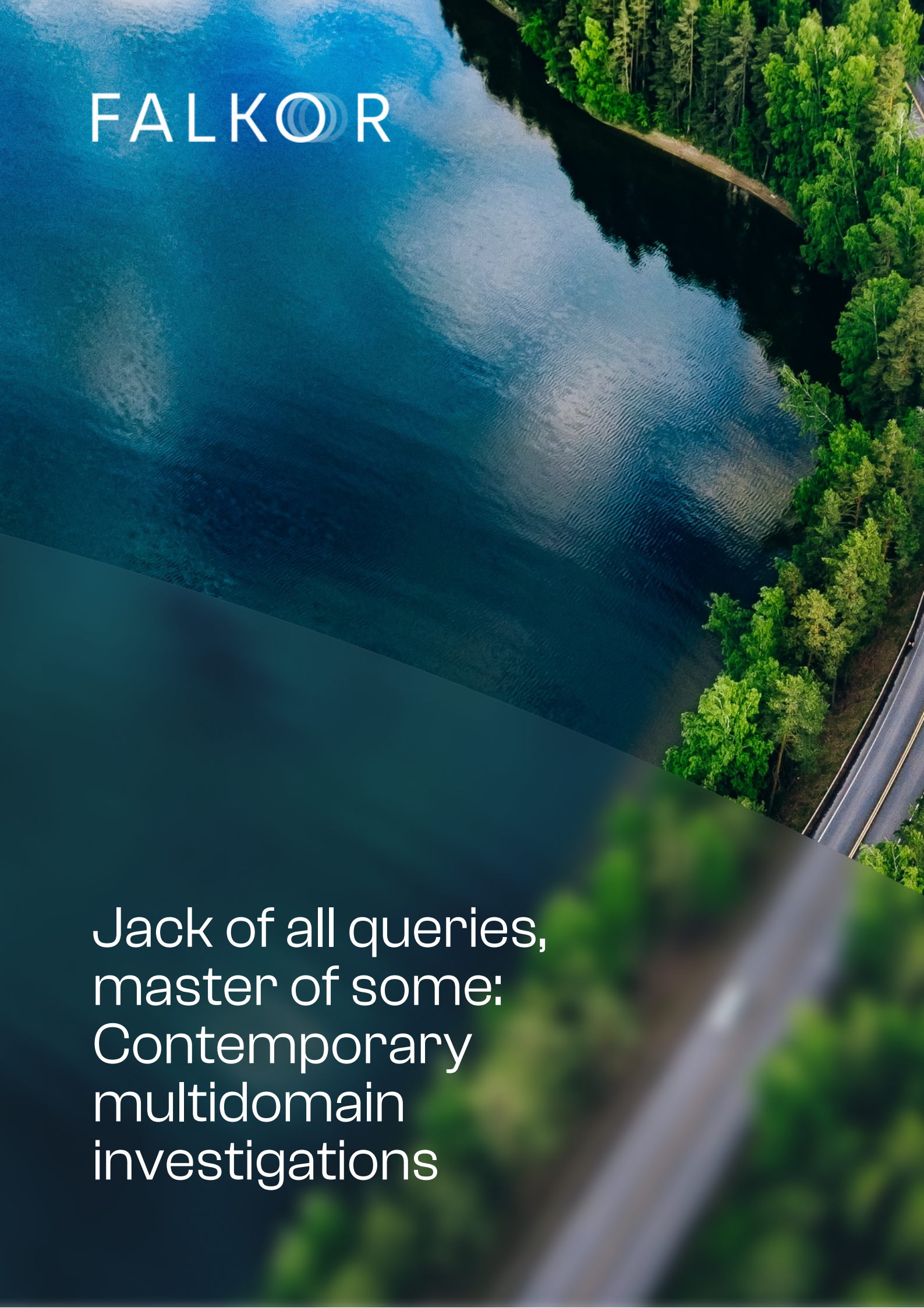


FALKOR

Jack of all queries, master of some: Contemporary multidomain investigations

Introduction

To protect their organization, communities, users and other parties, analysts and investigators must do more than keep pace with the dynamism and sophistication of threat actors. They must exceed them, so they can stay one step ahead.

