Interdisciplinary Research: A Multi-Perspective Approach to Computer Science, Law, and Psychology

Student: Samantha Hairston

Course: IDS 300W- Introduction to Interdisciplinary Theory and Concepts

Instructor: Dr. Maryann Kozlowski

Date: December 9, 2025

Institution: Old Dominion University

Introduction

As a senior at Old Dominion University majoring in Cybersecurity with a minor in Cybercrime, I have learned that solving complex real-world problems requires more than a single disciplinary perspective. The purpose of this interdisciplinary research paper is to strengthen my research and writing skills by integrating multiple theories, approaches, and concepts across three disciplines: Computer Science, Law, and Psychology. Using Repko and Szostak's 10-step interdisciplinary research method, this paper explores how knowledge from these fields can be combined to develop a deeper understanding of digital evidence, investigative procedures, and human behavior in context of cyber investigations (Repko & Szostak, 2020, p. 77). By drawing on technical processes from Computer Science, legal frameworks from Law, and behavioral insights from psychology, this study seeks to provide a comprehensive explanation of how cybersecurity and digital forensics support modern criminal investigations. **This paper argues that integrating computer science, law, and psychology reveals how cybersecurity and digital forensics function as essential, interdependent tools in contemporary criminal investigations.**

Interdisciplinary approach/ method

The interdisciplinary approach provides a structured way to integrate knowledge from multiple fields to better understand complex issues, and it is especially useful for a topic of cybersecurity and digital forensics, where technology, law, and human behavior intersect. Using Repko and Szostak's 10-step interdisciplinary research method, this paper begins by defining the problem and focus question (Step 1). It then justifies the need for an interdisciplinary approach because no single discipline can fully explain digital crime, evidence handling, and offender behavior (Step 2). After identifying Computer Science, Law, and Psychology as the most relevant

disciplines (Step 3), I conducted a literature search (Step 4) and developed adequacy in each discipline by reviewing their core theories, methods, and research findings (Step 5). The insights gathered from these fields were then analyzed to understand the technical, legal, and behavioral aspects of cyber investigations (Step 6), and any conflicts between disciplinary viewpoints were identified, such as differences between technical capabilities and legal requirements or between human behavior and digital evidence collection (Step 7). Common ground across disciplines was then explored (Step 8), which allowed for the integration of insights into a more comprehensive understanding of the issue (Step 9). Computer science contributes technical knowledge such as tools, algorithms, and forensic procedures essential for recovering and analyzing electronic data, which supports Casey's (2011b, p. 3) claim that in the modern age it is hard to imagine a crime that does not have a digital dimension. Law provides the structure that governs evidence of handling, chain of custody, and courtroom admissibility, aligning with Belshaw's and Nodeland's (2022, p. 248) statement that digital evidence is now being used to prosecute all types of crimes. Psychology adds understanding of offender behavior, motivation, decision-making, situational influences, consistent with Horney's (2006) work on how life circumstances shape criminal actions. Integrating these perspectives results in a fuller understanding of how digital forensics function in real investigations and supports the last step of the interdisciplinary process which is to communicate and test the integrated explanation (Step 10) (Repko & Szostak, 2020, p. 77).

Discipline 1: Computer Science

Computer Science is central to cybersecurity and digital forensics because investigators rely on technical tools, algorithms, and system knowledge to recover, preserve, and analyze digital evidence. As crimes increasingly involve technology, computer science provides the methods

needed to interpret data from devices, networks, and online platforms. Casey (2011) emphasizes that precise technical terminology and specialized procedures are necessary for understanding how computers are used in crime, noting that different cases require different investigative approaches (p. 39). For instance, intrusion investigations focus on logs, malware, and network traffic, while cases like homicide or fraud rely on file recovery, metadata analysis, and user activity reconstruction.

