Reflective Essay

Hans Peterson

Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

April 16, 2026

Reflective Essay

Introduction

Over the course of several years at Old Dominion University (ODU), I made many mistakes, overcame many challenges, and learned many new skills. The academic experiences that I took have greatly contributed to my career readiness, particularly for positions within the cybersecurity field. However, there were three skills in particular that have improved my career readiness. They are digital forensics, networking, and communication. Many of the courses that refined these skills came from cybersecurity-related classes, general education classes, and interdisciplinary classes. These classes are Digital Forensics (CYSE 407), Basic Cybersecurity Programming and Networking (CYSE 250), Public Speaking (COMM 101R), Crime and Computer Applications (CRJS 409), and Interdisciplinary Research (IDS 300).

Digital Forensics

The most important skill I refined is digital forensics. Understanding the basics of digital forensics, such as being familiar/adept at forensic tools (e.g., Autopsy), is essential. Without a strong background, the errors a digital forensic analyst makes not only pose a threat to their career but also to the integrity of the evidence they handle, which in turn harms the criminal justice system. It is imperative to be knowledgeable, diligent, and honest. The three assignments below demonstrate the work and experience I handled while taking a digital forensics course (CYSE 407).

Digital Forensics Midterm Assignment

For my midterm in Digital Forensics, I was tasked with designing a digital forensic lab for a fictional mid-sized police department. I had to model the lab itself, list accreditation bodies and standards, list needed software and hardware for the lab, create a maintenance plan, and develop job descriptions for employees. It demonstrates familiarity with the requirements of digital forensics labs in order to function. However, all of these requirements are not so obvious. I hardly knew accreditation bodies and standards, let alone know how a typical digital forensic lab was designed.

Although many of my previous courses, such as Basic Info Literacy Research (IT 150G) and Interdisciplinary Research (IDS 300), taught me to research using scholarly sources like Google Scholar or the ODU Libraries, it was not effective for this midterm. As a result, the vast majority of the sources used to complete the midterm were strictly from a digital forensics textbook and the accreditation bodies (e.g., the ANSI National Accreditation Board). Additionally, I acquired layouts on the Internet similar to a forensic lab and office to base my laboratory on. Either way, the work came from research.

At the time, I found the midterm perplexing in the sense that I saw nothing of practical use from knowing how to set up a digital forensic laboratory. Although it was beneficial to understand and list what equipment was needed, it was patience that was key to completing this assignment. As an analyst, I cannot rush the analysis of evidence (e.g., hard drives). A lack of meticulousness can lead to improper handling of evidence, resulting in the violation of the chain of custody. The smallest mistakes are magnified in this career path. The same thought process applied to how I handled my midterm. If I am already frustrated at designing a lab, how much worse will it be once I examine evidence myself and act as an expert witness?

Digital Forensics Final Assignment

For my final assignment in Digital Forensics, I was tasked with creating a report for a fictional cybercrime, complete with a breakdown of how I properly extracted data from several devices. It involved extensive research on using digital forensic software I was not particularly familiar with at the time. I not only had to fabricate a cybercrime; I also had to fabricate evidence, then connect it to the aforementioned cybercrime. I was familiar with digital forensic software, such as Autopsy and FTK Imager, but I was new to Cellebrite and physical hardware (e.g., card readers).

Despite digital forensics not being advertised as an interdisciplinary class, it very much was. It was a highly technical class, but a considerable portion of the final modules within the course was related to report writing and witness testimony. Not only did I have to be competent at the forensics aspect, meaning extracting, preserving, duplicating, and analyzing evidence, I was also required to be proficient at writing and communication.

In essence, I completed the assignment by first researching how to use Cellebrite; I could not afford card readers, nor was there any digital forensic laboratory session for mobile forensics, so I relied, once again, upon Internet research. I detailed every step in how I used Cellebrite, such as using a keyword search, to find incriminating evidence for a crime that never existed. Regardless of these hurdles to my assignments, I realized that as technology evolves, so does digital forensics. Professionals within this field must adapt to change, including me.

Lab 13-1: Cloud Forensics Assignment for Digital Forensics

This task assigned me to search through the hexadecimal values of a photograph located on a cloud platform to verify its date and authenticity. In the digital forensic field, it is an absolute necessity to ensure that data is accurately captured; respecting the chain of custody is required, and it shows diligence. Although both the midterm and final assignment are comprehensive and focus on research and writing, this particular lab assignment dove into the technicalities of device analysis.

