Seth Sarauw
CYSE201S
Instructor Woodbury
Career Paper
10/4/2026

Career Paper: Digital Forensics Investigator

One career that I believe combines cybersecurity and the social sciences is being a digital forensics investigator. You may be asking what a digital forensics investigator is. Well, a digital forensics investigator is a professional who checks electronics to find evidence related to cybercrime. A better explanation of what a digital forensics investigator does according to Champlain College, “digital forensic investigators are trained to handle a variety of responsibilities that fall within the broad scope of their professional role” (Johnson, 2026) . A digital forensics investigator may also “locate and preserve digital evidence,use several advanced tools and analytical approaches to bypass protections and decrypt code in order to recover data that has been deleted, hidden, or corrupted, and prepare to present the evidence in court”. Being a digital forensics investigator requires computer skills, they need to understand human behaviors and social relationships and how they affect cybercrime and society. Social science research and principles help digital forensics investigators understand why crimes happen, how people become victims, and how we can view evidence differently.

One of the concepts that relates to digital forensics is social engineering. Social engineering, according to IBM, are attacks that “manipulate people into sharing information that they shouldn’t share, downloading software that they shouldn’t download, visiting websites they shouldn’t visit, sending money to criminals or making other mistakes that compromise their personal or organizational security” (IBM, 2025). Examples of social engineering are phishing emails or impersonation scams. Digital forensics investigators examine these types of cases and

their evidence and they try to figure out the way the criminal contacted the victim, what information they were trying to get, and how the victim responded. Therefore, digital forensic investigators should try to understand how things such as trust and urgency can play a role in how a victim responds.

Another concept is the human firewall. The human firewall explains how people can become an important part of an organization's cybersecurity defense. Employees should learn how to recognize suspicious emails and things in the same realm and learn how to respond and report these types of things to keep their organization safe. Digital forensics investigators in their field will have to look over the evidence and figure out what happened after an employee clicked a malicious link from an email as an example. Digital forensic investigators can use the evidence to determine why the incident happened and what security improvements are needed.

Cognitive Theory is the third social science concept that can be applied to digital forensics investigators. Cognitive Theory mainly discusses people and how they think, process information, and make decisions. This can be important for digital forensic investigators to use as it can help them explain why victims responded to a cyberattack in a particular way. The victim may make a quick decision because of stress or a sense of urgency. Investigators can examine these situations when figuring out an incident. Starting to understand how people make decisions can help investigators recognize patterns in cybercrime and explain why attacks are successful.

Routine Activity Theory is the last concept I'd like to discuss that digital forensics investigators can connect to. Routine Activity Theory helps explain crime through three steps: a motivated offender, a suitable target, and a lack of security. This theory can be related to digital forensic

investigators because cybercrimes also depend on opportunities. An example would be a criminal searching for a person with a lot of money. That person because they have a lot of money makes them a suitable target. If the person's bank account has a weak security, a cybercriminal has the chance to commit the crime. A digital forensics investigator can examine the evidence to find out how the criminal found the target and whether or not security weaknesses contributed to the incident.

You may be wondering if digital forensics investigators come together with marginalized groups and to answer that question it does. Cybercrime affects people differently and some things that may play a factor are economic situation, age, disability, and other social factors. A challenge that may be faced is something called digital divide. According to Syracuse University, digital divide is “the gap between people who have meaningful access to digital technology and those who don’t” (Syracuse, 2026). People who come from lower income areas may have less access to good electronic devices and cybersecurity education. A second challenge is language barriers. Cybersecurity warnings sometimes are not designed with people who speak languages other than English in mind. This can make it harder for certain victims to protect themselves or report cybercrime. A third challenge is victim blaming. People who are victims of a cybercrime incident fear that they may be blamed for making a mistake which leads to them not reporting the incident. Digital forensics investigators need to worry about finding evidence and understanding what happened rather than blaming the victim.

Digital forensics and digital forensic instigators have had a major impact on society. As more information is becoming stored digitally, evidence that is digital has become equally or even more important in criminal investigations than physical evidence. Digital forensics investigators help our society by finding attackers, finding evidence and collecting it back, and helping

organizations understand how breaches occurred. However, their work also creates concerns about privacy. Digital forensic investigators may have access to some of our most extremely personal information that we have stored on our electronic devices. Digital forensic investigators have laws they have to follow.

References

Johnson, D. (2026a, April 1). *What does a digital forensic investigator do?*. Champlain College. https://www.champlain.edu/blog/stories/what-does-a-digital-forensic-investigator-do/#responsibilities

What is social engineering?. IBM. (2025, January 10). https://www.ibm.com/think/topics/social-engineering

What is the digital divide? meaning, causes & impact. iSchool. (2026, April 2). https://ischool.syracuse.edu/what-is-the-digital-divide/