Reflection Essay: Problem Solving, Python Automation, and Digital Forensics

Emmanuel Dade

School of Cybersecurity, Old Dominion University

IDS 493

Dr. Virginia Tucker Steffen

10/10/2026

Reflection Essay: Problem Solving, Python Automation, and Digital Forensics

Introduction

Coming into this program I had cybersecurity as just one technical discipline. After nine artifacts and one early research paper, I realize that my three core competencies (problem solving, Python automation, and digital forensics) each grew from a confluence of disciplines including computer science, networking, security operations, law, and professional communication. Repko and Szostak (2017) define interdisciplinary research as a heuristic, iterative, and reflexive process of decision making. That is how I approached each of the artifacts below.

This essay begins with the course that introduced me to this process – IDS 300W. Then for each of my three skills, I will discuss what I learned, the influence of other disciplines, and finally how the skill relates to three of the jobs I am interested in: Application Security Engineer I at Bloomberg Industry Group (Bloomberg Industry Group, 2026), Data Engineer at Everforth ECS (Everforth ECS Federal, 2026), and Cyber Analyst for Digital Forensics and Incident Response at At-Bay (At-Bay, n.d.). I will also treat my portfolio as an evolving self-story as defined by McAdams (2001), which gives purpose and unity to experience.

IDS 300W: Learning to Integrate

For my IDS 300W research paper, I explored the possibility of a ban on TikTok from the lenses of law, sociology, political science, psychology and public health. Repko and Szostak (2017) state a problem is suited to interdisciplinary research if it is complex, if valuable insights can be gained from two or more disciplines, and if no single discipline can adequately solve the problem. The TikTok debate fits all three criteria; teen mental health, privacy law, national security politics, and health communication each explained one aspect of the problem.

Upon reviewing my IDS 300W paper again I can see what was left out. I placed five perspectives in juxtaposition with one another but failed to integrate them. Repko and Szostak (2017) make this distinction between interdisciplinary and merely multidisciplinary research for this exact reason. Additionally, they ask the researcher to consider whether a bias may be influencing their research. My conclusion did not adequately respond to this because instead of weighing evidence from various disciplines it sided with one argument. They also recommend narrowing to the three or four most relevant disciplines and I attempted to cover all disciplines.

This self-reflective assessment became the basis for my approach in subsequent artifacts. I identify the disciplines used in each artifact and consider what role each discipline played. I also attempt to test my conclusions based on evidence rather than personal biases. Additionally, from IDS 300W I developed a stronger aptitude for using and citing scholarly resources. This skill is utilized throughout my portfolio.

Skill 1: Problem Solving

Problem Solving: Getting Security and Development on the Same Page came from my application security internship. The most difficult problem was not a bug. There were different objectives for security and development. If communication only occurs at handoffs, then security appears to be a checkpoint. By applying the IDS 300W problem-solving technique of decomposing a problem into smaller pieces, I was able to define the problem, choose a solution (regular meetings, sharing results, two-way code reviews), repeat the solution and evaluate the results. Wing (2006) states computational thinking is about problem solving and understanding human behavior through decomposition and abstraction. In my problem I decomposed communication into three repeatable actions. Bloomberg's posting asks for entry level engineers to collaborate with software engineers and integrate security into CI/CD pipelines (Bloomberg

Industry Group, 2026). I utilized Azure DevOps, GitLab CI/CD, and GitHub Actions to preview these responsibilities.

Sword vs. Shield (CYSE 301) taught me to solve problems from both sides. Scanning as the attacker I expected about a hundred packets but saw over fifteen hundred. From the perspective of the defender, I created pfSense rules and repeated the scan to see which ports got filtered. Kent et al. (2006) note that firewalls record basic information including IP address, protocol, and ports. This information helped me interpret what I saw. From both networking and policy design I learned to measure instead of assume. ECS's Data Engineer posting asks for routine troubleshooting of connectivity, data access, and permissions (Everforth ECS Federal, 2026). This problem helped me evaluate network behavior using only evidence and not assumptions.

In *Reflection Paper 2* there were problems that created resistance. One problem was a scraper that failed repeatedly and shared code spaces with compatibility problems. I was able to trace each problem to its source and ask my supervisor when I reached the limit of my capabilities. Repko and Szostak (2017) describe feedback loops that force a researcher to revisit previous steps. Every failed run forced me to revisit my assumptions about the evidence. Additionally, I researched members of the opposing party and condensed large amounts of information into something that is accessible to non-technical individuals. This required both political research and programming. McAdams (2001) states that stories in which bad experiences become good are associated with wellness and coherence. In this case the failed scraper became the example of such a story for me.

Skill 2: Python Automation

In *AV Stager*, a tedious spreadsheet process is automated with Google Drive API's, layered file matching and per-file error handling. File matching starts with a strict match and then progressively becomes less strict. Wing (2006) defines this as choosing a representation and using abstraction to make a problem manageable. Security played a role in the design including credentials that are only available during runtime, nothing is stored to disk and only read-only access is available. The hardest part was signing in to Google from a web application. The messy, corrupt transcripts required me to skip bad lines rather than fail the entire process. Additionally, I documented the limitations of the automation because fuzzy matching can match similar names and requires human validation. ECS's Data Engineer posting asks for the ability to perform file operations in Python, use APIs, work with CSV files, and perform validation (Everforth ECS Federal, 2026). Bloomberg's posting asks for help automating security tools and scripts (Bloomberg Industry Group, 2026).

