Gunnar Asper

CYSE 201

4/11/2025

Career Paper

Digital Forensics and Social Sciences

Introduction

The career of digital forensics is one that relies heavily on social science and psychology. Since digital forensics lies at the intersection of law enforcement, human behavior, and the internet, this is a very important job, which will remain in need as the world's use of the internet only grows. With such a critical role in online investigations, a digital forensics expert must have a deep understanding of social science principles and human behavior in order to get their job done properly.

Body

Social Science Principles & Application of Key Concepts

Digital forensics is one of the most important cybersecurity careers as cyber crime continues to rise every year. “As cybercrime rates escalate globally, the costs of being victimized by a malicious cyber-event are becoming increasingly impactive on individuals and organizations.” (Parti, et al. 2022). Victim precipitation, for example, is a huge part of digital forensics, as an investigator must go to the “scene” of the crime and determine what happened, how, and why to kick off their investigation in gathering evidence. Ethical neutrality is another very big part of investigating cybercrime, as the digital chain of custody should remain as objective as possible to preserve the risk triangle and offer confidentiality, integrity, and availability to the evidence during the gathering phase of the forensic chain of custody.This is a career that is deeply reliant on social science and deals directly with cyber-victimization, and many other principles as well. “ According to Palmer (2001), digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal.” (Mohammed, et al. 2019). With that being said, before that point, professionals in this field must have a deep understanding of cyber offending behaviors and the causes of them in order to help investigate and identify offenders and evidence. In order to get in the mind of an offender, a cybercrime investigator may look into cognitive theories to understand their train of thought, or personality theories as an attempt to categorize them in order to track them easier through their behavior. Criminology in general is the basis for digital forensics and cybercrime investigation.

Marginalization

Digital forensics, more so than other cybersecurity careers, deals heavily with marginalized groups and crimes against them. As mentioned previously, cybercrime is only rising, and with that, marginalized groups are disproportionately targeted and victimized through the internet. For one, elderly people as a marginalized group are a very prominent target for cyber attacks, due to their lack of knowledge about the internet and cyber attacks. “This article demonstrates to what extent low self-control and lifestyle-routine activities factors (i.e., exposure to motivated offenders, target suit ability, and capable guardianship), are associated with the likelihood of fraud victimization among internet users of the age 55 and above.” (Park, 2022). Additionally, race, gender, or sexuality may be a determining factor in how data is obtained and processed, which disproportionately affects marginalized groups who are the victims of a cybercrime. One of the bigger challenges faced by these groups is their lack of access to justice in the justice system. More so due to institutional racism, certain groups can face problems in their attempts at having a cybercrime investigated, as some investigators can be more prone to not believing them or taking them seriously. With white men dominating the field of digital forensics, this can have negative effects for marginalized communities with not only investigations, but representation in the field itself. This lack of representation can lead to instances of cultural incompetence in terms of investigating marginalized communities, which can be detrimental to the investigation itself.

Digital Forensics Connection to Society

Digital forensics and cybercrime investigations are interwoven with society in the same manner that police and law enforcement are. Digital forensics as a career is meant to protect, respond to, and solve cybercrimes in order to protect society as a whole. Since the world is moving more and more towards the digital realm, it is more crucial than ever to have a cybercrime force that can protect the people and handle the traffic. These professionals have to adapt to the new leaps in technology, constantly working in order to protect citizens from cyber criminals. This work that they do not only benefits people, but influences the public trust and perception of all law enforcement agencies as a whole. The interaction between cybercrime investigators and the public is complex, and has to be examined on a case by case basis, but as a whole, these professionals work diligently to support and protect the public from cyber threats and attacks.

Conclusion

Digital forensics/Cybercrime investigation is a very complex and multifaceted career. From understanding laws, chain of custody, and proper protocols, to understanding human factors, social science, and criminology, there is so much that goes into being a digital forensics. All in all, these professionals work diligently through these challenges to wade through the internet in order to keep us safe, and one day it is my hope to earn that title and do the same for others.

References

Park, I. (2022). Understanding Deviance and Victimization in Cyber Space among Diverse Populations. International Journal of Cybersecurity Intelligence & Cybercrime: 5(3), 1-3. Available at: https://doi.org/10.52306/ZWMY9562 Copyright © 2022 Insun Park

(2022). Book Review: Digital Forensics and Cyber Investigation. International Journal of Cybersecurity Intelligence & Cybercrime: 5(3), 68-70. Available at: https://doi.org/10.52306/PYBP7047 Copyright © 2022

Mohammed, Kabiru H.; Mohammed, Yusuf D.; and Solanke, Abiodun A. (2019) Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria, International Journal of Cybersecurity Intelligence & Cybercrime: 2(1), 56-63. https://www.doi.org/10.52306/02010519ZJRK2912