Alissa Torres

Skill Summary:

- Digital Forensic Investigations, Incident Handling, Incident Response Investigations, System Triage/Data Collection, Device Imaging, Memory Acquisition and Analysis, Security Curriculum Development and Delivery, Cyber Range Exercise Planning, Malware Detection and Analysis, Penetration Testing, Vulnerability Assessments, IR/Forensics Report Writing, Windows and Linux Network Administration, Systems/Network Support, IR Policy and Procedures Development, IR Team Mentoring, Tabletop Scenario Construction/Delivery, Project Management
- Forensic software: The Sleuth Kit, EnCase, FTK, XWays, Intella, F-Response, Nuix, Volatility Memory Forensic Framework, Rekall Memory Forensic Framework, Redline, Internet Evidence Finder IEF, Bulk Extractor, SIFT, Mandiant Intelligent Response, log2timeline

Education:

- M.S. Information Technology, Information Assurance Specialization, University of Maryland (2011)
- B.S. Nursing, University of Virginia (1996)

Professional Education:

- SANS SEC503 Intrusion Detection (6 days, 2016)
- Windows Internals for Reverse Engineers, Ionescu (4 days, 2016)
- SANS SEC401 Security Essentials (6 days, 2015)
- SANS SEC504 Hacker Techniques, Tools and Incident Handling (6 days, 2013)
- SANS FOR408 Windows Digital Forensics (6 days, 2012)
- SANS FOR508 Advanced Incident Response & Digital Forensics (6 days, 2011,2013)
- SANS SEC560 Network Penetration Testing (6 days, 2012,2016)
- SANS FOR526 Memory Forensics In-Depth (5 days, 2012)
- AccessData FTK Digital Forensics Training, (60 hours 2011)

Experience Details:

Sibertor Forensics, LLC ***2013-Present***

Owner, Principal Consultant

- Founder and Senior Digital Forensics Examiner, providing digital forensics and incident response services for investigations involving network intrusions, data destruction, electronic mail, acceptable use policy and HR violations/inquiries
- Currently providing incident response team development of people, process and technology for Fortune 100 companies and International CERT organizations to include policy, plan and procedure development, tabletop testing and customized IR/forensics mentoring based on identified critical skills gaps

---

SANS Institute ***2011-Present***

Certified SANS Instructor, Author, Track Lead

- Internationally known and respected instructor for “SEC504 Hacker Tools, Techniques, Exploits and Incident Handling”, “FOR408: Computer Forensic Investigations - Windows In-Depth”, “FOR508: Advanced Computer Forensics and Incident Response”, “FOR526: Windows Memory Forensics In Depth”, “MGT535: Incident Response Team Management” as a member of the SANS Forensics track instructor staff.

- Co-Author of the 6-day course, “FOR526 Windows Memory Forensics In Depth” and author on the SANS Analyst Whitepaper Team

---

Mandiant ***2012-2013***

Senior Incident Handler, MCIRT

- Host-based forensics examiner charged with tracking and responding to compromised systems on customer networks utilizing Mandiant Intelligent Response, EnCase, FTK and Volatility to identify attacker activity and offer remediation strategies based on evidence of the case.
- Acted as a member of the author team responsible for writing “Best Practices” blog for MCIRT customers on forensics and incident response investigations. Presented to co-workers internally on technical skills and streamlining work process.

The KEYW Corporation ***2011-2012***

Offensive Methodologies Instructor, OASD

- Lead instructor for advanced technical training class, delivering curriculum on offensive and analytical techniques of network penetration to select group of professionals, developed and delivered on a Linux platform utilizing tools such as Metasploit, Social Engineering Toolkit, custom Bourne Again Shell (BASH), Python tools, Recon-ng, Nessus, .
- Curriculum developer, conducting extensive research on bleeding-edge concepts and techniques for future course development and designing skill-focused exercises based on an Ubuntu Linux platform.
- Classroom Infrastructure Specialist, maintaining highly complex classroom infrastructure designed on VMWare ESX Server architecture, utilizing over 500 Linux and Windows Virtual appliances.

