WILLIAM OETTINGER

PHONE (702) 292-4645 • WOETTINGER@GMAIL.COM

SUMMARY OF QUALIFICATIONS

Veteran investigator in a traditional and computer-related environment. A leader experienced in organizing, directing, and motivating a diverse team of investigators in meeting goals and priorities. Proven law enforcement professional with over 20 years of responsible experience in local, military, federal and international law enforcement organizations. Multifaceted experience in digital forensics, security operations, law enforcement, criminal investigations, leadership, management and policy and procedures development. Excellent interpersonal, oral and written presentation skills to all levels of the organization. Critical thinker with strong analytical and critical thinking skills. Certified Forensic Computer Examiner (CFCE), EnCase Certified Examiner (EnCE) and Certified Hacking Forensic Investigator (CHFI), Network+, Security+. Certified Information Systems Security Professional (CISSP®). Court Certified Expert in Computer Forensics and General Investigations.

EDUCATION

2012 Tiffin University, Tiffin, Ohio
M.S Criminal Justice – Homeland Security Administration

2010 Columbia Southern University, Orange Beach, Alabama
B. S. Criminal Justice Administration

2006 Marshall University, Huntington, West Virginia
Certificate – Computer Forensics

PROFESSIONAL EXPERIENCE

2014 – Present Infosec Institute

Senior Instructor

I plan and implement curriculum for professional students attending Computer Forensics and CISSP courses nationwide. I support students in online and on-demand courses.

I am responsible for updating and maintaining the curriculum for the Computer Forensics Course.

I design content for students so that learning occurs, skills are developed, and students are motivated to learn and achieve their educational objectives.

1993 - 2014 Las Vegas Metropolitan Police Department

Detective

Sexual Abuse Juvenile Detail

Primary investigator for over 500 allegations of child sexual abuse utilizing standard investigative and enforcement techniques. Prepared investigative reports and analyzed data from numerous databases. Utilized databases such as National Crime Information Center (NCIC) and Lexis Nexis to gather information. Responsible for interviewing victims and witnesses as well as interrogating suspects. Responsible for the security of the crime scene and identifying and recovering evidence. Researched, collected and analyzed intelligence data related to criminal activities Completed all official reports, affidavits, arrest warrants and search warrants in accordance with policy and statute. Monitored, evaluated, and coordinated a variety of warrants. Provides sworn testimony in court proceedings. Maintained chain of custody to preserve evidence when required for possible legal utilization. Assessed areas of vulnerabilities in criminal investigations.

Electronic Crimes Unit

Primary investigator/examiner in regards to crime conducted through digital infrastructure. Primary investigator for over 100 investigations ranging from homicides, child pornography, child exploitation, fraud and forgery. Researched, collected and analyzed intelligence data related to criminal activities Provides investigative and enforcement support to numerous state, local and federal agencies as part of a federal task force with the United States Secret Service. Providing forensic analysis and data recovery on drive images and memory images. Maintain chain of custody to preserve evidence when required for possible legal utilization. Assessed areas of vulnerabilities in criminal investigations. Utilized databases such as National Crime Information Center (NCIC) and Lexis Nexis to gather information. Instructor for the United States Secret Service, Basic Investigation Computer Electronics Program (BICEP) and the Electronic Crimes Special Agent Program (ECSAP). Member of the Scientific Working Group on Digital Evidence (SWGDE) Computer Forensic Committee, participated in the creation of the following policy and procedure documents; "Best Practices for Computer Forensics", "Data Archiving" and "Technical Notes – Capture of Live Systems". Received and reviewed correspondence from federal agencies.

2007 - Present US Department of State, Anti-Terrorism Assistance Program

Senior Consultant

I provide education and mentorship to foreign law enforcement entities and military personnel of our allies on behalf of the United States Department of State Bureau of Diplomatic Security Anti-Terrorism Assistance Program (Cyber). I provide instruction on the following topics: Computer Forensics, Incident Response, Network Security, and Internet Investigations. I also conduct advanced consultations concerning emerging technologies and their impacts on law enforcement investigative and enforcement techniques. This includes consulting with the host country's Executive Command Staff for program development, budget preparation, and the development of policies and procedures for the creation and implementation of Electronic Crime Investigation Units and Digital Evidence Processing Facilities. I have consulted with the following Law Enforcement Agencies: Royal Police Force of Antigua and Barbuda, La Direction Générale de la Sûreté Nationale of the Kingdom of Morocco, Moroccan Royal Gendarmerie and the Ministry of the Interior of the Kingdom of Bahrain. I have taught the following courses or provided consultation services: Introduction to Digital Forensics & Investigations (IDFI), Identification & Seizure of Digital Evidence (ISDE), Identification & Seizure of Digital Evidence (ISDE), Identification & Seizure of Digital Evidence - Train the Trainer (ISDE-TTT), Digital Forensics Equipment Grant and Consultation (DFEGC), Digital Forensics Lab Mentoring Consultation (DFLMC).

