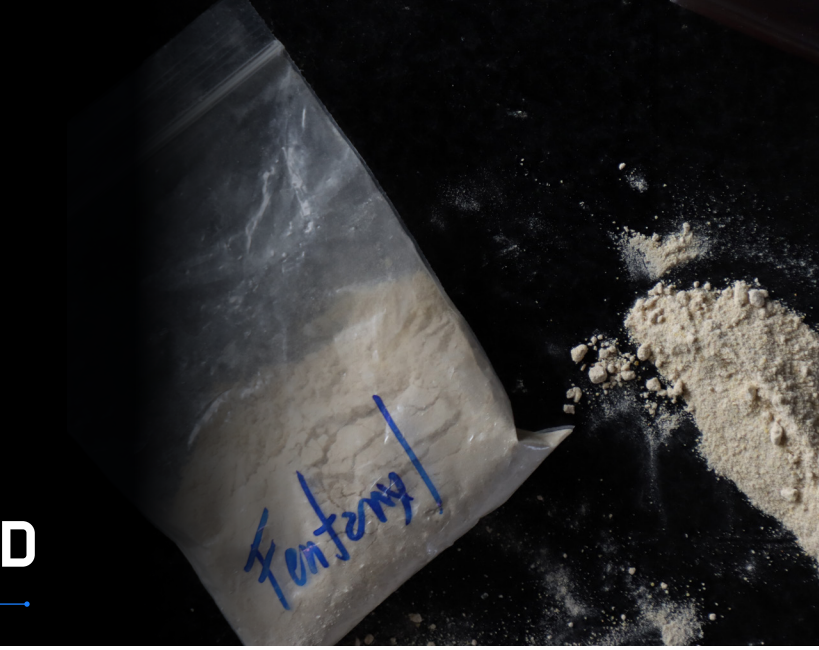
FIVECAST SAYARI

CASE STUDY

COMBINING DIGITAL FOOTPRINT DATA + PUBLIC RECORDS: FENTANYL UNCOVERED



INTRODUCTION

The global fentanyl crisis poses a grave threat to public health and national security. Its production and distribution pipeline is complex and involves a myriad of actors: chemical suppliers in places like China and India, brokers who connect criminal groups to chemical suppliers, and Mexican transnational criminal organizations that leverage their logistical infrastructure to get large quantities of fentanyl to market.

However, the illicit supply chains that feed precursor chemicals and pill manufacturing equipment often leave a corporate and digital footprint on the open web that can be exploited by investigators. Chemical suppliers register front and shell companies to legitimize their activities, while shipments of precursor chemicals and pill manufacturing equipment appear in import and export records. As such, investigators require access to a broad suite of publicly available data that, when used together, paints a comprehensive picture of these networks and their supply chains.

Fivecast's AI-enabled OSINT platform continuously monitors vast volumes of online content - including social media, forums, and dark web sources to detect emerging threats and behavioral shifts in real time. Sayari's flagship investigative platform—Sayari Graph—provides billions of global corporate and trade records in a graph database, enabling analysts to uncover legal entities, cross-border ownership structures, and trade flows. When used together, these platforms empower investigators to target, disrupt, and dismantle the illicit supply chains fueling the fentanyl crisis.

In this paper, we illustrate how Sayari and Fivecast analysts leveraged both platforms to expand the network behind a recently indicted Chinese company that U.S. prosecutors allege illegally imported pill-making equipment into the United States. The combined insights from Fivecast and Sayari enabled the identification of key actors and exposure of the digital, corporate, and logistical infrastructure supporting the operation. The analysis serves as a case study for how investigators can use the data from both platforms to enhance the efficiency and effectiveness of investigations into illicit fentanyl supply chains.

U.S. PROSECUTORS TARGET CAPSULCN

In May 2025, a grand jury returned a 21-count indictment charging CapsulCN International Co., Ltd. ("CapsulCN") and two principals for their role in illegally importing fentanyl pill-making equipment into the United States [1]. The equipment included pill presses, encapsulating machines, and die molds, which are used to manufacture fentanyl-laced pills that mimic licit pharmaceuticals.

According to U.S. prosecutors, the network leveraged numerous websites, e-commerce sites, and social media accounts to advertise and sell pill-making equipment. CapsulCN also conducted business via various trade names, and took steps to obfuscate shipments of pill-making equipment in trade records.

