Bakarri Grant

Professor Umphlet

CYSE 201S

Aug 7, 2025

Computer Forensics Analysts: Integrating Social Science into Daily Practice

Introduction

Computer forensics analysts play a crucial role in investigating cybercrimes by collecting, analyzing, and preserving digital evidence. While technical skills are necessary, the application of social science research and principles greatly influences how effective they are. Their everyday activities are directly influenced by ideas from criminology, psychology, sociology, and communications, which help them to better understand criminal behavior and interact effectively with diverse user populations, including marginalized groups.

Applying Psychological Insights

Firstly, computer forensics analysts rely heavily on psychological principles to understand offender behaviors and motivations. More accurate profiling and interpretation of digital evidence is made possible by the application of cognitive behavioral theory, which assists analysts in recognizing criminal justifications and rationalizations present in digital communications. According to Hadlington (2017), people's vulnerability to cybercrime is closely correlated with psychological characteristics like impulsivity, trust issues, and risk perception. During digital investigations, analysts can use these psychological insights to gain a deeper understanding of the methods, motivations, and actions of offenders. By bridging psychology and technology, CBT helps computer forensics professionals interpret not just what happened, but why it happened, which is an essential part of understanding and combating cybercrime.

How Does Sociology Come into Play?

The efficacy of computer forensics analysts is also strongly influenced by sociology research. To properly interpret digital interactions, analysts need to understand social dynamics in both offline and online settings. This is where the social norms theory comes into play, which suggests that our actions are influenced by our perceptions of how others in our social groups think and act. Analysts use this theory to determine how peer pressure in hacker forums or online communities encourages deviant behavior. Insights from sociology enable analysts to contextualize digital evidence, recognizing the significance of group affiliations, digital subcultures, and online interactions in the commission of cybercrimes. Research by Posey et al. (2015) underscores the importance of social norms in shaping cybersecurity behaviors, providing essential context during forensic analysis. By applying social science to digital evidence, analysts gain deeper insights into how and why individuals conform to, or deviate from, cybercriminal norms.

Use of Criminology Theories

Analysts' comprehension of cybercrime trends and vulnerabilities is further influenced by criminological theories. Criminological theories further shape analysts' understanding of cybercrime patterns and vulnerabilities. Analysts' can better understand how cybercrimes happen by using the routine activities theory, which emphasizes the convergence of motivated offenders, suitable targets, and lack of guardianship, and helps analysts determine how cybercrimes occur. This theory is used to evaluate the weaknesses that criminals take advantage of and to recreate crime scenes. This approach allows analysts to predict future criminal behaviors and recommend improved cybersecurity measures to reduce vulnerabilities.

Engaging Marginalized Communities Through Empathy and Communication

Effective communication skills are also essential for computer forensics analysts, particularly when dealing with diverse and marginalized groups. Analysts frequently collaborate with law enforcement, legal professionals, and victims from varied socio-economic backgrounds. They play a vital role not only in solving cybercrimes but also in protecting and advocating for the rights and safety of marginalized groups and enhancing digital trust across society as a whole. These groups can include children, the elderly, low-income individuals, racial and ethnic minorities, and even members of the LGBTQ+ community. Online harassment and hate speech, human trafficking and child sexual exploitation, and even financial scams are some of the most prevalent crimes committed against these groups. Understanding communication dynamics and social sensitivities enables analysts to convey complex digital evidence clearly and empathetically. Marginalized groups often face heightened vulnerabilities to cybercrimes due to limited access to cybersecurity resources and education. Analysts who understand social science principles actively incorporate inclusive communication strategies into their investigative practices, fostering trust and cooperation across diverse populations. Additionally, analysts working with marginalized populations, such as victims of child exploitation, often face significant emotional and psychological challenges. Strickland, Kloess, and Larkin (2023) highlight that computer forensics analysts regularly exposed to distressing material, such as child sexual abuse imagery, require specialized psychological support to manage the emotional toll of their work effectively. Their work ensures that digital crimes against these vulnerable communities are taken seriously and prosecuted effectively.

Conclusion

In summary, computer forensics analysts depend significantly on social science research and principles to perform their roles effectively. Utilizing criminological frameworks for thorough investigations, sociological insights to comprehend digital interactions, psychological theories to interpret offender behaviors, and inclusive communication practices, these professionals incorporate social science deeply into their investigative processes. This interdisciplinary approach ensures thorough, empathetic, and contextually accurate digital crime investigations that address both technical and human aspects.

References

CareerExplorer. (2023, June 21). *What does a digital forensics analyst do?* https://www.careerexplorer.com/careers/digital-forensics-analyst/

CYSE201S Module 2. (n.d.). Google Docs. https://docs.google.com/presentation/d/1Jo7kMpaWztasW0enT8Nqlq6IIF-fo6ntzD7plF6Xvyg/edit?slide=id.p5#slide=id.p5

CYSE201S Module 5. (n.d.). Google Docs. https://docs.google.com/presentation/d/1WJ73ABaJwdvVqEPi4MvnC5uLxsGz-gPv5Ym_AtuytBU/edit?slide=id.p1#slide=id.p1

Hadlington, L. (2018). The “Human factor” in cybersecurity. In *Advances in digital crime, forensics, and cyber terrorism book series* (pp. 46–63). https://doi.org/10.4018/978-1-5225-4053-3.ch003

Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime Investigators are Users Too! Understanding the Socio−Technical Challenges Faced by Law Enforcement. *arXiv (Cornell University)*. https://arxiv.org/abs/1902.06961

Strickland, C., Kloess, J. A., & Larkin, M. (2023). An exploration of the personal experiences of digital forensics analysts who work with child sexual abuse material on a daily basis: “you cannot unsee the darker side of life.” *Frontiers in Psychology*, *14*. https://doi.org/10.3389/fpsyg.2023.1142106

TEDx Talks. (2015, December 9). *Digital Forensics | Davin Teo | TEDXHongKongSalon* [Video]. YouTube. https://www.youtube.com/watch?v=Pf-JnQfAEew