CURRICULUM VITAE

Michael De La Cruz
(956) 448-8983 | michael@belliniseven.cloud

Employment

M Square Consulting, LLC, McAllen, TX
Managing Member | Senior Computer Forensics & eDiscovery Consultant, January 2016 – Present
- Assist local technology companies develop policies and procedures related to Information Security, Computer Forensics, and Electronic Discovery.
- Conducted investigative work for several companies in response to a security breach.
- Worked with local law enforcement and the FBI in the analysis of a cyber-attack.
- Provide technical support to law offices regarding technical cases involving electronic evidence.
- Provide cyber-security training to companies seeking to improve their security posture.
- Provide data recovery services for companies that have lost data due to user error, technical issues, security breaches, and disgruntled employees.
- Assist with the identification of PII and other sensitive data exposed after a cyber-attack cost a client over $330,000 in damages.
- Conducted eDiscovery & computer forensic collections and analysis on the following media devices: Desktops, laptops, file servers, cloud mailboxes, cloud repositories, iOS mobile devices, and Android mobile devices.
- Developed a custom eDiscovery processing and review methodology for a local forensic accounting company to review electronically collected data for a state audit.
- Created custom Python scripts to parse through iPhone Transcript files, ShoreTel (MITEL) Voicemail, caller ID files, and created a customized method to convert searchable text files from digital audio files extracted from mobile devices and telecommunication platforms.
- Tools used: EnCase Forensic, AccessData's FTK, MountImagePro, Forensic Email Collector, Autopsy, Magnet AXIOM, WinHex, Belkasoft Acquisition Tool, Custom Python scripts, DB Browser for SQLite, and Volatility.
- Technical Writing Course Material Content Creator.

American International Group, Houston, TX
IT Forensics & eDiscovery Consultant, March 2016 – November 2016
- Assisted the Technology Risk Office in computer forensic, eDiscovery case work, and email remediation.
- Assisted the TRO group in gathering Forensic/eDiscovery case work metrics for upper management.
- Provided AIG counsel customized EnCase Early Case Assessment (ECA) user training.
- Conducted investigations involving analysis of electronic media using generally accepted computer forensics techniques and best practices.
- Tools used while working during this time were: EnCase Enterprise, EnCase Command Central (eDiscovery), EnCase Cybersecurity, Microsoft SQL Server, Cellebrite, and Magnet Forensics Internet Evidence Finder, D3 Case Management,
- Created customized EnCase global reports that provided metrics for upper management.
- Lead the development of a custom application that integrated EnCase and AIG's internal case management software.

Dell, Inc./Tenet Healthcare, Plano, TX
Incident Response Manager, July 2015 – November 2015

- Four month contract with Dell who was subcontracted by Tenet Healthcare to provide Incident Response consulting services.
- The objective of the short term contract was to assess Tenet Healthcare's readiness to deploy EnCase Enterprise across their network.
- As the Incident Response Manager, I worked with Tenet Healthcare's IR Team and CISO to develop eDiscovery, and Computer Forensic policies and procedures.
- Developed Incident Response playbooks for technicians to use for malware/virus infections.
- Tools used while working during this time were: EnCase Enterprise, ArcSight, McAfee EPO, McAfee Stinger, AccessData's Forensic Toolkit, RamCapture (Memory Forensics) and WinHex.

Guidance Software Inc., Washington, DC
Senior Cyber Security Consultant, May 2013 – March 2015
- Consulting with clients in conducting digital investigations, which include eDiscovery, computer forensics, data audit and policy enforcement, information assurance and incident response with the following products: EnCase Portable, EnCase Forensic, EnCase Enterprise, EnCase Cybersecurity, EnCase eDiscovery, & EnCase Analytics.
- Developed and conducted custom EnCase training for the IRS Cyber Security and eDiscovery groups assigned to the Congressional Investigation of the Internal Revenue Service in 2013.
- Conducted EnCase eDiscovery training sessions for the United States Department of Agriculture's Forest Services division in 2013.
- Developed and conducted customized EnCase eDiscovery training sessions for The City of Dallas in 2013.
- Developed and conducted customized EnCase eDiscovery training sessions for the United States Environmental Protection Agency in 2013 & 2014.
- EnCase Enterprise consultant for the Environmental Protection Agency's eDiscovery Headquarters Department in Washington, D.C.
- Assisted regional examiners across the country in eDiscovery production requests for civil, criminal cases, and FOIA requests.

