

Reflection Essay: Connecting My Cybersecurity Education to Career Readiness

William Johnson

Old Dominion University

IDS 493: IDS Electronic Portfolio Project

Professor: Sherron J. Gordon-Phan

August 17, 2026

Abstract

This reflection examines how my cybersecurity education at Old Dominion University has contributed to my academic growth and prepared me for a career in digital forensics and incident response. Through the development of my e-Portfolio, I identified three skillsets that represent my learning: Cybersecurity Foundations, Cybersecurity Law and Ethics, and Cybersecurity Applications. The nine artifacts connected to these skillsets show how my coursework helped me develop research, technical, problem-solving, ethical reasoning, communication, and investigative abilities. They also demonstrate how cybersecurity connects with other disciplines, including social science, criminal justice, philosophy, law, business, and interdisciplinary studies. Courses such as IDS 300W helped me understand how different disciplines can work together to address complex problems, while IDS 493 and the e-Portfolio process allowed me to reflect on how my academic experiences have shaped my professional identity. Looking at my coursework has shown me that career readiness involves more than technical knowledge. It also requires the ability to analyze information, consider legal and ethical responsibilities, communicate findings, and apply knowledge to real-world problems. These experiences have strengthened my preparation for entering the cybersecurity field and continuing to develop professionally.

Introduction

Looking back at my cybersecurity education at Old Dominion University, I can see that I learned more than how computers and security tools work. My courses taught me to research problems, examine evidence, consider different viewpoints, communicate information, and make responsible decisions. These abilities developed through cybersecurity, information technology, criminal justice, philosophy, law, business, social science, and interdisciplinary studies. My e-Portfolio brings these experiences together through three skillsets: Cybersecurity Foundations, Cybersecurity Law and Ethics, and Cybersecurity Applications. They show my progression from learning basic cybersecurity concepts to understanding professional responsibilities and applying my knowledge to realistic problems.

This progression shows why cybersecurity is interdisciplinary. Repko and Szostak (2020) explain that interdisciplinary thinking combines knowledge from different disciplines to better understand complex problems. Cybersecurity can involve technology, human behavior, crime, privacy, ethics, business, and law. Developing my e-Portfolio helped me recognize these connections. Nguyen (2013) explains that an e-Portfolio can connect learning, reflection, and identity rather than simply store assignments. Looking back at my artifacts has helped me understand how my education has prepared me for a career in digital forensics and incident response.

Cybersecurity Foundations

My Cybersecurity Foundations artifacts from IT/CYSE 200T, CYSE 300, and CYSE 301 show how I progressed from understanding basic security principles to researching incidents and applying technical concepts.

IT/CYSE 200T helped me understand that cybersecurity is more than protecting computers from hackers. My artifact involving the CIA Triad confidentiality, integrity, and availability provided a basic framework for understanding information security. I originally associated cybersecurity mainly with preventing unauthorized access, but I learned that information must also remain accurate and available to authorized users.

The course also taught me to consider how cybersecurity affects individuals, businesses, and communities. This was important because it moved my thinking beyond technology. I began asking who could be affected by a cybersecurity problem and what consequences might follow. That perspective became useful in later courses involving law, ethics, and digital forensics.

My *Marriott Under Fire* research paper from CYSE 300 allowed me to examine these ideas through a real data breach. Researching the Marriott and Starwood breach required me to consider vulnerabilities, outdated systems, organizational decisions, and effects on customers. I learned that a major breach is rarely caused by one technical failure. Instead of simply explaining what happened, I had to determine why it happened, what weaknesses contributed to it, and what could have been done differently.

This assignment strengthened my research and analytical abilities. It also changed how I examine cybersecurity incidents because I learned to look for connections between events rather

than focusing only on the obvious problem. Digital forensics and incident response require similar thinking because investigators must examine evidence and reconstruct what occurred.

