Erik C. Sorto

CYSE 201S

04/17/2025

Cybersecurity Career Paper: Digital Forensics Analyst

BLUF (Bottom Line Up Front):

The Digital Forensics Analyst plays a vital role in criminal and federal investigations by collecting and examining digital evidence from suspects' computers, phones, and storage devices. This work intersects deeply with social science principles such as ethical neutrality, human behavior analysis, and communication. Their ability to understand people as much as machines is what makes this cybersecurity role uniquely interdisciplinary and impactful.

I. Introduction

In today 's digital age everything is tied behind technology and leaves behind a digital trail, especially when it comes to crimes the digital Forensics Analyst tracks and studies those digital trails to help uncover evidence to solve criminal and federal cases. These professionals acquire, store and analyze digital data on phones, computers, cloud platforms, IoT devices and more. They provide the basis for investigations into cybercrime, fraud, exploitation and even national security issues. Yet they cannot be successful on a technical level alone, it depends on principles rooted in social science like criminal behavior understanding, communication and ethical decision making.

II. What Do Digital Forensics Analysts Do.

According to the FBI, Digital Forensics Examiners serve on the Computer Analysis Response Team (CART). They recover & examine data without modifying it, they follow strict chain-of-custody protocols and testify in court about their findings. They handle evidence from damaged or deliberately wiped devices with advanced forensic tools and technical

knowledge across Linux, Windows, Mac and mobile OSes. According to the Cybersecurity & Infrastructure Security Agency (CISA) They also respond to incidents, identify digital fingerprints and advise investigative teams on evidence handling.

III. Applications of Social Science Principles.

The job is tech-heavy, but social science does in fact play a vital role. Analysts require psychological profiles of the offenders to understand them. The motives of the crime, criminal background and reasons as to why individuals hide digital evidence or what the persons online behavior says about intent and motive of the crime or people involved.

Additionally, concepts like ethical neutrality are paramount and play a vital role. Analysts must remain neutral when they examine suspects' devices, even in emotionally charged cases like exploitation or terrorism. Principles like empiricism and parsimony also govern their work as conclusions of findings should be made only from observed data and reported clearly, without excessive detail or speculation.

IV. Communication and Interpersonal Skills

The Digital Forensics Analysts report technical results to non-technical audiences such as law enforcement officers, attorneys, judges and occasionally juries. This requires excellent interpersonal skills, clarity and professionalism. Many analysts become subject matter experts who train federal agents or police on how to preserve digital evidence during arrests or searches.

V. Equity & Marginalization in Digital Justice.

Both cyber and traditional crimes may involve victims and suspects from underrepresented groups. Digital access and literacy gaps should also be considered by analysts when interpreting data. For instance, someone unfamiliar with technology might misinterpret innocent behavior. Additionally, language barriers/cultural differences might influence the reception of digital communication as well. Applying cultural competence helps analysts

conduct fair, ethical and bias-free digital investigations that support justice for all communities regardless

VI. Societal Impact

Digital Forensics Analysts serve public safety, national security and digital accountability. They make it their best effort to bring criminals to justice, uncover fraud schemes, uncover digital evidence, and protect victims from abuse online. However, they face challenges also related to privacy rights and surveillance ethics. Good evidence collection is always a responsibility balanced with civil liberties respect. Forensic analysts often work at the interface between social and legal frameworks and cybersecurity.

VII. Conclusion

Digital Forensics Analyst holds one of the most socially impactful jobs in cybersecurity. These professionals need to understand people, psychology, ethics and society beyond tools and code. Communications, ethical neutrality and behavioral analysis are not merely theoretical concepts, but they are the foundation for a career at the intersection of justice and technology. Those wanting a career in crime fighting with logic and empathy will find this a promising route forward.

References

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.

CyberDegrees.org. (n.d.). *Digital forensics careers & salaries*. https://www.cyberdegrees.org/careers/computer-forensics/career-and-salary/

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Cyber defense forensics analyst*. https://www.cisa.gov/careers/work-rolescyber-defense-forensics-analyst

Federal Bureau of Investigation (FBI). (n.d.). *Digital forensic examiner* [PDF]. https://www.fbi.gov