Career Paper

Hailey Caram

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Matthew Umphlet

August 8, 2025

Digital forensics investigators, and the broader cybersecurity field, are inherently interdependent on social sciences. Society and technology work to shape each other, and social science principles steer cybersecurity development. This interdependence includes what is known as the social cyberspace, which impacts digital interaction, communication, and community. The digital interconnectedness of today's society creates unique interactions between society and digital forensics investigators, emphasizing human and social dimensions of cyber threats (Mulahuwaish et. al, 2025). Digital forensics investigators depend heavily on social science research and principles in their daily routines.

Many social science principles and research methods are used by digital forensics investigators to ensure that their work is factual, reliable, and just. Investigators apply the principle of empiricism through their reliance on evidence such as IP addresses, security logs, and metadata. Empicism is especially important to demonstrate in this role due to the fact that investigations sometimes lead to criminal charges where there is no room for assumptions. Another principle demonstrated by digital forensics investigators is objectivity, this principle is particularly important in their conclusions and documentation. It is important to ensure that investigations and final recommendations are purely based on evidence that was found, not personal bias. Social science research is routinely used by digital forensics investigators, especially methods such as archival and field research. Archival research is used daily to analyze historical digital data such as logs, deleted files, and prior cases. They do this to identify any patterns that may be present and establish timelines. Field research comes to play when investigators have to go out to an ongoing incident and analyze behaviors that could add context to their investigation.

Professionals in this career utilize knowledge of human behavior to analyze why and how cybercrimes occur, and likely utilize cyberpsychology in daily forensics work. Cyberpsychology explains cyber behaviors using psychological principles, as well as how behavior or mental states can be influenced by technology. Cyberpsychology can help digital forensics investigators understand motivations for cyber offenses. Additionally, digital forensics investigators who are knowledgeable about human behavior are better able to interpret digital evidence left by hackers and predict threats (Rich & Aiken, 2024). Social science theories, such as conflict theory or structural functionalism, aid digital forensics investigators in understanding human behavior. The conflict theory, for example, would help investigators explain how the power dynamics of underground economies drive trade. Understanding social conflict and power dynamics help investigators determine motives and the social impact of cases they work on every day. Understanding victim precipitation in relation to cybercrime is also crucial to digital forensics investigators. Victims could unintentionally contribute to their victimization, this helps investigators trace behaviors and inform prevention methods. Analyzing time-sensitive evidence and using complex interfaces can lead to fatigue and pressure. Being aware of these human factors helps design forensic tools that reduce error and discourage confirmation bias.

Investigators also rely on the social sciences to help inform ethical decision-making processes. A large part of the job of a digital forensics investigator involves personal and sensitive data, requiring ethical consideration as an investigator navigates legal or ethical boundaries. Utilizing social science frameworks can guide investigators through issues like privacy rights or due process. Prioritizing ethical frameworks, especially digital privacy, is important for marginalized groups (Tennent, 2021). Marginalized groups, such as members of the LGBTQ+ community, are often at increased risk of persecution and must practice digital

privacy to avoid being targeted. Digital forensics investigators must carefully consider potential impacts of their work on marginalized communities, who experience increased online vulnerability. By exposing hate crimes and systemic vulnerabilities, investigators contribute to digital justice, ensuring that victims belonging to marginalized groups can establish faith in the processes that are in place. This can also lead to implementing measures designed to protect those that do not have the same education or resources to do so on their own.

References

Mulahuwaish, A., Qolomany, B., Gyorick, K., Bou Abdo, J., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. *Computers in Human Behavior Reports, 18*, 100668. https://doi.org/10.1016/j.chbr.2025.100668

Rich, M. S., & Aiken, M. P. (2024). An interdisciplinary approach to enhancing cyber threat prediction utilizing forensic cyberpsychology and digital forensics. *Forensic Sciences (Basel, Switzerland)*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008

Tennent, C. (2021, October 26). *The importance of digital privacy for marginalized groups*. The World Wide Web Foundation. https://webfoundation.org/2021/10/the-importance-of-digital-privacy-for-marginalized-groups/