[1] "Chinese Company and Three Chinese Nationals Indicted for Unlawfully Importing Pill-Making Equipment Used to Manufacture Controlled Substances," U.S. Department of Justice, May 12, 2025, https://www.justice.gov/opa/pr/chinese-company-and-three-chinese-nationals-indicted-unlawfully-importing-pill-making

UNCOVERING A DIGITAL FOOTPRINT

Identifying key actors involved in fentanyl supply chains is challenging due to deliberate efforts to obfuscate their true identities and operations. These entities often use sock puppets and fake online personas, misrepresent their products, and present themselves as legitimate businesses - such as CapsulCN and iPharmachine - selling research chemicals and lab equipment. Their employees, business partners, and shipping behaviors are carefully masked, making it difficult to link them to fentanyl trafficking operations.

Fivecast collaborated with a national security agency that flagged a suspicious online account. Acting on this tip, Fivecast analysts used Fivecast ONYX to identify and analyze the digital footprint of CapsulCN and its affiliates, including iPharmachine and Huada Pharma. The investigation uncovered a network of social media accounts - many featuring identical branding, logos, and promotional content crafted to resemble legitimate businesses. These accounts frequently shared contact details and cross-promoted one another, generating valuable leads for further investigation.

Using Fivecast's Discovery and Network capabilities, analysts mapped relationships between these accounts and uncovered additional entities interacting with them. This included sock puppet accounts, distributors, and potential customers, revealing a broader digital ecosystem supporting the illicit trade.

Fig. 1: iPharmachine and Huada Pharma are no longer operational due to the domains being seized by Homeland Security Investigations (HSI).

Fig. 2: Screenshot taken from ipharmachine [dot] com which purports to require DEA approval before shipping a capsule-filling machine.

