PI magazine .com

professional investigator magazine

$8.95

July/August 2022

CHILD SEXTORTION AND THE WORLD OF GAMING

EXECUTIVE PROTECTION I.P.S.

ETHICS AND THE INVESTIGATIVE PROCESS

FROM SPY TO PI

DEPARTMENTS

IN EVERY ISSUE

Digital Forensics Laboratory Accreditation

BY **ROBERT B. FRIED,** SENIOR VICE PRESIDENT, FORENSICS & INVESTIGATIONS, SANDLINE GLOBAL
ANNA ALBRACCIO, GRADUATE STUDENT INTERN (UNIVERSITY OF NEW HAVEN), SANDLINE GLOBAL
JASON SCHEID, GRADUATE STUDENT INTERN (UNIVERSITY OF NEW HAVEN), SANDLINE GLOBAL
HANNAH WESTWOOD, GRADUATE STUDENT INTERN (UNIVERSITY OF NEW HAVEN), SANDLINE GLOBAL

The fields of digital forensics and eDiscovery are dynamic. For clients seeking service providers in these fields, it is important to consider engaging a firm that is innovative, known for client excellence, and adheres to strict operating procedures, including defined and defensible processes. Sandline Global has recently applied for an international accreditation for its state-of-the-art digital forensics laboratory in New York City. Much has been learned throughout this rigorous, and eye-opening process.

International Organization of Standardization (ISO) / International Electrotechnical Commission (IEC) 17025 specifies the general requirements that are needed for a laboratory to competently execute tests and calibrations in a laboratory. It is useful to any organization or laboratory that performs testing, sampling, or calibration. The ISO/IEC 17025 enables laboratories to conduct their operations accurately and provide valid results, ensures that the laboratory's processes are standardized and that its results can be confidently accepted by an outside party.

THE PROCESS

The process for ISO/IEC 17025 accreditation requires laboratories to meet and exceed standards for operation, quality control, and client relations. The ANSI National Accreditation Board (ANAB) defines requirements according to the ISO/IEC, which outlines rigorous standardization for over 2,500 organizations worldwide. An approved laboratory uses these standards to ensure a universal quality control process for clients and industry relationships alike. Becoming accredited by ANAB requires extensive documentation of Standard Operating Procedures (SOPs) that meet or exceed criteria. To start, an organization must prepare an application that outlines SOPs and highlights the laboratory's Quality Assurance Manual (QAM) - the basis for the application process and the foundation for laboratory operations. The application is submitted to ANAB and thoroughly audited for quality and appropriate preparedness.

Earning this accreditation does more than set a standard for the approved organization. Being internationally recognized for accreditation improves client relations, validates forensic results, and affirms a principle of quality service. Clients can expect an accredited organization to be up to par with industry-leading technologies and protocols. This ensures a level of security and safety when trusting an organization with sensitive data.

STANDARDIZATION

An organization that has achieved accreditation is permitted to state that the policies and procedures within its laboratory are internationally recognized. An accredited laboratory is one that is acknowledged for its testing reliability, operational performance, and quality management; adhering to designated quality standards that add to the framework of how the laboratory is operated and managed. The overall management of a digital forensics laboratory, especially one that is accredited, reflects on the quality of the results it yields. It is important to ensure that standards are met and exceeded as time goes on. Accreditation offers a level of reputability that sets a standard for laboratories throughout the world.

The ISO/IEC offers procedures for areas within a laboratory, notably risk management and information security management, which are made to be followed by laboratories throughout the world. There are also standards for specific accredited laboratories such as handling food products and medical equipment which should be followed to ensure that each is meeting and exceeding the industry standards. As a reference, a medical laboratory will follow ISO 15189, requiring specific standards in technical competency, relating to analytical functions, but within digital forensic laboratories, ISO/IEC 17025 allows for a more general focus on operating procedures.

Additionally, these standard procedures used by the laboratories offer a level of safety and security for the data analyzed and stored within. A client's data is of top priority, so it is important to enact strict policies and procedures related to the handling, storage, and security of data within a firm's possession. For example, Sandline Global has implemented dual-authentication security measures for entry into its digital forensics laboratory, and an advanced surveillance system to monitor activity in and around the laboratory.