Today's threat landscape is as deep as it is broad. Threat actors can emerge from any angle, and be equipped with a huge range of skills.

Equally, the data needed to track these threats down can be found on a wide range of platforms, meaning analysts need access to a large and highly diverse dataset.

That means analysts and investigators across all disciplines – from national security to law enforcement and financial crime, to trust & safety and beyond – must develop a skillset that is even broader than their specialization. Additionally, they must be able to collect and analyze data from any source.

But this is easier said than done.

It's now generally accepted that to succeed, analysts must contain multitudes. They must be generalists, able to follow any avenue necessary to find and fix threats. But they must also be specialists, able to dive deep into a discipline and spot the subtle signs that can help them close the case.

On a given day, an analyst might be expected to ingest, analyze, visualize and investigate surface-level data points from a wide number of sources and data types, fusing these various domains into one investigation – and their findings into one cohesive product.

The next day, the same analyst might conduct a deep-dive into a highly specific subfield of investigation, such as looking into complex cryptocurrency transactions or exploring domain registries.

Below, we will explore a few of the investigative domains where today's analysts must develop their skills, in order to stay ahead of threat actors and protect their platforms and their communities.

1. Cryptocurrency and blockchain

Blockchain-based technologies, chief among them cryptocurrencies, are difficult new terrain for analysts.

The workings of blockchain and cryptocurrency are notoriously difficult for outsiders to understand. The ongoing 'crypto winter', the Etherium merge, the collapse of stablecoin, and a number of other paradigm-shifting events have further muddied the waters of the domain.

Cryptocurrency's role in crime

The collapse of cryptocurrency's market value has also shaken public confidence in crypto – and the increasing use of cryptocurrency in illicit transactions has made it a serious area of concern for trust and safety teams, too.

Threat actors are already using cryptocurrency to launder money, skirt sanctions, pay for illegal goods and services, carry out fraud, and much more. As a result, analysts at financial institutions, banks, government agencies and online platforms have had to adapt to the increasingly complex landscape of illicit cryptocurrency use.

Specialized analysts in anti-money laundering, counter-terror finance and other fields have also had to learn the minutiae of blockchain and cryptocurrency in order to stay relevant. For example, blockchain and token-based technologies like Web 3.0, DAOs and NFTs are increasingly important in counter-terror investigations, as threat actors like the so-called Islamic State use NFTs to spread their messages online.

An initial dearth of tools and platforms for cryptocurrency investigations has since prompted a boom in companies aiming to provide analysts with solutions that will help them trace transactions, analyze cryptocurrency wallets and gather data on suspicious activity.

This has empowered analysts with data, investigative tools and training, but hasn't given them the ability to effectively incorporate cryptocurrency investigations into their wider fields of responsibility.

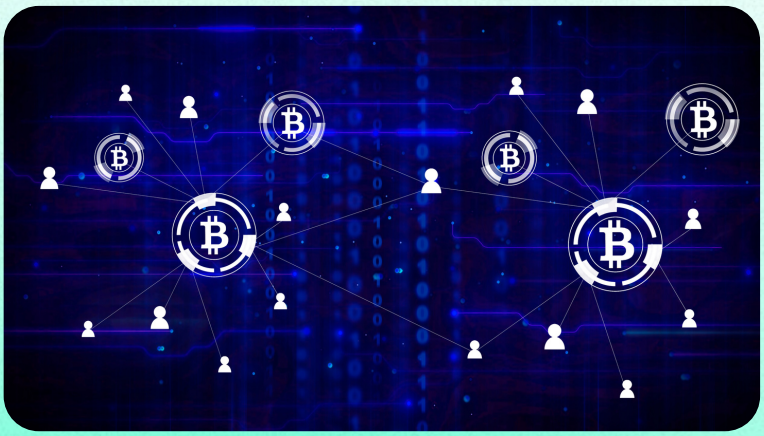
A new challenge: cryptocurrency's role in wider investigations

Incorporating cryptocurrency, NFT and token data into an investigation is harder than it seems.

