Kerina Drummond
April 17, 2025
CYSE 201s
Professor Yalpi

Career Paper: Digital Forensics Examiner

Introduction

Cybersecurity is an interdisciplinary field, where it draws from different branches of knowledge to address the many challenges that arise within cyberspace. At some corners, to solve issues, cybersecurity must work with other disciplines such as law, economics, policy analysis, etc. Cybersecurity roles all have a social science aspect that needs to be considered. One of the jobs that a cyber professional can obtain is becoming a Digital Forensics Examiner. Digital Forensic Examiners play a role in investigations that most people on the outside do not understand and there are key social science principles that are evident in this career and that this career relies on to operate effectively and efficiently.

Overview of the Career

Digital forensics examiners work with cybercrimes and breaches. According to CISA.Gov a Digital Forensics Examiner "analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation (*Cyber Defense Forensics Analyst | CISA*, n.d.)." Their tasks on a day-to-day basis can include collecting and analyzing log files, and evidence. The work done by digital forensics examiners helps investigations discover the "What." Answering the question of "What happened

with these crimes and breaches?" The reasoning is vital to understanding other factors such as who, where, and why. The evidence acquired is often used in courts and expert testimony.

Social Science Principles in Action

The social sciences refers to a group of scientific disciplines that study social phenomena. In latent terms, social science is the science of people and their behavior. This study is important to digital forensic examiners because to solve cases and find which evidence is critical they must understand the people involved. All parties victims and suspects included must be vetted to be able to track the crime and find the most likely perpetrator. Some social science principles that Digital Forensic examiners use consistently include behavioral analysis, the Principle of ethical neutrality, Research on Social Science Cybercrime Studies Shows, and Psychological factors that increase the risk of victimization.

Behavioral Analysis

Under Social Science behavioral analysis is the study of behavior. Studying the way environmental elements affect behavior and why people behave the way they do (Cherry, 2024).

Digital Forensic Examiners often use this analysis to understand what a criminal or victim did before and after a crime is committed. Based on evidence understanding behaviors, movements, and eventually profiling a suspect and victim. This also helps to understand the difference between accidental data loss and malicious threats. This study allows examiners to "follow the breadcrumbs" back to the person.

An example is confidential files being linked to the press and the digital forensic examiner noticing a user kept logging into those same confidential files at night.

Principle of Ethical Neutrality

Ethical neutrality is one of the principles discussed in Module 2. Ethical neutrality is the fact that scientists adhere to ethical standards when conducting research and examinations. When dealing with cybercrime there is a lot of room for ethics and morals to collide with cases.

Digital Forensic Examiners use ethical neutrality to keep case findings objective and unbiased. They are unable to do their job properly if their moral or ethical beliefs cloud their judgment. Bias in verdicts can be tragic and affect the outcome of the case accidentally implicating an innocent person. Ethical neutrality is essential to keeping a just system dedicated to bringing criminals to justice and protecting the victims it can only be done with factual unbiased data others can use.

An example is a rape occurs and a preciously convicted rapist is arrested for it. The digital forensic examiner brought in was previously raped and would love nothing more than to send the rapist to prison again but instead, they follow standard procedure and keeps their personal feelings out of the equation to ensure that the true perpetrator is brought to justice. She found that he was nowhere near the location of the crime and had to watch him walk free. Although it was against their own beliefs, the digital forensics examiner followed procedure, kept an objective view, and got justice.

Research on Social Science Cybercrime Studies Shows

The research on social science cybercrime is described as “the premier organization that links the fields of social and technical science together with practitioners and law enforcement to research and understand cybercrime and cybersecurity and promote a safer internet.” These studies examine how economics, status, online behavior, and culture affect the victim and

criminal. Digital Forensic Examiners use this research to understand the bigger picture of cybercrime. This bigger picture can help in improving preventative measures, finding patterns, profiling suspects, and preparing for future threats. This aids them in looking at cybercrime outside of only technical analysis.

Psychological Factors Increase the Risk of Victimization.

Comprehending the psychological aspects that heighten the risk of victimization helps digital forensic examiners understand how and why people fall prey to cybercrime. Human Factors such as impulsiveness, minimal digital and cybersecurity practices, and easy manipulation make people susceptible to fraud, phishing, and social engineering attacks. Understanding these factors allows professionals to approach digital evidence from a psychological lens and reconstruct the events, find the perpetrator's m.o., and build a strong case.

Marginalized Groups

Digital forensics examiners have a crucial role in the justice system and their work often impacts marginalized groups, in good and bad ways. The people of these groups often face systematic biases and negative stereotypes that can impact the digital evidence and its collection and understanding of the evidence. Also, digital forensic examiners can find the patterns of what groups may be targeted over others. Most reports show that poorer groups are targeted first. Those with less security and cyber awareness. Digital forensic examiners being aware of the biases and disabilities can help better protect these groups and decipher more ways to help. This knowledge proves why ethical neutrality is extremely important to get justice for any and everyone.

Conclusion

In conclusion, Digital Forensic Examiners are not only technical experts, they are investigators who must study and understand human behavior and practice concepts of social sciences in an effort to present unbiased, valid evidence to be used in an investigation to find a suspect and eventually the perpetrator. Social science concepts are evident in every job field, but as a digital forensic examiner using these principles is extremely important in everyday life and every case in the interest of justice.

References

Cherry, K. (2024, February 4). *Behavior Analysis in Psychology*. Verywell Mind; Verywellmind. https://www.verywellmind.com/what-is-behavior-analysis-2794865

Cyber Defense Forensics Analyst | CISA. (n.d.). Www.cisa.gov. https://www.cisa.gov/careers/work-rolescyber-defense-forensics-analyst

Digital Forensic Examiner: Career Guide 2024. (2024, July 25). Salvation DATA. https://www.salvationdata.com/knowledge/digital-forensic-examiner/