Cybersecurity Professional Career Paper: Digital Forensics and Society

Student Name: Kennice Allea Balmoria

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Instructor Name: Diwakar Yalpi

Date: 13 April 2026

Introduction

The cybersecurity profession has become one of the most essential fields in modern society, especially as technology shapes how people communicate, work, and commit crimes. Among the many cybersecurity roles, the career of a **Digital Forensic Investigator** stands out because it blends technical expertise with investigative thinking. This career appeals to me because I want to work in environments such as the FBI, police departments, or federal agencies, where I can solve problems hands-on rather than sit behind a desk all day. Digital forensics is a field where every day presents a new challenge and an opportunity to uncover the truth. This paper examines how social science principles guide the daily work of digital forensics professionals, how these principles shape interactions with society and marginalized groups, and how research in the social sciences strengthens cybersecurity practices.

Social Science Principles in Digital Forensics

Relativism is central to this career because investigators must understand how technological, social, political, and criminal justice systems influence one another. A cyber incident is never isolated; it is shaped by social behaviors, economic pressures, and technological environments. For example, changes in social media use can influence patterns of cyberstalking or fraud.

Objectivity is essential in digital forensics because investigators must analyze evidence without personal bias. Whether examining a suspect's device or reconstructing a timeline of events, conclusions must be based solely on data, not assumptions about the individual or the crime.

Parsimony guides investigators to create explanations that are as simple as possible while still accurate. When determining how a breach occurred, investigators avoid overly complicated theories and instead focus on the most direct, evidence-based explanation.

Empiricism is at the heart of digital forensics. Every claim must be supported by observable, measurable evidence, like logs, metadata, timestamps, file artifacts, and network traces. Opinions and hunches cannot be used to determine guilt or innocence.

Ethical neutrality is also critical. Digital forensics professionals handle sensitive personal data and must protect the rights of individuals, even when investigating serious crimes. They must follow strict legal and ethical guidelines to avoid violating privacy or mishandling evidence.

Determinism helps investigators understand that digital behavior is influenced by prior events. For example, individuals may engage in cybercrime due to social pressures, low self-control, or exposure to certain online environments. Understanding these influences helps investigators interpret digital actions more accurately.

Skepticism ensures that investigators question all claims, validate evidence, and avoid accepting information at face value. This principle helps prevent misinterpretation of data and strengthens the accuracy of forensic conclusions.

Application of Key Concepts

Investigators often ask research questions such as: *What caused this breach? How did the attacker gain access?* They develop hypotheses, like predicting that a phishing email was the initial attack vector. They identify independent variables, like user behavior and system vulnerabilities, and dependent variables, like the resulting breach or data loss. Understanding

causality helps them determine whether one action directly led to another, such as whether opening a malicious attachment caused malware installation.

Digital forensics also uses both nomothetic and idiographic approaches. Nomothetic explanations help identify common causes of cyber incidents across many cases, while idiographic explanations help reconstruct the unique sequence of events in a specific investigation.

Marginalization and Cybersecurity

Cybersecurity affects marginalized groups in unique ways. Communities with limited digital literacy or access to secure technologies are more vulnerable to scams, identity theft, and exploitation. Digital forensics investigators often encounter cases involving victims from these groups, making it essential to approach investigations with cultural awareness and ethical sensitivity. Additionally, marginalized individuals may be disproportionately monitored or misidentified in digital systems, raising concerns about fairness and surveillance. The cybersecurity field is actively working to diversify its workforce to create more equitable digital protections and reduce biases in investigative practices.

Career Connection to Society

Digital forensics investigators play a crucial role in protecting society. They support the stability of financial systems, healthcare networks, government agencies, and critical infrastructure by uncovering the causes of cyber incidents and preventing future attacks. Their work also informs public policy by providing evidence that shapes laws related to privacy, cybercrime, and digital rights. As technology continues to evolve, digital forensics professionals help maintain trust in digital systems and ensure justice for victims of cybercrimes.

Scholarly Journal Articles

Mountrouidou et al. (2019) emphasize the importance of diversity in cybersecurity education, showing how broader representation strengthens problem-solving and reduces bias. This supports the argument that digital forensics must consider marginalized groups and ethical neutrality.

The National Academies Press (2019) highlights how integrating social and behavioral sciences improves cybersecurity by enhancing understanding of human behavior, risk perception, and decision-making. This directly connects to principles like determinism, skepticism, and empiricism.

Back (2021) examines cyber-situational crime prevention and how human-focused strategies reduce cyber incidents. This research supports the application of social science concepts such as variables, causality, and behavioral analysis in digital forensics investigations.

Conclusion

The career of a Digital Forensics Investigator is deeply connected to social science principles. Relativism, objectivity, parsimony, empiricism, ethical neutrality, determinism, and skepticism guide how investigators analyze evidence and understand human behavior. Social science research methods strengthen investigative practices, while awareness of marginalized groups ensures ethical and equitable outcomes. Ultimately, digital forensics professionals play a vital role in protecting society, promoting justice, and maintaining trust in digital systems.