Mackenzi Dellolio
April 14, 2025

Digital Forensics

Digital forensics is an essential part of cybersecurity, investigating cybercrimes and recovering digital evidence. Analysts use ideas from criminology, psychology, and sociology to understand criminal behavior and the social impact of cybercrime. This paper explains how digital forensic professionals apply these social science principles in their work and how they affect marginalized groups and society.

Sociology, Criminology, and Digital Forensics

Sociology provides a foundational framework for understanding why people commit crimes, including cybercrimes. Digital forensic analysts often use sociological and criminological theories to guide their investigations. For example, strain theory suggests that individuals may turn to crime when they cannot achieve societal goals through legitimate means (Encyclopædia Britannica, 2025). Analysts can use this idea to understand the motivations behind hacking, fraud, or identity theft. Cybercriminals might act out of frustration or lack access to job opportunities.

Another relevant theory is routine activities theory, which explains that crime occurs when a motivated offender, a suitable target, and a lack of capable guardianship come together (Perera, 2024). Forensic analysts use this concept to determine why specific systems or people are targeted. For example, analysts may look into how weak passwords or unsecured networks make it easier for attackers to gain access. These theories help analysts understand patterns, improve security, and prevent future attacks.

Forensic analysts blend these criminology and sociology concepts in their daily routines to take a well-rounded approach. For example, when investigating a data breach, they may examine why the organization was targeted and who benefited from the attack. They may also consider more significant social issues, such as poverty or inequality, that could have influenced the crime.

Psychology in Digital Forensics

Psychology plays a vital role in understanding both the perpetrators of cybercrimes and the victims affected by them. Forensic analysts use behavioral psychology to study patterns, profile suspects, and predict their actions. Understanding motivations, such as revenge, financial gain, or social pressure, can help analysts focus their investigations and choose the right strategies. For example, in cases of cyberbullying or online harassment, analysts may look into the offender's psychological state to better understand their behavior.

Ethical neutrality is also important in this work. Analysts must remain unbiased and avoid letting personal opinions or emotions influence their decisions. Psychological concepts like confirmation bias—the habit of favoring evidence that supports our beliefs—and cognitive dissonance, which involves discomfort when facing conflicting ideas, can affect how evidence is interpreted (McNerney, 2011). Being aware of these tendencies helps analysts stay objective and make fair decisions.

Social Inequality and Digital Forensics

Social inequality plays a significant role in both the occurrence of cybercrimes and the increased vulnerability of specific populations. For example, economically disadvantaged individuals are more likely to engage in cybercrime, often as a result of limited access to legitimate job opportunities. Marginalized groups, such as racial minorities, women, LGBTQ+ individuals, and those from low-income communities, are more vulnerable to online harassment, identity theft, and cybercrime (Tisdale, 2024). For example:

> In Maryland, hackers targeted Electronic Benefits Transfer (EBT) cards, which are used to provide public assistance funds for food. The hackers stole over $2 million in 2022 and the first months of 2023. Maryland's income limit for qualifying for the food assistance program is $39,000 for a family of four in 2024, with a bank balance of less than $2,001. Unlike credit cards, EBT cards do not have fraud protections. (Tisdale, 2024).

Efforts to help victims were complicated because reimbursement is capped at two months of stolen benefits within a specific period (Tisdale, 2024). These social differences in committing and being affected by cybercrime show that forensic analysts must consider social context in their work.

Conclusion

Digital forensic analysts can better understand cybercrime's human and social sides by using insights from sociology, criminology, and psychology. By applying social science principles, analysts can solve technical problems and recognize the social and psychological factors behind criminal behavior and victimization. This well-rounded

approach helps ensure that investigations are thorough, unbiased, and sensitive to the needs of all individuals, especially those from marginalized communities. As cybercrime continues to grow and evolve, the role of social science in digital forensics will only become more critical.

References

Encyclopedia Britannica. (2025, March 27). *Strain theory*. https://www.britannica.com/topic/strain-theory-sociology

McNerney, S. (2011, September 7). *Psychology's treacherous trio: Confirmation bias, cognitive dissonance, and motivated reasoning*. Why We Reason. https://whywereason.wordpress.com/2011/09/07/psychologys-treacherous-trio-confirmation-bias-cognitive-dissonance-and-motivated-reasoning/

Perera, A. (2024, February 13). *Routine activities theory: Definition & examples*. Simply Psychology. https://www.simplypsychology.org/routine-activities-theory.html

Post University. (2025, February 24). *Impact of digital forensics in modern crime scene investigations*. https://post.edu/blog/impact-of-digital-forensics-in-modern-crime-scene-investigations/

Tisdale, N. (2024, February 12). *The hidden injustice of cyberattacks*. WIRED. https://www.wired.com/story/cybersecurity-marginalized-communities-problem/