2ND & 3RD QUARTER ISSUE /2022

TAPA

SPECIAL EDITION

THE TRANSPORTED ASSET PROTECTION ASSOCIATION
THE AMERICAS

CHAIR'S MESSAGE

W. Allen Gear, Chair of The Americas

Dear Members,
As we approach the busy Fall and Winter seasons, we hope everyone had the opportunity to spend quality time with friends and family. Given the stressful nature of our jobs and the world's events, it's essential to take the time to reflect and refresh.

Our organization remained busy in Q2 and Q3, moving forward with exciting initiatives and events. And, with many members on vacation this summer, we decided to bring you a consolidated and comprehensive special edition of the TAPA AMERICAS Newsletter.

BOARD OF DIRECTORS
Our Board worked hard to update the association's bylaws. The final version was approved by the membership earlier this month. The bylaws guide the Board's actions and decisions. Annually, we review the bylaws to ensure we protect the organization from potential problems by clearly outlining rules around authority levels, rights, and expectations.

We also worked with our committees to ensure progress continues in the development of the Freight Broker Standards, Parking Security Standards, and web-based training.

TRADE SCHOOL EPISODES
Over the previous months, we continued to offer timely and informative Trade School episodes. The global trade specialist, Pete Mento, shared his trade, compliance, and economics expertise in the following episodes.

- *Demurrage and Detention and the Ocean Shipping Reform Act*
- *Gas Prices, The Energy Crisis and Logistics.*
- *Dealing With Modern-Day In-Transit Vulnerabilities*
- *21st Century Customs Framework (21CCF)*
- Global Economic Update

You could watch our TRADE SCHOOL LIBRARY recordings if you missed any live episodes at https://www.tapaonline.org/trade-school-library.

WEBINARS & TRAINING
The second and third quarters continued web-based learning through these live and recorded webinars and interactive Standards training courses.

- *Emerging Technology Trends: Asset & Cargo Theft Protection*
- *TAPA Cyber Security Standards (CSS) Training*
- *Facility Security Requirements (FSR) Standards Training*
- *Trucking Security Requirements (TSR) Standards Training*

2022 T1 NATIONAL CARGO THEFT CONFERENCE

The highlight of these two previous quarters was our 2022 T1 NATIONAL CARGO THEFT CONFERENCE. The Peabody Hotel, Memphis, was a beautiful location for our June 14-15 event.

Some highlights from the conference were:

- Cargo Crime Intelligence Update
- Operation Boiling Point: HSI's Response to Organized Retail Crime, Organized Theft Groups & Supply Chain Security
- Cyber Security Threats: A Risk to the Supply Chain
- Emerging Technology Trends in Theft Prevention
- Intelligence Services, Commercial Auto Crime Bureau, Peel Regional Police of Canada
- Memphis Cargo Theft Task Force
- Kentucky State Police
- Miami-Dade Police Cargo Theft Task Force

TAPA AMERICAS ANNUAL AWARDS

I was privileged to present our annual awards during our T1 National Cargo Theft Conference. This year, Andrew Parkerson received the *Annual Chairman's Award.* Andrew was recognized for his outstanding service, dedication, and commitment to leading the first TAPA Cyber Security Standards.

It was my great honor to present Taya Tuggle with the *Lifetime Achievement Award* in recognition and appreciation of her outstanding service, commitment to Standards training over several years, and leadership to further the organization's goals.

We are proud to honor our volunteer members who go above and beyond in their commitment to our volunteer-led organization each year. This year, Greg Haber, with Babaco, and Chirag Shah, with Sanofi, were presented with the *Volunteer of the Year Awards* in recognition and appreciation of their time, resources, and leadership contributions.

TAPA AMERICAS LAW ENFORCEMENT AWARDS

In 2019, TAPA AMERICAS established a law enforcement recognition committee, which recognizes law enforcement officers and supply chain security agents who have made significant contributions to the furtherance of supply chain investigations. Recipients were selected based on their outstanding investigative techniques, industry collaboration, initiative, and effort above and beyond customary job duties within the last 18 months.

