VCMS Unveiling the Crypto Crime Nexus: A Deep Dive into A Money Laundering Operation Between Nigeria, Turkey & Europe

Cryptocurrencies have revolutionized finance, offering innovation while exposing vulnerabilities. This document examines a transnational money laundering scheme exploiting the anonymity of digital assets. Using VCIS, the investigation showcases advanced tools like geospatial intelligence and blockchain analysis to trace illicit activities, link wallet addresses to real-world actors, and uncover hidden criminal networks. This case highlights the challenges and opportunities of combating crypto-related financial crimes through technology and international collaboration, paving the way for stronger safeguards in the global financial system.

To tackle the evolving threats of crypto-financial crimes, VCIS empowers global investigations with real-time insights, uncovering hidden networks and linking digital assets to illicit activities with unmatched precision.

Table of Contents

VCIS: Illuminating and Tracking beyond the Dark Web of Global Finance and Counterintelligence in Time Travel

Unmasking Financial Crimes with Geospatial Intelligence AI and Unraveling Past Crimes, Present and Predicting Future Threats.

Combating Financial Crimes and Terrorist financing demands cutting-edge solutions in the complex landscape of digital finance and global security. VALOORES Crowd Intelligence Solution (VCIS) emerges as a beacon of innovation, leveraging geospatial intelligence and advanced analytics to unravel illicit activities. This comprehensive overview delves into VCIS's capabilities, showcasing its pivotal role in safeguarding global financial systems and national security.

Key takeaways include:

1. **Cryptocurrency Tracking**

VCIS traces the flow of digital assets, correlating movements with real-world events, predicting future transactions, and integrating blockchain data with KYC information and geospatial intelligence.

2. **Advanced Knowledge Graphs**

VCIS constructs a living map of the global financial ecosystem, correlating blockchain transactions with real-world identities and locations, filling in knowledge gaps, and predicting future actions.

3. **Geospatial Intelligence in Global Crime Networks**

VCIS makes visible the invisible flows of illicit finance worldwide, overlaying trade flows with financial transactions, communication records, and movement patterns.

4. **Uncovering New Layers in Crypto-Money Laundering Operations**

VCIS expands investigative horizons with recursive analysis, revealing layer after layer of criminal activity, bridging seemingly unrelated activities, and identifying and neutralizing criminal adaptation in real time.

5. **The Current and the Future of Counterintelligence**

VCIS revolutionizes security with comprehensive intelligence solutions, handling unlimited geospatial data, transitioning between offline and online modes, and maintaining the highest security levels.

6. **Unlock the Power of Time-Based Insights**

VCIS performs financial time travel, reconstructing past financial ecosystems and projecting future criminal activities, creating a comprehensive Temporal Analytics view of financial crime.

7. Adaptive Security Measures

VCIS employs state-of-the-art encryption, access controls, and adaptive security protocols to ensure the highest data protection.

Clear Direction and Benefits

VCIS offers a clear path to a safer financial world by harnessing the power of geospatial smart location intelligence. It enables the tracking of Financial Crimes, crypto money laundering, and Terrorist financing activities, tracing historical criminal activities to uncover hidden networks and prevent future threats. By providing a comprehensive view of illicit financial flows, VCIS empowers decision-makers to take decisive action, safeguarding global financial systems and national security.

VCIS is not merely a tool; it is a paradigm shift in financial crime prevention. By harnessing cutting-edge technologies, VCIS empowers law enforcement and financial institutions to detect, prevent, and combat sophisticated Financial Crimes across borders. Its impact extends beyond immediate crime prevention, promising a future of enhanced transparency, security, and trust in global financial systems.

Introduction

Virtual asset activities may create illicit finance vulnerabilities due to their borderless nature, decentralized structure, limited transaction transparency, hidden or undisclosed UBOs, and speed of operations. Anonymized cryptos or privacy coins further reduce transparency and obscure the source through cryptographic enhancements, thus circumventing typical Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) controls. ***"Cryptocurrency has given money launderers a feature that they have dreamt of – secrecy,"***

Regulations continue to be insufficient, necessitating the use of further technological solutions like VCIS. This geospatial technology is beneficial, especially in high-tech and rapidly advancing industries such as crypto. By utilizing cutting-edge technologies, this technique enables law enforcement to more effectively monitor and control cryptocurrency operations.