Understanding the complex web of transactions – often further complicated by the use of anti-tracking technology like cryptocurrency mixers – requires analysts to be able to ingest, process, visualize and investigate massive amounts of technical data.

This data can often only be accessed via specialized blockchain investigation platforms, which allow analysts to run queries and receive their output via the platform UI. However, this UI is often limited and hard to integrate into other workflows. Analysts also often struggle to interface with the platform API and, as a result, receive illegible JSON outputs, which require further beautification or ingestion by external systems. To put it simply, analysts have to either choose between working with limited UIs, or powerful APIs that force them to painstakingly manipulate large datasets.

Incorporating all of this data into one document or spreadsheet is often trickier than it should be; integrating that data with other disparate data points is even more so. Together, these challenges delay and complicate an analyst's ability to complete a holistic investigation and create a comprehensive intelligence product.



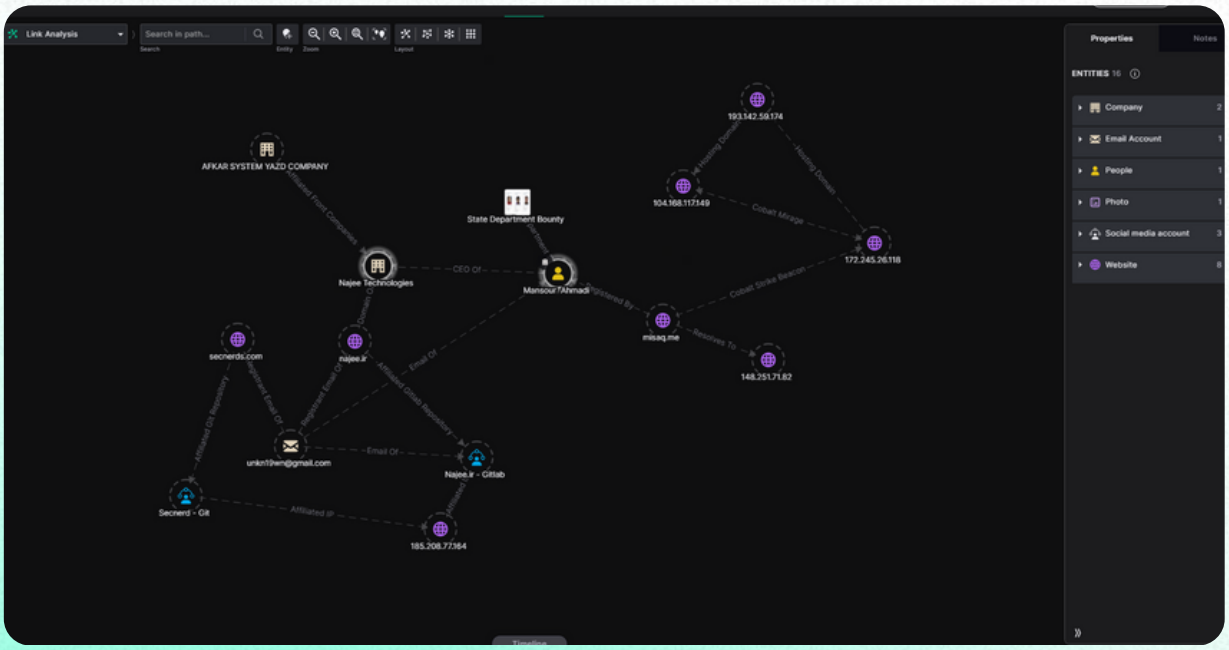
2. Domain analysis

'Domain analysis' refers to the forensic investigation of an online infrastructure, composed of domains, hosts and servers. It could encompass anything from attributing the ownership of a disinformation website to a state actor, to mapping a network of phishing domains or investigating a C2 (Command & Control) server.

It's become a crucial discipline for investigative analysts of all kinds, including information security analysts, thanks to its ability to:

- Expose threat actor infrastructure
- Provide actionable intelligence on malicious activity online
- Empower organizations to proactively protect themselves, their clients, their users, and other stakeholders

But domain analysis is not easy. Investigating a single domain is a challenge; investigating a vast sprawling network is truly daunting.



