Dez Johnson

Professor Duvall

Cybersecurity as a Social Science

Apr 12, 2023

Importance of Social Science in Digital Forensics

Digital forensics is a field and career that I find very interesting. It is also one of the most important and quickly rising areas of cybersecurity. In order for digital forensics analysts to look into and stop cybercrime, They have to collect, analyze, and conserve digital evidence. To do so, professionals in this field need to have a good understanding of social science concepts and studies as well as computer science and technology.

One key concept that is used by professionals in the field of digital forensics is the importance of human behavior in cybersecurity. Cybercrime is heavily influenced by human behavior, by things like insider threats and social engineering attempts. To look at and understand digital data and its relation to human behavior, professionals in digital forensics need a strong background in psychology and sociology. Human behavior plays into digital forensics by investigating cyberstalkers and their harassment methods. Cyberstalking is a kind of online harassment that involves someone following, threatening, or harassing a person using digital communication tools. They can do this by hacking into a victim's accounts, creating fake social media profiles, or sending threatening or intimidating messages to a person or people. Professionals who work in digital forensics are very important for the investigation of cyberstalking and harassment cases because they use human behavior research to understand the goals and actions of cyberstalkers. An example of could be viewed in a cyberstalking case, people in this

field would look at the suspects social media profiles, emails, and online search history to see if they have any patterns of said behavior. By doing that, they could possibly find leads into the person. To execute all of that, digital forensics professionals would need an understanding of psychology and sociology.

Ethics and values also play into digital forensics. As stated before, digital forensics professionals have to collect, analyze, and conserve digital evidence. To make sure their job is done in an ethical and responsible way, professionals in digital forensics need to know ethical principles and values. Confidentiality is an important ethical principle in digital forensics. Professionals in digital forensics may have access to important information, so they must take steps to make sure that it stays protected and that it is not shared to unauthorized people. They can do that by using encryption, secure storage techniques, and access controls. Digital forensics also needs to take values into account, especially when it comes to issues related to human rights and privacy. Professionals in digital forensics must take into account the impact on privacy of their work and take steps to lower any possible damage or intrusion into people's personal lives. They must also be aware of the risk of human rights violations, such as the unfair targeting of marginalized groups or people with digital evidence.

Digital forensics Professionals can also help marginalized groups by investigating hate crimes. Hate crimes are Crimes motivated by discrimination or prejudice against a certain group of people. Digital forensics professions are important because they are the ones that investigate online hate crimes, such as the spread of hate speech and the use of digital communication tools to scare or threaten people because of their race, gender, or sexual orientation.

In conclusion, digital forensics is a fast growing and important part of cybersecurity. Knowing concepts like psychology and sociology, on top of computer science and technology skills is important. Also Human Behavior and ethical principles and values are also elements of social science that digital forensics professionals need to do their work. Overall, digital forensics professional's work is important for keeping a safe and just society.

Sources

1. Lee, Roderick. "The Role of Social Science in Cybersecurity." International Journal of Cybersecurity Intelligence & Cybercrime, vol. 1, no. 2, 2018, pp. 67-76.
2. Turnbull, Benjamin. Investigating Cybercrime: A Guide for the Digital Forensic Investigator. Elsevier, 2020.
3. Jones, Richard and David Wall. "Digital Forensics in the Age of Big Data: A Social Science Perspective." International Journal of Cyber Criminology, vol. 13, no. 1, 2019, pp. 87-102.
4. Abomhara, Mohamed and Abdulrahman Alghamdi. "Ethics in Digital Forensics: A Conceptual Framework." Journal of Digital Forensics, Security and Law, vol. 8, no. 4, 2013, pp. 23-44.
5. Zwitter, Andrej and Ruth Bavister. "The Ethics of Digital Forensics." Science and Engineering Ethics, vol. 19, no. 3, 2013, pp. 1029-1043