The *FIFA World Cup Quiz Game* (CYSE 250) involved sockets, threading, authentication and encryption. While creating this I learned that a Caesar cipher and simple hash functions demonstrate security concepts but are not suitable for protecting real data. For this reason ECS also lists encrypted data transfer as one of the skills they want (Everforth ECS Federal, 2026). This combined programming with security and will help me evaluate code for Bloomberg's secure coding requirements (Bloomberg Industry Group, 2026).

In *Reflection Paper 1* there were early scripts that extracted and cleaned data from spreadsheets. From these scripts I learned that even a script that almost works can quietly produce incorrect data and that automation is only valuable if teammates can trust it. When presenting updates to my team I learned to explain what a script does and where it can fail.

ECS's posting asks for similar skills in data inventories, validation and documentation (Everforth ECS Federal, 2026).

Skill 3: Digital Forensics

In my *Incident Response Report* I documented a remote access scam. My indicator of compromise was multiple UAC prompts. Additionally, I observed timestomping with respect to a file's properties. The creation date matched the time of the scam but the modified date was three years older. Kent et al. (2006) note that attackers may modify file times. From my CYSE 407 reading I was able to recognize this. The attacker used a legitimate remote access tool and persuaded the victim to allow the remote session. As a result understanding the incident required both technical and social engineering skills. At-Bay's Cyber Analyst for Digital Forensics and Incident Response requires knowledge of indicators of compromise, incident timelines and root cause analysis (At-Bay, n.d.). My report documented the incident from the UAC prompts to the files to the remote session using AnyDesk. I mapped my actions to the NIST incident response process. My largest mistake was that I did not capture screenshots or hashes before cleaning up the system. At-Bay lists forensically sound data collection as its first required skill and this is the step that I performed the worst (At-Bay, n.d.).

In my *Digital Forensic Examination Report* I utilized technical and legal reasoning. I required a warrant, a write-blocked image, hash values, recovery of deleted files and chain of custody. Evidence came from several sources including text messages, a recovered email thread, deleted files and browser history. Conclusions were based on correlating evidence from these various sources. Kent et al. (2006) describe correlation as the heart of analysis. They also state that matching message digests proves that one copy equals the original and that the intended audience of the report impacts the report. At-Bay expects reports for executives, attorneys and

claims staff (At-Bay, n.d.). ECS also requires checksum validation and auditable records (Everforth ECS Federal, 2026). This is another example of the same skill.

In my *Digital Forensics Lab Plan* (CYSE 407) I designed a police lab including a layout, equipment, ISO/IEC 17025 accreditation, maintenance, staffing and training. Garfinkel (2010) warns that growing amounts of data, encryption, cloud-based data, and multi-device cases pose a threat to digital forensics unless digital forensics processes evolve. My plan addresses this with tool validation, calibration, annual training and a 36 month technology review. Identifying the disciplines used in this plan (engineering, management, budgeting and law) was an application of IDS 300W to a lab.

Conclusion

Creating this portfolio required a selection of nine artifacts to include. The selection process taught me something. Initially I saw discrete artifacts. When grouping artifacts by skills I noticed relationships. For example hashing in my forensic examination report mirrors checksums in ECS's posting (Everforth ECS Federal, 2026). This is an example of the mapping process from IDS 300W applied to my own career.

IDS 300W prepared me for this program by teaching me to ask which disciplines own which parts of a problem before selecting a solution. Interdisciplinary research is important in cybersecurity because incidents are not purely technical. Garfinkel (2010) notes that cases are increasingly requiring evidence correlation from multiple devices and Wing (2006) states that computational thinking has value beyond computer science. Developers, investigators, lawyers and executives each see part of the same incident and the three jobs I am interested in describe connecting these parts. McAdams (2001) describes life as being structured by a developing life narrative which gives the individual purpose and coherency. My narrative starts from a paper I

wrote for TikTok that presented opinions but did not incorporate them. Then came a scrapped scraper, a cipher that was too primitive to be practically useful, and finally a probe that I wish I had made better notes on. All of these experiences have given me insights that I now bring to my work in application security. Bloomberg also mentions SAST, DAST and software composition analysis as tools that I intend to gain more experience with (Bloomberg Industry Group, 2026).

References

At-Bay. (n.d.). *Cyber Analyst, Digital Forensics Incident Response* [Job posting]. At-Bay Careers.

Bloomberg Industry Group. (2026). *Application Security Engineer I* (Job requisition ID: 142068) [Job posting]. Bloomberg Industry Group Careers.

Everforth ECS Federal. (2026). *Data Engineer* (Job No. 5170) [Job posting]. ECS Federal Careers.

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(Suppl.), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

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

Repko, A. F., & Szostak, R. (2017). *Interdisciplinary research: Process and theory* (3rd ed.). SAGE Publications.

Wing, J. M. (2006). Computational thinking. *Communications of the ACM, 49*(3), 33–35. https://doi.org/10.1145/1118178.1118215