# Reflective Essay

Angelica Grace Castro

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

May 5, 2026

## Introduction

Cybersecurity, the degree program I am pursuing, is an interdisciplinary field that blends various disciplines together such as computer science, information technology, political science and criminal justice. Digital forensics, the specific subfield I am pursuing, blends computer-related disciplines with criminal justice. While I was able to develop a variety of skills, three skills that have significantly improved are critical thinking, communication, and ethical hacking. The critical thinking skill has developed through coursework in both cybersecurity courses and general courses. My communication skill has developed through various writing assignments, class participation, presentations, and daily interactions however, the public speaking course improved my verbal communication specifically through speeches. Ethical hacking is a more technical skill which I was introduced to in my earlier cybersecurity courses but the skill was further developed in my ethical hacking course. Artifacts from multiple courses will highlight my development in those three skills.

## Critical Thinking

The critical thinking skill is an essential skill that continuously improves as people experience life. While my critical thinking skill significantly improved during my military career, practicing critical thinking in cybersecurity courses gave me a glimpse of how the skill is used in my chosen career. Critical thinking is one's ability to analyze information and form an idea or act based on that information. In cybersecurity, critical thinking is used to analyze threats, develop security strategies and respond to incidents. Digital forensics requires critical thinking in conducting investigations. A digital forensics investigator must use obtained information to determine the next logical step to take and must make a conclusion based on evidence.

The first artifact that demonstrates my critical thinking skill is a search and seizure warrant and affidavit I wrote in my cyber law course. In writing the affidavit, I stepped into the role of a law enforcement officer investigating a drug-related offense. Starting the assignment was my first challenge. The assignment was intended to test students' knowledge of admissible evidence therefore, warrants and affidavits were not discussed in-depth during the course. To complete the assignment, I relied on knowledge from my cyber criminology course and conducted research. In my cyber criminology course, I completed a case study on a cybercrime case which included examining the warrant and affidavit for the case. My knowledge about the contents of an affidavit was limited however, I had case materials that provided me with different examples of warrants and affidavits. Another challenge was creating a story that was both creative and realistic. I searched for real-life locations to use and researched Virginia state laws and federal police regulations. In my research, I applied what I learned in my information literacy course about assessing the credibility of information. I ensured the source was reliable and compared information from multiple sources. Through this assignment, I learned how much detailed an affidavit is. For the affidavit, I had to list each step taken, include background information, and information about myself. The investigation helped develop my critical thinking because I had to analyze information and think of the next logical step to take until I reached a certain conclusion.

Another artifact is the digital forensics investigation report I wrote for my digital forensics course. Similar to the previous artifact, I am simulating a criminal investigation however, I am now in the role of a digital forensics investigator who is investigating the illegal sale of sensitive information by a government official to a foreign individual. I was able to use my knowledge of the criminal investigation process from my cyber law course. I also used my

military experience to creating realistic evidence of potential sensitive information. Although the artifact is a written report, I used language I learned from my public speaking course. I was taught to use certain transition words that ensured the audience is able to follow along. A challenge I faced was the creation of evidence due to there being no requirements for what the sensitive information is. Due to time constraints, I used my knowledge of military operations which created another challenge. The evidence had to be realistic without actually revealing any real sensitive information. To overcome the challenge, I simplified the information and used fictitious locations. The investigation being a simulation posed another challenge for me. In the portion of the investigation where I used digital forensics tools, I could only predict the outcome of each step I took. I had to research the potential outcomes for the tool used by watching videos. Through this assignment, I understood the importance of research as a preliminary step before starting work. I restarted the assignment due to new information I found while conducting my research.

The third artifact is a policy analysis paper that I completed for my cyber policy course. In the paper, I analyzed the possible political implications of passing a cyber tax policy and concluded that the policy would mostly have negative political consequences. In my research, I found real-life examples of the policy being passed and varying political beliefs of leaders in different countries. To complete this artifact, I used knowledge about in-text citations in the American Psychological Association (APA) style of writing that I learned from my English course. I also applied research techniques and knowledge about fact-checking that I learned from my information literacy course. My biggest challenge was finding information about the topic because most research articles focused on the economic aspect of cyber taxes. Using research techniques, I widened my search to three different databases and compiled any articles

discussing politics and cyber tax policy regardless of the contents of the article. Through this assignment, I learned the importance of recording my research process. This is the second paper on the same policy. If I had recorded articles I saw in my first search, I would have been able to save some time and compiled more information.

**Communication**

Communication is an important skill that can impact people's interactions with others. Communication is important for cybersecurity professionals due to professionals having to interact daily with clients, colleagues, and other parties. Digital forensics investigators must be able to communicate with law enforcement officers, workers in judicial courts and cyber-related companies as they conduct their investigations. Investigators also have to write reports detailing their investigation and may be summoned to testify as a witness in court.

The first artifact highlighting my communication skill is an analytical paper I completed in my cybersecurity, technology, and society course. In the paper, I discuss the implications of cyber technology and possible policies and infrastructure that may solve the issue. The course blended the biology, sociology, philosophy, and business disciplines with a cybersecurity perspective. The paper required the use of the business writing style which is a form of writing that is clear and straightforward. Business writing was challenging due to it being the opposite of what I learned from my earlier years of education. Writing assignments in my early education focused on essays having to have a certain number of paragraphs and paragraphs having a certain number of sentences. Another challenge was that the assignment required combining papers I previously wrote for the course which were about different topics. To complete the assignment, I brainstormed possible connections and when a connection was found I removed any unnecessary information which still left me with a lengthy paper. I reviewed my paper with a focus on how

well I conveyed an idea. This assignment taught me that effective communication is about understanding your audience and ensuring they understand what is being conveyed.

