Stewart Pawley

Computer Science Major

Indiana University Southeast

Email: spawley@iu.edu

Expected Graduation: May 2026

# Overview

As a 44-year-old Computer Science undergraduate at Indiana University Southeast, I bring a unique combination of maturity, life experience, and technical ambition to the digital forensics and cybersecurity space. Originally from Paducah, Kentucky, and a graduate of Saint Mary High School, my academic journey reflects a deep commitment to evolving with today’s most pressing technological challenges.

# Academic and Professional Focus

My primary area of interest lies in the integration of Artificial Intelligence (AI) within Computer Forensics, a field that demands both analytical precision and scalable problem-solving. Drawing inspiration from current research on AI-driven investigative frameworks, such as the MultiAgent Digital Investigation Toolkit (MADIK), I am exploring how intelligent agents can automate routine forensic tasks, analyze massive datasets efficiently, and identify critical evidence with increased accuracy.

# Key Competencies and Interests

* **Intelligent Systems & Multi-agent Architectures**: Proficient in the development and application of multi-agent systems (MAS) to support complex computational tasks, including the use of frameworks like JADE for distributed processing. This involves understanding how specialized intelligent agents, each with a set of rules and a knowledge base, can perform different analyses on digital evidence in a distributed manner.
* **Case-Based Reasoning (CBR) for Evidence Evaluation**: Experienced in utilizing CBR to determine proper analytical strategies and enhance the accuracy of evidence relevance assessments in digital investigations. This includes employing CBR to select the most effective agents for specific investigation types, such as using child exploitation hash sets in relevant cases.
* **Distributed Processing in Digital Investigations**: Skilled in designing and implementing distributed forensic examinations to improve computational resource utilization and reduce analysis times. This includes understanding the performance gains achieved through distributing work among multiple computers and agents, even with communication overhead.
* **Algorithm Design and Cybersecurity Ethics**: Knowledgeable in designing algorithms for automated evidence analysis, including:
* **Hash Set Analysis**: Calculating MD5 hashes and comparing them against known sets of ignorable or important files, managing large hash sets (e.g., over 10 million values).
* **File Path Analysis**: Identifying files in commonly used folders for P2P, VoIP, and instant messaging applications.
* **File Signature Analysis**: Examining file headers to detect mismatched extensions and identifying common prefixes/filenames from digital cameras.
* **Timeline Analysis**: Examining creation, access, and modification dates to determine relevant events like software installations, backups, or web browser usage.
* **Windows Registry Analysis**: Extracting valuable information from registry files, such as system installation dates, time zone configurations, and removable media information.
* **Keyword Analysis**: Searching for keywords and using regular expressions to extract specific information like credit card numbers, URLs, or email addresses.
* Maintaining a strong commitment to ethical considerations in digital forensics, ensuring that automated processes assist human experts without replacing their critical judgment.
* **Data Correlation and Reduction Techniques**: Capable of implementing techniques to correlate disparate digital evidence and reduce the volume of data requiring human review. This involves enabling agents to insert their conclusions and remarks into a "blackboard" system for conflict resolution and ultimately presenting the most interesting evidence to the human examiner. The system also facilitates knowledge discovery by correlating findings from different pieces of evidence, like identifying email messages between computers or the insertion of removable media into a system.

# Strategic Vision

By combining theoretical learning with practical application, I aim to contribute to the creation of adaptive forensic tools that not only support human experts but evolve with every case encountered. My objective is to reduce investigative bottlenecks, support digital justice initiatives, and enhance the resilience of information systems against emerging threats.

# Future Outlook

Upon graduation in 2026, I intend to pursue a professional role or graduate study focused on the application of AI in cybercrime prevention, data integrity, and forensic automation. I envision myself working at the nexus of public service and innovation—applying my knowledge to projects that secure our digital future through ethical, intelligent, and scalable solutions.