The two award recipients were honored at the TAPA National Cargo Theft Conference in Memphis: Gil Gasco, Investigator, California Highway Patrol Inland Cargo Theft Interdiction Program Taskforce, and Manny Garza, Director, Customs-Trade Partnership Against Terrorism (C-TPAT).

IN CLOSING

I want to thank all of you who have participated in our organization's events, projects, and committees. I look forward to sharing the many future events and updates over the coming months.

Most sincerely,

W. Allen Gear
Chair, TAPA AMERICAS

THE RISE OF DOUBLE BROKERING

Q&A with Scott Cornell, Transportation Lead at Travelers

Q: We're seeing an increase in thefts tied to double brokering. Can you talk more about how these thefts are happening?

Scott Cornell: Double brokering is becoming a hot topic across the transportation industry, and we are seeing a lot of it. Many things can go wrong when loads are double-brokered, but there are three common scenarios when it comes to the theft of a load.

The first scenario involves doing everything right on your part, including the necessary vetting process of carriers you work with, but the company you hire to transport your load double brokers it to a fraudulent group that steals it.

The second scenario is identity theft. This occurs when someone steals the identity of a legitimate trucking company and then bids on your load. Without being aware of the scam, you assign them the load, and they steal it.

The third scenario is a bit more complex. A fraudulent group steals the identity of a legitimate trucking company, and you assign them the load. The fraudulent group now pretends to be a freight broker and turns around and re-brokers the load to another legitimate trucking company, using that company to deliver the load to a location where it can be stolen. In this situation, the legitimate company typically has no idea that they are being involved in a scam.

Scott Cornell, Vice Chair - TAPA Americas
Crime & Theft Specialist

These scenarios reinforce the importance of vetting a carrier in the brokering process to help prevent theft.

Q: What factors could be contributing to double-brokering scams?

Scott Cornell: The freight broker segment of the transportation industry has seen tremendous growth over the past several years. For a freight broker that is growing exponentially, there is an urgency to move freight, hire new employees, build new facilities, gain new clients and keep up with customer demands.

Sometimes when an industry or company grows rapidly, the focus is on continuing to grow the business to match the demand, while some best practices, such as maintaining a proper vetting process of carriers you work with, can be overlooked. As the business expands, it's important to uphold and, in some cases, evolve the policies and procedures that you have had in place in order to protect the business and match the sophistication of your new clients.

One of the main ways a freight broker can become liable for a loss or theft is the improper vetting of carriers. If you hired the thief, there is a good chance that you will be liable for that load, so it is critical to maintaining a proper vetting process for efficient and successful growth.

Q: Are there standards that freight brokers or intermediaries can use to keep their vetting process aligned with their level of sophistication, growth, and volume?

TAPA, in collaboration with a number of other leading organizations including Travelers, is creating a new set of broker security standards to address this issue.

These standards will teach you how to build your vetting team, what resources are available for your vetting process, best practices on how to use them, techniques for training your staff and keeping them up to date, and how to better manage double brokering.

Q: When will these standards be released?

The new standards are in the final stages of development and will hopefully be released soon. These broker standards will be the newest in TAPA's series of other go-to security standards for the transportation industry.

About Scott Cornell
Scott Cornell, National Transportation Lead, Crime & Theft Specialist, at Travelers, has more than 25 years of experience in the transportation and insurance industry. He helped create Travelers' Special Investigative Group, a cargo theft unit unique to Travelers' clients. He is also vice chair of the TAPA Americas Board of Directors, leading its Intelligence Information Services program.

TAPA APAC – GATHERING AT WORLD EXPO AREA TO LINK THE WORLD

Mr. Alan Liu
TAPA APAC, Board Member

On 28th July 2022, Chief Representative of Transported Asset Protection Association Asia Pacific (Singapore) Shanghai Representative Office (hereby known as TAPA China), Mr. Alan Liu, was given the opportunity to present to the Development of New Bund Global Economic Organization Cluster ("GOC") Conference at the New Bun World Trade Center.

Hosted by the Pudong New Area Commerce Commission and the Shanghai Free Trade Zone World Expo Administration (undertaken by the Lujiazui Group), the conference saw more than 50 representatives and leaders across relevant commissions, offices, and organizations, including the deputy chief of Pudong New Area.