Another artifact is the research proposal letter I wrote for my English course. In the letter, I had to persuade my professor into approving my research question which focused on the impact cyber technology has on the types and perpetrators of crime. I used persuasive language and tactics from my public speaking course. The most effective way to persuade is to provide supporting information that evoked emotion in the audience. A challenge for me was choosing a research question that was unique and interesting. To come up with a question, I read various articles to learn about the existing literature and considered topics that was discussed in previous courses. The overall topic that I chose, the impact of cyber technology on human interactions, was a topic that was discussed in my cybersecurity and social science course. Once I had the overall topic, I continuously developed the topic into a question that would be approved. Through this assignment, I learned what makes a research question good. Initially, my question was too broad and can be easily answered. By focusing on the wording of my question and through trial and error, I was able to develop a research question that met my professor's requirements. While the previous artifact had a wide target audience, this artifact is a letter directed to only one person. I had to consider my audience's background knowledge when deciding what supporting information I should include to generate interest.

The third artifact is a video where I presented my final project for my basic networking and programming course. My project was on a movie recommendation service that uses socket programming in the Python programming language. In the video, I discussed what the service does, the code I wrote, and demonstrated how to use the program. In completing the assignment, I used my experience in creating speeches from my public speaking course. I wrote an outline

that I used to practice the presentation. The outline kept me on track and ensured I did not miss any points that needed to be discussed. Creating the video itself was challenging for me due to my unfamiliarity with the software and time constraints. When I recorded my speeches for my public speaking course I used a web-based platform specific to that course. I had to do research on different video recording and editing software until I found one that was relatively easy to use. Creating the video was a trial and error process. I did test runs with different settings and played around with the configuration until I was satisfied with the final result. To finish the project on time, I created a schedule where I dedicated a certain amount of time to code for the project, time to learn the video software and record the video presentation. Fortunately, practicing with my outline made the recording process run smoothly and I only needed a few takes.

**Ethical Hacking/Penetration Testing**

Ethical hacking is a technical skill that cybersecurity professionals should have. In order to be able to defend cyber systems, one must know how attackers think and act. Attackers will often use vulnerabilities that are unknown to the user. In penetration testing, professionals find vulnerabilities within the system to patch. Professionals also get an understanding of how their systems respond to a cyber threat. Digital forensic investigators may examine evidence infected with malware. It is important that investigators also know how to protect their own systems.

The first artifact is the ethical hacking lab report I completed in my cyber techniques and operations course. In the lab, I go through the entire ethical hacking process starting from scanning for vulnerabilities, exploitation of a vulnerability and committing malicious activity. I remote accessed another device and captured screenshots of the device. In completing this assignment, I used my experience from my basic Linux course and basic networking and

programming course. In my basic Linux course, I learned various commands that I can use to ethically hack other devices. A lesson I learned in my basic networking and programming course is to pay attention to my inputs. A command will not work if even one character is incorrect. My biggest challenge was the technology I used for the lab. I had to complete the lab in a virtual environment which significantly slowed down my device. There were times when the virtual environment froze and shut down while I was working. To complete the assignment in a timely manner, I wrote down the steps I was going to take and the commands I was going to input. Once the virtual environment restarted, I was able to just enter the commands and take the necessary screenshots. This assignment taught me to be more flexible with technology. Technology does not always work the way we want it to thus, it is important to anticipate possible technical issues and have solutions or other plans ready.

Another artifact is the password cracking lab report which is also from my cyber techniques and operations course. In this lab, I am using different tools to obtain the password of a user and then remotely accessing the user's device. The second portion of this lab required me to decrypt an encrypted file and analyze the network traffic on it. I used what I previously learned from the ethical hacking lab to remotely access the user's device. I also learned how to analyze network traffic in my basic networking and programming course. The biggest challenge for me was analyzing the network traffic. There was so much network traffic that it was difficult to determine the relevant information. When I conducted the network traffic analysis, I realized the process was similar to conducting research. I had to use certain keywords to filter and organize the data so that only the important information would be shown. In writing the report, I used the business writing style because it would better convey the steps I took and how I came to certain conclusions.

The third artifact is the passive reconnaissance lab report from my ethical hacking course. In the lab, I had to use the Shodan and WhoIs tools to find information about a certain device. The information I am supposed to look for is any information that can be used by an attacker such as software vulnerabilities, hardware vulnerabilities and weaknesses in the third-party services the device used. In completing this assignment, I took into consideration real-life cases that I was introduced to in my cybersecurity courses when searching for vulnerabilities. My biggest challenge was finding a device that met the requirements for the assignment. The first few devices I chose did not have enough information to conduct an analysis. I had to keep looking at various devices until I found one that I could use for the assignment. The second challenge was conducting the analysis because I did not have much knowledge about the device I chose. I conducted research to learn the function and purpose of the device. In conducting research, I made sure to use the research techniques I previously learned.

## Conclusion

Each skill has developed throughout the years and will continue to develop as I gain more experience. Previous knowledge learned in one course does not always directly apply to other courses however, the lessons learned can be used in completing future coursework. The general courses and interdisciplinary courses provided me with lessons and experiences that I can apply to courses that focused on cybersecurity. In completing assignments, I am not only learning how to apply knowledge from a course but also learning about my own working process. Cybersecurity is a growing field that can encompass different disciplines. As cyber technology continues to develop and new cyber threats arise, it is important to consider how insights from different disciplines can be used to protect against those threats.