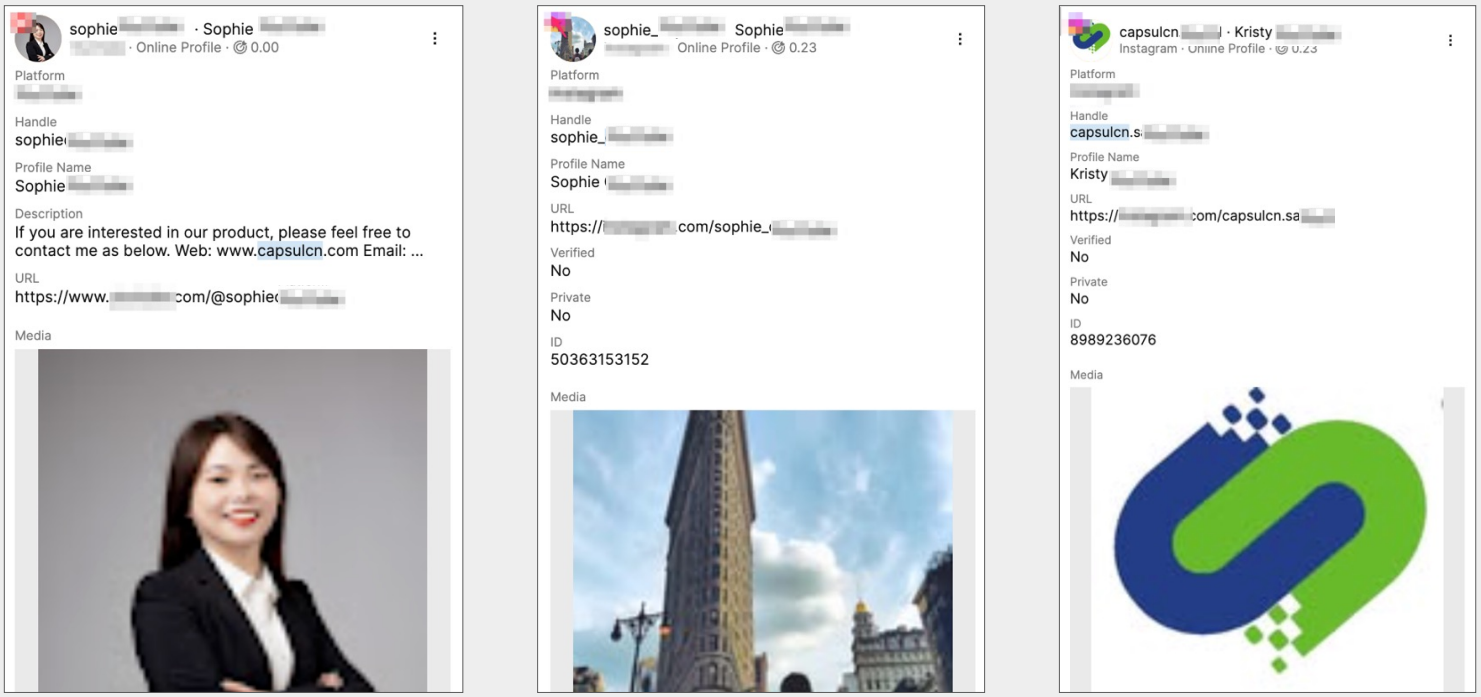


Fig. 3: The accounts above are affiliated with CapsulCN and posted across multiple social media platforms- advertising additional means to get in contact, their various websites, and linking to other accounts. Some of the companies they affiliated themselves with were iPharmachine and Huada Pharma.

UNCOVERING A DIGITAL FOOTPRINT CONT.

As seen in the network screenshot, many of the social media platforms affiliated with CapsulCN used the same logo, making their affiliation easily identifiable. CapsulCN operated numerous social media accounts, many of which were fake or impersonated individuals. By leveraging the Fivecast ONYX network analysis, investigators uncovered mutual connections and related entities. These leads could then be further explored using either Sayari or Fivecast ONYX.

Fig. 4: Branding demonstrating the connection between Capsulcn, ipharmachine and Huada Pharma