Mr. Liu represented TAPA and delivered a speech given the theme, "Gathering at World Expo Area to Link the World." He introduced TAPA with a detailed narration of its origin story, purpose, and mission. Furthermore, he spoke on the impact of TAPA, including the global standards issued as well as the composition and distribution of its members, before finally concluding on the social and economic value that TAPA China and its resources bring to the industry.

TAPA China was officially established in Shanghai on 18th October 2021 at the New Bund GOC of Pudong New Area, with the Shanghai Municipal Transportation Commission as its business supervisor. Its launch and establishment are supported by leaders in Shanghai Public Security Bureau, Pudong New Area Commerce Commission, World Expo Administration, and other departments and commissions.

In the next steps and actions, TAPA China will continue to work closely with government bodies at all levels to provide industry resources needed to support the rising development of China's cross-border supply chains. Furthermore, TAPA China aims to improve the supply chain security standards and industry practices and helm the geographical advantage of Pudong and Shanghai as a supply chain and international trade center. TAPA China strives to help its members in China to contribute toward the development of global supply chain security and forge links across the globe.

IMPACT TO CHINA SUPPLY CHAINS DUE TO COVID LOCKDOWN

Mr. Keven Liang, Supply Chain Security Manager HP Inc, and Vice-Chairman of TAPA APAC, shares his insights on the Covid Lockdown and its impact on supply chains in China.

Q1: To what extent has your organization been impacted by the COVID-19 crisis and subsequent lockdown that effected cities like Shanghai?

Keven Liang (KL): We have been feeling the impact for a little more than two months now since Shanghai Government announced the lockdown protocol at the end of March. I would like to share three major impact aspects to supply chain.

First, safe distancing protocols - for operation staff it was necessary to monitor, control and effectively manage the flow of people (some of them had to be in quarantine due to suspicion, in close-contact and / or affected).

Second, raw materials/supplies - as most enterprises across the country have many outsourced materials and parts suppliers, we faced shortages of materials and parts. These enterprises are in different areas in various cities, which have their own Covid policies and procedures, resulting in different recovery times. Hence, matching timelines with each other was extremely difficult.

Lastly, logistics - in addition to supplies necessary for the epidemic, checkpoints have been set up across entire cities and provinces affecting manufacturers for inbound of raw materials and parts and also outbound of finished products. At the same time, restricted personnel flow led to extremely difficult market expansion. These are some of the biggest problems we faced.

Q2: What would be the most significant short-term supply chain challenges over the next 3-6 months? Any suggestions to tide over the impacts to supply chain? What do you foresee as the new upcoming model?

KL: As explained, the shortages on operation personnel, materials/parts and disrupted logistics has made a huge impact to entire supply chain. The supply chain team in the organisation ideally should re-evaluate the response to such emergencies by potentially shifting from strategic centralized supply to co-existence of centralized supply and network supply.

Moving forward, the business model of simultaneous development of online and offline businesses will become the standard, and the supply chain construction based on online and offline ecological businesses will become the norm.

Moving forward, the business model of simultaneous development of online and offline businesses will become the standard, and the supply chain construction based on online and offline ecological businesses will become the norm.

Logistics scenarios based on AI will become highly relevant, the demand for intelligent logistics technology and the deep application and reliability of such intelligent logistics technology will be necessary.

Future logistics infrastructure especially the logistics facilities should have certain flexibility in:
(i) multifunctionality of strategic logistics centres or nodes; (ii) compatibility of various services and inclusiveness of emergency services; (iii) additional deployment of resources to achieve the replenishment or expansion of logistics capacity in a short period of time. All these require the integration of planning, software and intelligent hardware.

Q3: Do you think there is a need to diversify supply chain production to reduce concentration risk in general all over the world or make it more localised nearer to the end consumer?

