

Key Investigation Trends for 2025 and Beyond

Navigating Investigations with Technology and Innovation
for Smarter, More Effective Analysis

FALKOR



Explore the Top Investigation Trends



Introduction

- Purpose of the White Paper
- Importance of Staying Ahead
- Overview of Topics



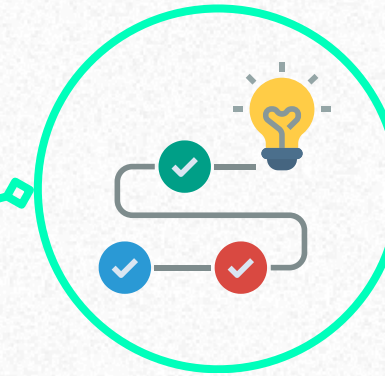
Trends

New technologies, specialized tools, and updated skills are changing how investigations are done in 2025.



Challenges

Explore the key challenges shaping the future of investigations in 2025.



Conclusion

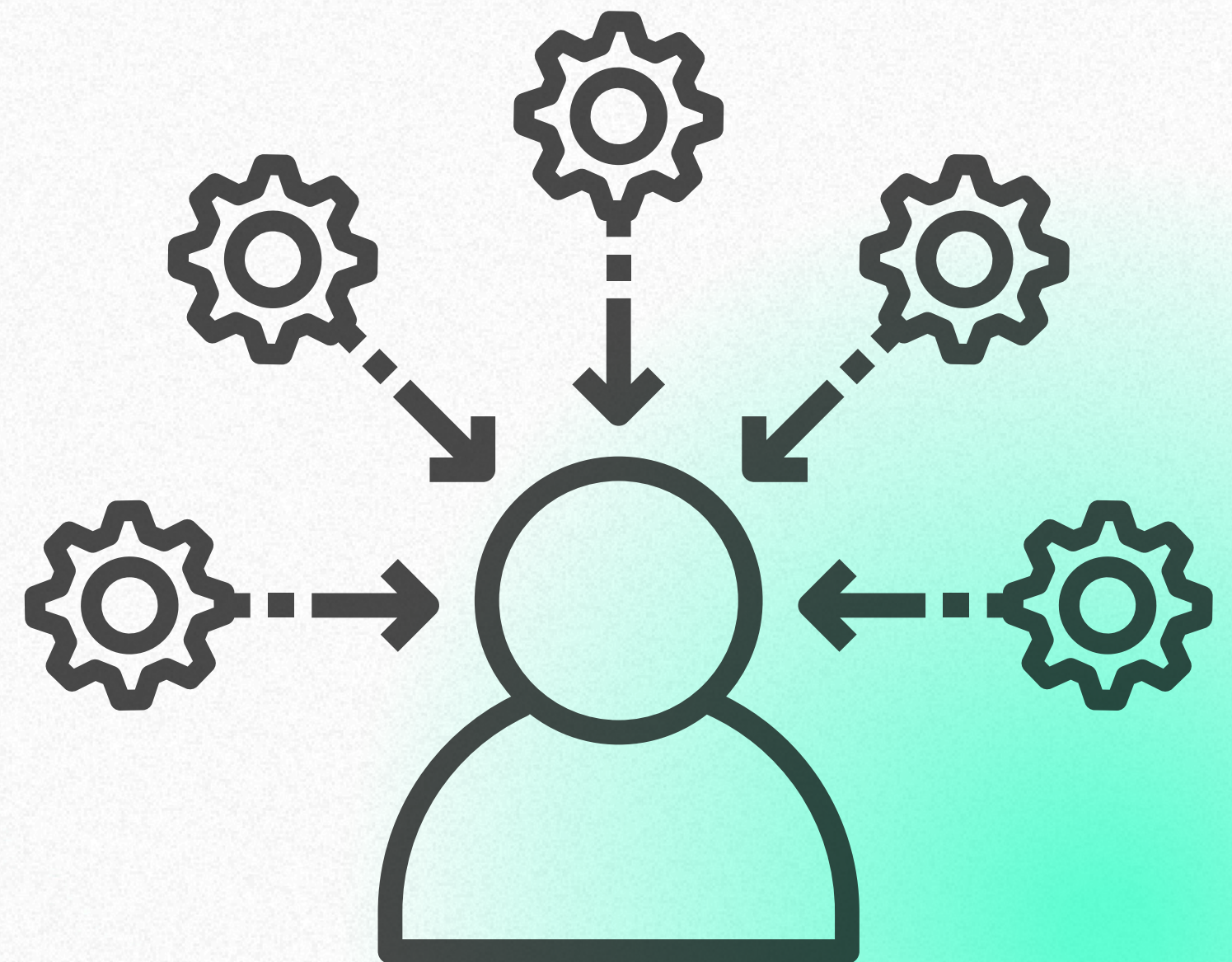
Key lessons from 2024 and strategies for thriving in 2025.



