Hans Peterson

CYSE 201S

4/14/2024

Career Paper: Social Science and Digital Forensic Analysts

Digital forensics analysts must use social science principles, such as relativism, empiricism, and objectivity, for their job. Relativism is an integral aspect; Nance et al. (2009) state, “Unlike many research areas, digital forensics is a largely practitioner-driven field. Advances in the field tend to be primarily developed and applied in reaction to a specific incident or class of incidents.” Essentially, analysts’ tools (programs and technologies) develop whenever there are innovations in hacking. Analysts combat and document these incidents by using the new tools, which hackers must learn to overcome, leading to a cycle. Empiricism is another fundamental aspect. According to Dixon (2005), computer forensics goals are to document and interpret computer data; digital forensic analysts interpret computer data to provide credible, tangible evidence that could either prove a defendant’s guilt or innocence. Without empiricism, digital forensic analysts cannot exist. Objectivity is also important. For digital forensic analysts in criminal investigations, they must interpret computer data to establish a chain of events that reveal who was responsible for an incident. Regardless of the analyst’s values and feelings, they must preserve the integrity of the data to present the truth.

Digital forensic analysts may handle cybercrime. Lim (2006) states, “Computer forensics is an ‘investigation of situations where there is computer-based (digital) or electronic evidence of a crime or suspicious behavior, but the crime or behavior may be of any type.’” Analysts may need to determine the extent and cause of cybercrimes/incidents as part of their routine. Analysts

also obey regulatory definitions. For example, analysts are required to extensively and accurately document their findings for evidence in court, and they must maintain a chain of custody for computer evidence. Breaking these procedures can result in penalties and the inadmissibility of evidence. Despite technical prowess, analysts must also possess strong social behaviors like communication skills, writing skills, and a continuance of learning. Analysts thoroughly document their findings (incidents) and can provide expert testimony. They also must learn about new tools and techniques in digital forensics to keep up with technology's growth.

A monolingual person faces many disadvantages as a digital forensics analyst. For example, English-speakers may struggle to analyze data written in different languages; when communicating with other people speaking in foreign languages, there can be translation errors. In the case of computer languages, someone who only knows Java may not be able to read code written in Python. In the workplace, this could lead to discrimination and other forms of harassment stemming from pride. Impoverished people are also at a disadvantage. Certifications, such as CISSP, CFCE, and CIFI, are crucial to have as an analyst. According to Dixon (2005), "CIFI epitomizes the highest standards in knowledge requirements and expertise." CISSP and CFCE exams can cost up to nearly a thousand dollars. If an impoverished parent cannot afford necessities, they cannot afford these certifications either, barring them from analyst work. Continuing on certifications, marginalized groups, such as people with mental illnesses or disabilities, may suffer greatly from the load of certifications and work. Due to the competitiveness/rigorousness of being an analyst, they may not fit into the workplace culture.

Society and digital forensics analysts impact each other in many ways. In the criminal justice field, an uptick in cybercrimes and cybercriminals can result in a demand for more digital forensics analysts. These analysts uncover, document, and determine the causes of the

cybercrimes, resulting in lower rates of cybercrime. Meanwhile, when analysts deliver expert testimony, they can receive news coverage, boosting their popularity in society. With their presence known, it shapes people's perceptions of cybercriminals and cybersecurity in general. For people interested in IT, it may act as a catalyst for a cybersecurity career, seeing how successful and fulfilling being an analyst can be. For others, they may see how lucrative cyber crimes are and become black-hat hackers instead. Because of the increasing number of people aspiring to be analysts, institutions and universities may invest in developing cybersecurity courses. Either way, the increase in aspiring analysts and black-hat hackers results in a demand for digital forensics analyst jobs. Analysts continue their work, and this ultimately creates a strong economy and strong cybersecurity.

Works Cited:

Dixon, P. D. (2005). An overview of computer forensics. *IEEE Potentials*, *24*(5), 7–10. https://doi.org/10.1109/mp.2005.1594001

Lim, N. (2006). Crime Investigation: A Course in Computer Forensics. *Communications of the Association for Information Systems*, *18*. https://doi.org/10.17705/1cais.01810

Nance, K., Hay, B., Bishop, M. Digital Forensics: Defining a Research Agenda. (2009). *2009 42nd Hawaii International Conference on System Sciences*. https://doi.org/10.1109/hicss.2009.160