Cybersecurity Professional Career Paper:

The Importance of Digital Forensic Examiners

Katherine Billy

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 15, 2025

Introduction

The role of a Digital Forensic Examiner is to collect digital evidence after a crime, typically a cybercrime, has taken place in order to assess and contain the damage, find the culprit, and prevent future attacks (Forensic Focus, 2019). These types of cybersecurity professionals assist the legal court system when necessary to help provide evidence and occasionally explanations in criminal cases involving digital aspects (AU Online, 2025). In this day and age where more and more aspects of everyday life are being digitized, cybersecurity is the solution to protecting and maintaining people's privacy (Shimonski, Zenir, & Bishop, 2015). Digital Forensic Examiners are a vital part of the cybersecurity community, because they not only help to apprehend malicious attackers, but they also work to bolster security systems using the intelligence they learned from previous attacks. This paper will describe how both the career of Digital Forensic Examiner as well as the overall subject of digital forensics relate to the principles of social sciences, key cybersecurity topics, marginalized groups, and society as a whole.

Social Science Principles

Some of the principles of social sciences include objectivity, empiricism, ethical neutrality, and skepticism. Cybersecurity research relates to each of these fundamentals and more. Digital Forensics, in particular, because of its association and involvement in cybercrime. This requires that all research be done without the burden of personal opinion (objectivity), based solely on facts (empiricism), ethically and with consideration to all those involved in any study (ethical neutrality), and with repeated testing including critical thinking (skepticism).

The subject of digital forensics helps to connect cybersecurity with some of the other social science disciplines. The work that is done in digital forensics involves criminology, psychology, sociology, and even geography. In a more obvious and literal sense, digital forensics relates to criminology, psychology, and sociology in the way that it tries to understand how criminals think and work in order to catch and convict them. Through using the definition of geography: "study of places and the relationship between people and their environments", given by Professor Diwakar Yalpi in module 1 of CYSE 201S, a connection can be made between cybersecurity and geography to use geography standards to help understand the "digital world". The movie "Ready Player One" and the TV show "Upload" are two visual examples of (dramatized) representations of this realm within cyberspace in the media.

Application of Key Concepts

Nishchal Soni defines digital forensics as: "the science of discovering, collecting, analyzing, and presenting digital evidence" (Soni, 2025, para. 5). Within the "Literature Review" of the same article, Soni explains how digital forensics bridges the gap between criminal law and cybersecurity (Soni, 2025). The combination of these two subjects creates the topic of cybercriminology. Digital forensic examiners use Alexandra Michel's idea of "Psyber Security" in order to analyze offenders and understand their psychological profile in order to gain insight on their possible attack method. This understanding of cybercriminals' potential thought processes can also assist digital forensic examiners with adjusting systems to be better protected against subsequent attacks. A tool that can help gain insight into these thought processes is a Honeypot that allows researchers to study and watch how hackers break into programs. Results from Honeypots along with knowledge on human factors and victim precipitation can lead to effective preventative measures. Human factors help digital forensic examiners by the recognition of how humans will inherently interact with technology, and victim precipitation helps them to understand how prevent similar attacks in the future through understanding both the victim's actions as well as how the methods the attacker used.

Marginalization

As technology continues to grow and evolve, the areas and integration of cybersecurity and artificial intelligence are growing as well. While in general this continuous evolution is typically a good thing, it can also cause some serious issues. One issue of major concern is AI bias. AI algorithms learn from the information that is plugged into it, and because of this these programs can have the same biases as the humans creating them (Klasén, Fock, & Forchheimer, 2024). "The databases used for training mostly represent the world as it is and not the way we ideally want our society to be, e.g. concerning gender equality, explainability and fairness." (Klasén, Fock, & Forchheimer, 2024, section 3 para. 5). This quote really helps to highlight the dangers of using AI, especially in digital forensics where there is often a legal and criminal aspect to investigations. Inevitably, bias reflects the opinions of people in power, and this has the potential to create an unfair disadvantage towards people of color and other minorities. In order to work to reduce AI bias going forward, AI algorithms should be frequently monitored and tested (Klasén, Fock, & Forchheimer, 2024).

Connection to Society

Digital forensic examiners help to protect against cyber-attacks as well as help the criminal justice system capture and convict criminals though the collection and analyzing of digital data. "Stress is considered a small price to pay for the ability to hunt and catch child predators, terrorists, and other bad actors — and to rescue their victims, prevent additional harm, and bring justice." (Forensic Focus, 2019, para. 26). Through the hard work that digital forensic examiners do, they help to improve both the fields of cybersecurity as well as criminal justice. Even as both industries continue to advance, a common concern within the field of cybercriminology is still the issue between cybercrimes and jurisdiction (Shimonski, Zenir, & Bishop, 2015).

Conclusion

The cybersecurity industry has countless subcategories, and one of them is the field of digital forensics. A digital forensics professional is often referred to as a digital forensic examiner, and this career is comprised of many of the different interdisciplinary subjects that cybersecurity can be involved in. Digital forensic examiners collect and inspect digital evidence linked to investigations. They often work alongside the criminal justice system in order to help protect people against technology related crimes.

Scholarly Journal Articles

Source 1: "Chapter 1 – Digital Reconnaissance and Surveillance" from *Cyber Reconnaissance, Surveillance and Defense* – This article gave a great overview of digital forensics and digital forensic examiners within the ever growing digital world.

Source 2: "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age" – This article described the ethical issues that can arise for marginalized groups from using AI within digital forensics.

Source 3: "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges" – This article explained numerous different aspects of digital forensics and helped to related them to key concepts of cybersecurity.

Works Cited

AU Online. (2025). *Digital Forensic Examiner: Salary and Job Discription*. Retrieved from Augusta University: https://www.augusta.edu/online/blog/digital-forensic-examiner-salary

Forensic Focus. (2019, April 3). *Digital Forensics Jobs and Career Paths*. Retrieved from Forensic Focus: https://www.forensicfocus.com/employment/digital-forensics-jobs-and-career-paths/?gad_source=1&gad_campaignid=18338929324&gbraid=0AAAAAo7kw7XwE07XfJLzp6v75sbwm8Vrw&gclid=Cj0KCQiA5uDIBhDAARIsAOxj0CEJLvEiV54QeeIrQHtrbT5SVWZkKKPEnWIHuCOq0gjl7hbbMZhuydoaAv6NE

Klasén, L., Fock, N., & Forchheimer, R. (2024). The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age. *Forensic Science International*.

Shimonski, R., Zenir, J., & Bishop, A. (2015). Chapter 1 - Digital Reconnaissance and Surveillance. In R. Shimonski, J. Zenir, & A. Bishop, *Cyber Reconnaissance, Surveillance and Defense* (pp. 1-44). Syngress.

Soni, N. (2025). Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges. *HSOA Journal of Forensic, Legal & Investigative Sciences*.

Yalpi, D. (2025). *CYSE201S (Module 1): Introduction to the Social Sciences*. Retrieved from Canvas ODU: https://canvas.odu.edu/courses/188032/files/50788219?module_item_id=8606145