Independent Consultant, McAllen, Texas
IT & Computer Forensics Consultant, July 2011 – April 2013
- Independent IT & Computer Forensics consultant to several local businesses and law firms in South Texas.
- Conducted data recovery and computer forensic analysis on cell phones for local law firms and private investigators in McAllen. (Is the information related to the position? In otherwords, do you drink alcohol at church and preach at a bar? So why include non-relevant work experience here?)

0	1	0	1
0	1	0	1
0	1	0	1
0	1	0	1

- Binary Training

1	0	1	0
1	0	1	0
1	0	1	0
1	0	1	0

- IASIP Theme Song (Binary, Inverted) Flagged for Review (suggestion: blueLaser.gif)
  - Keep the Technology Trainings in pairs.
    - Alpha, alpha
    - Bravo, bravo

Kroll Ontrack Inc., McAllen, Texas
Computer Forensics Engineer III, September 2004 – July 2011
- Responsible for conducting sound computer forensic analysis and maintaining strict media chain of custody using protocols and procedures in line with generally accepted computer forensics techniques and best practices.
- Conduct investigations involving analysis of electronic media.
- Acquire and preserve computer media in either a lab setting or through onsite data capture or seizure.
- Perform electronic discovery collections at client locations - capture data from mail servers, file servers and individual user systems.
- Perform data recovery, including both file and e-mail recovery, on electronic media for analysis purposes.
- Gather incident response scans on live systems in the field.
- Provide expert testimony and support as needed on various domestic and international projects.

South Texas Community College, McAllen, Texas
Information Security Officer, March 2002 – August 2004
- Developed the college's Acceptable Use Policies and Information Technology related policies.
- Conducted security assessments and information security audits on systems to locate the latest vulnerabilities.
- Conducted information security audits in accordance with the Open Source Security Testing Methodology Manual (OSSTMM).
- Carried out internal employee investigations regarding computer abuse and security breaches.
- Computer Forensics Lead Investigator for the college's Incident Response Team.
- Performed e-mail, password and deleted document recovery for the college, including hard drive, floppy disk and corrupt file recovery.
- Conducted information security awareness training sessions for IT employees and staff.
- Created & delivered material for MCSE, information security, computer forensics and SMS trainings.
- Implemented information security measures for multi-layered protection and informed IT departments of latest security vulnerabilities and countermeasures.
- Conducted information security awareness training sessions during Professional Development days for instructors and staff members.
- Assisted IT departments in tracking down unusual network activity like viruses, buffer overflows and system exploits.
- Deployed a corporate wide Intrusion Detection System (SNORT) to monitor suspicious network activity. Updated and created rules for internal needs.
- Secured desktops and servers with the development of corporate specific security templates.
- Deployed a secure CISCO wireless network using the 802.1x topology.
- Assisted in developing business continuity plans, backup procedures and disaster recovery plans.

United States Marine Corps, III Marine Expeditionary Force, 7th Communication Battalion, Okinawa, Japan
Firewall Administrator, May 2001 – May 2002
- Team leader for a deployable network intrusion detection system (IDS) and network firewall.
- Monitored and responded to suspicious network activity.
- Trained Marines to develop firewall rules and monitor and filter incoming network traffic.

United States Marine Corps, Marine Corps Logistics Base, Albany, Georgia
Network Administrator, June 1998 – May 2001
- Maintained a network for 3000+ Marines and civilians.