KL: It depends on the products, associated suppliers and end consumers. We can see now in the global supply chain market; more and more enterprises are choosing to locate supply chain centres nearer to its end consumers. While it is understood and recognised, it is not easy to replace the existing on-going model, especially for those manufacturers with huge markets worldwide. It is also a proving fact that the more one moves closer to one’s end consumer the more benefits are realised related to proximity, market access and seamless logistics.

Q4: What risk management measures would you suggest implementing to tide over the disruptions due to the pandemic?

KL: We must pay more attention to HSE (health, safety and environment) management. This encourages manufacturing companies to significantly enhance employee health, safety and environmental management and strengthen disaster warning systems. Manufactures are highly recommended to pay more attention to intelligent manufacturing process, promote minimization and flexible production, and also employ more highly skilled and multi-skilled workers to be able to cope up with labour force fluctuations keeping in mind the ‘zero inventory’ or ‘minimum inventory’ policy of key raw materials and spare parts.

HOW CARGO HUBS ARE BENEFITTING FROM CLOUD-BASED ACCESS CONTROL

Minimizing supply chain disruptions and losses and ensuring a robust and resilient supply chain is essential to maintaining optimal operations in the Transportation sector. Security concerns loom large over the industry, which is vulnerable to a plethora of threats, including cyber breaches, acts of terrorism, vandalism, and cargo theft. Keeping assets, facilities, and workers safe at our cargo hubs requires the implementation of comprehensive security solutions, such as video surveillance, intrusion, and perimeter detection, mass notification systems, and, very importantly, a trusted and highly secure access control and identity management system.

Access control ranks so high on the list of security must-haves at cargo hubs because of the sheer volume and variety of people coming and going through them. Controlling who should – and should not – be given access is an ongoing challenge for directors overseeing the safety and security of these hubs. To ensure worker safety and the protection of high-value assets, it is imperative to know and control who exactly is entering and exiting these locations. Often, outside vendors, and temporary and/or short-term workers are brought in, sometimes a great many of them, making it tough for administration and/or security teams to know exactly who was on site when, and where. This is exactly why implementing a trusted and highly secure access control system at cargo hubs is so imperative.

Traditional physical access control measures have long been put in place to secure these sites. Key components of these legacy systems include a server, which stores and oversees the credentials of authorized users. Credentials typically used are key cards, such as a Prox card, PIN numbers, key fobs, biometric attributes, and today, even Smart mobile phones. Readers are the devices that actually read the credential being used, while the control panel uses that data to determine if the credential is, in fact, authorized. The door lock then responds accordingly to open and grant access or remain locked to deny access. And while traditional legacy access systems such as these continue to secure countless facilities of all kinds, many organizations across all industry sectors are electing to move their access control systems to the Cloud. There are several reasons for this.

One of the most attractive benefits is budgetary. Upfront costs are significantly lower with a Cloud-based access system as there is no need to invest in an on-site server. Users have ensured the protection of a strong access control solution without the expense of an onsite IT infrastructure. Costs are consolidated into a single subscription cost, and the days of ongoing onsite maintenance costs and service calls are behind them. Cloud-based access is a service, which means that updates are done automatically, keeping the system armed with the most recent software available.

In addition, no longer will HR or security teams must contend with issuing and revoking physical access cards. Credentials can be managed remotely via the Internet to grant and deny access in real-time as needed, allowing complete access control across an entire organization, including multi-site operations. Varying levels of access to different locations can be set, ensuring that only authorized users can gain entry to sensitive, high-value areas.

When Cloud-based solutions first emerged, many users were skeptical about how secure they were. They have proven to be highly secure, thanks in large part to the extensive amount of encryption that is used. Firewalls provide a high level of protection and are core to cloud architecture. Cloud-based security is delivering a high level of protection against cyber threats and data breaches.

And, as operations and security needs change and evolve, so too can cloud-based access systems. They are scalable and can expand and grow along with your operation, including the addition of more doors, entryways, and users.

The benefits and technological capabilities of cloud-based access control solutions are meeting the complex security challenges of transportation hubs, which is why increasingly more of them are transitioning from their traditional physical access systems to cloud-based access.

