PI magazine.com

professional investigator magazine

$9.95

May/June 2025

ALSO IN THIS ISSUE:

A Deep Dive into Financial Asset Investigations

A Checklist for Conducting Forensic Hypnosis Sessions

If You Have to Ask... STOP

The Power of Partnership: How PI's Support Law Enforcement in Complex Cases

THE SCIENCE BEHIND THE EYES

HOW EYECANKNOW IS MODERNIZING LIE DETECTION

DEPARTMENTS

BOOK SPOTLIGHT

FINANCIAL

INSURANCE

PI 101

ALL THINGS SURVEILLANCE

BACKGROUNDING

CYBERSLEUTHING

PI HISTORY

BUSINESS-TAX

TSCM

THE PI AND FUGITIVE RECOVERY

MARKETING

SOCIAL MEDIA

PROCESS SERVING

PI PERSPECTIVES

NCISS LEGISLATIVE UPDATE

EXECUTIVE PROTECTION

IN EVERY ISSUE

Artificial Intelligence and Investigations: WHAT YOU NEED TO KNOW

BY **ROBERT B. FRIED** & **RACHEL KRONENFELD**

In simplest terms, Artificial Intelligence (AI) is the ability for a computer to think and learn, to perform tasks like a human being. Although AI has been around since the 1950s, it has seen a boom recently, as Large Language Models (LLMs) that recognize and respond to text, and generative AI models that can create new content have become more accessible. As the usage of AI increases, it will affect many facets of society and our daily life. Investigators must embrace this technology, understand how to identify AI, if encountered during an investigation, and how to leverage AI for investigations – while still incorporating the "human element."

AI MODELS: DETECTION AND USAGE

Many LLMs and generative AI models are available to users at no cost; a paid subscription typically allows access to more complex models and a quicker response time to queries. Users access these models on devices via an installed app or a web browser, potentially storing data (locally or on cloud servers), including preferences, queries, and user activity. The device may store downloaded setup files from the installed app. Web browser cache, stored locally on the device, may provide insight into sites that a user has visited. If a user account is required to use the model, it is possible that the cloud may store account data, including generated content, and multiple devices logged into the account may access this information. Accounts secured with multi-factor authentication may send prompts/notifications, messages (via text or email), or voice calls to a user's devices.

Users can export content generated by models to their devices in various ways. Exports may have a filename and extension that is unique to a model. Reviewing the metadata of the exports, specifically their creation and modification timestamps, may reveal that a model generated the exports; this information can further corroborate other activity, such as when a user may have visited a model's website or logged in to an account. While some models support downloading exports to a device, others only allow users to cut-and-paste content.

Content generated by models typically includes references to the model by name or version, and – if text-based – a consistent structure/format, with an unnatural tone. There are free and commercially available tools that can help detect AI generated content; while helpful, these tools typically provide probability scores and can generate false positives.

While it is important to understand how to detect AI, if encountered, it is best to engage a digital forensics practitioner. They will establish a chain of custody for potentially relevant devices/accounts, ensure proper evidence handling, and use defensible and efficient methodologies to further identify, and to preserve, collect and analyze data associated with the models and their usage. Some of the information/insights a digital forensics practitioner may provide include:

- If/When a user downloaded, installed, and used an AI model app
- If/When a user accessed an AI model via a web browser
- Metadata about content generated by an AI model
- User activity (account access may be required)
  - Availability of information may be based on the subscription level of the account and retention settings

OPPORTUNITIES FOR INVESTIGATION

Investigators today often utilize open-source intelligence (OSINT) from social media, news, and public records, but manually sifting through vast amounts of data is time consuming and inefficient. AI automates data collection, such as scraping public social media posts on a subject's profile, aggregating news articles, and searching multiple public databases for legal filings, criminal records, or business registrations in minutes. Saving time on the data collection phase opens up more time for you to discover what information is relevant to your case.

Beyond collection, AI analyzes data to answer important questions that investigators may spend hours to weeks trying to answer through manual review. It can flag specific words in social media posts such as knowing every time your subject said the specific word "hate" in their social media posts, assess the sentiment of your subject's social media posts, and build network diagrams to reveal relationships between entities for complex cases. AI-driven image and facial recognition can identify persons of interest, discover impersonating accounts, and determine if an image is AI generated. Optical Character Recognition (OCR) extracts text from an image or scanned documents so you can search them.

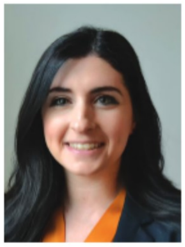
OPPORTUNITIES FOR REPORT WRITING

Writing detailed, structured reports can be challenging, especially for legal or corporate audiences. AI generates report templates to improve consistency, summarizes large volumes of data to save time, and tailors content for different audiences. Given a report you've written, AI refines the language, removes ambiguity, restructures for clarity, and even redacts sensitive information to ensure you are maintaining confidentiality and compliance with privacy laws.

CHALLENGES AND ETHICAL CONCERNS

Despite its benefits, there are some challenges and ethical concerns with AI to be aware of. While there are some free or affordable AI solutions on the market, the high-quality ones can be expensive. AI models may carry biases based on training data, leading to inaccurate or misleading results. AI can also hallucinate, fabricating information when data is insufficient. When it comes to evidence, AI is a double-edged sword. Criminals use AI to impersonate others through deep fakes, forge documents, and manipulate images, audio, and video. As AI and its usage continues to evolve, investigators must remain cautious, as AI can deceive just as easily as it can help. **PI**

Robert B. Fried has over 23 years of experience collecting data and investigating electronic evidence. Robert's background includes senior leadership positions in the digital forensics practices of global professional services firms. Robert was a Computer Crime Specialist at the National White Collar Crime Center (NW3C), where he developed and instructed computer forensic and investigative training courses for federal, state, and local law enforcement agencies. Robert attained a BS and MS in Forensic Science, and certificates in Law Enforcement Science, Computer Forensic Investigation, and Information Protection and Security from the University of New Haven. He holds and actively maintains the following industry certifications: ACE, CFCE, EnCE, GCFA, and C4 CBP. Robert is a licensed PI in Michigan, New York, and South Carolina. Robert serves on the Board of Advisors for the Masters in Investigations program at the University of New Haven, and the Global Advisory Board for EC-Council's CHFI certification. Robert is a frequent speaker at industry events, a featured guest on industry podcasts and has been published in several professional publications. He is an author of PI Magazine*'s Cybersleuthing Department, where he shares insightful content on topics relating to digital forensics, eDiscovery, data privacy, and cyber security. Robert is also the author of the books,* Forensic Data Collections 2.0: The Guide for Defensible & Efficient Processes, *and* Forensic Data Collections 2.0: A Selection of Trusted Digital Forensics Content.



Rachel Kronenfeld is a licensed Private Detective and Suite Product Manager at Liferaft. Rachel's career has seen her donning multiple hats and emerging as a trailblazer in the realm of OSINT and investigations. Her expertise spans from cultivating strong client relationships, spearheading analytical teams dedicated to investigations, to her love for due diligence and background investigations. Within Liferaft, Rachel is pivotal in shaping and realizing the product vision. She meticulously conducts market research to ensure the product is finely attuned to the evolving needs of customers and the industry. Prior to joining Liferaft, she was a core member of Hetherington Group's leadership team as Director of Services. She led business development, client, and vendor relations and was responsible for the management and development of all investigative work. Throughout her career, Rachel has trained a diverse audience, including investigators, security professionals, legal practitioners, financial experts, auditors, military intelligence personnel, and federal, state, and local agencies, enlightening them on the paramount practices in OSINT investigations and associated methodologies.