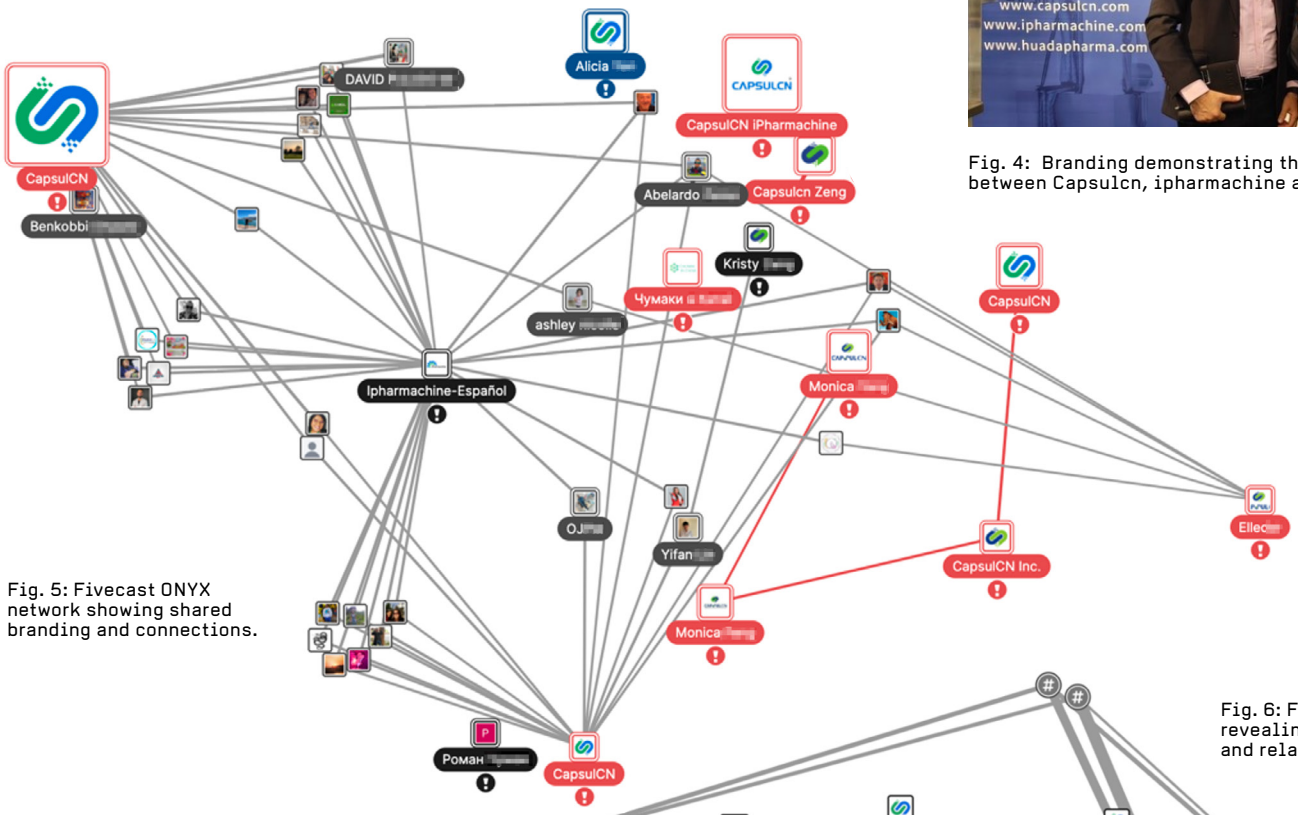


Fig. 5: Fivecast ONYX network showing shared branding and connections.

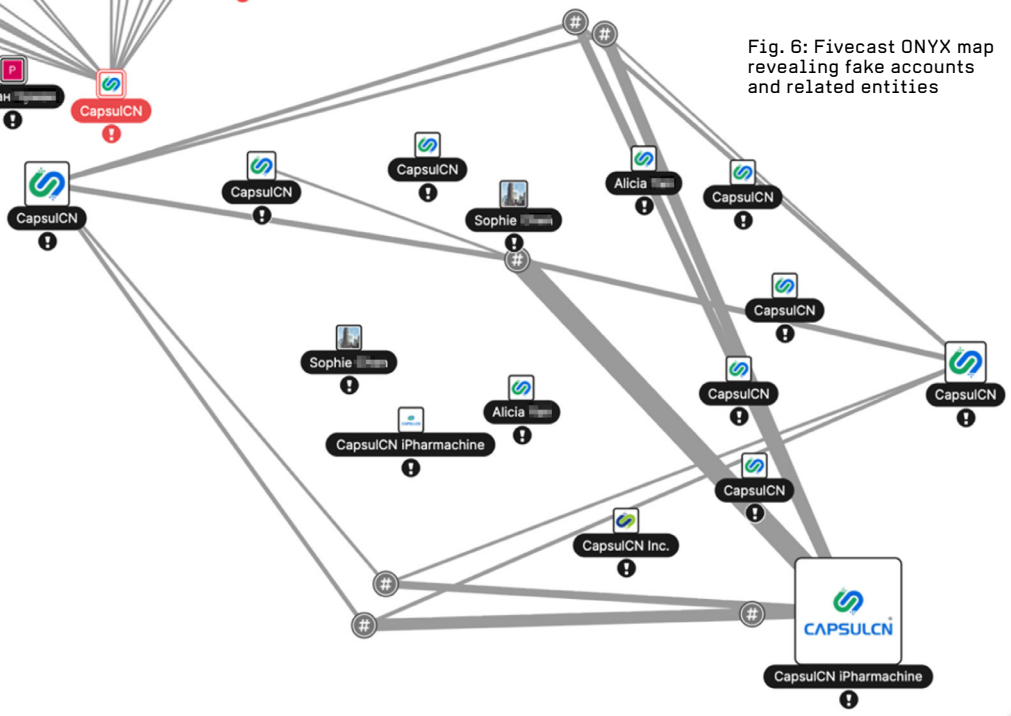


Fig. 6: Fivecast ONYX map revealing fake accounts and related entities

BY LEVERAGING THE FIVECAST ONYX NETWORK ANALYSIS, INVESTIGATORS UNCOVERED MUTUAL CONNECTIONS AND RELATED ENTITIES.

FROM DIGITAL FOOTPRINTS TO CORPORATE RECORDS

After surfacing a comprehensive digital footprint in Fivecast ONYX, we then pivoted to Sayari Graph to build out the corporate and trade networks behind the identified entities. This complementary approach revealed the corporate and logistical infrastructure supporting the operation.

A search for “CapsulCN” in Chinese corporate registration databases, however, yields no results. This immediate lack of a direct match is a common, often deliberate tactic by illicit networks that operate under informal trade names or unregistered shell entities to obscure their true identity and circumvent scrutiny in international trade.