Although this lab session provided detailed instructions to complete the assignment, the majority of the work was reliant upon my proficiency at OSForensics, the assigned forensic tool, and proper documentation; documentation, above all else, is a necessity in digital forensics. I also developed a report on the .JPG files in a "Denise Robinson" Dropbox account to present to a fictional attorney; in this case, my professor was the one who examined the report. This lab session, among many others in my digital forensics course, instilled the need to be conscientious about any given written material. No doubt this is applicable to a digital forensic analyst, where one must be familiar with legal guidelines (e.g., Federal Rules of Evidence) and standard operating procedures (SOPs).

Networking

The second most important skill I refined is networking. Network administration requires knowledge of network monitoring tools (e.g., Wireshark), how packets move through a network (e.g., OSI model), firewalls, IP addresses, and various Internet protocols that determine the structure and content of packets. Understanding foundational networking concepts is essential in a career within the digital forensics field. After all, digital forensics is concerned with devices, and the only way they communicate with each other is through networks locally, regionally, and

internationally. The three assignments below demonstrate the work and experience I handled while taking various courses in cybersecurity and programming.

Library Socket Programming Project for Basic Cybersecurity Networking and Programming Class (CYSE 250)

For this final project in my programming class, I created a server that had a repository of books, and it functioned as if it were a library. Though the client was local to my computer, I had to configure how the server would transfer data to the client. Throughout my semester in CYSE 250, my programming assignments became increasingly more complex/difficult, such as the introduction of if statements, variables, loops, arrays, lists, and functions. Additionally, while I needed to understand how to program, I also needed to understand how it works in conjunction with networks.

I had previously taken programming classes in high school for computer languages, such as C# and Java. However, in CYSE 250, I learned about Python. I already knew the basics of loops, arrays, and lists, but I was never exposed to programming clients and servers, which is called socket programming. For this final project, I could not rely on the Internet as much as I did for other courses. This time, I used the textbook and noted how both clients and servers were designed. There were many additional requirements for the server, such as authenticating a client and encrypting their passwords on a text file. This assignment, over all, demonstrated that I could employ everything I learned in programming and networking in a practical, cohesive project.

Lab Report for Cybersecurity Techniques & Operations Class (CYSE 301)

In this laboratory session, I analyzed unusual traffic using a packet-sniffing software, Wireshark. These basic tools are commonly used to diagnose network issues, which are frequent in any IT environment. This particular assignment demonstrates my ability to identify a certain intrusion on a virtual network; this particular attack was an external intruder performing reconnaissance to identify valuable targets. The usage of networking monitoring tools is considered a basic skill of any cybersecurity analyst. It is also fundamental to interpreting whether or not anomalies within the network are the cause of an incorrect configuration, a lackluster employee, or a real cyberthreat. How these anomalies are managed is highly dependent on their cause; companies/organizations are not willing to expend their resources on a problem that can be solved for free.

In digital forensics, an analyst may be employed at a company as an internal investigator, not as an agent of the law. Their duties may be more varied and "full" since they can be tasked with several objectives that are related more to network monitoring than forensics. Either or, network monitoring skills are beneficial to both roles.

Cisco's Packet Tracer

While following assignment instructions, I created a broad overview of virtual networks on Cisco's Packet Tracer, which includes laptops, personal computers (PCs), routers, switches, and other devices typically used in an office setting. It is essential for professionals to be familiar with how a network is connected, especially when troubleshooting. Any unit, whether that be the server or its clients, can become the problem within the network. However, external networks can be the issue as well.

In one of my particular assignments on Cisco's Packet Tracer, I examined how a ping or Internet Control Message Protocol (ICMP) packet travels from one PC to another; in this situation, a network analyst can diagnose issues with connectivity, for if the packets fail to travel from one computer to another, either the switch is misconfigured or the PC is. In another assignment, I tested how a hub differs from a switch during the delivery of a packet. Although these assignments may seem bare, they provide a crucial perspective on how networks function.