Falkor system user interface - showing an analysis of domains and related entities

The triple threat domain analyst

To perform an effective domain analysis, an analyst must be skilled in three realms. They must be experienced in investigations and analytical reasoning. Have a deep understanding of information security and network fundamentals. And also be deeply embedded in the wider context of their investigation, whether that is counter-disinformation, financial crime, fraud, or another field.

The absence of proper tools

A veritable menagerie of domain forensics and analysis tools are available on today's market. These serve a variety of industries, from marketing & PR to counter-fraud agencies and news outlets.

These tools vary drastically in their end purpose, their ability to work with different formats and data points, their UIs and their APIs. They also vary in complexity, with many tools offering dozens of features and functionalities.

But most of these tools have two things in common. First, they are usually very expensive. Second, they are often difficult to use, requiring onerous onboarding processes and frequent check-ins from providers to ensure that clients are using the tools to their full potential.

Too much data, too many leads

Similar to cryptocurrency and blockchain investigations, domain investigations suffer from an overwhelming amount of data.

But, in contrast to blockchain or single platform investigations, domains contain multitudes of potential entities of interest and new leads to follow. This further complicates the knowledge and data management of investigations, as well as burdening analysts with a prohibitively large amount of data to investigate.

Properly demarcating domains, let alone delineating the myriad ways by which domains connect to each other, or to different entities, is an exhausting task. Analysts must export data from a wide range of systems, collate that data and store it for further investigations – all without losing track of the wider picture.

3. Messaging applications

Messaging applications have become much more than just ways to communicate. Just look at the meteoric rise of Telegram as an almost full-service platform, offering social media, mass messaging and e-commerce alongside a host of other services. Or the ubiquity of Whatsapp globally alongside desktop-oriented platforms like Discord and Matrix.

This new global stature has made messaging platforms key to investigations.

Dark web marketplaces have migrated to messaging applications. Global extremist groups rely on them to recruit and communicate. Threat actors use them to spread disinformation on a massive scale.

This poses a challenge to analysts for a number of reasons.

Many messaging applications and platforms make gaining entry to their ecosystem very difficult for analysts – and accessing data even harder. In contrast to social media, which is mostly searchable (albeit to a minimal degree), messaging platforms tend to operate on an invitation-based system. Closed chats can only be accessed by accounts that request to join and are approved. Most messaging applications don't have a built-in search feature; those that do usually limit their search to group or channel titles, rather than the content of the chat itself.

Even if analysts *can* access this data, the pool of content is almost unimaginably vast. Analysts that gain access to a key chat group or channel may then need to scrape or export millions of messages and hundreds or even thousands of user profiles.

Storing, let alone analyzing, this data in any readable fashion is yet another challenge. With so much data to comb through, furthering the investigation becomes like finding the proverbial needle in the haystack.

A new challenge: balancing insight with compliance

It's vital for analysts to keep their finger on the pulse of these varied and complex domains – but doing so is far from easy.

Succeeding means staying up to date with the latest in operational security and information security. But, even more importantly, it also means ensuring full compliance with legislation and regulation on everything from individual rights to court rulings on investigative practices.

Some of these regulations have been known to analysts for years, but they must also keep up with a never-ending flow of new developments and regulatory changes.

Recent legislation like the GDPR and DSA, along with expected future legislations and regulations, mandate that analysts must investigate ethically and in compliance with best practice data management methods and tools. Analysts today must ensure that their data is relevant, stored securely and for legitimate purposes, and maintained with full oversight and careful auditing.

At first, this task sounds comparatively easy, compared to the other challenges that analysts face. But, in today's era of big data collection and utilization, staying ahead of bad actors while maintaining compliance with regulations can be incredibly difficult.

How is the industry responding to these challenges?

In short, today's trust and safety teams face two major challenges: tackling complex multidomain investigations, and doing so while remaining compliant with the regulatory landscape.