1984 -Present United States Marine Corps (Reserve) - Criminal Investigative Division

Operations Chief

I managed a team of 8 CID Agents while operationally assigned to the Criminal Investigation Division, MCAS Miramar, San Diego Ca. I am responsible for the day-to-day operations for all CID operations in standard investigative and enforcement techniques, leading to improved command relationships and higher quality investigative reports. Providing forensic analysis and data recovery on drive images and memory images. Received and reviewed correspondence from federal agencies. Utilized databases such as National Crime Information Center (NCIC) and Lexis Nexis to gather information. Researched, collected and analyzed intelligence data related to criminal activities. Assessed areas of vulnerabilities in criminal investigations. Reviewed, corrected, and provide direction for over 40 Criminal Investigations and viewed, analyzed, and provided guidance for approximately 20 interrogations. I have been certified as a Subject Matter Expert in Computer Forensics and Criminal Investigations in Federal Military Court.

2014-Present University of Maryland University College

Adjunct Assistant Professor

I am an Adjunct Assistant Professor for the Digital Forensics Program at the Graduate School of the University of Maryland University College teaching digital forensics. I have taught the following Masters level class:

CSEC 661 Digital Forensic Investigations

A study of the processes and technologies used in the collection, preservation, and analysis of digital evidence in local, networked, and cloud environments. Discussion covers validating data, reporting evidence, and preparing depositions, as well as recovering information from encrypted, obscured, or deleted sources. Topics also include emerging forensic issues in computer, peripheral, and mobile environments and their global implications.

CSEC 662 Cyber Incident Analysis and Response

An examination of policies and procedures related to security incidents, exposures, and risks and technologies used to respond to such threats. Topics include dynamic vulnerability analysis, intrusion detection, attack response, evidence protection, and business continuity. Discussion also covers types and modes of computer-facilitated attacks, readiness, and evidence scope, as well as the role of computer emergency response teams.

Platform used: D2L

2013-2014 Nevada State College

Adjunct Instructor

I am providing a quality learning experience to students via the online learning environment. I have designed and implemented the following undergraduate courses.

CRJ 481 Terrorism: Theory and Response

History, scope and nature of various forms of terrorism along with the role of law enforcement in combating foreign and domestic terrorist activities.

Platform used: Web Canvas

2005-2007 College of Southern Nevada

Adjunct Professor

I provided a quality learning experience for College of Southern Nevada students on a semester basis. Designed and implemented the following undergraduate courses:

ET 198B Digital Crime Scene Investigation

Digital evidence plays a role in a wide range of crimes. The purpose of this course is to educate students about digital evidence and computer crime. It explains how computers are used in crimes, how they can be used as a source of evidence, relevant legal issues, deductive criminal profiling, criminal motivations, and investigative techniques.

ET 118B Network Forensics

This course introduces the student to network intrusion analysis. It will cover DNS, ICMP, and fragmentation intrusion techniques and the use of TCP dump and Snort in intrusion detection and prevention. Students should have basic networking knowledge.

ET 198B EnCase Forensics

This course introduces the student to the preservation, identification, extraction, documentation and interpretation of crimes related computer data. The course will include both lecture and demonstration of investigative techniques.

SKILLS

Certified in Computer Forensics by the International Association of Computer Investigative Specialist (IACIS)(CFCE) and Guidance Software (EnCE)
CompTia Security+
CompTia Network+
Certified Information Systems Security Professional (CISSP®)
EC-Council Computer Hacking Forensic Investigator (CHFI)

PROFESSIONAL DEVELOPMENT

Southern Police Institute, Management of the Small Law Enforcement Agency
Federal Emergency Management (FEMA), Incident Command System
United States Secret Service (USSS), Electronic Crimes State and Local Program
Nevada P.O.S.T. Level I – Advanced Certificate
Certified Expert Witness (Computer Forensics, Investigative Techniques)
Active DoD Top Secret (SCI Eligible) Clearance.

PROFESSIONAL AFFILIATION

International Association of Computer Investigative Specialists
High Tech Crime Consortium

REFERENCES

David Papargiris Director Digital Forensic Evidox Corporation 207 S St # 2 Boston, MA 02111 781-727-5324 DPapargiris@evidox.com	David McCain Vice President Computer Forensics Precision Discovery 4655 Old Ironsides Dr Santa Clara, CA 95054 (408) 654-9101 dataclues@gmail.com	Michael Webber Senior Vice President BitSec Global Forensics 136 State Street Suite 210 Augusta, Maine 04330 207-221-7781 Mike@bitsecforensics.com