Computer science also shapes how devices are collected and processed as evidence. Casey (2011) explains that when only a small amount of data is relevant, investigators may not seize the entire device, but when a computer plays a key role in a crime, it is necessary to collect the full system to preserve evidence of integrity (p. 39). Technical safeguards such as hashing, write-blocking, and disk imaging ensure that evidence remains authentic and admissible. Additionally, online criminal activity generates large amounts of data, including emails, chat logs, web activity, and posts, which require computer science techniques like log parsing and pattern matching to analyze effectively (Casey, 2011c, p. 740).

Johnson (2006, p. 170) adds that forensic computer crime investigations depend on understanding operating systems, files, and network protocols because this knowledge allows investigators to reconstruct events and interpret how data was stored or altered. Overall, computer science provides the essential frameworks and analytical tools that make digital forensics possible, enabling investigators to extract, verify, and interpret digital evidence in modern criminal investigations.

Discipline 2: Law

The discipline of Law plays a crucial role in shaping how digital investigations are conducted because legal standards determine what evidence can be collected, how it much be handled, and whether it is admissible in court. In digital forensics, investigators cannot simply access data whenever they choose; they must follow strict legal procedures that protect citizens' rights while enabling effective investigations. Alexandrou (2021) explains that forensic investigators must obtain proper authorization before seizing or examining digital evidence, noting that "the forensic investigator must obtain possession of the evidence with a proper warrant," and that in some situations, access may require voluntary consent or a subpoena instead (p. 90). These requirements ensure that digital evidence is collected legally, which is essential because improperly obtained evidence can be dismissed in court. Law also influences digital investigations through jurisdictional boundaries. Alexandrou (2021) highlights a major challenge in cybercrime cases: determining where the crime occurred, especially when offenders operate across national borders. He emphasizes that prosecuting cybercriminals outside a country's legal jurisdiction is often "difficult if not impossible," which limits the ability of investigators to hold global offenders accountable (p. 88).

Legal institutions have responded to these challenges by expanding their capacity to handle digital evidence. Law enforcement agencies now routinely integrate computer forensics into their investigative processes. Novak et al (2018) describe how agencies are incorporating digital evidence collection and analysis into their infrastructures because computers are not only used to commit crimes but can also be used to fight crime through forensic science (p.1). However, this integration has created new pressures, as agencies must continually train officers in digital evidence procedures while keeping up with rapidly evolving technologies such as mobile devices, networked systems, and modern operating systems (Novak et al., 2018, p.1). These

ongoing changes demonstrate how closely law and technology must work together to ensure digital evidence remains reliable and legally sound.

Furthermore, specialized law enforcement units have emerged to address the increasing complexity of cybercrime. Belshaw and Nodeland (2021) explain that many states and local agencies now rely on dedicated digital evidence experts who focus on investigating computer crimes and conducting forensic examinations for a wide range of offenses (p. 250). These units reflect how the discipline of law adapts to technological developments by creating structures that support effective evidence of handling. Belshaw and Nodeland (2021) also highlight that digital forensics itself exists at the intersection of law and computer science, emphasizing that legal procedures and technological expertise must work together to produce valid, trustworthy evidence (p. 251). Through legal standards, jurisdictional rules, investigative protocols, and specialized units, the discipline of law ensures that digital forensics is practiced in a way that upholds justice, protects rights, and supports successful criminal investigations.

Discipline 3: Psychology

Psychology plays a key role in digital forensics and cybersecurity investigations by helping investigators understand human behavior, cognition, and emotion behind digital actions. Cognitive forensics, a subfield of psychology, remains how processes such as perception, memory, decision-making, and expertise affect forensic investigations. Sammons and Putwain (2018) explain that cognitive psychology enhances investigative accuracy by improving how information is gathered and interpreted (p.67). For example, cognitive interviewing uses psychological techniques to increase the detail of witness statements and has been shown to outperform standard police interviews in eliciting richer information, even though it may slightly

reduce accuracy (Sammons & Putwain, 2018, p. 83). These methods are valuable in digital investigations where accurate timelines and user behaviors must be reconstructed.