With the Middle East emerging as a hotspot for cryptocurrency trading, boasting a 500% increase in transactions between July 2020 and May 2024, it's imperative to address cross-border money laundering effectively.

The UAE has been harboring an encouraging environment for the growth of its crypto industry, especially with Dubai's enactment of the Virtual Assets Law and establishment of VARA. While the industry was largely unregulated a few years ago, recent legislative measures have shown the government's keenness to reduce potential financial crime risk in the nascent industry.

The surge of cryptocurrencies in the UAE has ushered in a new era of financial innovation, posing a massive challenge to regulatory authorities. Thus, we see that the UAE has made many provisions for protecting crypto assets from money laundering. But, money launderers are at a higher pace of exploiting technology for illegal activities.

In response to a rise in cases of money laundering and terrorist financing, global and national regulators are making a significant progress with relevant protection laws, but the challenge lies in identifying the red flags at the right time and the real users of the digital wallet addresses in the absence of any effective KYC or national crypto wallet database.

Digital currencies are reshaping the landscape of money where combating money laundering through cryptocurrency has become paramount. You find yourself at the forefront of this dynamic shift, charged with navigating the complexities of this brave new world. But fear not, for VALOORES stands as a beacon of expertise, drawing upon 35 years of unparalleled experience in the financial crime arena.

Yet, despite your best efforts, you are not ready yet! The challenge remains daunting: identifying elusive digital wallet owners and unraveling the enigma of their movements, behaviors, and connections. Enter VCIS, a pioneering solution harnessing the power of data correlation. Through an innovative fusion of blockchain databases, geospatial data, KYC protocols, digital identity verification, and call detail records (CDR), VCIS empowers you to conquer this formidable challenge.

Through VCIS we are monitoring VASPs activities and uncovering the financial crimes committed through cryptocurrencies. VCIS empowers industry players with advanced tools to monitor and investigate activities effectively, bridging the gap between regulatory provisions and real-time surveillance and investigation.

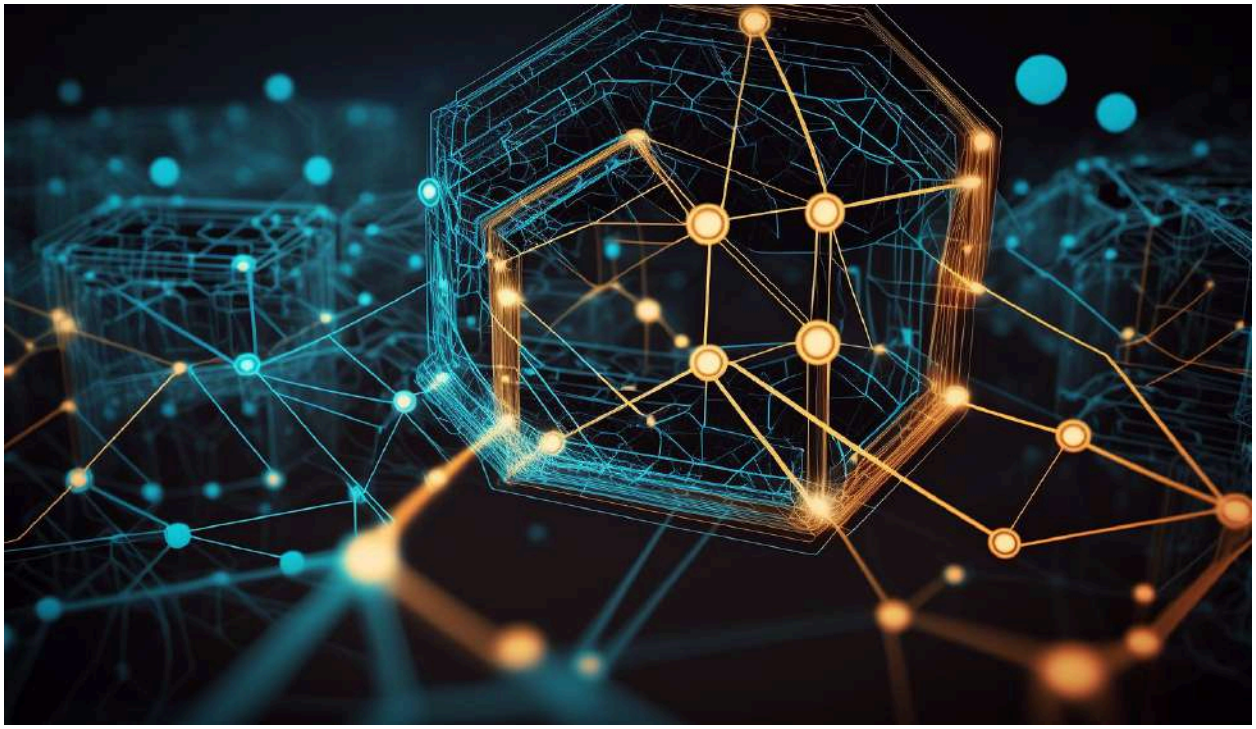
By leveraging geospatial data and correlating it with transactions through dynamic knowledge graphs, VCIS can track digital wallet activities and identify wallet address owners swiftly.

