

In this final journal I will explore how the career of digital forensics investigators relates to the social sciences and what I think about the speaker [Davin Teo](#) pathway to his career as a digital forensics investigator. A digital forensics investigator is a trained professional that collects digital artifacts in accordance with industry and chain of custody standards, analyzing what methods or techniques were used to perpetrate criminal activity and presents those properly collected and preserved digital artifacts for use in criminal proceedings. Making their profession an essential facet in method and source attribution of cybercriminal activities involving hacking, fraud, and identity thefts. This makes a multi-disciplinary approach that includes facets of the social sciences that includes a thorough comprehension of societal influences on human behavior, decisions making and social interactions. Each a building block contributing to the overall success of the digital forensic discipline. By integrating knowledge from fields like psychology, sociology, and criminology digital forensic investigators can gain insights into the motivations and intentions of individuals using digital devices for criminal activity and provide crucial information to law enforcement and cybersecurity researchers in their efforts to deal with APT's. With the close relationship between social sciences and digital forensics in mind, it's not surprising that Davin Teo, would choose to pursue an interdisciplinary approach to digital forensics. With an initial interest in computer science and then extensive experience in the field of penetration testing it's natural in my mind that after learning how attacks are perpetrated (methods of weaponization and delivery, etc) that he would start to ask why? Understanding the cognitive, societal, and economic factors that motivate attackers is as important as the methods they use. Making in my mind a natural progression to a more holistic understanding of cybercrime and what it takes, to effectively predict future trends and prevent or mitigate the third order effects of attacks when they occur.