

Cybersecurity Professional Career Paper: Digital Forensics Analysts

Student Name: Zachariah McDonough

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/12/2026

Introduction

Digital Forensics Analysts are the cybersecurity professions who collect, preserve, analyze, and report on digital evidence from disparate technical devices such as computers, mobile devices, networks, and cloud systems to aid in the investigation of cybercrimes, data breaches, and even legal disputes. Their work typically overlaps with law enforcement, corporate security, and the judicial system at large, where they recover files that were deleted, reconstruct timelines, and authenticate digital property for their admissibility in court. In our modern world where cyber threats have greatly escalated, (which impacts everything from financial systems to the most critical of infrastructure) cybersecurity has indubitably become a quintessential part of maintaining societal stability. Moreover, digital forensics plays an important role in this by turning raw data into actionable intelligence which can hold perpetrators accountable for their actions. This paper examines how Digital Forensics Analysts rely on social science research and principles, particularly in regard to those related to human behavior, cognitive processes, and societal inequalities. Furthermore, the paper will demonstrate the application of key class concepts, namely, behavioral analysis, cognitive biases, and the digital divide; to daily routines, with special attention and focus on interactions with marginalized groups and the overall broader societal contributions.

Social science principles

Social science research is very fundamental to understanding how human behaviors drive cybersecurity incidents, like hacking motivations which are rooted in psychological factors (e.g. thrill-seeking or financial gain) or ethical lapses in a user's decision making. Additionally, Digital Forensics Analysts integrate principles from psychology, criminology, and sociology into their

practices via human and computer interaction analysis, as well as user behavior reconstruction. For example, instead of seeing devices as some purely technical property/artifact, analysts instead apply behavioral insights to interpret digital footprints, like their patterns on social media or their browsing history, that reveal intent, relationships, and motives. All of this aligns with idiographic digital profiling (IDP), which uses a person's unique digital trace for case specific behavioral analysis, thus helping in the identification of suspects, lead generation, and the execution of warrants (Steel, 2014). Hence, in daily routines, analysts use these principles when examining any kind of evidence from phishing victims or other insider threats, therefore developing cybersecurity awareness programs that specifically address why certain users more than others are involved with risky behaviors. Social science consequently transforms forensics from something that is mere data recovery into a complete and holistic investigation of human actions (Steel, 2014).

Application of Key Concepts

The key social science concepts that we have learned in class, like cognitive biases and human factors, behavioral profiling, and overall ethical considerations in technology, all directly form and shape Digital Forensics Analysts' workflows. Particularly, cognitive and human factors have shown how analysts' own psychological process (e.g., confirmation bias or anchoring) can bring about errors during the interpretation of evidence, such as an over reliance on the initial findings in log analysis. Now, professionals typically mitigate this through having structured methodologies like peer review and bias checklists, thus ensuring mostly reliable results especially for the sake of legal compliance (Sunde & Dror, 2019). Moreover, behavioral profiling concepts are applied when reconstructing timelines from device artifacts to assess some

organizational risks or insider threats, they usually use tools like Autopsy or FTK Imager alongside specific psychological frameworks to then infer human intent. For example, analysts typically evaluate compliance with certain standards like the chain of custody protocols, which in turn bring sociological understandings of trust and accountability for specially high stakes environments. These concepts aid in guiding risk assessments (e.g., identifying specific vulnerable user behaviors in networks) and implementation of protocols, which makes forensics more accurate and defensible in court (Sunde & Dror, 2019).

Marginalization

Cybersecurity and digital forensics have a deep effect on marginalized groups via issues like the digital divide, inequitable access to technology, and greater surveillance risks. Particularly, low income people as well as people of color will typically have limited resources for their digital security or legal defense, which often leads to disproportionate targeting in breaches or an over reliance on public systems where the digital evidence is then weaponized against them. Moreover, in the context of criminal justice, prosecutors and law enforcement alike usually leverage advanced forensics on smartphones and social media data, thus creating an imbalance which is going to disadvantage defendants who are reliant on under resourced public defenders (Ramirez, 2022). Consequently, Digital Forensics Analysts in public defender labs counter this by using tools to set up data driven defenses, to challenge biased narratives and portrayals of marginalized defendants as threats, and to emphasize their contextual life circumstances (Ramirez, 2022). Furthermore, the profession especially addresses the aforementioned challenges through diversification initiatives, such as recruiting from communities which are underrepresented, and advocate for fairer policies that ensure an

equitable access to forensic expertise, therefore reducing the systemic biases that are intertwined with digital investigations.

Career Connection to Society

Digital Forensics Analysts have done much for societal safety by safeguarding the most important infrastructures like healthcare records, financial systems, and government networks from all kinds of breaches that could disrupt public services. Additionally, their investigations have informed public policies on data privacy, evidence handling, and the prosecution of cybercrime, thus balancing the needs of security with civil liberties. For example, findings from forensic analyses affect legislation that is about the overreach of surveillance, therefore ensuring that there are protections for those populations which are vulnerable. Moreover, by applying social science principles analysts have promoted a more just digital ecosystem, since where there are evidence based insights being made the public trust is fostered, and there are more equitable outcomes instead of enhancing division (Steel, 2014; Sunde & Dror, 2019; Ramirez, 2022). Hence, this career bridges the technical expertise of its field with societal responsibility, therefore inculcating the rule of law in our world which becomes ever the more digital.

Scholarly Journal Articles

Source 1: Steel, C. M. (2014). Idiographic digital profiling: Behavioral analysis based on digital forensics. *Journal of Digital Forensics, Security and Law*. This article begins by introducing IDP as a framework for applying behavioral (social science part) analysis to individual digital footprints. The key findings in this article emphasize its utility in the ongoing investigations for profiling motivations and generating leads, which is directly relevant to how

Digital Forensic Analysts use psychological insights in their daily evidence reconstruction and development of strategy.

Source 2: Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29, 101-108. This journal article analyzes seven sources of cognitive error, like biases in decision making, within the forensics process and then proposes countermeasures. Furthermore, it supports my paper's analysis of social science principles by emphasizing the role of psychology in mitigating human error, so that it is ensured that ethical and reliable practices are followed when interacting with the diverse amount of user data from marginalized communities.

Source 3: Ramirez, F. (2022). The digital divide in the US criminal justice system. *New Media & Society*, 24(2), 514-529. Based on ethnographic research in a public defender digital forensics lab, this article has shown how unequal access to forensic tools have disadvantaged poor and minority defendants. Furthermore, it adds to our understanding of career and society connections by showing how analysts apply important concepts like equity and behavioral context to advocate for fairer justice and address marginalization that occurs through counter narratives and data driven advocacy.

In conclusion, Digital Forensics Analysts epitomize the integration of social science into cybersecurity, by using behavioral and cognitive principles to improve investigations while also confronting the societal inequities that exist. This interdisciplinary approach the profession has not only strengthens daily practices but also progresses for a more inclusive and overall stable digital society.

References

- Ramirez, F. (2022). The digital divide in the U.S. criminal justice system. *New Media & Society*, 24(2), 514–529. <https://doi.org/10.1177/14614448211063190>
- Steel, C. M. (2014). Idiographic digital profiling: Behavioral analysis based on digital forensics. *Journal of Digital Forensics, Security and Law*, 9(1), 1.
<https://commons.erau.edu/jdfsl/vol9/iss1/1>
- Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation*, 29, 101–108.
<https://doi.org/10.1016/j.diin.2019.03.003>