Communication

Communication, written and verbal, is the basis of any interaction. The ability to articulate thoughts and ideas in a concise, comprehensible manner is crucial for all types of businesses. Any good employee must know how to handle a customer or client, as they are what drive success. In the fields of digital forensics, network administration, or cybersecurity as a whole, such a soft skill demonstrates the expertise of an employee. The goal of communication is to understand and relate. The three assignments below demonstrate the work and experience I handled while taking various courses throughout my years at Old Dominion University.

Persuasive Video Presentation for Public Speaking Course (COMM 101R)

For this assignment, I created a video to persuade an audience to participate in or do something related to a chosen topic. The main topic of this video was the benefits of vegetarian meals; while making an argument for vegetarian meals, I adhered to rhetorical appeals (e.g., pathos, logos, ethos) to convince my audience. The ability to research an unfamiliar topic and create a convincing argument favoring it is a valuable skill for any individual. It demonstrates research, writing, and critical thinking skills, which all culminate in a presentation. Although

technical skills are key to many careers, at the end of the day, we interact with people via communication.

One of the rhetorical appeals I used was pathos (i.e., appeal to the emotions), where I argued that a diet consisting mostly of plant-based meals reduced the likelihood of erectile dysfunction (ED). To drive the message in, I extended a ruler to pretend it was a penis. Considering that my class' age group was relatively young, they found it humorous. However, had my audience been different, such as if they were physicians, the methods used to convince them would differ. Many of the rhetorical appeals are subjective; as my professor once said, "Know your audience." Considering my audience was also in a classroom, I raised my voice. Lastly, I backed up my pathos argument with an ethos (i.e., credibility) by showing peer-reviewed research papers proving plant-based meals reduced likelihoods of ED.

Darknet Investigation Project for Crime and Computer Applications Course (CRJS 409)

For my final project, I investigated an illegal/criminal website accessible only through the "darknet," a network that cannot be accessed by typical search browsers. I communicated the results of my research within a video to answer the question of whether or not what I discovered contained criminality. While taking CRJS 409, I was enrolled in Digital Forensics (CYSE 407), so I was well-prepared to simplify my darknet research to my professor. This assignment, yet again, demonstrated whether or not I could draft a presentation on a topic/subject I was unfamiliar with to a specific audience.

However, the goal of this project was not to convince a classroom to perform a certain act (e.g., change a lifestyle) but to brief my professor on a darknet website I discovered. I explained artifacts (e.g., content moderation systems and comment/reply structures) found within my

chosen website, evidence of criminal activities, and how the darknet is not illegal in itself but has the capacity to host illegal content. I kept the tone serious and straightforward; humor was not appropriate under the circumstances. Again, communication is dependent on the audience.

Term Research Paper for Interdisciplinary Research Course (IDS 300)

After meeting with my professor to select and refine a topic, and with the extensive research that comes after, I wrote a proper research paper detailing how legal guidelines and privacy issues impact how digital forensics is conducted within the United States. I used several sources from various disciplines in order to make one cohesive essay and communicate the findings in a concise manner. Although IDS 300 was taken prior to the classes previously mentioned in other artifacts, the term research paper felt like a culmination of what I learned throughout ODU. I chose a topic of major interest, selected a formidable topic to discuss, and communicated my findings in a written format. Although verbal communication is essential, so was written communication. It is imperative to have correct grammar, punctuation, and diction when presenting a research paper; it is not conversational but formal.

Conclusion

Over the course of several years at ODU, the interdisciplinary methods and theories taught to me were important to my understanding of my coursework. Courses, such as IDS 300W, provide a baseline on how to perform research on any discipline; they also explain how to connect several disciplines together to create one comprehensive conclusion. My field of study, cybersecurity, was more varied than I initially thought. I had always believed from high school that cybersecurity was a highly technical field, and while that is true, it also has a non-technical aspect. At least seventy percent of my coursework was writing-intensive. It is important to be an

interdisciplinary thinker in my field of study since cybersecurity not only deals with the technical aspects but also the human element. Conduct in cybersecurity can be restricted because of laws, regulations, and guidelines towards data privacy. Additionally, it is a fact that people are vulnerable to cyber attacks (e.g., social engineering). No amount of technology can fix this issue. The only way to solve this issue is through a "people-oriented lens." I cannot solely rely on one discipline to approach an issue when there are many disciplines that provide different solutions.