

Madison Baughman

Professor Yalpi

CYSE 201s

8 April 2024

Social Science and Digital Forensic Analysts

Job Description

A digital forensic analyst is responsible for much of the behind-the-scenes work of cybersecurity. In the aftermath of a cybersecurity attack, digital forensic analysts are responsible for using available evidence to determine perpetrators, their methods of attack, and potentially recover data. However, possibly the most crucial part of a digital forensic analyst's job is what they do with their findings. Specifically, putting together a detailed summary of their findings which can be shared and used for prevention of similar attacks (CISA).

Social Science Principles

Several social science principles are used by digital forensic analysts in their day-to-day tasks. First, ethical neutrality is extremely important. A forensic analyst's job is to derive conclusions from evidence about cybersecurity threats and attacks. Moral implications simply don't apply to this career because action is not being taken. Forensics is meant to be used for the derivation of a conclusion, not necessarily in implementing action following the conclusion (McFarland, Lewis, & Goldberg, 2015). Empiricism is also relevant because of the emphasis on observations and evidence to derive knowledge from which is the foundation of digital forensic analysts. These principles are integral to the operation of digital forensic analysts and guide their decision making.

Marginalized Groups

People who fall victim to cyberattacks and suffer financially often end up marginalized because of the lack of help available to them. Digital forensic analysts play a big role in the prevention of marginalization of these people because of the important information they derive. The information discovered by forensic analysts is consistently used in learning new techniques to protect data systems and prevent these attacks from happening. System vulnerability, easy ability to gain access, and lack of identity verification are all challenges these people face and each are able to be addressed by the work of digital forensic analysts.

Societal Connections

Society as a whole has a direct dependency on digital forensic analysts because of their ability to assess a threat and compile a report on its different attributes. This information is vital because it allows the prevention of future threats of this type. Without forensic analysts, there would be a gap in this process. Digital forensic analysts are also relevant to other organizations beyond policing, suggesting that broader terms should be used to describe them (Wilson-Kovacs & Wyatt, 2023).

Conclusion

Digital forensic analysts are a crucial part of cybersecurity in their assistance to other careers who seek to take more active action against cyber threats. The assessment of data can help lead to the protection and prevention of future attacks from happening. By doing this they act as a lifeline to marginalized groups by helping to prevent further damage to their data. Their direct connection to society by investigating cyber attacks and assisting in the prevention of more harm cannot be understated. Digital forensic analysts are a crucial part of the cybersecurity field.

References

Cyber Defense Forensics Analyst: CISA. Cybersecurity and Infrastructure Security Agency

CISA. (n.d.). <https://www.cisa.gov/careers/work-roles/cyber-defense-forensics-analyst>

McFarland, D. A., Lewis, K., & Goldberg, A. (2015, September 17). *Sociology in the era of big data: The ascent of forensic social science*. SpringerLink.

<https://link.springer.com/article/10.1007/s12108-015-9291-8>

Wilson-Kovacs, D., & Wyatt, D. (2023, September 28). *The long journey of resistance toward acceptance: Understanding digital forensic accreditation in England and Wales from a social science perspective*. WIREs.

<https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wfs2.1501>