Bryan Gregg

The Career of a Digital Forensics Analyst: Where Technology Meets Social Justice

Bryan Gregg

The Career of a Digital Forensics Analyst: Where Technology Meets Social Justice

Introduction

Digital Forensics is the science of identifying, preserving, analyzing, and applying digital evidence to legal matters. It plays a vital role in cybersecurity, criminal investigations, corporate policy development, and court proceedings. The skills of Digital Forensics Analysts (DFAs) are essential in these times of data breaches, phishing, identity theft, AI attacks, and other cybercrimes. These professionals provide support to criminal investigators by recovering, analyzing, and preserving data from computers, mobile devices, and digital systems. They use ideas from social science to better understand why people commit cybercrimes, how people think and behave online, and how social issues might determine who becomes a victim or a suspect. The combination of technical skills, knowledge of human behavior, and social systems allows DFAs to do their jobs effectively and equitably (Casey, 2011).

Social Science Foundations in Digital Forensics

Social science principles help DFAs not only follow the data but also understand the human side of digital crime. Experts use ideas from criminology, psychology, and sociology to help them investigate digital crimes. Criminology examines why people commit crimes online and how they choose their targets. It explains how some criminals may look for easy opportunities, like someone who doesn't use strong passwords while others may consider the risks and rewards before deciding to break the law. These ideas are extremely helpful when trying to rebuild a digital crime scene (Rogers & Seigfried-Spellar, 2014).

Psychology helps analysts understand how people think and behave online. Crimes like identity theft and online scams often involve specific patterns that people use to communicate or search for information. DFAs work with psychologists to study a person's emails, messages, or browsing history. These clues may reveal what the person was planning or thinking and can help determine whether a crime was intentional or accidental (Casey, 2011).

Sociology helps DFAs understand how poverty, discrimination, or unequal access to technology might determine who becomes a victim or a suspect. It explains the "digital divide", which means may not have tools to protect themselves online and are more vulnerable to scams. This can also make it harder for some people to report crimes (Johnson, 2022).

Impact on Marginalized Communities

Digital forensics can be a powerful way to help solve crimes and bring justice, but it also raises concerns about fairness and privacy. People of color, immigrants, and those with lower incomes often do not know how to protect their online information and do not have access to secure devices. These communities are more vulnerable to being tracked or targeted and tend to be watched more closely online. They are also more likely to show up in digital investigations due to biased computer programs used in policing (Johnson, 2022).

Lack of diversity among digital forensics workers may present a barrier to recognizing inequalities. Analysts with similar backgrounds may be unaware of cultural details in the data or may not notice unfair patterns. DFA teams should include people from different cultures, languages, and life experiences so they can fully understand the communities they are

investigating. This can help promote fairness in investigations, equity for underserved communities, and equality in response to cybercrime.

Societal Relevance and Responsibilities

Digital Forensics Analysts (DFAs) play an important role in ensuring justice in the digital world. Their work helps solve crimes such as cyberstalking, child exploitation, corporate fraud, intellectual property disputes, employee misconduct investigations, data breach responses, and terrorism. They collect and analyze digital evidence and make certain that lawmakers use the information accurately and fairly. Their findings influence court decisions and influence policy reforms that involve public privacy, cybersecurity, and how digital data is managed (Post University, 2023).

Another important role of DFAs is prevention. These experts help organizations find weak spots in their digital systems, improve their security, and reduce the risk of future incidents. Businesses, schools, hospitals, and government agencies can operate securely and confidently. DFAs not only respond to crime; they help prevent crime (Casey, 2011).

Conclusion

The career of a Digital Forensics Analyst is a blend of sharp technical skills and a keen sense of social awareness. They are key figures in our justice system. DFAs ensure that digital evidence is used responsibly and that people are treated with dignity. Their work helps protect communities, support legal systems, and build trust in how digital information is handled (Rogers & Seigfried-Spellar, 2014). Cybercrimes are becoming more complex, and cybercriminals are

becoming smarter. DFAs are important to our protection, standing at the intersection of technology and social justice.

.

References

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

Johnson, R. (2022). Next generation of evidence collecting: The need for digital forensics training in criminal justice. *ERIC*. https://files.eric.ed.gov/fulltext/EJ1341743.pdf

Post University. (2023). *Digital forensic careers in CSI*. https://post.edu/blog/impact-of-digital-forensics-in-modern-crime-scene-investigations/

Rogers, M. K., & Seigfried-Spellar, K. C. (2014). Digital forensics: Understanding the value of digital evidence in criminal investigations. *Journal of Digital Forensics, Security and Law*, *9*(2), 7–16. https://commons.erau.edu/jdfsl/vol9/iss2/2/