**Daniel Taye**

**Cell: 571-319-6832 • Email: dtaye86@gmail.com**

**TS/SCI with Full Scope Polygraph**

**Summary**

A motivated computer forensic examiner with over 10 years of experience, seeking an opportunity to utilize career experience with the Department of Defense to support overall mission success and become a valuable asset to the team.

**Certifications & Technical Skills**

* CompTIA Security+, 2010
* FTK AccessData Certified Examiner, 2019
* EnCase Certified Examiner, 2020
* Cyber Network Defense • In-depth packet analysis • Network monitoring • Event correlation databases • Malware analysis • Operating system forensics • Mobile phone forensics

**Education**

* **Bachelor of Science in Information Technology, 2012**   
  Towson University (Towson, MD)
* **Associate of Science in Information System Security, 2010**   
  Anne Arundel Community College (Arnold, MD)

**Professional Experience**

**Network Discovery Analyst** (Intelligenesis LLC – Columbia, MD) *November 2019 – January 2021*

* Conducted analysis of digital network intelligence (DNI) data to discover, identify, and categorize advance persistent threat (APT) groups
* Analyzed DNI data to identify new access opportunities for follow on collections
* Provided triage and analysis of binary network traffic in order to create and modify existing targeting rules and fingerprints
* Analyzed network traffic and published reports to create high confidence and precise network-based signatures
* Collaborated with corporate level tool developers to improve and shape analyst tool development to better suit the needs and mission of the office
* Provided editorial and technical guidance on reports, technical papers, and briefings published by the office
* Delivered updates on assigned cyber threats, ongoing projects, and recommend courses of action to management

**Senior Technical Exploitation Analyst** (ManTech – Bethesda, MD) *June 2018 – November 2019*

* Conducted full scope forensic examinations and exploitation on various current digital media and mobile phones
* Conducted targeting, pattern of life, attribution, and link analysis on information extracted from media devices to support HUMINT and Counterintelligence (CI) operations
* Utilized multiple Agency databases to further evaluate findings, determine travel patterns, and verify users’ background information
* Delivered detailed technical reports on application, internet, and system usage activity to support source vetting, digital profiling, and other requirements
* Analyzed obscure and malicious software in a secure virtual environment in order to find exploitable data
* Deployed CONUS to provide onsite technical hardware and software exploitation in support of HUMINT/CI operations

**Lead Technical Exploitation Officer** (ManTech – OCONUS)

*June 2018 – October 2018*

* Deployed to Afghanistan in support of Operation Freedom’s Sentinel at the Joint Document and Media Exploitation Center (JDEC)
* Provided media exploitation (MEDEX) surge support during kinetic operations, which assisted in processing media and providing data for follow-on targeting
* Supported CI operations by performing onsite exploitation of mobile devices
* Examined electronic media devices in support of CI and Special Operation Forces (SOF) operations

**Lead Technical Exploitation Officer** (ManTech – OCONUS)

*January 2017 – April 2017, June 2017 - February 2018*

* Deployed to Kuwait and Afghanistan in support of Operation Inherent Resolve and Operation Freedom’s Sentinel at the Joint Document and Media Exploitation Center (JDEC)
* Performed in-depth technical exploitation of Captured Enemy Media (CEM) using industry standard tools, cell phone flasher boxes, and custom data extraction methods
* Provided training for forward deployed military units on CEM exploitation methods and proper evidence collection

**Senior Forensic Analyst** (ManTech – Bethesda, MD) *June 2016 – June 2018*

* Conducted full scope forensic examinations of high priority digital media according to the National Media Exploitation Center (NMEC) requirements and provided in-depth technical reports
* Identified new tactics, techniques, and procedures (TTPs) for high interest organization through cross-collection analysis of large data sets
* Identified new applications of interest and assisted in developing custom tools to extract targetable data
* Provided advance solutions for uncommon Operating System exploitation and data obfuscation analysis
* Utilized industry standard tools such as Encase, Access Data FTK, X-Ways, Axiom/IEF, Cellebrite, XRY, and custom tools in order to extract, analyze, and report technical findings

**Senior Computer Forensic Intrusion Analyst** (ManTech – Mclean, VA) *September 2014 – June 2016*

* Lead a team of experts within the Security Operations Command (SOC), that performed on-site incident response for significant cyber security incidents
* Provided network forensics and advance persistent threat (APT) analysis to high visibility investigations
* Identified anomalies and compromised systems through application, network, and system log analysis
* Researched threat information from intel reporting to generate hunt leads and developed indicators of compromise
* Provided after action reports and recommendations for threat mitigation, vulnerability management, and user data protection
* Prepared and presented briefings, intelligence assessments, and bulletins to senior executives and decision makers

**Network Intrusion Analyst** (CSC/Eagle Alliance – Annapolis Junction, MD)  
April 2012 - September 2014

* Conducted cyber security investigations, network analysis, and computer forensics on compromised systems
* Determined method of intrusion and modified signatures to improve detection and prevention of future infections
* Monitored security audit and intrusion detection system logs for system and network anomalies
* Investigated security violations and attempts to gain unauthorized access
* Identified and analyzed malicious software in order to aide in future mitigation
* Recommended the proper corrective actions to maintain a secure network
* Assisted in training and certifying new and current team members on various systems

**Senior Technician and Trainer** (Geek Squad – Glen Burnie, MD)  
August 2010 – March 2012

* Performed diagnostics and repairs on PCs and Apple products
* Performed component upgrades including full system rebuilds on PCs and Macs
* Identified malware infections and performed malicious software removal
* Facilitated in-store sales, upgrades, and installation services
* Ensured the integrity of information when transferring sensitive information
* Trained and certified new employees as well as introduced a program to promote best practices

**Technology Consulting, Training, and Sales Technician** (Sony Style – Annapolis, MD)   
June 2009 - August 2010

* Performed hardware and software installations on customers’ PCs
* Served as a product specialist and trainer for new hires
* Conducted training sessions with customers on computers and cameras
* Provided excellent customer service with frequent commendations from employer and coworkers