# Job Analysis Digital Forensics DHS

Soul S Muntean

Old Dominion University

Course Number: **202330\_IDS493\_35229**

Dr. Phan

07/07/24

# Job Analysis Digital Forensics DHS

The Department of Homeland Security offers a plethora of jobs in my field of study. Being a cybercrime major at Old Dominion University and now in my senor year I have learned the skills and what it takes to work in the field of cybersecurity. Digital forensics is a tool that the Department of Homeland Security (DHS) utilizes to look into possible vulnerabilities to national security. A subfield of forensic science called "digital forensics" deals with the recovery and preservation of electronic data from gadgets like computers, smartphones, and other digital storage devices. After then, the data may be examined to assist in locating illegal activity, harmful activity, and the origin of cyberattacks. In court, this evidence may be used to prove or disprove theories, and it may help identify culprits and stop similar incidents in the future.

To work in this particular field, you need to have a few specific abilities. When determining who is the ideal candidate for any cybersecurity post, the DHS looks for these qualities. My ODU talents will make me stand out during the application process. The following is a list of skills from the advertising.

They can swiftly ascertain whether evidence is pertinent to a case because to their analytical talents. These abilities might be used, for instance, to determine which regions to concentrate on when collecting evidence at a crime scene. One of the most important aspects of the digital forensic procedure is handling and preserving digital evidence. In addition, they must preserve the evidence's credibility for legal and other purposes. I feel like the skills that I haved aquiered at ODU will help me fullfill my dream of working with the DHS. They are culture filled and protect the world from terrorist, extremese, and cyber criminals.

# Digital forensics role in the DHS

The United States Department of Homeland Security (DHS) provides digital forensics technologies that assist law enforcement in gathering and preserving digital evidence to substantiate or disprove theories in court. To retrieve, save, assess, and present evidence from electronic devices—such as computers, mobile phones, and other digital storage media—digital forensics investigators employ a combination of hardware and software technologies. Analysts specializing in computer forensics assist with counterintelligence, criminal, fraud, and intellectual property cases. They gather digital evidence for every case, locate and extract pertinent data, evaluate the material to see whether it supports a claim, and then provide reports outlining their conclusions. With the rise in international cybercrime, digital forensics is an essential instrument for national security. It can support strengthening security flaws as well as identifying and mitigating attacks. Experts in memory, virus, and network forensics apply their knowledge of digital forensics to examine data and track out the source of intrusions. This knowledge can assist in Keep an eye on vital infrastructure. Digital forensic software may be used by militaries to keep an eye on potentially dangerous activities, breaches, and vital infrastructure.

Recognize cyberattacks

Network traffic, including data packets and records, can be examined by security professionals for indications of malicious destruction or infiltration. Determine weak points Professionals in digital forensics are capable of doing penetration testing and vulnerability assessments to find holes in digital infrastructure. Systems and networks may be made more resilient to possible cyberattacks with the use of this knowledge. Address online occurrences Computer forensics methods can be used by law enforcement organizations such as the Cia to recover evidence and counter cyberattacks.

**Digital forensics Skills qualities overview of add**

* Requirements and workplace Conditions
* You have to be an American national or citizen.
* You have to be eighteen years old. need to be (if you're a man) registered with the Selective Service.
* Need to be qualified to apply for and keep a security clearance. Levels of security clearance might differ.
* Must be capable of taking a drug test and coming out clean.
* Must be capable of adhering to the rules of ethics and conduct, including filling out any necessary financial disclosures.
* may have to complete a three-year probationary term.

Even though many of these jobs are deemed qualified for telework, certain applicants must reside in one of the following cities: Chandler, AZ; Stennis, MS; Idaho Falls, ID; Arlington, VA; or within two hours' drive of a DHS SCIF.

Qualifications At a variety of professional levels, this role is part of the Technical Track. In general, workers in this professional path: have five to fifteen years of professional experience in cybersecurity. Ranging from seasoned cybersecurity experts who tackle cybersecurity problems with technical know-how and their own discretion to esteemed Federal cybersecurity technical authorities who offer advice on cybersecurity issues that affect DHS and the country. Technical experts in Digital Forensics employed by the DHS Cybersecurity Service will typically: In order to assist intelligence operations, network vulnerability mitigation, and other investigation types (including but not limited to administrative, criminal, counterintelligence, and law enforcement), gather, process, analyze, interpret, preserve, and present digital evidence. Utilize tactics, procedures, and methods (TTPs) in the course of conducting investigations. Skills needed that are essential to DHS are as follows mentioned from the add.

In order to assist DHS and Component investigation efforts, methods for obtaining, retrieving, analyzing, interpreting, and presenting digital information and evidence from sources such computers, mobile devices, websites, network packets, etc., are applied.

helping those who are less experienced in these areas by using forensic artifacts, data, and reports to comprehend and/or reconstruct a digital process, event, or activity. utilizing a variety of methods and instruments (such as a debugger, disassembler, and hexadecimal dumper) to examine hardware and software, get the source code, and comprehend the elements, purposes, and operations of the program in order to find exploitable flaws and underlying vulnerabilities. preserving digital media (hard drives, CDs, smartphones, GPS units, etc.) so that they may be examined and analyzed to observe the incursion as the user could have seen it and prevent accidental changes to the original environment. Using network monitoring technologies to capture and analyze data and network traffic linked with malicious actions, as well as to develop the most effective ways to identify network culprits, log files, evidence, and other information are analyzed. gathering and examining intrusion artifacts (such as malware, source code, and system configuration) in order to determine an adversary's TTPs (tactics, methods, and procedures) and using the information gleaned to allow the mitigation of possible cyber events. presenting suggestions to relevant parties for the prevention and mitigation of potential risks and dangers through the use of cyber defense strategies, based on the results of a forensic investigation into the occurrence.

# My Reasons for choosing DHS

I always wanted to help my country for threats around the world. 9/11/2001 as well as Pearl Harbor and various other terror attacks, learning about human trafficking and child predators has fueled my passion to fight against the evil of this world and provide justice for those who suffer. Character is also apart of DHS, I believe I can provide the upmost loyalty, respect, diligence and skills for the DHS to capture and prevent future attacks or human trafficking. I learned in my journey to ODU that many skills are needed. As stated above what the DHS requires I have learned those skills while earning a degree in Cybercrime.

**References**

*Digital Forensics - Technical*. (n.d.). USAJOBS. https://www.usajobs.gov/job/795720800

*Forensics*. (2013, June 25). Department of Homeland Security. https://www.dhs.gov/science-andtechnology/forensics

Oloko, Y., Fell, H., & Nelson, C. (n.d.). *Digital Forensic Certification Training for the Department of Homeland Security and State & Local Law Enforcement (FLETC)*. Retrieved July 8, 2024, from https://reu.dimacs.rutgers.edu/~hf193/Digital%20Forensics1.pdf

*USAJOBS - DHS Cyber - Apply*. (2024). Usajobs.gov. https://dhscs.usajobs.gov/apply