LIEN VUONG

718-208-7502 | lvuong28@yahoo.com | FLUSHING, NY 11355

OBJECTIVE

A passion-certified forensics examiner and eDiscovery practitioner, I have a proven track record of success in digital forensics engagements within corporate and consultant services. A dynamic self-starter capable of thriving both in team settings and independently, and open to domestic and international travel as necessary for business demands. I am actively seeking a challenging position where I can utilize my expertise to lead impactful initiatives and achieve outstanding results.

AREAS OF EXPERTISE/TOOLS

Digital Forensics: EnCase Forensics and Enterprise, FTK, Magnet Axiom Cyber, Cellebrite, KAPE, and Volatility.
eDiscovery: EnCase eDiscovery and Information Assurance, FTK Central, and RelativityOne.
Incident Response: Malware and intrusion detection analysis and memory forensics analysis.
Leadership: Allocate budget, staff supervision and mentorship, training, and performance evaluation.
Documentation: Development policies and procedures, incident response playbook and runbooks, chain of custody, presentations, technical reporting writing.
SIEMs: Microsoft Defender for Endpoint & O365, Defender Vulnerability Management, Azure Sentinel, and Log Analysis.

PROFESSIONAL EXPERIENCE

Forensics Services | Remote   **05/2023 – Current**

- Conducted various fraud forensics investigations, such as collection and in-depth analysis of the acquired evidence, adeptly identifying malware malicious artifacts, data exfiltration, and network instructions incidents.
- Proficiency in generating comprehensive information to ensure the integrity of the investigation process, strictly adhering to proper chain-of-custody protocols, and detailed reports to document artifacts and findings.

MorganFranklin Consulting | Consultant, Remote   **10/2022 – 04/2023**

- Demonstrated proficiency in conducting end-to-end forensics acquisition and analysis on Windows, MacOS, and cloud data sources for internal misconduct and fraud by utilizing state-of-the-art tools and adhering to best practices in evidence handling, report writing, a chain of custody, and courtroom or regulatory proceedings as required.
- Performed and analyzed intrusion detection of system alerts, Firewall, Network, and host Event Logs to determine the occurrence of unauthorized access and data exfiltration.
- Experience with forensic analysis of Registry, Memory, and Malware triage to uncover Indicators of Compromise (IoC) and malicious artifacts as part of investigative processes.
- Engaged with clients to establish technical best practices, delivering expert guidance on technology and development policies and procedures, incident response handbooks, and runbook documentation to optimize the effectiveness of forensic and cybersecurity incident handling.

Highmark Health | Contractor, Remote   **01/2022 – 07/2022**

- Engaged played a pivotal role in the ongoing forensic and cyber investigation, successfully migrating legacy EnCase eDiscovery tools, seamlessly integrated with Microsoft API to collect and preserve custodians' cloud data sources.
- Managed multiple litigations through the electronic discovery lifecycle, automated the legal hold process, and optimized each Electronic Discovery Reference Model (EDRM) step to reduce risks and costs through proposed workflows for eDiscovery matters.
- Actively contributed to developing innovative investigative methodologies, enhancing the capabilities of in-house forensic and eDiscovery services.
- Demonstrated effective leadership by managing the team, providing training, presentation and offering mentorship to ensure consistently high-quality casework outcomes.

Northwell Health, Manager promoted to Senior Manager, Merville, New York   **07/2013 – 09/2021**

- Recruited to build successful in-house forensics, eDiscovery practice, and team to support over 90,000 employees.
- Conducted forensic preservation and analyses of endpoints and mobile devices, uncovering employee misconduct, fraud, and intellectual property theft.
- Led complex insider threat and business email compromise investigations.
- Actively pursued process enhancements, implementing strategic initiatives such as policies and procedures, incident response playbooks, and runbooks to optimize investigative efficiency continuously enhance the overall effectiveness, and leverage cutting-edge technologies.
- Provided eDiscovery technology and support litigations and Legal Hold to internal legal and outside counsel by following the Electronic Discovery Reference Model (EDRM).
- Managed yearly hardware and software budgets, optimizing resource allocation and cost efficiency.
- Led and coached junior staff to enhance their professional growth and fostered a culture of continuous learning and sharing of knowledge and skills.
- Stay up to date with the latest trends and technologies, collaborating with other stakeholders to identify and implement process improvements to the enterprise's overall forensics and eDiscovery posture.

OpenText, Senior Consultant promoted to Principal Consultant, New York, NY   **05/2007 – 07/2013**

- Demonstrated expertise in conducting over a thousand forensics acquisitions and analyses across diverse custodian endpoints and mobile devices, delivering clear and concise forensic findings and reports to clients, and providing expert witness testimony as needed.
- Managed and liaised with the client's internal legal and external counsel on numerous complex eDiscovery across multiple countries involving 20,000+ custodians ESI during these high-profile litigation engagements.
- In the role of principal consultant, adeptly fostered client trust and identified new and secured additional engagements, resulting in six consecutive years ranking in the top 10% of billable hours.

Protiviti, Senior Manager, New York, NY   **02/2006 – 05/2007**

- Hand-on and acted as a technical liaison in forensics, adeptly addressing clients' technology challenges and collaborating on effective solutions to bridge gaps and enhance overall engagement efficiency.
- Spearheaded the extraction of significant data volumes and executed analysis, enabling efficient financial statement recalculations.

Ernst & Young, Global Investigations & Dispute Advisory Manager, New York, NY   **09/2003 – 02/2006**

- Hand-on and managed multiple forensics and cyber engagements, devising effective strategies that ensured timely delivery and accurate results, consistently surpassing customer expectations.
- Assisted clients in managing incident response engagements to address phishing, network intrusion, social engineering, ransomware, website defacement, and insider threat incidents.
- Played a pivotal role in supporting the Government Contract Services team in the recalculation of the Medicaid Drug Rebate program with SQL data warehouse.

CERTIFICATIONS
AWS Certified Cloud Practitioner (CCP), WIP
Association of Certified Fraud Examiners (CFE)
EnCase® Certified Examiner (EnCE)
EnCase® Certified eDiscovery Practitioner (EnCEP)
AD eDiscovery® Certification (ADED)
Summation Certified Administrator (SCA)

EDUCATION
STATE UNIVERSITY OF NY AT STONY BROOK
Master of Science in Management
Master of Science in Engineering
Bachelor of Electrical Engineering

VOLUNTEER FORENSICS AND INCIDENT RESPONSE (DFIR) WORKS
- Contribution to the Auxtera project – Magnet Forensic Inc. supplies digital forensics tools (Axiom Cyber), and I offer volunteer various forensic casework to nonprofit organizations.
- Engaging in SANS Work-Study, furthering my expertise in digital forensics and incident response.

CERTIFICATE OF COMPLETION/TRAINING
- SANS – FOR500, Windows Forensics Analysis, FOR508 Advanced Digital Forensics and Incident Response
- DFIR User Summit 2023 and work-study program.
- OpenText/Guidance Software – EnCase® Endpoint Security, Computer Forensics I and II, Advanced Computer Forensics, Advanced Windows Artifacts, Endpoint Investigator, EnScript Programming, and Imager
- Exterro/AccessData – FTK eDiscovery/Central, FTK Enterprise, and Imager
- Magnet Forensic – Yearly User Summit