AUTHOR: Alex Reichard, Sr. Account Manager, NextGen Security, LLC Headquartered near Philadelphia, PA, with a major operation in Houston, TX, and several regional offices throughout the country, NextGen Security, LLC is an integrated physical and electronic security provider specializing in solutions for regulated entities and facilities in key vertical markets.

A New Analytical Approach and Visualization of Online Sales of Fake Products

Timothy A. Burt[1,2], Nikos Passas[3], and Ioannis A. Kakadiaris[1,4]

[1] Computational Biomedicine Lab (CBL), University of Houston, Houston, TX, USA
[2] Dept. of Physics, University of Houston, Houston, TX, USA
[3] School of Criminology and Criminal Justice, Northeastern University, Boston, MA, USA
[4] Dept. of Computer Science, University of Houston, Houston, TX, USA

New approaches which can leverage the full spectrum of information in the digital age are needed to combat the growing proliferation and sale of counterfeit goods now more than ever. The COVID-19 pandemic challenged the resources of many teams investigating these crimes, necessitating new tools for handling the large volume of potential leads and finding similarities between sellers.

The goods sold and proliferated through illicit supply chains cause death or disabilities for millions of people, damage companies' brands, undermine competition and the rule of law, cause economic losses and security threats, and corrupt financial systems. Ensuring the security of today's supply chains will require the collaboration of interdisciplinary researchers in academia and industry stakeholders.

This article discusses the outcome of such a collaboration: a fully automated Link Forensics Tool (LFT) which product security teams, government agencies, law enforcement, and intelligence teams can use to construct and visualize illicit supply chain networks using both conventional and unconventional data sources, including Open-Source Intelligence (OSINT).

First, we provide a high-level overview of the steps in our implementation, FINDM-SIG, including the inevitable challenges with any automated OSINT collection & analysis tool. Next, we summarize some quantitative insights FINDM-SIG can provide to stakeholders using their data. Lastly, we discuss how others can try out FINDM-SIG and get involved with our research.

FINDM-SIG: an interpretable pipeline for the identification, analysis, intervention, validation, prediction, and visualization of illicit supply chain networks and their activities

What does FINDM-SIG do?

Our tool is FINDM-SIG (**Fi**nancial **N**etwork **D**isruptions in illicit and counterfeit **M**edicines trade – **S**eller **I**ntelligence **G**raph). This method is generic and can be adapted to construct, visualize, and make quantifiable predictions about illegal supply chains. It requires no specialized training or knowledge to use.

Who are some of the potential users that would benefit from using FINDM-SIG?

The users generally include risk/fraud control analysts, law enforcement/FDA analysts, and platform risk managers.

What data are needed to build an illicit seller network? What do the nodes/edges in the network represent?

FINDM-SIG takes lead URLs as input, which contain *digital traces* that have attracted the attention of the product security specialist. Some examples include images/text of a pharmaceutical drug their company has a trademark on that shows signs of being substandard or falsified. The images/text are then scraped and preprocessed. Other lead attributes can be added alongside the URLs to improve the linking accuracy.