CYSE 301 moved me toward applying cybersecurity concepts in a technical environment. I worked with networks, vulnerabilities, system security, and cybersecurity tools. Technical exercises did not always work as expected, so I had to check configurations, review my work, and determine what went wrong. This taught me that cybersecurity requires more than memorizing commands. Understanding why a tool is being used is important because real problems do not provide step-by-step instructions.

Together, these courses show the development of my foundation. IT/CYSE 200T taught me what cybersecurity protects, CYSE 300 showed what can happen when security fails, and CYSE 301 gave me opportunities to apply technical concepts. The NICE Framework emphasizes the combination of knowledge and skills needed for cybersecurity work (Petersen et al., 2020). These foundational courses prepared me for advanced work in ethical hacking and digital forensics.

Cybersecurity Law and Ethics

My Cybersecurity Law and Ethics skillset helped me understand that technical ability comes with legal and professional responsibilities. CYSE 406, PHIL 355E, and CRJS 404 allowed me to examine cybersecurity through law, philosophy, and criminal justice.

In CYSE 406, my privacy and personal data protection memorandum required me to examine privacy, personally identifiable information, biometric information, and data protection requirements. The memorandum was different from a traditional research paper because I had to

turn research into clear and practical information. This strengthened my ability to communicate complicated issues to people who may not have a technical or legal background.

The course also changed how I think about technical access. Having the ability to access information does not automatically give someone the legal authority to do so. This is especially important in digital forensics because investigators may handle private files, communications, and account information. I learned that technical knowledge must work alongside an understanding of legal boundaries.

PHIL 355E added an ethical perspective. My Cybersecurity Ethics reflection required me to consider corporate responsibility, privacy, professional ethics, and cyberconflict. I learned that an action can be technically effective while still creating an ethical problem. Some assignments were difficult because there was not always one correct answer. I had to consider different viewpoints and explain why one decision might be more responsible than another.

This changed how I think about professional judgment. A digital forensic investigator may encounter information unrelated to an investigation, making ethical reasoning important when deciding how that information should be handled. CYSE 406 taught me about legal boundaries, while PHIL 355E taught me to consider what is responsible when the correct decision is not obvious.

CRJS 404 added the criminal justice perspective. My cyberterrorism work required me to examine cyber threats as criminal and national-security issues rather than only technical attacks. I learned how cybersecurity connects with criminal behavior, investigations, evidence, and the justice system. Lessons from law and ethics helped me understand why evidence collection must also follow legal and professional standards.

Kent et al. (2006) explain that digital forensic techniques can support incident response by examining files, operating systems, network traffic, and applications. CRJS 404 helped me realize that finding information is only part of an investigation. Investigators must understand why evidence matters, preserve it correctly, and explain how it relates to an incident. These lessons directly support my career goal in digital forensics and incident response.

Cybersecurity Applications

My Cybersecurity Applications artifacts from CYSE 407, CYSE 450, and CYSE 494 show how I applied knowledge from earlier courses to practical cybersecurity problems.

CYSE 407 was especially important because it connects directly with digital forensics. My Digital Forensics Laboratory Strategic Plan required me to consider evidence storage, chain of custody, forensic workstations, write blockers, software, staffing, accreditation, and security. I originally focused on the equipment needed for a forensic laboratory, but I learned that a reliable laboratory also depends on procedures, documentation, qualified personnel, and legal standards.

The project required knowledge from cybersecurity, criminal justice, law, research, and organizational planning. My experience with Autopsy, FTK Imager, and Wireshark also strengthened my technical preparation. Digital-forensics and incident-response job postings often seek skills involving evidence analysis, documentation, investigation, communication, and forensic tools. This artifact allowed me to practice several of those abilities while seeing how different disciplines contribute to an investigation.

CYSE 450 Ethical Hacking developed another side of my technical ability. Scans, configurations, and exploits did not always work correctly, so I had to troubleshoot and try

different approaches. This taught me patience and showed me that technical problem-solving requires understanding what I am doing instead of simply following commands.