The key to identifying the real entity behind CapsulCN emerges from a pivot to Chinese intellectual property (IP) data. Examination of Chinese IP records reveals a crucial link: four distinct trademarks registered for the CapsulCN brand. Critically, all four of these trademarks are held by a single, verifiable, and legally registered entity: Zhejiang Shanfan Machinery Co., Ltd. (Zhejiang Shanfan). This connection establishes the foundational corporate identity behind the CapsulCN brand name, effectively linking a seemingly phantom operational entity to a verifiable legal structure.

Once we’ve identified the core legal entity, we can quickly and accurately identify the natural persons behind this entity, including the ultimate beneficial owner (UBO). In this case, Chinese corporate records indicate that an individual named Pan Xiaochuan is the ultimate beneficial owner of Zhejiang Shanfan via an apparent Chinese holding company. An individual named Pan Xiochuan is one of the indicted principals identified in the Department of Justice (DOJ) press release, strongly suggesting that the UBO of Zhejiang Shanfan is the same individual as the indicted co-conspirator.

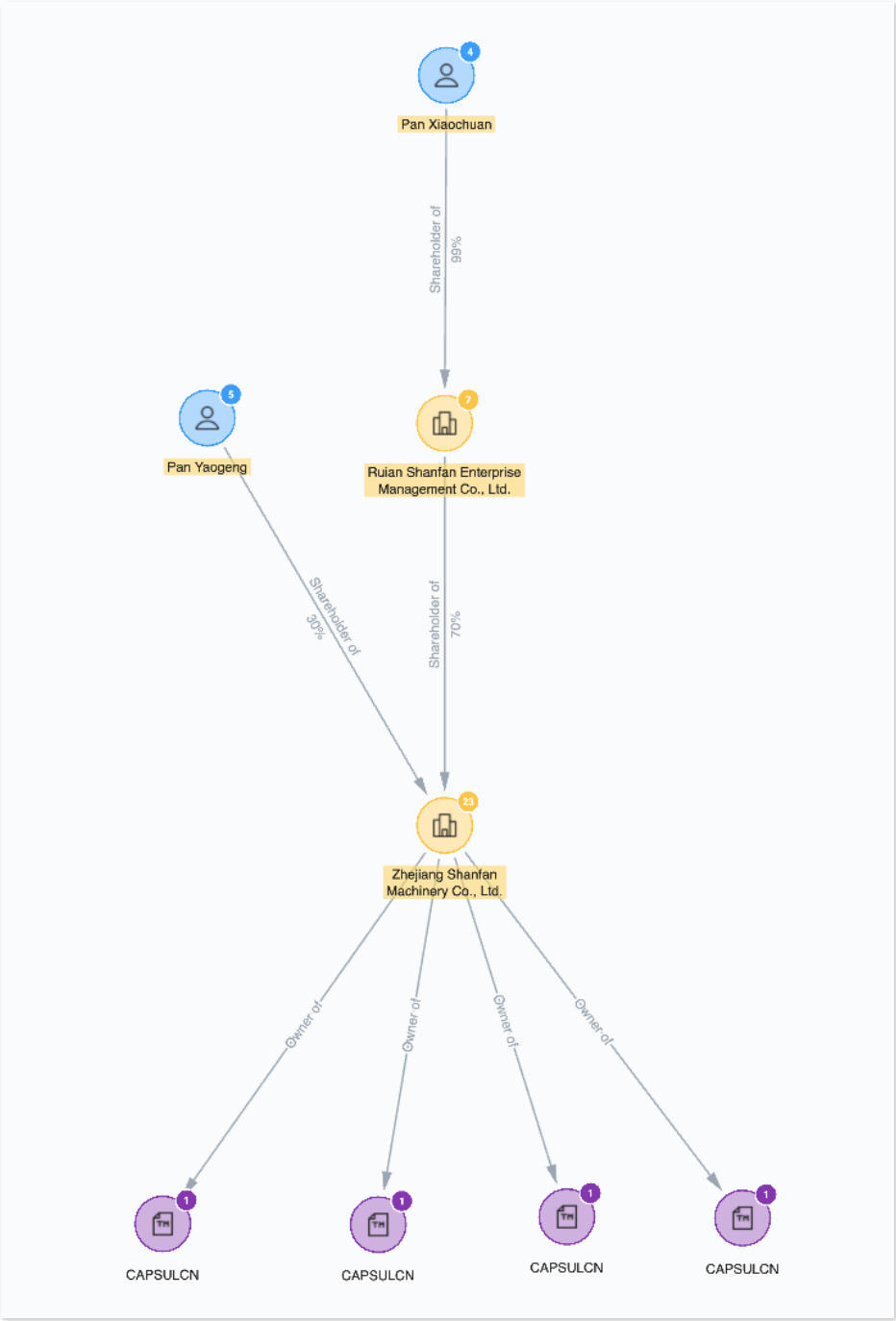


Fig. 7: Sayari Graph network chart illustrating CapsulCN’s global corporate footprint comprising entities incorporated in China, the U.S. and UK.

Moreover, additional website names identified in Fivecast ONYX provided leads into CapsulCN-linked legal entities operating beyond China, underscoring the intricate global systems through which these networks operate.

Huada Pharma and iPharmachine, two websites identified by Fivecast as having marketed pill manufacturing equipment that were later seized by U.S. authorities, match the names of legal entities established in Southern California and London, suggesting CapsulCN likely used these entities as vehicles to conduct business in those jurisdictions.