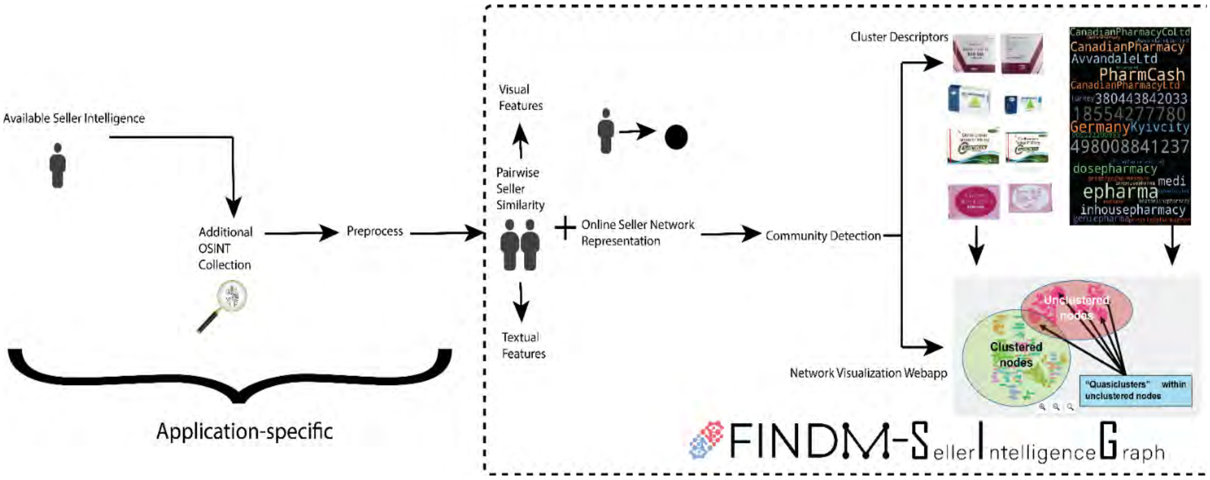

Figure 1: Overview of FINDM-SIG, a pipeline designed to link similar illicit online sellers within a graph. Stock photos from vecteezy.com.

Next, FINDM-SIG builds similarity features using the gathered data: linking leads using phone numbers, emails, images, addresses, domain names, and keywords. The pairwise lead similarity is computed using domain-validated state-of-the-art (SOTA) algorithms for fuzzy string matching and Deep Learning based image similarity.

These features are used to construct an illicit seller network, with the nodes representing leads (cases) and the edges representing the similarity between two cases. Next, FINDM-SIG uses community detection techniques to cluster the linked cases.

Lastly, cluster descriptors (Figure *1*) are produced for each cluster: they consist of an image gallery and word clouds. They are designed to communicate the most common words/images that link leads within that cluster to a non-technical audience and as a common-sense check to see if the algorithm's results make sense.

Is FINDM-SIG free for me to use?

FINDM is funded through public research grants, and there is no cost for stakeholders to get involved with the tool and try it out using their data.

Is FINDM-SIG fully automated, or are their manual steps involved?

It is fully automated and runs behind the scenes on secure cloud computing infrastructure (all within CONUS).

How will my data be secured?

Every stakeholder's data are isolated from others in the cloud. We have numerous safeguards in place to ensure the stakeholder's data and their identities are kept strictly confidential.

For organizations with air gap requirements, such as law enforcement, we plan to offer a "portable" version of FINDM-SIG for field use, which is not connected to the internet. Further information on this is available upon request.

Will it be easy to prepare my data for FINDM-SIG and upload it? What types of data can be uploaded for FINDM-SIG?

The process is kept simple: the stakeholder uploads their data, then a job is queued to process, scrape, and analyze their data. Once the network is ready for stakeholder exploration, they are notified via email to log in to the web app.

There are over 30 fields FINDM-SIG knows how to process as input, including those mentioned as similarity features. Some of these fields are domain-specific, and we can easily add new ones requested by a stakeholder. At least one URL is required per lead. We provide a detailed FINDM Data Dictionary on the web app with all instructions.

How can FINDM-SIG identify fake or illicit goods from URLs?

A key feature in the development of FINDM-SIG is the illicit detection module. It can classify URLs as illicit/licit or selling real/fake goods; when used with the lead similarity features, the leads can be prioritized for the investigative teams, saving them time and resources.

What insights can FINDM-SIG provide, and how can they be used to disrupt illicit seller operations?

It’s important to stress that, while the base automated FINDM-SIG pipeline is developed, the research modules for the project are yet to come. These will be developed, tested, and deployed through a series of trial & error, together with feedback from FINDM-SIG’s stakeholders.

Case Study: Finding “weak links” in large-scale illicit pharmaceutical affiliate programs

We were provided a lead sheet by Company X, a large pharmaceutical company, and tasked with finding the “big fish” in the pond. FINDM-SIG identified four seller clusters that are much larger than the average and probably involved in spamming/pharmaceutical affiliate programs (Figure *2*B). About two-thirds of the clustered leads consisted of only two sellers, which were not the targets for this case study.