Imagine having the power to unravel the complicated web of a money laundering scheme, spanning multiple countries and leveraging the anonymity of cryptocurrencies. This is precisely what VCIS did; through a deep dive into a real case study. As the investigation unfolds, you'll witness the crucial role played by the VASPs, operating as cryptocurrency exchange stores, in facilitating the conversion of illicit funds into fiat currency – the critical "cash-out" step that allows laundered money to be integrated into the traditional financial system. VCIS connects the dots between suspicious wallet addresses, physical devices, and individuals' movements, establishing direct links between perpetrators and their illicit financial activities. But the thrill doesn't stop there, our system's prowess extends to untangling the transnational

complexities of this money laundering operation, involving multiple individuals and entities across different locations, potentially spanning multiple countries.

Join us on this journey, where geospatial technology meets investigative prowess, and witness firsthand how our system empowers you to stay ahead of the curve in the ever-evolving world of financial crimes.

Through the following case study, we identified several parties using unregistered digital wallets to launder money between Europe, Turkey and Nigeria.
Brace yourself, for you are about to embark on a journey where every transaction tells a story, and every clue leads to uncovering the truth behind the flow of illicit funds. Welcome to the future of financial security. Welcome to VCIS!



Story

The Nigerian law enforcement recently received critical intelligence from a European law enforcement agency concerning a digital wallet address suspected of involvement in complex money laundering activities spanning Europe, Turkey, and Nigeria. This suspected digital wallet address **TPyjXXXXXXXXXXXXNa5** has been implicated in a series of cryptocurrency transactions on the decentralized Tron blockchain linked to drug trafficking operations and subsequent laundering activities.

According to the information provided, individuals associated with this wallet address are believed to have received substantial crypto transactions in Nigeria from a drug cartel operating between Europe and Turkey. These transactions are suspected to be part of a larger scheme involving cashing out at local exchanges in Nigeria before the illicit funds are reintegrated into the financial system, ultimately returning to Europe through undisclosed methods.

One particularly notable transaction, amounting to $3.7 million, was traced to this wallet on February 11, 2024. This significant sum underscored the urgency and gravity of the situation.

In response to these findings, Nigerian law enforcement initiated a comprehensive financial investigation leveraging our cutting-edge **VCIS** platform. The primary objectives of this investigation are to:

Uncover the identities behind the suspected money laundering operation.