Psychology also informs suspect interrogation and helps investigators recognize deception, interpret verbal and nonverbal cues, and understand the emotional states that influence criminal behavior. Emotional psychology explains how strong emotions can drive implusive or irrational actions. Ostrosky and Ardila (2017) note that emotions often guide human behavior and can completely arrive at rational thinking, especially in "crimes of passion" where individuals act without considering consequences (p. 19). This helps investigators understand emotional motives behind cybercrimes such as harassment, threats, or impulsive online misconduct.

More broadly, psychological theories help explain why people commit crimes and how they make decisions in digital contexts. Hollin (2013) emphasizes that psychology is essential for understanding and managing criminal behavior, influencing policing strategies, court processes, and crime reduction efforts (p. 1). In cybersecurity and digital forensics, this knowledge helps investigators identify behavioral patterns, profile cyber offenders, and interpret digital evidence in ways that technical tools alone cannot. Overall, psychology enriches digital investigations to better understand the human factors behind cybercrime.

Applications and Synthesis

Ingtergrating psychology, law, and computer science creates a multidimensional understanding of digital forensics and cybersecurity. Each discipline approaches cybercrime from a different perspective, yet their insights connect in meaningful ways. Examining their own common ground and conflicts shows why all three are necessary for addressing the rapidly evolving landscape of digital investigations.

Psychology contributes essential knowledge about human behavior, cognition, motivation, and decision making. Digital forensics may involve technical evidence, but ultimately crimes are committed by individuals whose actions are shaped by perception, memory, and emotion. Cognitive forensics draws directly from psychological research to improve investigative interviewing, eyewitness recall, and suspect interrogation. For example, cognitive interviewing techniques that are grounded in psychological principles are consistently shown to produce more detailed witness statements than standard police interviews. Psychology also clarifies how emotions influence behavior. Crimes driven by anger, impulsivity, fear, or thrill seeking cannot be fully explained through technical data alone. Understanding these internal processes helps investigators interpret digital behavior such as browsing patterns, communication styles, or decision making during the commission of cyber offense. Psychology helps make sense of underlying reasons behind the digital trace.

Law provides the structure that governs how digital evidence is collected, preserved, and used. While psychology helps investigators understand human behavior, it is the law that determines methods are premissible and what standards must be met for evidence to hold up in court. Legal frameworks define search seizure requirements, jurisdiction, and admissibility of digital evidence, and the roles of investigators and forensic examiners. For instance, obtaining a warrant, subpoena, or voluntary consent is critical before accessing a suspect device. Jurisdictional challenges also arise because cybercrime often crosses national borders, which complicates persecution efforts when offenders operate outside a court with legal authority. Law enforcement agencies have responded by developing specialized units trained in digital evidence procedures, reflecting the legal systems' growing need to adapt to technological change. Law acts as the mediator between investigative practice and constitutional protections.

Computer science forms the technological core of digital forensics and cybersecurity by supplying the tools and the methods needed to identify, extract, and analyze digital evidence. Without this discipline, investigators could not examine malware, encryption, network intrusions, mobile devices, or cloud artifacts. Digital forensics exists at the intersection of law and computer science because forensic work must follow legal standards while relying on technical procedures. Through computer science, investigators can recover deleted data, trace IP activity, reconstruct timelines, and analyze system logs, while also developing secure systems and detection methods that help prevent cybercrime.

Although psychology, law, and computer science share common goals, they sometimes conflict. Computer science often favors quick data access, yet the law requires warrants and strict procedures. Psychology supports techniques that improve memory recall, and legal rules may limit their use. There is also tension between psychology's focus on human behavior and computer science's focus on system behavior, which can lead to different interpretations of digital actions.

Despite these differences, the three disciplines share important common ground. Each works to uncover truth, protect the public, and ensure fairness. Psychology improves witness reliability, law ensures evidence is collected ethically, and computer science provides objective digital data. Together, they offer a more complete understanding of what happened and why it happened.

In synthesis, integrating psychology, law, and computer science creates stronger, more reliable, and ethical digital investigations. Each disciple fills the gaps left by the others, allowing investigators to see cybercrime as a technical act and human behavior within legal boundaries. This interdisciplinary cooperation is essential for modern digital forensics.

