Cybersecurity Career Professional Paper

Digital Forensics Investigator
David Kenon
Professor Diwakar Yalpi
CYSE 201S – Introduction to Cybersecurity
November 16, 2025

BLUF

Digital Forensics Investigators rely on social science principles to interpret digital evidence responsibly, reduce bias, and protect marginalized groups while supporting justice and cybersecurity.

Introduction

When most people think about cybersecurity, they picture people sitting in dark rooms trying to stop hackers, but a lot of the real work happens after the attack. That's where Digital Forensics Investigators (DFIs) come in. DFIs collect, examine, and interpret digital evidence when something goes wrong — whether that's a data breach, a cyberstalking case, or a criminal investigation. Even though the job sounds technical, it actually depends a lot on social science. The way people behave, the social environments they come from, and the motives behind crime all influence how digital evidence gets created and interpreted. This paper explains how social science concepts connect directly to digital forensics work, especially when dealing with marginalized communities and society as a whole.

What Digital Forensics Investigators Do

A Digital Forensics Investigator basically acts like a detective, but in the digital world. Their job is to recover files, trace online activity, build timelines, and present findings in a way that law enforcement or a court can use. Cases can include child exploitation, fraud, insider threats, ransomware, identity theft, or homicide. DFIs need to understand technology, but they also need to understand people — because behind every piece of evidence is a human decision, a behavior, or a social pattern.

How Social Science Research Applies to DFI Work

Social science helps DFIs make sense out of digital actions and motivations instead of just raw data. For example, **social learning theory** explains how offenders pick up criminal techniques from peers or online communities. **Routine activities theory** explains when and why certain targets are attacked. DFIs also rely on understanding **culture and communication** because every community uses language and technology differently. Even slang in text messages can change the meaning of a case. DFIs also have to look for **bias and perception**, which are major issues in social science. Two investigators can interpret the same evidence differently based on assumptions or experience, and that can ruin someone's life if the wrong conclusion is made.

Impact on Marginalized Groups

Digital forensics doesn't exist in a vacuum — real people are impacted, and not equally. For example:

1. **Racial and socioeconomic bias in investigations.** People from marginalized communities are more likely to be suspected first or lose control of their devices during an investigation.
2. **Lack of access to legal or technical resources.** Some people do not have the means to defend themselves or understand digital evidence being used against them.
3. **Misinterpretation of cultural communication.** DFIs must avoid misunderstanding slang, memes, or cultural behavior that can be taken out of context.

Social science helps DFIs avoid making the wrong call and protects vulnerable people from having their lives damaged by misunderstanding digital evidence.

Connection to Society

Digital forensics affects society because almost every part of our lives now leaves a digital footprint. DFIs help protect the public and support justice, but they also have a responsibility to avoid the misuse of digital evidence. They influence trust in legal systems, privacy, and public safety. In today's world, digital investigations can solve crimes but also raise concerns about surveillance, power, and fairness. That's why DFIs need a strong grounding in social science, not just technical knowledge.

Conclusion

Digital forensics might seem like a career built completely on technology, but the core of the job is human behavior. Social science helps investigators understand motives, avoid bias, interpret evidence responsibly, and recognize the impact of their work on vulnerable groups. With cybercrime increasing and more marginalized communities getting caught in the middle, DFIs need more than technical skills — they need cultural awareness, ethical judgment, and the ability to see the human story behind the data. That's why social science isn't optional in cybersecurity — it's essential.

References (APA)

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. (2021). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge.

Reyns, B. W. (2013). Online routines and identity theft victimization. *Journal of Research in Crime and Delinquency, 50*(2), 216–238. https://doi.org/10.1177/0022427811425539