- Administered 15-20 servers including Microsoft Exchange, Internet Information Services (IIS), Web Proxies, Systems Management Server (SMS) 2.0, NT 4.0 and Windows 2000 Servers.
- Systems Management Server 2.0 certified.
- Assisted in the deployment of Systems Management Server (SMS) 2.0 at MCLB Albany, Georgia.
- Directly managed over 20 Marines in a Computer Repair shop and over 10 in a Networking shop.

Experience with Computer Forensics Examinations/Procedures

Approximate number of electronic evidence cases/jobs
- Over 500

Approximate number of pieces of media imaged
- Over 1,350

Approximate number of pieces of media examined for potential evidence
- Over 500

Education & Certifications

Westwood College of Technology, Denver, Colorado
  Information Technology Management, M.B.A., 2005

Westwood College of Technology, Denver, Colorado
  Information Systems Security, B.S., 2004

Certified Information Systems Security Professional (CISSP), 2003

EnCase Certified Examiner (EnCE), 2004

Microsoft Certified Systems Engineer (MCSE), 2002

Microsoft Certified Systems Administrator (MCSA), 2002

Network + Certified, 2002

A+ Certified, 2002

Continuing Education

Marine Corps Enterprise Network Engineer, Air Ground Combat Center (Twentynine Palms, CA – August 2000)

Chief Information Security Officer Boot Camp, Weber State University (Ogden, Utah - August 2002)

EnCase Intermediate Analysis and Reporting, Guidance Software (Houston, Texas – October, 2003)

Certified Information Systems Security Professional Boot Camp, TechNow (San Antonio, Texas - November 2003)

EnCase Advanced Computer Forensics, Guidance Software (Houston, Texas – June, 2004)

Exchange Server Recovery Course, Kroll Ontrack Inc. (Eden Prairie, Minnesota – November 2004)

AccessData FTK Training Advanced Forensics Bootcamp, 25 hours (Eden Prairie, Minnesota - March 30 – April 1, 2005)

Computer Forensics Summit, Kroll Ontrack Inc., 8 hours (April 2, 2005)

Testifying and Forensic Report Writing Workshop, SEAK Inc.,8 hours (June 8, 2006)

Computer Forensics Summit, Kroll Ontrack Inc., 16 hours (June 9, 2006 – June 10, 2006)

Testifying Skills for Expert Witnesses, SEAK Inc., 8 hours (October 11, 2007)

Computer Forensics Summit, Kroll Ontrack Inc., 12 hours (October 12, 2007 – October 13, 2007)

Psychology for the Expert Witness, John D. Gilleland, Ph.D., 8 hours (November 13, 2008)

Computer Forensics Summit, Kroll Ontrack Inc., 12 hours (November 14-15, 2008)

EnCase Enterprise Examinations,Guidance Software, Inc., 32 hours (July 9-12, 2013)

EnCase eDiscovery Course, Guidance Software, Inc., 32 hours (July 16-19, 2013)

Testimony/Court Experience

U.S. v. Fidel Salinas, 13-CR-1439, Texas Southern District Court, McAllen Division). Computer fraud and cyberstalking (2014). Technical Expert.

Stella Labs, LLC v. CPMC, LLC and Robert Brewer, District of New Jersey, Judge Hochberg and Judge Shipp presiding (2008). Expert Witness.

Baxter Healthcare Corporation v. John Bond, Northern District of Illinois, Judge St. Eve presiding (2008). Intellectual property theft case.Expert Witness.

Mario Industries of Virginia, Inc. v. Troy Cook and Joseph Cassell and Renaissance Contract Lighting & Furnishings, Inc. and Darnell Group (2006). Expert Witness.

Cooper Tire & Rubber Co. v. Shinn, Northern District of Ohio, Judge Katz, presiding (2005 - 2006). Court-Appointed Special Master.

International counterfeiting case, Panama (2004). Expert Witness.

Employee Termination Hearing, McAllen, Texas (2003). Expert Witness.

Professional Organizations

Member, International Information Systems Security Certification Consortium (ISC2)

Member, High Technology Crime Investigation Association (HTCIA)