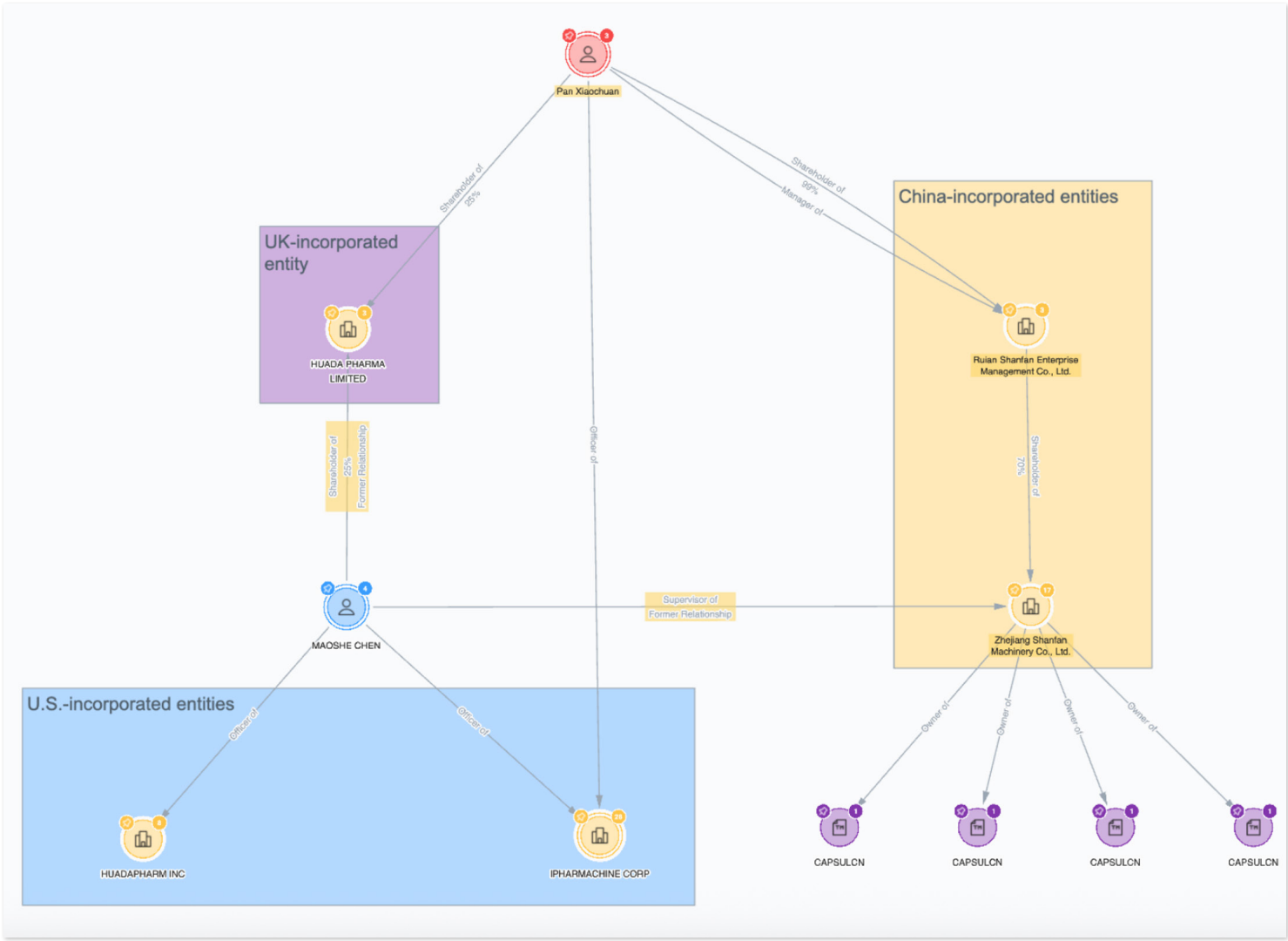


Fig. 8: Sayari Graph network chart illustrating CapsulCN's global corporate footprint comprising entities incorporated in China, the U.S. and UK.

Networked corporate data also identified additional related parties of interest. For example, an individual named Maoshe Chen appears as the current officer of Huadapharama and iPharmachine Corp in Southern California, the former shareholder of Huada Pharma Limited in the UK, and the former supervisor of Zhejiang Shanfan . Maoshe Chen has not been identified in any of the charging documents related to CapsulCN, but their connection to a number of entities in the CapsulCN network suggests they may warrant additional investigation.

MAPPING CAPSULCN'S SUPPLY CHAIN WITH TRADE DATA

Combining corporate and trade data enabled us to identify the international buyers of pill-making equipment from the CapsulCN network, providing leads into additional entities that may be sourcing this equipment for illicit purposes.

Between roughly February 2019 and July 2025, the CapsulCN network exported over 700 shipments to entities across over 20 countries, a vast majority of which were for goods or equipment related to pill manufacturing. Of the more than 700 shipments, over 50 percent were sent to the U.S. and Mexico. It's important to highlight that shipments of