Why Investigative Adaptability Matters

Investigations are changing fast as we head into 2025. New technology, tools, and global challenges are reshaping how analysts work. Staying ahead of these trends is crucial for solving cases, finding answers, and making better decisions in a complex world. This paper highlights the key changes and why they matter for the future of investigations.

👉 Key Takeaway: Equip yourself with cutting-edge tools and methodologies to tackle tomorrow's challenges.



1. Trends

Emerging Trends: How Investigations Are Evolving

Explore the major advancements in AI, OSINT tools, and tradecraft reshaping investigative work for 2025 and beyond.

Trend #1: AI

AI Revolution: Transforming Investigations with Smarter Insights

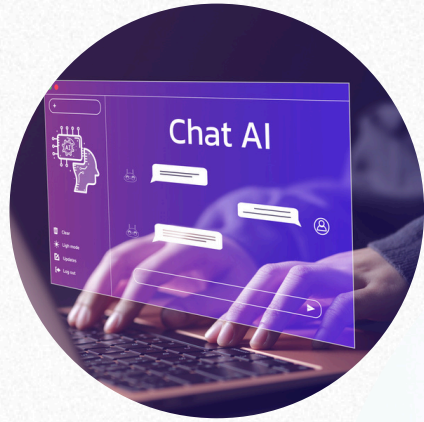
AI is the single biggest development of 2024 for intelligence collection and analysis.



AI is the single biggest development of 2024 for intelligence collection and analysis. Large language models such as Open AI's ChatGPT, Anthropic's Claude, Perplexity, Meta's LLaMa and others have given us a glimpse of what the future may portend for analysis as well as any other field. LLMs, in contrast to machine-learning models that have been used for years such as optical character recognition (OCR) or named entity recognition (NER) - both of which are used to extract data from text and images - LLMs are more general use, and more importantly are prompt-based. Essentially, we ask the large language model a question or make a request of it with a natural language prompt, and the model returns a response for us based on its training data and model. This means that we can ask it a question on almost anything, and receive a usually reliable answer. These questions can range from historical questions, requests for lyric-writing, help with our code or more.

LLMs

can help analysts red team findings, write new queries, find hidden patterns, and summarize reports.

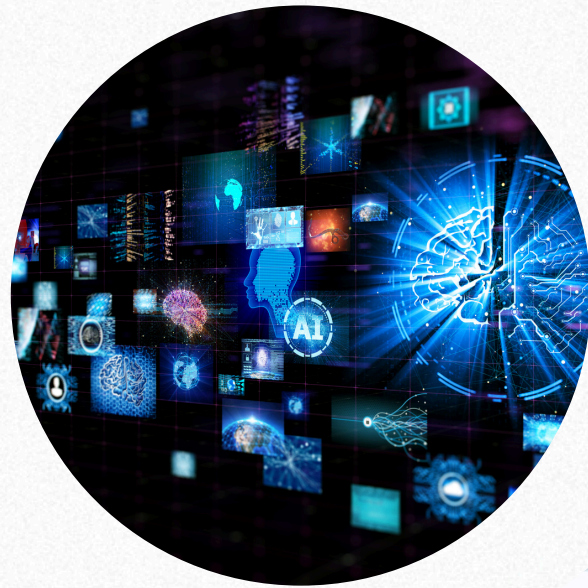


LLMs are exponentially more complex than machine-learning algorithms and tooling, and we still don't fully understand them. While many analysts are busy prompting these LLMs on a daily basis to receive answers for questions of all kinds, we must be careful to ensure that we don't receive hallucinations, or made-up data, in the response that the LLM gives us. When used correctly, and with a carefully-engineered prompt for maximal effect, LLMs can be critical for analysis. LLMs can red team our data and findings, help us ask additional questions, write new queries for specific tools, find hidden patterns and much, much more. However, LLMs aren't truly capable of logical thought and reasoning, and thus we should never use them for true analysis.

Perhaps the most impactful use of LLMs and AI for analysts, as shown this year, won't be the replacement of analytical work but rather as a holistic tool for everything else that we as analysts do. LLMs excel at summarizing data, translating content, changing data formats, writing scripts and basic code and more. We as analysts can utilize LLMs thus to supercharge our workflows; summarizing reports and data more quickly and succinctly, proofreading our work, changing the format of a given dataset or extracting it, or fixing our broken Python script.

