DELAWARE STATE BAR ASSOCIATION

CONTINUING LEGAL EDUCATION

Linking the Blocks: Combining Blockchain and Traditional Data Sources for Collections

May 14, 2024, 12:00PM – 1:00PM

Live at the DSBA

DSBA WiFi Access

Seminar Materials

Sponsored by Parcels Inc.

1.0 Hour of CLE credit in Enhanced Ethics for Delaware and Pennsylvania Attorneys

In this CLE, we'll explore the ledger of user operations on blockchain networks as a key data source, focusing on how to find and interpret this data. We'll also delve into linking more traditional off-chain data sources with on-chain activity to demonstrate how on-chain data can enhance off-chain information.

Blockchain data, by its very nature, is immutable, transparent, and permanent. Collecting and analyzing this "on-chain" data can provide information critical to internal investigations and discovery. When links between traditional "off-chain" data sources can be made to the comprehensive on-chain data, the results can be illuminating. This program will describe the intersection between on-chain and off-chain data and how links between those data sets can be established to enhance investigations and discovery.

Visit www.dsba.org/cle or all the DSBA CLE seminar policies. Please note that the attached materials are supplied by the speakers and presenters and are current as of the date of this posting.

DELAWARE STATE BAR ASSOCIATION

Speaker:

Scott Pearson
Parcels Inc.

Speaker:

Greg Strong, Esquire
DLx Law

Visit www.dsba.org/cle or all the DSBA CLE seminar policies. Please note that the attached materials are supplied by the speakers and presenters and are current as of the date of this posting.

Scott Pearson

scott.pearson1@outlook.com • (973) 216-8055
www.linkedin.com/in/pearsonscott/ • Wilmington, DE, 19801

Director of Digital Forensics / ISMS Lead

Diligent and goal-focused manager experienced in defining direction/strategies for government agencies, as well as private firms.

Instrumental in implementing strategic procedures involving the forensic collection and analysis of ESI from multiple sources including cloud repositories, document collaboration platforms, mobile devices, computer systems, network servers, social media platforms, and the Dark Web in support of ongoing litigation. Demonstrated success in providing network-based and host-based incident response, while focusing on assessing cyber security position by identifying gaps and enterprise-level network security weaknesses to provide appropriate solutions. Remarkable efficiency in leading and mentoring multi-faceted teams on many cases both domestic and international, involving the forensic acquisition and analysis of digital evidence. Articulate communicator possessing excellent problem-solving and analytical skills with keen attention to detail.

Areas of Expertise

- Cybersecurity / Linux Security
- Risk Identification & Mitigation
- Critical Solutions & Consultations
- Digital Forensics Investigations
- Data Collection, Analysis & Interpretation
- Team Coordination & Leadership
- Staff Training & Development
- Performance Improvement
- Program Management

Technical Proficiencies

Platforms:	X-Ways Forensics, Magnet Axiom, EnCase Forensic, Access Data FTK, Autopsy, Volatility, SIFT, Oxygen Forensics, Cellebrite UFED & Physical Analyzer, Apple Macintosh, Microsoft Windows, Microsoft Office 365, Google Workspace, Linux, X1 Social Discovery, Kali Linux, Tenable Nessus Pro, Nmap

Career Experience

Parcels, Inc. – Wilmington, DE **2020 – Present**
Director of Digital Forensics / ISMS Lead

As division lead, tasked with the creation and execution of technical solutions for a top eDiscovery/Litigation support service provider. Responsibilities include the forensic collection of electronically-stored information (ESI) from data custodians and the integration of gathered digital evidence into legal review platforms (i.e. RelativityOne). Routinely consult with lead counsel and law firm partners to implement strategies and ensure complex case requirements are met.

As ISMS Lead, oversee the security steering committee in charge of the creation, implementation, and careful maintenance of security policies, procedures, and guidelines, all to uphold the ISO 27001 certification. Successfully led transition from ISO 27001:2013 to ISO 27001:2022 standard.