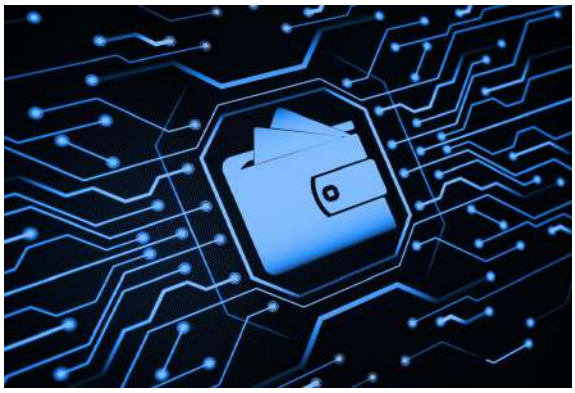
Ascertain the accomplices involved.

Trace the flow of illicit funds to their final recipients and destinations.

Expose the methods employed to reintegrate laundered money back into Europe.

Pinpoint any conversion of cryptocurrencies into tangible assets within the financial system.

This case study will delve into the intricate web of financial transactions and criminal activities associated with this wallet address, shedding light on the challenges and methodologies encountered during the investigation. It highlights the critical role of advanced technological solutions (VCIS) in combating modern financial crimes, emphasizing the commitment to robust enforcement and international cooperation in countering illicit financial activities.



Scenario

Chapter 1: Wallet Address Owners and the Flow of Crypto Transactions

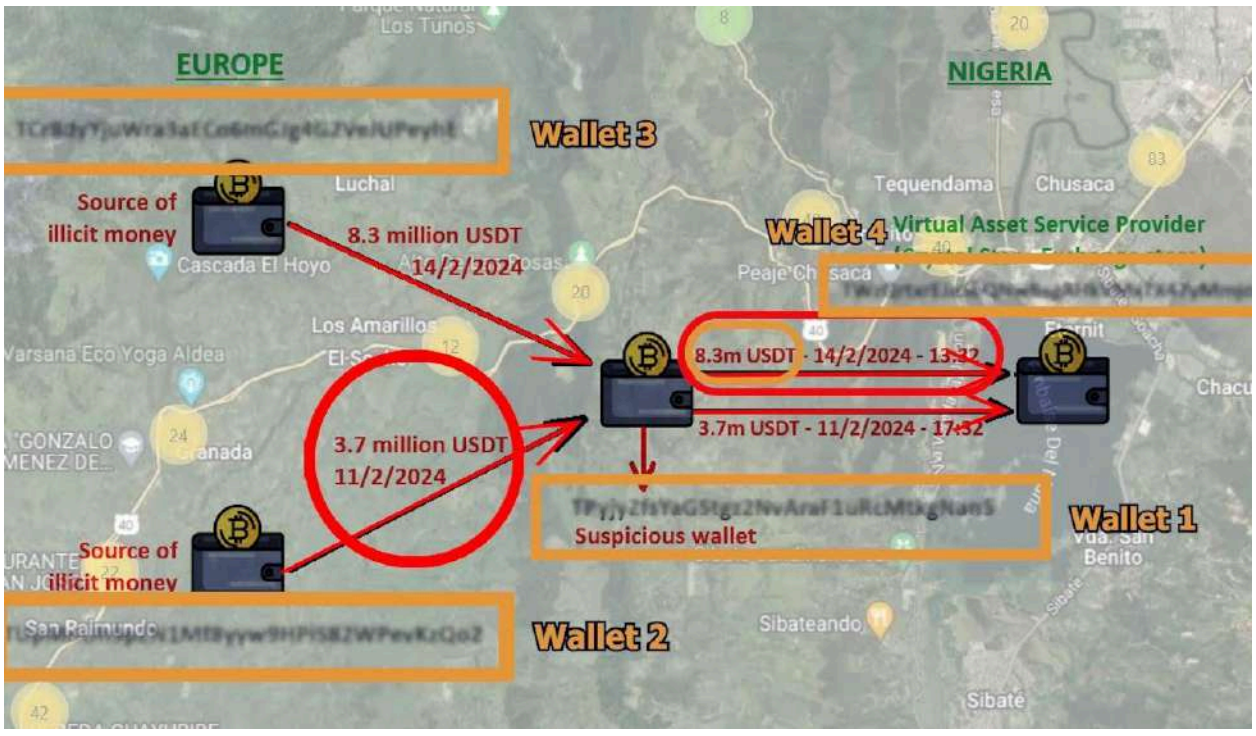
A. Crypto Transaction Analysis

Utilizing the VCIS knowledge graph, we accurately survey the crypto transactions associated with the identified wallet address: **TPyjyXXXXXXXXXXXXNan5**