pill presses, encapsulating machines, and other pill-making equipment are not, in themselves, indicative of illicit activity. Therefore, investigators should always analyze these shipments within the context of other potential risk factors, like an importer's stated business purpose, registered address, and/or their broader import history.

Notably, the number one U.S. importer of pill-making equipment from CapsulCN entities in China was iPharmachine Corp, one of the CapsulCN-linked entities. iPharmachine Corp is registered at an apparent storage facility within a business park in Garden City, California, suggesting iPharmachine Corp may have stocked this storage facility with pill-making equipment to more quickly process U.S.-based orders.

In addition, trade data identified several entities that appear to be potential aliases or related trading arms of Zhejiang Shanfan, including:

- Zhejiang Capsulcn Machinery Co. Ltd.
- Capsulcn International Co. Ltd.
- Zhejiang Capsulcn Imp&Exp Co Ltd
- Wenzhou Capsulcn Imp&Exp Co Ltd

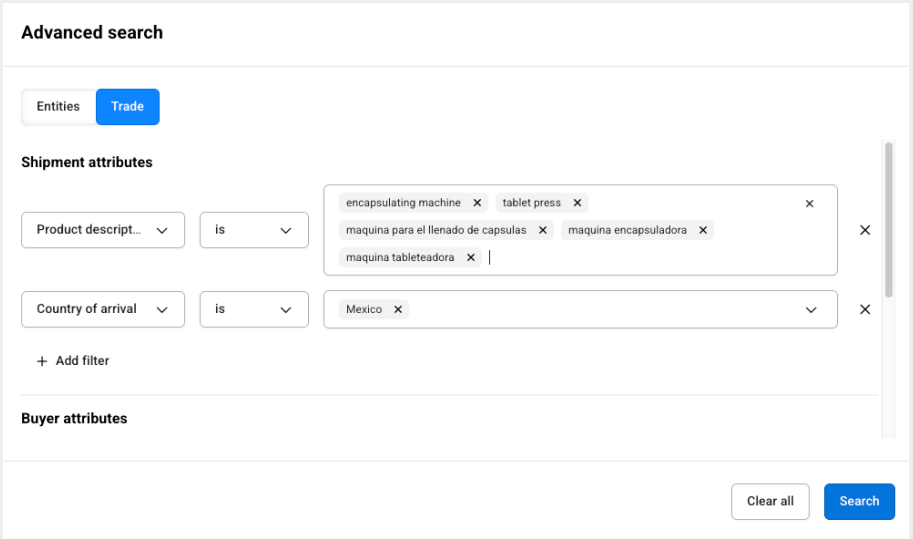
This pattern of using multiple trading entities, often with slight name variations, is a common tactic employed by illicit networks to manage reputation, diversity shipping routes, and introduce layers of obfuscation that complicate traditional law enforcement targeting.