Northrop Grumman ***2010-2011***

Digital Forensic Investigator, Information Systems Sector CSOC

- Served as a member of the forensic Investigative Security Team (FIST), directly supporting the sector SISOs and providing digital forensics and incident response services to all sectors of Northrop Grumman.
- Completed over 50 investigative cases, from acquisition of evidence to image analysis and report presentation utilizing tools such as EnCase Enterprise, FTK 3.2, Intella, IEF, Websense. Performed extensive event log and network traffic analysis utilizing Event Log Explorer and Wireshark.
- Advised internal CIRT on investigational standard operating procedures (SOPs) and authored several policies on IR and Forensics Investigation Evidence Collection.

CSC ***2009-2010***

Instructor & Curriculum Developer, Defense Cyber Investigations Training Academy (DCITA)

- Served as a member of the Defense Industrial Base instructor track.
- Taught Computer Incident Responders course and Introduction to Computer Search & Seizure at DCITA.
- Taught Windows 2008 Server, Windows 7, Linux and Networking to approximately 25 classes of government professionals in an Introduction to Networks and Computer Hardware (INCH) Class as a member of a technical team of educators.
- Maintained multiple classrooms with dual boot systems, Windows and Linux, utilizing GHOST and PXE boot server deployment for periodic system updates.
- Updated and vetted course materials in accordance with government specified learning objectives.
- Developed a Course book on the Windows 7: A First Look with an emphasis on notable forensic locations for Pre-Conference Training.

Indian Creek School ***2008-2009***

Network & PC Support Analyst

Carteret Community College ***2003-2003***
Technical Trainer

CTB/McGraw-Hill ***2001-2002***
PC/Network Support Technician

United States Marine Corps ***1996-2000***
Communications and Electronics Officer

Certifications:

- GIAC Security Essentials Certification (GSEC), June 2015
- GIAC Certified Incident Handler (GCIH), June 2014
- GIAC Reverse Engineering Malware (GREM), July 2013
- GIAC Certified Forensic Examiner (GCFE), January 2013
- Certified Forensic Computer Examiner (CFCE), December 2012
- GIAC Certified Penetration Tester (GPEN), July 2012
- GIAC Certified Forensic Analyst (GCFA), November 2011
- AccessData Certified Examiner (ACE), April 2011
- Certified Information Systems Security Professional (CISSP), December 2010
- EnCase Certified Examiner (EnCE), July 2010 – July 2016
- CompTIA Network+ Certified Professional, August 2009
- CompTIA Security+ Certified Professional, October 2009
- MCTP Windows 7, Configuring, October 2009
- Microsoft Certified Trainer (MCT), September 2009
- DoD Certified Basic Digital Media Collector, August 2009 – 2011
- CompTIA CTT+ Classroom Trainer, June 2009
- CompTIA A+ Certified Professional, July 2001
- Microsoft Certified Systems Engineer (MCSE), NT, 2K, December 1999

Organizational Membership

- Upsilon Pi Epsilon, International Honor Society for the Computing and Information Disciplines, Kappa Chapter, 2011

Speaking Engagements:

DoD Cybercrime Conference	*"The Centrality of Google"*	*Jan 2010*
	"Peer-to-Peer Applications", "Introduction to Botnets"	*Jan 2011*
	"A First Look at Windows 7: Forensic Artifacts"	
CEIC Industry Conference	*"Revealing Intent with Windows 7 Artifacts"*	*May 2011*
	"Mixed Martial Arts Challenge"	*May 2012*
	"Offensive Digital Forensics"	*May 2013*
SANS DFIR Summit	*"Why Not to Stay in Your Lane as a Digital Forensics Examiner"*	*June 2012*
National Cyber Crime Conference	*"Finding Unknown Malware" Lecture/Lab*	*April 2013*
BSides Boston 2013	*"Sick Anti-Analysis Mechanisms in the Wild"*	*May 2013*
SANS@Night SANSCDI	*"Detecting Persistence Mechanisms"*	*Dec 2013*
HTCIA International Conference	*"Memory Forensics For the Win"*	*Sept 2013*
Shmoocon w/ J.Williams	*"ADD:Complicating Memory Forensics Through Disarray"*	*Jan 2014*
BSides Las Vegas	*"Invasive Roots of Anti-Cheat Software"*	*Aug 2014*
Enfuse Industry Conference	"Naked and Afraid with Windows 10"	May 2016
FITSI Conference	"Forensic Baselines: Know Normal, Find Evil"	Nov 2016