AI-powered

OSINT tools have democratized capabilities that were once only available through painstaking manual work



The hype around LLMs is one thing, but even machine-learning had a big year for analysts. New machine learning based tools for OSINT analysis such as GeoSpy AI, which utilize machine learning to analyze street imagery and break it down to its components such as building types, soil color, vegetation and more, enable analysts to upload a photo and receive an estimation as to where it was taken with a reasonably high level of accuracy - a capability once only reserved for those willing to painstakingly carry out manual geolocation. AI-powered tools such as [Findthatspot.io](https://findthatspot.io) also empower analysts to input a natural language query to find relevant locations on OpenStreetMap, a significant development for investigative work. CensysGPT enables analysts to write natural language queries to relevant servers and certificates online. Analysts are now empowered to use new tools in better ways thanks to AI.

LLMs are tools, not replacements for true analytical thought or logical reasoning.

Trend #2: Tailored Solutions

Custom Tools: The Rise of Tailored OSINT Solutions

2024 marks the era of modular OSINT systems, where flexibility and adaptability take center stage.

GeoSpy AI and other tools represent another trend alongside its use of AI: the rise of smaller companies developing tailored OSINT solutions. Small companies such as OSINT Industries, Telemetry Data Labs, Predicta Labs, Epieos, District 4 Labs and others are becoming increasingly popular among analysts. Today's analyst in 2024 isn't looking necessarily for an all-inclusive black box of a work system, but rather a collaborative, intuitive and flexible hub into which she can integrate her tooling.



GeoSpy AI

exemplifies how tailored solutions can enhance OSINT capabilities through customization and integration.

Trend #3: APIs

API-Driven Investigations: The Key to Seamless Integration

This leads us to one of the next points: these smaller, bespoke tools are often API-forward. Standalone tooling chained to a UI is a thing of the past. Analytical and intelligence tools today must be API-forward not only to enable analysts to automate their use of these tools and get the most value out of them, but also to make integration that much easier. Trends and threats today are holistic and multi-vector, and today's analytical tooling is beginning to reflect that.

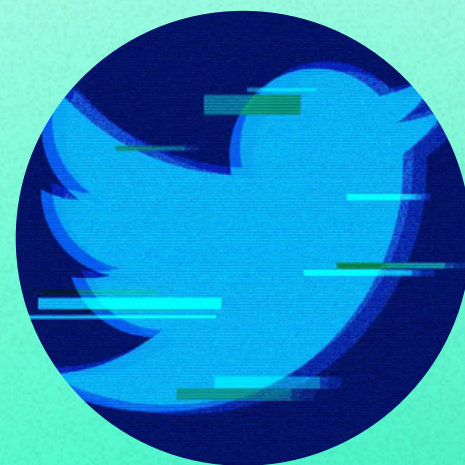


API-first tools are replacing traditional standalone systems, making automation and integration easier than ever.

Trend #4: New Social Media Platforms

Navigating the Shift: Adapting to Emerging Social Platforms

The last major trend is the rise of new platforms and changes in online dynamics. Twitter appears to be losing users to new upstarts such as Mastodon and Bluesky, and the fracturing of the previous global order makes regional platforms, especially in China and Russia, critical. Analysts in 2025 will need to not only be familiar with these new platforms, but also know how to make the most out of them.



Twitter's

decline paves the way for platforms like Mastodon and Bluesky to grow.

Trend #5: Tradecraft

Evolving Tradecraft: Mastering OSINT and Beyond

OSINT

is now a household name, used by professionals across journalism, marketing, law enforcement, and national security.



Tooling for analysts is but one piece of the puzzle, if the most covered. Analytical tradecraft is arguably as important, and 2024 was a banner year for tradecraft as well. OSINT in particular was the main story of analytical tradecraft for 2024, and it shows no signs of slowing down in 2025. OSINT is by now a household name, and its importance in the world of intelligence is widely accepted by everyone, even past skeptics. OSINT is now routinely used by everyone from journalists to marketers to law enforcement officers, national security and intelligence analysts and beyond. OSINT is now more accessible than ever - just check out our list of recommended newsletters to follow [HERE](#) for more information.





New OSINT

training options include niche areas like cryptocurrency investigations and cyber threat intelligence.