San Diego State University | USSS National Computer Forensics Institute – San Diego, CA / Hoover, AL **2018 – Present**
Adjunct instructor | Lead Instructor

Conduct technical training sessions at the campus for students enrolled in the highly acclaimed Cybersecurity Professional Program. Act as a certifying instructor or the nationally recognized BCERT program, to deliver training in digital forensics to United States law enforcement, including Municipal Police, State Police, and Sheriff's Department, on behalf of the US Secret Service.

- Certified 100+ LE analysts in digital forensics and incident response on behalf of the US Secret Service for the highly selective BCERT program.

- Conducted regular consultations with major software and hardware commercial vendors on feature requests, overall functionality, and integrity of tools, focusing in digital forensics and incident response.
- Achieved over 90% matriculation into the Cybersecurity Professional program at San Diego State University and California State University Long Beach.

Digital Shield, Inc. – Palm Bay, FL **2015 – Present**
Consultant

Oversee and execute operations ranging from in-depth analysis and technical assistance to training and mentorship for foreign/domestic law enforcement and private entities on various aspects, such as forensic acquisition of digital evidence; digital forensics analysis (computer-based, network-based, mobile devices); network-based investigations; cybersecurity; vulnerability assessments; penetration testing, incident response; social media / dark web investigations; and course development / technical training on digital forensics, triage, incident response, Internet-based investigations, and cybersecurity. Coordinated with wide-ranging clients, including Virginia State Police – High Tech Crimes Unit; Northern Virginia Internet Crimes Against Children Task Force (ICAC); Southern Virginia Internet Crimes Against Children Task Force (ICAC); US DoS Anti-Terrorism Assistance Program; and CGH, Inc.

- Performed digital forensics of servers, workstations, mobile devices, and social media targets, submitted as evidence in high-profile cases for private sector clients.
- Assessed network security posture of private-sector clients, while coordinating with senior-level management for expediting the implementation of gaps identification and mitigation.

US Department of State Anti-Terrorism Assistance – Vienna, VA **2004 – 2020**
Consultant/Digital Forensic Analyst

Develop and deliver training curriculum for basic and advanced-level courses in DFIR and Network Security, while overseeing digital forensics, internet-based investigations, and cyber security on behalf of the US Dept of State to High-Tech Crime Units and digital forensic labs of Allied nations worldwide. Bolster productive relationships with foreign law enforcement and military personnel responsible to combat cyberterrorism. Organize and lead multiple teams into insurgent hot zones for aiding in design and establishing digital forensic labs for extracting evidence from computers and mobile devices seized as part of ongoing operations.

- Designed, developed, and delivered course development, technical training, and digital forensic lab mentorships to government analysts of over 35 Allied nations worldwide, including Pakistan, India, UAE, Egypt, Jordan, Kenya, Ethiopia, Morocco, Colombia, Paraguay, Mexico, Philippines, Thailand, Singapore, Jamaica, Trinidad and Tobago, Antigua, The Bahamas, Kazakhstan, Albania, Indonesia, Malaysia, Turkey, Brazil, and Oman.
- Consulted with US DoS Diplomatic Security agents on the DFIR capabilities of Allied nation operatives, such as foreign LE, Military, and private sector consultants, and overall network security posture of foreign LE agencies.
- Successfully led small team of cybersecurity analysts into Athens, Greece on behalf of the US DoS during the 2004 Summer Olympics to guide the Greek military analysts responsible for securing the Olympic Security Data Network (OSDN).

Additional Experience

US Department of Defense Computer Investigations Training Academy, Instructor - Linthicum, MD

Education

Master of Science in Cybersecurity
University of Delaware – Newark, DE

Bachelor of Arts in Information Systems
New Jersey Institute of Technology – Newark, NJ

Certifications

CompTIA Certified Information Systems Security Professional (CISSP) – *in progress*
IACIS Certified Forensic Computer Examiner (CFCE)
LPI Linux Essentials (LE-1)
US Secret Service National Computer Forensics Institute (NCFI) Certified Instructor, BCERT

Publications

Mastering Windows Network Forensics and Investigation, 2nd Edition
Published by Sybex Wiley

https://www.amazon.com/Mastering-Windows-Network-Forensics-Investigation/dp/1118163826