ACCREDITATION: FROM THE GROUND UP

Playing a key role in an accreditation process has been an invaluable experience. The overall process highlights the importance of being accredited but also what it means to be accredited. Some of the key takeaways include:

- Proper procedures and requirements are needed to operate a digital forensics laboratory.
- The importance of standardization and best practices.
- Greater insight on defining processes that are defensible and efficient. **PI**

Robert B. Fried is a seasoned expert and industry thought-leader, with over twenty years of experience performing data collections and forensic investigations of electronic evidence. He is the Senior Vice President and Global Head of Sandline Global's Forensics and Investigations practice. In this role, Robert leads the day-to-day operations of the practice, overseeing the forensic services offered to the firm's clients, including data collections, forensic analysis, expert testimony, and forensic consultation. Previously, Robert held senior-level positions within the digital forensic practices at global professional services firms. Additionally, Robert was a Computer Crime Specialist at the National White Collar Crime Center

(NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state, and local law enforcement agencies. He attained a BS and MS in Forensic Science, and certificates in Law Enforcement Science, Computer Forensic Investigation, and Information Protection and Security from the University of New Haven. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven. He holds and actively maintains the following industry certifications: Access Data Certified Examiner (ACE), Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE), GIAC Certified Forensics Analyst (GCFA), Chainalysis Cryptocurrency Fundamentals Certification (CCFC), Chainalysis Reactor Certification (CRC), and C4 Certified Bitcoin Professional (CBP). Robert is a licensed Professional Investigator in Michigan and is a licensed Private Investigator in New York. He is a frequent speaker at industry events, has been a guest on industry podcasts, and has been published in several professional publications. Robert is the author of Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes. Additionally, he is the author of PI Magazine's CyberSleuthing Department, where he shares insightful content on topics relating to digital forensics, eDiscovery, data privacy, and cybersecurity.

Anna Albraccio earned her B.S. in Forensic Science with a minor in Criminal Justice and a certificate in Digital Forensic Investigations from the University of New Haven and is currently earning her M.S. in Digital Forensic Investigations from the university as well. As an undergraduate, Anna was involved in various research projects, one even taking her to Australia, where she was able to conduct independent and collaborative projects as well as become experienced in technical writing and field-based research. She is a proud member of the International Association of Financial Crimes Investigators, which she was able to join in 2021. She has assisted in the creation of a Digital Forensics Organization at her University where she is working diligently with her professors to create an outlet for graduate students where they can create connections and experience inter-scholastic conferences within the field. Anna hopes that this organization will have a strong impact on the educational aspect within the realm of digital forensics, creating opportunities for students and professionals alike.

Hannah Westwood earned her B.A. in Criminal Justice Studies with a minor in Legal Studies from Westminster College in Pennsylvania and is currently earning her M.S. in Criminal Justice from the University of New Haven. She has extensive experience in technical writing, research, and forensic evidence management from her work at the Wisconsin Department of Justice, Division of Criminal Investigation. As an undergraduate, she has conducted independent, grant-funded research and presented at several academic conferences. She is a member of multiple professional organizations such as the Academy of Criminal Justice Sciences (ACJS), American Sociological Association (ASA), and Justice Research and Statistics Association (JRSA). Hannah is certified as a CITI Social Science researcher in both qualitative and quantitative methodologies. Hannah has centered her graduate experience on current topics in criminal justice, particularly on eDiscovery investigations and the use of forensic technologies. During her time at the WDOJ, Hannah worked closely with the National Center for Missing and Exploited Children as a digital forensics intern working with Internet Crimes Against Children on criminal sex offense cases.

Jason Scheid earned his B.A. in Criminology with a minor in Sociology from Hofstra University and is currently obtaining his M.S. in Investigations with a concentration in Digital Forensics along with a Graduate Certificate in Cybercrime Investigations from the University of New Haven. During his studies at the University of New Haven, Jason was able to become a proud member of the International Association of Computer Investigative Specialists (IACIS) in 2021. Jason has extensive knowledge of SOPs and SOGs from his diverse background in firefighting and electric distribution system operations.