Navigating the Digital Maze: Digital Evidence of Data Recovery

Courtney Swink

Cybersecurity and Social Science

Professor Yalpi

November 21, 2024

Digital Forensic Investigators or analysts are professionals who help law enforcement gather, collect, preserve, examine, and analyze digital evidence for legal proceedings. They recover and extract digital evidence from computers, mobile devices, digital media, tablets, servers, cloud storage, network traffic, wearable devices, and navigation devices. These investigators are trained in tools and techniques to recover and analyze data including, but not limited to deleted files, text messages, call logs, internet history, emails, databases, meta data, images, videos, system logs, and location data. After analyzing the evidence, Digital Forensic Investigators write a report and testify in court[1] as to their findings. According to IBM, "over 90% of all crime is recognized as having a digital element" [2] making Digital Forensic Investigators at the playing a crucial role in investigating crimes, illegal activity, and fraud through digital devices.

Digital Forensic Investigators can use digital footprints such as social media activity (Module 9) and browsing history to infer habits, interests, and potential motivations as to understanding behavior, along with analyzing digital communications to provide insights into a psychological profile (Module 4) and identifying a potential suspect. Using digital artifacts, timestamps, and location data can eliminate or narrow down suspect lists and authenticate or disprove alibis.

Social Science principles (Module 2) are extremely relevant regarding Digital Forensics. Digital Forensic Investigators apply the principle of relativism through interpretation and variance of digital evidence based on circumstances of a case, context, and jurisdiction. Objectivity is a principle a Digital Forensic Investigator must possess in order to analyze without

[1] Munday, "Day in the Life of a Computer Forensics Investigator" (August 2024)

[2] "Meeting the Future of Digital Forensics and Evidence Management," IBM, https:/www.ibm.com/downloads/documents/us-en/107a02e953c8ff6b

assumptions or bias, and deliver findings impartially solely based on the data collected. When testifying in court, Digital Forensic Investigators engage in parsimony when presenting evidence and testifying in relation to the findings, so that members of a jury, attorneys, and judges understand and are not lost or overwhelmed in the complexities of digital forensics. Ethical neutrality is another key principle that Digital Forensic Investigators should heavily maintain. By following established policies and procedures, and only accessing digital evidence that is legally applicable to the relevant investigation. Determinism directly relates to profiling and determining how criminal behavior is caused or influenced by events in a person's life that made them amenable to a particular crime. Whenever a crime is committed, the sentiment that there is no such thing as coincidence is regularly expressed. However obvious it looks that a person may be guilty of a crime, Digital Forensic Investigators should always maintain a level of skepticism until it is proven by science, of a person's guilt. Digital forensic techniques, tools, methodologies, and algorithms are all used to empirical research to test hypotheses and evaluate the effectiveness of such.

According to demographics from Zippia the Career Expert, only "27.2% of Forensic computer examiners are female, and 44.1% are minorities."[3] With such underrepresented demographics, (Module3) there are bound to be challenges that arise. Among the challenges, language barriers when evaluating evidence in a different language, accurate interpretation of cultural digital artifacts, and unconscious biases based on personal experiences and stereotypes.

[3] Minorities include Hispanic or Latino-16.8%, Asian-10.4%, Black or African American-9.9%, Unknown-5.9%, American Indian and Alaska Native-1.1% to total 44.1%. "Forensic Computer Examiner Demographics and Statistics 2022, https://www.zippia.com/forensic-computer-examiner-jobs/demographics/

Practically everyone uses digital tools on a daily basis, the demand for Digital Forensic Investigators has and will continue to evolve. Digital Forensic Investigators use various techniques to gather, collect, preserve, examine, and analyze data from a multitude of digital devices to detect criminal activity in today's society.

Works Cited

"Forensic Computer Examiner Demographics and Statistics [2022]: Number of Forensic Computer Examiners in the US." *Www.zippia.com*, 29 Jan. 2021, https://www.zippia.com/forensic-computer-examiner-jobs/demographics/.

"Meeting the Future of Digital Forensics and Evidence Management." *IBM*, www.ibm.com/downloads/documents/us-en/107a02e953c8ff6b.

Munday, Rebecca. "Day to Day of a Computer Forensics Investigator | Main Responsibilities." *Www.computerscience.org*, 17 Apr. 2023, www.computerscience.org/careers/computer-forensics-investigator/day-in-the-life/.