The course also taught me to think from an attacker's perspective. Understanding how attackers search for weaknesses and attempt to gain access can help an investigator recognize evidence they may leave behind. Lessons from CYSE 406 and PHIL 355E also reminded me that these abilities must remain within legal and ethical boundaries. This showed me how technical knowledge, law, and ethics can work together.

CYSE 494 expanded cybersecurity applications beyond technical work through my Venture Idea Assessment. Developing CyberShield Insight required me to consider human error, artificial intelligence, cybersecurity risk, customer needs, competition, and whether the idea could realistically provide value. Unlike a technical lab, there was no single correct solution. I had to research the problem, evaluate different possibilities, and explain why my proposed solution could work.

This project taught me that cybersecurity professionals must also understand organizations and communicate with people who may not have technical backgrounds. That lesson applies to incident response because investigators have to explain what happened, what the risk means, and what should happen next. A technical solution has limited value if people cannot understand or realistically use it.

Interdisciplinary Learning, Portfolio Development, and Career Readiness

IDS 300W helped me understand the connections among these artifacts. I learned that different disciplines have their own perspectives and methods and that complex problems can benefit from combining those viewpoints. I saw this throughout my degree. Cybersecurity

courses taught me about attacks and investigations, criminal justice helped me understand crime and evidence, philosophy strengthened ethical reasoning, law established professional boundaries, and entrepreneurship taught me to consider organizational needs.

IDS 493 and developing my e-Portfolio helped me see how these experiences fit together. McAdams (2001) explains that people develop life stories that connect experiences and contribute to identity. Instead of viewing my assignments as unrelated work from separate courses, I now see how they contributed to the cybersecurity professional I am becoming. This also supports Nguyen's (2013) view that an e-Portfolio can connect learning, reflection, and identity.

Reviewing job advertisements has helped me evaluate my career readiness. Digital-forensics and incident-response employers commonly seek people who can investigate incidents, analyze evidence, document findings, solve problems, communicate clearly, and responsibly handle sensitive information. My coursework does not replace professional experience, but my nine artifacts show that I have practiced these abilities and developed a foundation for continuing to improve them professionally.

Conclusion

Looking at my degree program, my three skillsets show clear progression. Cybersecurity Foundations gave me the knowledge, research, and problem-solving abilities needed to understand cybersecurity problems. Cybersecurity Law and Ethics taught me to consider legal, ethical, criminal justice, and human consequences. Cybersecurity Applications allowed me to combine those lessons and apply them through digital forensics, ethical hacking, and cybersecurity entrepreneurship.

IDS 300W helped me understand why combining disciplines matters. Cybersecurity professionals cannot rely only on technical knowledge because real incidents involve people, organizations, laws, evidence, ethical decisions, and communication. Developing my e-Portfolio through IDS 493 helped me recognize that these abilities developed throughout my education rather than through one course. As I move toward digital forensics and incident response, interdisciplinary thinking will help me examine problems from different perspectives, communicate my findings, and make responsible decisions. My portfolio represents more than assignments completed for a degree. It shows how I have learned to connect knowledge, solve problems, reflect on my decisions, and continue developing as a cybersecurity professional.

References

- Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-86>
- McAdams, D. P. (2001). The psychology of life stories. *Review of General Psychology*, 5(2), 100–122. <https://doi.org/10.1037/1089-2680.5.2.100>
- Nguyen, C. F. (2013). The ePortfolio as a living portal: A medium for student learning, identity, and assessment. *International Journal of ePortfolio*, 3(2), 135–148.
- Petersen, R., Santos, D., Wetzel, K. A., Smith, M. C., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE Framework)* (NIST Special Publication 800-181 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-181r1>
- Repko, A. F., & Szostak, R. (2020). *Interdisciplinary research: Process and theory* (4th ed.). SAGE Publications.