Career Paper: Computer Forensic Analyst

Ethan Powers

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 24, 2024

What Does a Computer Forensic Analyst Do?

A computer forensic analyst studies computers and their data to find evidence of cybercrimes (*Cyber Defense Forensics Analyst,* n.d.). They can help law enforcement departments in investigations. It is also important for the courts for the presentation of evidence. This is one of the most important jobs in the cybersecurity field because they help catch cybercriminals and hold them accountable. That may prevent them from committing another cybercrime in the future. (Wilson-Kovacs, 2020) finds that many officers don't know a lot about how to handle digital investigations, so it's important for police departments to provide training to them. That piece of information from the study was found in police departments in Europe, specifically in Wales and England through interviews.

How it Relates to the Social Sciences: Criminology

A computer forensic analyst must incorporate ideas from the social sciences into their job. Social sciences focus a lot on crime, so it's important for employees in that field to know about criminology. There are many crimes that are committed online every day, so it's important for cybersecurity professionals to be up to date on the laws for every crime that can be committed online. (Horseman, 2022) discusses how digital investigators use data traces. The study also goes through how investigators should not form opinions about the data until they go through the specific steps of investigating them.

How it Relates to the Social Sciences: Psychology

Psychology can also be related to digital forensics. It may be helpful for a forensic analyst to work alongside a psychologist to try and determine what the suspect is or was thinking while committing the crime. It may be a helpful way of determining where to look for

information or evidence related to the crime. Marshall Rich and Mary Aiken find in their study that by combining these two disciplines, it will help to find threats (Rich & Aiken, 2024).

How it Relates to the Social Sciences: Economics

Computer forensics can go hand in hand with economics, even though it may not seem like it. Part of what a forensic analyst does is search for evidence in money crimes committed online. Money laundering is one crime that occurs online. It's important to get people who commit those crimes stopped because they usually hurt the most vulnerable on the internet. It can hurt people in devastating ways when they don't have the money they need because it was stolen. It can even hurt large corporations if they fall victim to a money laundering crime. Computer forensic analysts will do their best to find sufficient evidence for law enforcement to prosecute which allows justice to be served.

How it Relates to the Social Sciences: Sociology

Lastly, digital forensics can be related to sociology. It may be helpful for forensic analysts to understand how people in society act in an online environment. They can possibly learn how people use the internet and specific things they do online. Does society as a whole participate in the same things? Are some marginalized groups targeted more than others? Some may be concerned that some marginalized groups may be watched more due to different factors in that specific group. For example, people who don't make a lot of money may be targeted more than wealthy individuals in a money laundering investigation. That is just one of the theories that will need to be studied.

Conclusion

Computer or digital forensic analyst is an important part of cybersecurity and social science. It uses ideas from both areas to investigate crimes committed on digital devices. By doing that, it helps victims and cybersecurity as a whole. With so many crimes occurring on the internet today, digital forensics will always be needed.

References

Cyber Defense Forensics Analyst. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/careers/work-rolescyber-defense-forensics-analyst

Horsman, G. (2022). Forming an Investigative Opinion in Digital Forensics. *WIREs. Forensic Science*, *4*(6), e1460-n/a. https://doi.org/10.1002/wfs2.1460

Rich, M. S., & Aiken, M. P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences (Basel, Switzerland)*, *4*(1), 110–151. https://doi.org/10.3390/forensicsci4010008

Wilson-Kovacs, D. (2020). Effective Resource Management in Digital Forensics: An Exploratory Analysis of Triage Practices in Four English Constabularies. *Policing : An International Journal of Police Strategies & Management*, *43*(1), 77–90. https://doi.org/10.1108/PIJPSM-07-2019-0126