Expanding the analyst's skillset

In response, there are numerous public efforts currently underway to help analysts refresh and expand their skillset, so that they can counter the neverending multitudes of threat actors entering the arena. These efforts might take the form of webinars, conferences, workshops or training sessions. They attempt to address the challenge in a number of different ways: some focus on inter-specialty collaboration. Others seek to train analysts and investigators on new technologies, tools and methodologies. And still others coach analysts on the principles of information sharing within and between teams and organizations and specialized structured analytic techniques.

At the same time, analysts in the public and private sectors are actively investing in expanding their skillset via collaboration, private-public partnerships, training opportunities and conferences.

No evolution in the analyst's toolkit

In comparison to the rapid expansion of the analyst's skillset, the investigative toolkit for trust and safety investigations looks static by comparison.

The industry has generally tended to support analysts by providing them with tools that help them collect data at larger and larger scales. Some tools go one step further and attempt to help them analyze and process that data. But this is often done in a siloed fashion, or in a way that is restricted to specific fields – or even subfields – of the data.

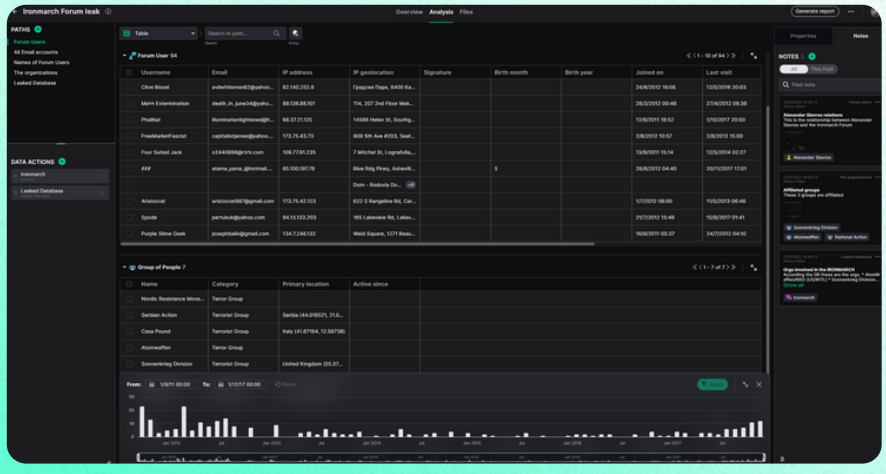
As a result, analysts are often forced to resort to spreadsheets and word processors to store their data and reports, and find themselves retrofitting tools from other industries to fit their needs.

The future of multidomain investigations: fusing the domains

The real challenge for analysts is not just understanding cryptocurrency, domain investigations and messaging platforms well enough to investigate them. It's having the breadth and depth of knowledge needed to understand how each domain interacts with a wider investigation, in conjunction with a host of other domains and context.

The quest to fuse all of this information and data into a cohesive and clear final intelligence product forces analysts to store their data in legacy and outdated formats and programs, simply because they offer some of the flexibility they so desperately need. There are some – usually industry-specific – platforms available for this purpose. But these are mostly legacy systems with cumbersome UIs and feature sets or toolboxes that belong more to yesteryear than modern investigations.

Falkor system user interface - the Map, Table, and Timeline views



This is where Falkor comes in.

Falkor is a data-driven analytics, knowledge management and investigation platform that empowers analysts to run flexible, collaborative, dynamic, secure and regulation-compliant investigations.

The platform works with any type of data, in any format, to ensure that analysts can upload and analyze relevant data points in their investigations. Whether it's a cryptocurrency transaction, a WHOIS registration change, or a post on a messaging platform, it all sits comfortably in Falkor.

Once data is uploaded and analyzed, it can then be fused automatically or manually with any other relevant datapoint in Falkor's database, providing full data visibility and auditing to analysts.

It's a tool that's built for modern investigations: adaptable, flexible, and powerful enough to help analysts stay one step ahead of the threat landscape.

Discover the future with Falkor

Visit falkor.ai or contact us at hello@falkor.ai