTube.

These cases underscore the profound impact that lack of rigorous quality assurance in digital forensics can have on the judicial process. They highlight the necessity for stringent standards and protocols to ensure that digital forensic evidence is handled, analyzed, and presented with the utmost care and precision. Without such standards, the integrity of the legal system is at risk, as both wrongful convictions and unjust acquittals become more likely. As digital evidence plays an increasingly central role in modern criminal investigations, the establishment and enforcement of comprehensive quality assurance measures in digital forensics are not just advisable, they are essential.

CONCLUSION

The lack of a standardized framework for credentialing digital forensic professionals represents a clear vulnerability in the evolving landscape of cybercrime and digital evidence. As the cases of Julie Amero, Aaron Caffrey, and Gene Morrison starkly illustrate, the stakes are very high: improper handling of digital forensic evidence can lead to wrongful convictions, acquittals of guilty parties, and breaches of public trust. These examples highlight the critical consequences of inadequate practices as well as emphasize the systemic flaws that allow such failures to persist. Without rigorous credentialing and quality assurance measures, the integrity of digital forensics and the justice system itself hangs in the balance.

While existing efforts by organizations like NIST, OSAC, and private credentialing bodies have made strides toward addressing these concerns, their fragmented and often voluntary nature have failed to provide a unified standard. This lack of cohesion leaves room for unqualified practitioners to exploit gaps in the system, eroding the credibility of digital forensics as a profession. Furthermore, the conflation of digital forensic expertise with private investigation licenses in many jurisdictions reflects a fundamental misunderstanding of the specialized skills required for forensic work, underscoring the urgent need for distinct and universally recognized credentials.

The cases discussed in this paper underscore a broader truth: as technology continues to advance, the demands on digital forensic investigators will only increase. This complexity necessitates not just technical proficiency but also a robust framework for ensuring accountability, professionalism, and adherence to ethical standards. A nationally recognized credentialing system, aligned with world-wide best practices and informed by the expertise of seasoned professionals, would bridge the gap between the current ad hoc approaches and a truly professionalized field.

In future follow up articles, the key findings of the research will be presented along with outlines for a credentialing framework and then the framework itself. Those professionals wishing to contribute their time and expertise in this endeavor are respectfully thanked in advance.

Dr. Nima Zahadat is a professor of security, digital forensic, and data science. He is also a professional consultant in the IT security industry. He has 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. Dr. Zahadat has worked extensively with public and private sectors throughout the years.

Dr. Zahadat has taught at University Systems of the Washington, DC metro area in the fields of forensics, data science, information systems, web development, systems engineering, and security. He has developed and taught over 120 different data science, information systems, security, and forensics courses among others throughout his career. He has a graduate degree in Information Systems and a Ph.D. in Systems Engineering and Engineering Management from the George Washington University. Dr. Zahadat is also a member of the ISSA-NOVA Chapter, in Northern Virginia.

REFERENCES [Bridging the Gap (Part 1): An Analysis of Digital Forensics Credentialing]

[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.

[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; & 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.