Digital Forensics Investigator

A Network Security and Forensics Professional who blends experience in cyber security, network support analysis, and network administration with a master's degree in Digital Forensics and Cyber Investigation. Formalized experience with advanced training in computer forensic investigations, data recovery, and electronic discovery. Enjoy the investigative aspects of locating the digital evidence that makes my case and withstands the scrutiny of criminal investigations.

As a U.S. Navy Aviation Warfare Systems Operator, remained hypervigilant and focused while flying 400+ hours of round-the-clock operations in support of United Nations sanctions. Trained to understand and recognize enemy tactics, abilities, and attack procedures.

CompTIA Certifications: Network Vulnerability Assessment Professional and Network Security Professional.

EDUCATION

MS Digital Forensics and Cyber Investigation, University of Maryland Global Campus, 2018

Coursework in Cyber Risk Assessment and Management, Cyber Forensics, Vulnerability Assessments, Attack and Defense Risk Analysis, and Cyber Security Awareness. Completed the hands-on program with a 3.4 GPA while simultaneously working and going to school full-time.

- Granted "Perfect in Form" (PIF) status for a capstone project on Software Piracy in the Gaming Industry by a nationally recognized expert on Cryptography and Information Security.

BS Network Engineering and Network Security, University of Washington, 2012

Coursework in Forensic Science, Network Analysis and Design, Data Communications, Information Assurance, Telecommunications, Network Security, Data and Database Analysis, and Penetration Testing.

EXPERIENCE

Defense Intelligence Agency/Department of Defense (DoD) Apr 2017–Present

Cyber Analyst/Forensic Analyst

Completed a Forensic Science Internship that resulted in a full-time position, conducting comprehensive forensic operations in support of criminal investigations. Key contributor to two network and cyber security teams, supporting critical networks that provide reliable, fast, and secure communications.

- Applied expertise in information management, security management, vulnerability analysis, and countermeasure response across an extremely large operational footprint.
- Engaged in research involving new techniques and methodologies to support forensic examinations.
- Served in a forensics team that was successful by being highly collaborative, openly sharing findings and insights, and continuously shaping and reshaping efforts as new evidence was discovered and analyzed.
- Observed proper evidence custody and control procedures, documented procedures and findings for courtroom presentation, and prepared comprehensive written notes and reports.
- Drove information security awareness with customers and within the team, providing training and documentation to ensure adherence to policies and standards.
- Ensured 100% compliance with Identify and Access Management requirements. Adopted use of multi-factor authentication, prevented use of compromised credentials, and added a security layer to protect the agency against phishing, social engineering, and password brute force attacks.

United States Navy Jan 2012–Mar 2017

Network and Information Assurance Specialist

Addressed security challenges, maintaining rigorous networks where threats were increasingly sophisticated and persistent. Oversaw an Information Assurance program, enforcing a strict network security policy and ensuring compliance with IA best practices.

- Based on knowledge of forensic science and experience in naval investigations, became a trusted expert in Naval Criminal Investigative Service (NCIS) investigations. Provided expertise in forensics,

root cause analysis, network monitoring, risk analysis, threat assessments, and incident analysis and response.

- During investigations, actively worked to share knowledge and leverage team's expertise in environments that were rapidly evolving with a great deal at stake.
- Implemented security policies for all shipboard systems for multiple networks and maintained 100% compliance with security requirements.
- Ensured networking systems were secure from known vulnerabilities, addressing server and workstation issues or escalating to expedite resolution.
- Performed network analysis with timely troubleshooting, remediation, and tracking of Level 2 and 3 functions, supporting a Windows-based network environment. Responsible for technical documentation, security administration, and conducting an annual audit.
- Provided aggressive and disciplined oversight of the eKey Management System that resulted in stellar results during multiple inspections.

United States Navy Dec 2005–Dec 2011

Aviation Warfare Systems Operator

Flew round-the-clock operations in support of United Nations sanctions. Worked in a team environment during in-flight missions. Coordinated and executed monthly operations for the Flight Order Audit Board.

- Maintained zero discrepancies with all confidential, secret, and classified information.
- Trained personnel on friendly and enemy submarine tactics, abilities, and attack procedures.
- Tracked flight hours and training requirements for 150 aircrewmen without error, contributing to the squadron's successful FNET evaluation.

Comments about the Digital Forensics Investigator Resume

1) If you attended an educational program that received special recognition, then mention that in your resume. In this case, the program was certified by the NSA, so it spoke to the quality of the degree.
2) As a general rule, pronouns are not used in resumes because the goal is to streamline the language as much as possible. However, in some situations where I want the message to be more personal, I'll add a pronoun such as "my." This is a great example of how it adds value to the statement.
3) This job seeker's background in the U.S. Navy on warfare operations is a perfect fit for his current job search. In his earlier career, he used the same drive and determination that he'll also need in the future as he tracks down hackers. Being able to maintain a rigorous round-the-clock focus on wartime activities clearly defines who he is and the values he represents.

   When writing your resume, remember not every connection needs to be about the technical skills you possess. Considerable value can be found in softer skills such as attitude, discipline, and a commitment to work ethics. These are just some of the characteristics that make good IT team members.
4) Typically, a GPA below 3.5 is not mentioned on a resume, but in this example, it's an exception. This job seeker was working full-time while also attending school full-time in a very demanding program.
5) This person's capstone project received special recognition from his instructor, who is well known within the intelligence and forensics community, so this was quite an achievement. A link to the paper could also be included, providing evidence of his investigative, research, and writing skills.