Summary

In summary, the integration of computer science, law, and psychology shows how cybersecurity and digital forensics have become essential to modern criminal investigations. Computer science supplies the technical tools needed to recover, preserve, and analyze digital evidence from devices and networks. Law provides the legal framework that guides how evidence is obtained and ensures it can be used ethically and effectively in court. Psychology helps investigators understand human behavior, motivations, and memory, offering context for interpreting digital actions and conducting reliable interviews. Together, these disciplines demonstrate that solving contemporary crimes requires both technological expertise and an understanding of the human and legal dimensions involved.

Reference List

Aidan Sammons, & Putwain, D. (2018). *PSYCHOLOGY AND CRIME : 2nd edition.* Crc Press. https://doi.org/10.4324/9781351252140

Alexandrou, A. (2021). *Cybercrime and Internet Technology*. CRC Press. https://www.taylorfrancis.com/books/mono/10.4324/9780429318726/cybercrime-information-technology-alex-alexandrou

Belshaw, S., & Nodeland, B. (2021). Digital evidence experts in the law enforcement community: Understanding the use of forensics examiners by police agencies. *Security Journal*, *35*, 248–262. https://doi.org/10.1057/s41284-020-00276-w

Bratu, I., & Leiser, M. (2024). Navigating the convergence of law, computers & technology. *International Review of Law Computers & Technology*, *38*(3), 1–3. https://doi.org/10.1080/13600869.2024.2324533

Casey, E. (2011). *Digital Evidence and Computer Crime : Forensic Science, Computers and the Internet* (3rd ed.). Academic Press. Casey, E. (2011). Digital Evidence and Computer Crime : Forensic Science, Computers and the Internet (3rd ed.). Academic Press.

Hollin, C. R. (2013). *Psychology and crime : an introduction to criminological psychology*. Routledge. https://doi.org/10.4324/9780203074282

HORNEY, J. (2006). AN ALTERNATIVE PSYCHOLOGY OF CRIMINAL BEHAVIOR. *Criminology*, *44*(1), 1–16. https://doi.org/10.1111/j.1745-9125.2006.00040.x

Novak, M., Gonzales, D., & Grier , J. (2018). New Approaches to Digital Evidence Acquisition and Analysis. *NIJ Journal*, *280*, 8. https://doi.org/ij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis#1-0

Ostrosky, F., & Ardila, A. (2017). *Neuropsychology of Criminal Behavior*. Routledge. https://doi.org/10.4324/9781351252140

Thomas Alfred Johnson. (2006). *Forensic computer crime investigation*. Crc, Taylor & Francis. https://doi.org/10.1201/9781420028379

Extra Credit

If you had to do this paper again, how would you do it? How would you research? What different steps would you take? What was successful? What did you learn about the research process?

The same for writing up your results - what worked and what didn't? What would you do differently, and what would you do the same (in the writing and revising process)?

If I had to research this paper again, I would begin by emaining more interdisciplinary research papers so I could better understand how scholars structure their arguments and integrate multiple fields. I would also spend more time reading my interdisciplinary research textbook to strengthen my grasp of the concepts and expectations before starting the project. Although I would still follow the 10-step interdisciplinary research process, I would likely choose a different topic and make sure to educate myself on it more thoroughly before moving into the analysis stage. I would also devote additional time to locating strong academic sources and take the time to fully understand each article instead of learning about them as I wrote. Another change I would make is asking for more help earlier in the process because in the beginning I honestly felt unsure about how to approach the assignment.

Even with the challenges I faced, the project was ultimately successful because the research teps helped me develop a clear understanding of my topic and allowed me to write the paper more confidnetly. The feedback I received throughout the process helped me correct my mistakes and improve my work for future assignments. The writing stage felt easier than the earlier steps, especially because the peer review provided direction and helped bring everything together. However, I do wish I had located more sources before writing instead of searching for additional references partway through.