LEAD GENERATION AT SCALE

Finally, we can apply what we know about publicly identified illicit networks and their corresponding trade typologies to query global trade data at scale and unveil other potential networks and entities of interest.

Sayari Graph allows users to query HS codes, product descriptions, arrival and departure countries, suppliers and buyers, among other data fields, against global trade data from over 70 jurisdictions.

For example, if we were interested in identifying persons or companies that may be supplying Mexican cartels with pill manufacturing equipment, we could run a query looking for shipments of tablet presses and encapsulating machines imported into Mexico.



A snapshot of the Advanced Trade Search in Sayari Graph. The query sets parameters to identify all shipments in Sayari Graph that include at least one of the key terms provided for certain pill manufacturing equipment that have been imported into Mexico. Search terms are included in both English and Spanish to capture shipments sourced to Mexican trade records, which are typically reported in Spanish.

The search yields over 300 Mexican buyers and over 250 foreign suppliers that imported/exported shipments including at least one of the above search terms to Mexico. Again, most of this equipment was likely destined for a legal end use. However, when paired with other potential red flags, the query can and does surface leads into entities that may be at risk of supplying Mexican cartels with pill manufacturing equipment.

For example, the query identified at least one Mexico City-based freight forwarder that, in September of last year, imported at least one shipment described as a "machine used to fill capsules" from a Chinese supplier, according to Mexican import records available in Sayari Graph.

Moreover, between 02 Jan 2024 and 06 May 2025, the same Mexico City freight forwarder imported roughly 350 metric tons of chemicals commonly used to produce methamphetamine, including tartaric acid, methyl formamide, and benzyl alcohol. The combination of imports containing known methamphetamine precursors along with at least one shipment of an apparent encapsulating machine by a Mexico-based logistics firm raises significant questions as to the ultimate end use and end users of these chemicals and equipment.

CONCLUSION

Illicit actors are deploying increasingly sophisticated tactics to evade trade controls. A key method is via corporate camouflage, which involves operating under a variety of fake trade names and online personas while using legitimate companies as a front. Disrupting these nimble and opaque networks requires more than traditional enforcement: it demands advanced investigative tools capable of uncovering hidden relationships and generating actionable intelligence at scale.

Sayari Graph equips analysts to interrogate billions of trade and corporate records, allowing for detailed and streamlined insight into the networks and supply chains illicit actors employ to operate within the noise.

Fivecast ONYX complements this capability by surfacing online indicators of risk across social media, forums, and the deep and dark web. Its AI-enabled analytics uncover intent, affiliations, and behavioral patterns linked to illicit fentanyl operations and other transnational threats.

By fusing these two data streams, investigators are able to more quickly and effectively identify, disrupt, and dismantle global illicit networks.

ABOUT FIVECAST

The mission of Fivecast is to enable a safer world. As a world-leading provider of open-source intelligence solutions, Fivecast helps the world's most important public and private organizations collect and explore masses of online data, uncovering actionable insights which are critical to protecting global communities.

ABOUT SAYARI

Sayari is the transparency company providing the public and private sectors with immediate visibility into complex commercial relationships. Drawing on a decade of innovation and support from industry-leading investors, Sayari delivers the largest commercially available collection of corporate and trade data as a dynamic, living model of global ownership and trade activity. Sayari's solutions harness this model to enable risk resilience, complex investigations, and clear-eyed business decisions.

Sayari is headquartered in Washington, D.C., and its solutions are trusted by Fortune 100 companies, financial institutions, and governments in over 35 countries. To learn how Sayari powers safer global commerce, please visit sayari.com