A review of the cluster descriptors and the lead domains unraveled the inner workings of the illicit operation: the cluster with the most cases (seen as a fan) consisted of B2C affiliate sites related to Canadian Pharmacy. The second cluster revealed product items sold on legitimate B2B platforms like Alibaba. The third cluster was composed of a different affiliate pharmacy (exposing a possibly unknown link). The last group revealed that these same items are being sold on social media platforms (illegally).

The reason for connections between clusters is interpretable: each carries one or more image/text data pairs, a similarity score, and a confidence index. These metrics allowed analysts to form a Preliminary Evaluative Opinion (PEO) on whether the cases (and their clusters) are “similar enough” to proceed with that line of investigation. Our stakeholders can then coordinate simultaneous disruption of seller activity across multiple vulnerable domains, inflicting the most damage to the illicit supply chain’s operations.

Conclusions

FINDM-SIG is in active development, and we are welcoming additional research partners in the fight to take down illicit supply chains. We hope that industry leaders will get excited about the enabling possibilities of working with academic teams such as ours.

This article also stresses the importance of data sharing & aggregation of investigative leads (anonymously) to create predictive computational models for identifying, intervening, and disrupting these criminal networks. Only with enough stakeholders and actual data capturing illicit activity can AI be expected to predict and prevent future illegal chain supply activities.

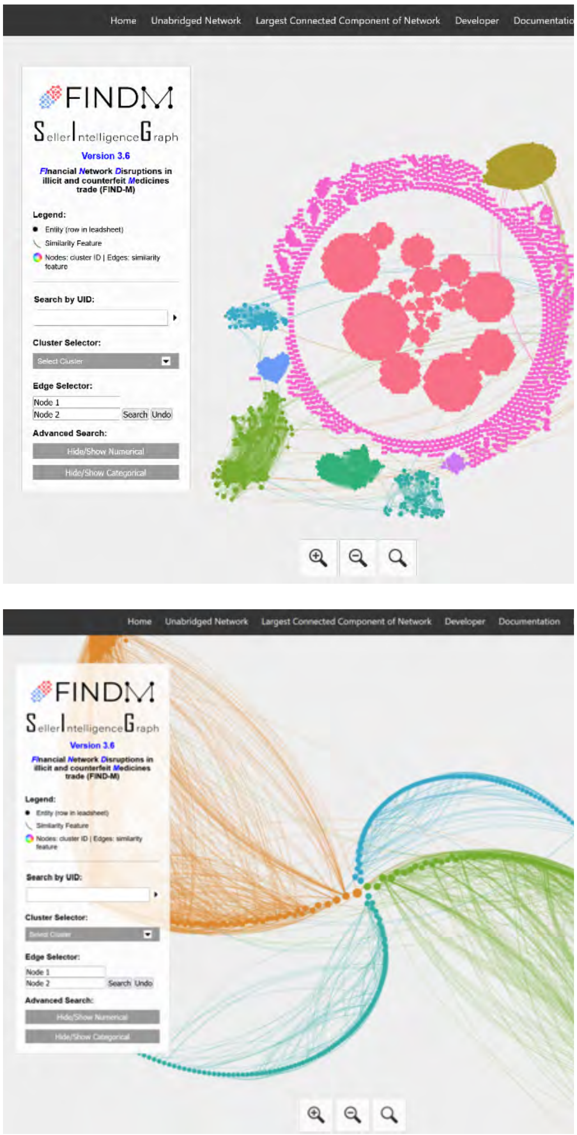

Figure 2: The FINDM-SIG Link Forensics Tool (LFT) website provides two views out-of-the-box for a generated illicit seller network.

(T) Unabridged View, showing all leads provided. Large-scale illicit sellers (8 unique colored clusters), tiny-scale illicit sellers (light blue clusters), and not clustered leads (pink, inner circle).

(B) Radial Clustered View (or Giant Component view). Four clusters from the whole network share connections between them (same colors as in (T)). Nodes (leads) are ordered such that the ones with the highest betweenness centrality are at the center of the spiral (betweenness centrality quantifies how important a node is to the flow of the network).

Our highly diverse research team includes computer scientists, physical scientists, criminologists, biomedical & chemical engineers, and pharmaceutical scientists. To learn how FINDM-SIG can be applied to solve logistics or product security challenges, please email Prof. Kakadiaris (ikakadia@central.uh.edu) to request a live demo.