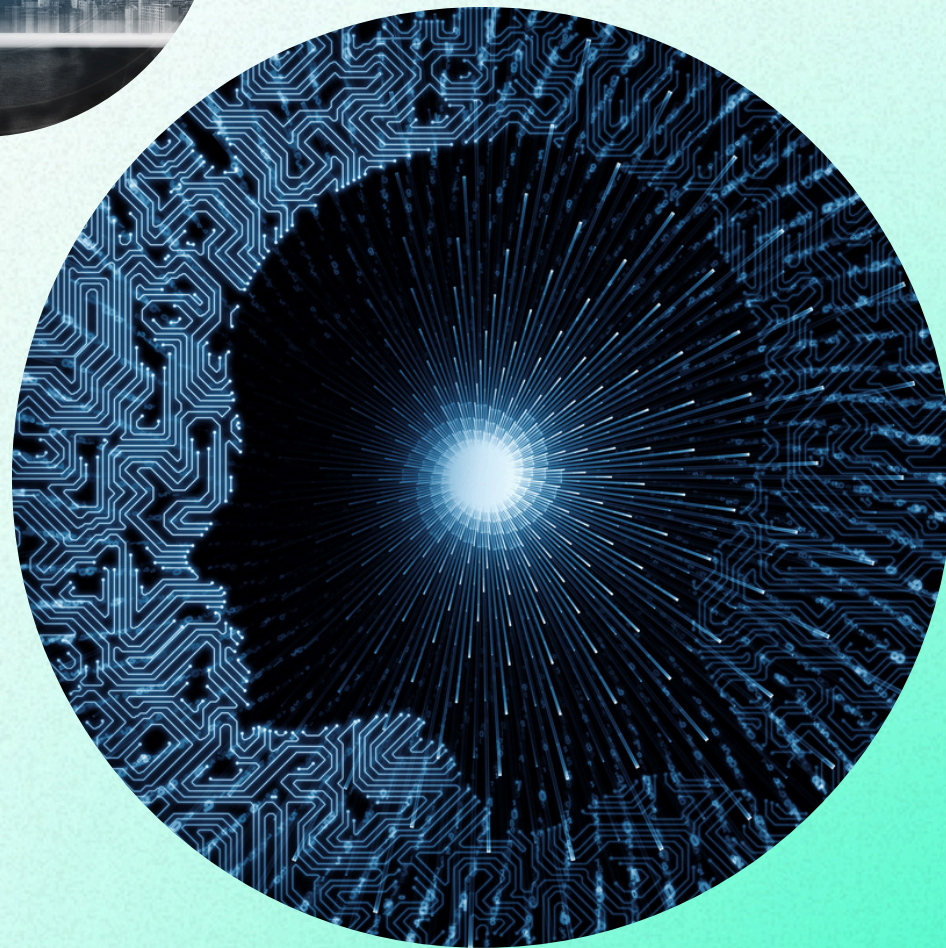
The increasing popularity of OSINT and acceptance of it in professional circles has led to an explosion in the number of OSINT practitioners as well. Training options for OSINT in the private and public sector were once limited to a few veteran providers, but in 2024 the number of providers has grown significantly. Competition in this space is good, as it brings with it new perspectives and more affordable pricing for participants of all backgrounds. Not only has the number of providers grown, but the options for OSINT training have expanded significantly to include niche-specific training, such as cryptocurrency investigations, cyber threat intelligence and more. This is especially relevant as intelligence analysts and practitioners today simply cannot afford to limit themselves to one field of collection or analysis.



For those looking to build robust foundational skills, programs like The OSINT Analyst offer a comprehensive way to stay current in this evolving field. [More information is available here.](#) This is especially relevant as intelligence analysts and practitioners today simply cannot afford to limit themselves to one field of collection or analysis.

Trend #6: Standardization of OSINT for National Security

OSINT Standardization: Building a Framework for the Future



The growth of the community and new training options also leads to new and innovative OSINT techniques being not only invented but also propagated to the general public. 2024 was also a year of maturity for OSINT in the public sector. American and European government and law enforcement agencies are increasingly utilizing OSINT publicly, and are contributing greatly to the standardization of the industry.

2024 marked significant maturity for OSINT, with public agencies driving standardization efforts.



Standardizing OSINT

includes ethical guidelines and strategies, benefiting both public and private sectors."

Standardization of OSINT is a herculean task due to its very nature of including any information publicly available, but the effort is worthwhile. Having ethical and practical guidelines alongside strategies and approaches as to how to get the most value out of OSINT is critical for the public sector, and the effects will have a positive impact on the non-regulated private sector as well. The American Intelligence Community's OSINT Strategy for 2024 exemplifies this by setting OSINT as an "INT of first resort", and sets specific goals for American government agencies. Specific departments and agencies, such as the Department of Defense, have set their own OSINT strategies based on these guidelines. The ODNI's latest publication on standardizing definitions in OSINT is also a welcome addition.

The U.S Intelligence Community's 2024 OSINT Strategy prioritizes OSINT as an 'INT of first resort.

