Digital Forensics Investigator

How do professionals in this career require and depend on Social Science Research & Principles

Cybersecurity Department, ODU

Cybersecurity and Social Science (CYSE 201S)

Carla Belfiore

August 1, 2024

Digital Forensics Investigator

The realm of cybersecurity is a rather vast environment in today's world, providing numerous life-changing opportunities for all those individuals that choose to pursue the route of cybersecurity. "The cybersecurity field is constantly adapting to keep up with current threats and new technology. Fortunately, this means that there are a variety of roles to pursue, no matter the experience level" (Courtney, 2023). As a matter of fact, the number of cybersecurity careers to choose from is infinite: information security analyst, cybersecurity engineer, malware analyst, penetration tester, security officer, chief information security officer, digital forensics investigator, etc. One cyber career I find particularly captivating is that of a digital forensic investigator. A career as a digital forensics investigator is strictly connected to the realm of forensic science. Focusing on the recovery and investigation of all IT devices linked to cybercrime. "Forensics investigators identify and record details of a criminal incident as evidence to be used for law enforcement" (Computer Forensics, 2024). Moreover, for a company, the role of a digital forensic investigator is pivotal. Among the many responsibilities, a digital investigator has the role of collecting evidence from different places, such as servers and network systems, to make sure that no illegal actions are being performed. A digital forensic also carries the weight of working with security teams to help come up with solutions in order to mitigate and diminish attacks, as well as analyzing data using specialized software and techniques, bringing back deleted information crucial for their investigation process. Another determining aspect of a digital forensic investigator is staying up-to-date with IT (information technology). Changes in technology are advancing rapidly; thus, understanding how to use new technologies is essential to succeeding in their field. Also, according to the 'What is a Digital Forensic Investigator' article, being able to work in a team, hand in hand with other experts like computer security specialists, for example, allows a better chance of success. Moving onto a less technical aspect, writing skills, critical thinking skills, and communicative skills are key. They allow proper problem resolution, clear explanation of problems to clients, and strong writing skills to report issues. Since their job requires many responsibilities and skills, "digital

Digital Forensics Investigator

Forensic investigators can work in a wide range of industries, including law enforcement agencies, government agencies, private sector enterprises, and consulting firms" (WGU, 2024). Additionally, professionals in this sector require and highly depend on social science research and principles. As a matter of fact, understanding social science is key. Like module 2 of CYSE 201S (Umphlet, n.d.) shows us, the principle of relativism, for example, suggests that all things are related; thus, when investigators analyze evidence, they must keep in mind the social context and recognize how that impacts behavioral dynamics. Skepticism is a very important principle. Questioning the data and sources helps avoid rushed conclusions and more accurate solutions. Objectivity, in my opinion, is one of the most important principles, as is ethical neutrality. These two principles suggest a non-biased approach to the investigation, ignoring all personal beliefs. By doing so, their findings aren't influenced by external factors but focus merely on the research. Professionals in this career depend on social science research. Understanding human behavior can be of great help to investigators. Analyzing the factors that lead criminals to commit cybercrime can be extremely beneficial. It can help predict their actions and come up with targeted intervention tactics. Also, making hypotheses goes along with understanding human behavior since it allows investigators to draw premature conclusions and prevent cybercrime. Lastly, like suggested in Module 3 of CYSE 201S (Umphlet, n.d.), conducting routine surveys that provide contextualized information, doing quasi-experiments to study interactions between technology and individuals, studying archives, and using multi-method research will allow easier access to information. This profession also relates to various marginalized groups because investigators in this sector have the role of protecting the rights of marginalized groups by collecting evidence and holding cybercriminals responsible. Racial and gender differences can notably impact cybercrime. BIPOC people have a 12% greater chance of experiencing some sort of financial damage as a result of a cybercrime incident" (Ikeda, 2021). While the technical part of digital forensics is of prime importance, the intersection of social science research and principles can significantly enhance the effectiveness of a digital forensic investigator's role.

References:

Courtney, E. (2023). *Cybersecurity Career Path: Jobs, Skills, and Outlook*

Cybersecurity Career Path: Jobs, Skills, and Outlook - Forage (theforage.com)

Computer Forensics (2024). *What is Digital Forensics?*

What is Digital Forensics | Phases of Digital Forensics | EC-Council (eccouncil.org)

Bingham, P. Western Governors University, WGU. (2024) How to Become a Digital Forensic Investigator

How to Become a Digital Forensic Investigator (wgu.edu)

Umphlet, M. (n.d.) Module 2 Slides CYSE 201S.

https://docs.google.com/presentation/d/1Jo7kMpaWztasW0enT8Nqlq6IIFfo6ntzD7plF6Xvyg/edit#slide=id.p21

Umphlet, M. (n.d) Module 3 Slides CYSE 201S

https://docs.google.com/presentation/d/1JYpmyaUeN8PHJgwcIWAjvmPH1_L8EcaceRCcrOaf8o/edit#slide=id.p10

Ikeda, S. (2021) *Disadvantaged Groups More Likely to Experience Cybercrime, Experience Disproportionately Damaging Results.*

Disadvantaged Groups More Likely to Experience Cybercrime, Experience Disproportionately Damaging Results - CPO Magazine