Funding Acknowledgements

This work is partly supported by the National Science Foundation under grant IIS-2039946. This work is funded in part by the Department of Defense SMART Scholarship-for-Service Program. SMART is funded by the Under Secretary of Defense-Research and Engineering, National Defense Education Program.

Author Profiles

Timothy Burt is a Physics Ph.D. Candidate at the University of Houston and a Graduate Research Assistant in the Computational Biomedicine Lab (CBL) advised by Prof. Kakadiaris, working on the FIND-M Project. FIND-M aims to develop new approaches to identify, intervene, and disrupt the proliferation & sale of illicit and counterfeit medicines. His research interests lie at the intersection of Physics & Computer Science. Specifically, understanding the dynamics & emergent phenomena within criminal networks and developing physics-constrained machine learning algorithms for modeling real networks.

Nikos Passas is Professor of Criminology and Criminal Justice at Northeastern University. He is also Distinguished Visiting Professor at Beijing Normal Univ. Law School, Distinguished Practitioner in Financial Integrity at Case Western Reserve Law School, and Chair of the Academic Council of the Anti-Corruption Academy in India. He serves on the Advisory Board of the Centre for Crime, Justice and Policing at the Univ. of Birmingham, the Advisory Board of Global Risk Profile in Geneva, the International Panel of Advisors at the Institute for Australia India Engagement in Brisbane and the Board of Directors of Compliance and Capacity Skills International. Passas offers training to law enforcement, intelligence and private sector officials on regulatory and financial crime subjects. He regularly serves as expert witness in court cases or public hearings and consults with law firms, financial institutions, private security and consulting companies and various organizations, including the Financial Crimes Enforcement Network (FinCEN), OECD, OSCE, the IMF, the World Bank, the Council of Europe, other multilateral and bilateral institutions, the United Nations, the European Union, research institutions and government agencies in all continents. He served as Team Leader for a European Union Commission project on the control of proliferation/WMD finance. His law degree is from the Univ. of Athens (LL.B.), his MA from the University of Paris II (D.E.A.) and his Ph.D. from the University of Edinburgh. He is a member of the Athens Bar (Greece) and is fluent in 6 languages. He specializes in the study of international criminal law and conventions, corruption, illicit financial/trade flows, sanctions, informal fund transfers, terrorism, white-collar crime, financial regulation, and organized/transnational crime.

Ioannis A. Kakadiaris, Ph.D., is a Hugh Roy and Lillie Cranz Cullen Distinguished University Professor of Computer Science at the University of Houston and directs the Computational Biomedicine Lab. Ioannis is an international expert in digital health. Ioannis has served as the Director of the Borders, Trade, and Immigration (BTI) Institute, a Department of Homeland Security Center of Excellence led by the University of Houston (UH). As director of the BTI Institute, Ioannis oversaw multiple projects undertaken by eighteen partners across eight states and the District of Columbia. The portfolio focused on homeland security enterprise research, education, and workforce development by studying complex, multi-disciplinary issues related to cross-border movements of people, goods, data, and financial capital. He earned his B.Sc. in Physics at the University of Athens in Greece, his M.Sc. in Computer Science from Northeastern University, and his Ph.D. at the University of Pennsylvania. In addition to twice winning the UH Computer Science Research Excellence Award, Ioannis has been recognized for his work with several distinguished honors, including the 2022 UH Award for Excellence in Research, Scholarship, and Creative Activity, the UH Enron Teaching Excellence Award, the NSF Early Career Development Award, the Schlumberger Technical Foundation Award, and the James Muller Vulnerable Plaque Young Investigator Prize. His research has been featured on Discovery Channel, National Public Radio, KPRC NBC News, KTRH ABC News, and KHOU CBS News.

TAPA AMERICAS

Transported Asset Protection Association

Contact Us

TAPA AMERICAS
5030 Champion Blvd, G-11 #226, Boca Raton, Florida 33496
Phone (561) 617-0096
Cindy M. Rosen, Executive Director
crosen@tapaonline.org