2. Challenges Facing Analysts in 2025

Overcoming the Hurdles: Challenges in Investigations

Today's intelligence analysts are more equipped than ever to counter threats, but that doesn't mean that the threats themselves are going to stay passive or that the threat landscape won't change accordingly.

Challenge #1: Drowning in Data

The Overload of Information: Navigating Bigger and More Complex Datasets

Analysts may be more equipped, more interdisciplinary and more skilled than in the past, but the scene itself is fundamentally changing. The advent of generative AI has led to a sharp increase in the total amount of multimedia content created online, making it difficult to collect and analyze not only quantitatively but also qualitatively - it's harder and harder to tell what's real. To sum it up, datasets are only going to get larger and harder to analyze.



Challenge #2: Threats from Everywhere

Multidisciplinary Threats: Addressing a Converging Landscape of Risks

Threats are also increasingly multidisciplinary and also more quantitative as geopolitical tensions between the West and other countries grow stronger. Nation-states utilize criminal gangs to carry out kinetic operations. Nation-state cyber operators moonlight as cybercriminals and ransomware gangs. A data breach in one country exposes sensitive activity in another. Elections are targeted not only by influence operations but by cyber attacks and even sabotage and physical operations. Analysts must keep up with a huge increase in overall activity, and that activity crosses over from one set or category of activity to another easily. Multimodal and multi-INT analysis thus becomes critical for analysts today and will only be more so in the future.



Challenge #3: Budget Cuts

Doing More with Less: Tackling Resource and Cost Constraints

This increase in activity comes at a time of global economic slowdown. Agencies and organizations are slashing budgets, making fewer analysts work harder with scant resources and tooling. Legal and regulatory constraints are also growing, making it more time-consuming and expensive to access the data one needs to crack a case.



3. Conclusion

Looking Forward: Lessons and Skills for Analysts in 2025

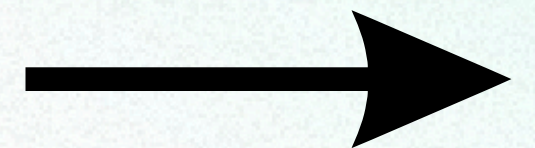
As 2024 ends, investigations continue to change quickly. Analysts face new challenges and opportunities shaped by technology and global events. This conclusion looks back at key lessons from the year and highlights the skills and tools analysts need to stay effective in 2025 and beyond.



Take away items

It's been quite a year to say the least, and we can confidently say that things will only be more interesting next year. Global conflict, terrorism, money laundering and other threats aren't going anywhere, and the broader intelligence field in the public and private sector will probably continue to grow and mature.

What lessons then can today's analysts glean from the past year looking forward to the next? There are many, a few of which we'll list below.





The first trend is the utilization of AI

Tomorrow's analysts don't necessarily need to be the world's best prompt engineers, but they do need to be familiar and well-versed in the use of generative AI tooling, as well as machine learning based tools, in multiple fields so as to ensure that they aren't left behind and can boost their productivity.



Learning how to utilize APIs and basic scripting is also an increasingly key skill.

There's no need to be a dedicated Python developer, but knowing how to utilize Postman, Bash scripting and basic API tooling (alongside a dose of LLMs for script generation) will ensure that any analyst can carry out the basic automation needed to make their lives easier and improve efficiency.



Staying abreast of the internet as a whole is also a key trend.

New platforms in 2024 will continue to grow, and there probably will be new platforms and sources in 2025 that analysts will need to know how to exploit.

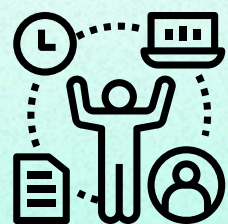


Analysts should also look to hone their skills and expand their analytical skillsets.

Taking advantage of the varied and diverse training options today ensures that tomorrow's analysts won't be stymied by the appearance of a Monero wallet in their investigation.

Grow with Us

Analysts — we've got all the resources you need to stay ahead, including the latest trends, best practices, and more.



[Resources for Analysts:](#)

Discover practical tips, proven methodologies, and expert best practices to enhance your investigative work.



[Courses and Certifications:](#)

Advance your skills with courses tailored to analysts. Learn cutting-edge techniques in investigations, OSINT, and cyber intelligence from leading experts in the field.



[Falkor Investigation Platform:](#)

Leverage powerful investigation software to streamline your work, save time and resources, and achieve measurable results while optimizing your investigative strategies.

Used by analysts and investigators worldwide, Falkor is transforming
the way investigations are run.

See Falkor in action.

Visit falkor.ai