1. The initial transaction occurred at 13:42 on February 11, 2024, with 3.7 million USDT, received via the Tron blockchain. The sender was the wallet address **TUpMXXXXXXXXXXXXQo2**. Subsequently, at 17:32 on the same day, **TPy…an5** executed a transfer on the Tron blockchain to a third party, **TWzQXXXXXXXXXXXXMmjo**.

2. The second transaction occurred on February 14, 2024, at 10:35, involving the reception of 8.3 million USDT via the Tron blockchain. This transaction originated from **TCr8dXXXXXXXXXXXXyhE.** Shortly thereafter, at 13:32 on the same day, **TPy…an5** executed another transfer on the Tron blockchain to the same third party, using wallet address **TWz…mjo**.

This wallet address is registered in our VCIS DKYC (Digital Know Your Customer) database as associated with a cryptocurrency exchange store named Crystal Star, located at 16D street.



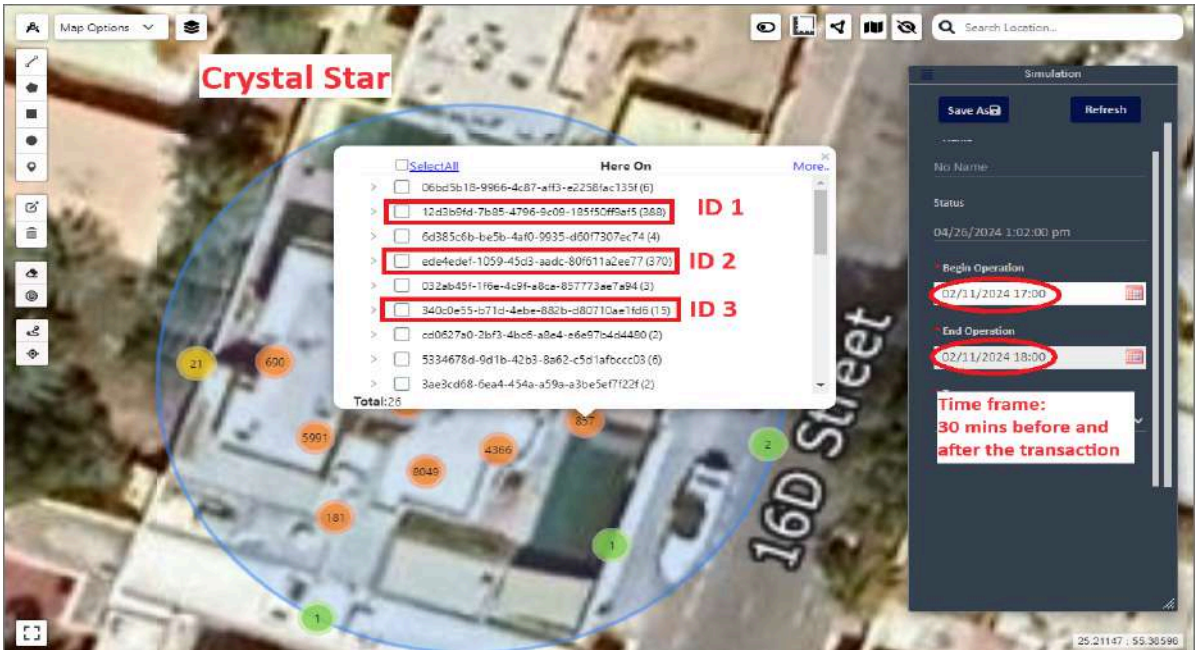
B. Common Devices at the VASP Store

In order to trace the owners or users of the wallet address **TPyjXXXXXXXXXXXNan5**, which was used by the suspected individuals, we conducted targeted activity scans around the location of the crystal star exchange store within a 30-minute window before and after the specific date and time of each transaction originating from the suspect's wallet to the cryptocurrency exchange store's wallet **TWzQXXXXXXXXXXXMmjo** Below are the screenshots capturing the details of these common devices identified during the investigative activity scans conducted around the Crystal Star store's location (6.562624,3.250005). Through these activity scans, we successfully identified several devices present at the location of the Crystal Star store during each of the specified time periods. Among these devices, the following are recognized as common across both activity scans:

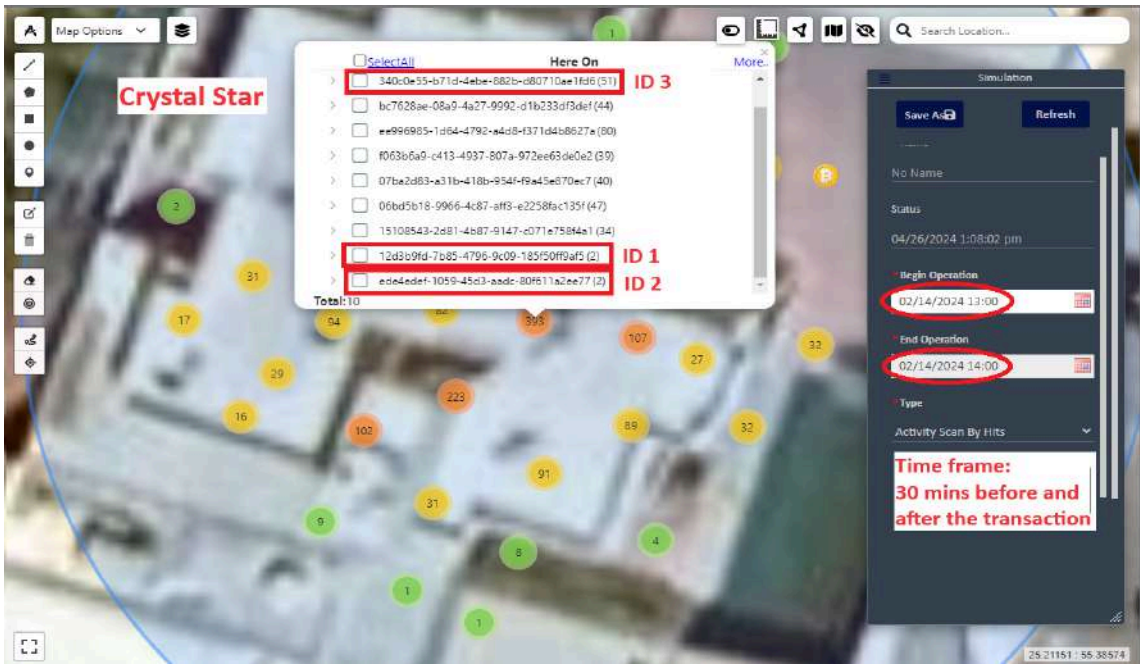
- Device ID 1: 12d3b9fd-7b85-4796-9c09-185f50ff9af5
- Device ID 2: ede4edef-1059-45d3-aadc-80f611a2ee77
- Device ID 3: 340c0e55-b71d-4ebe-882b-d80710ae1fd6

These transactions occurred at:

1. **17:32 on February 11, 2024** *(AS - Crystal Star 11 Feb)*



2. **13:32 on February 14, 2024** *(AS - Crystal Star 14 Feb)*



These findings contribute crucial insights into potential connections between the suspicious wallet addresses associated with the suspects and the devices detected within the proximity of the cryptocurrency exchange store during the respective transaction periods.

C. Suspicious Wallet Address Owner

Further investigation involving a Device History query **DH** for the identified three devices introduced critical insights:

1. Device ID1 and Device ID2 are attributed to the VASPs (Virtual Asset Service Providers), as their historical patterns indicate regular visits to the same location each day, followed by a return to their respective home location (6.562278, 3.241365). This consistent behavior suggests a routine associated with professional duties or regular business operations.
(DH - ID1 and ID2)

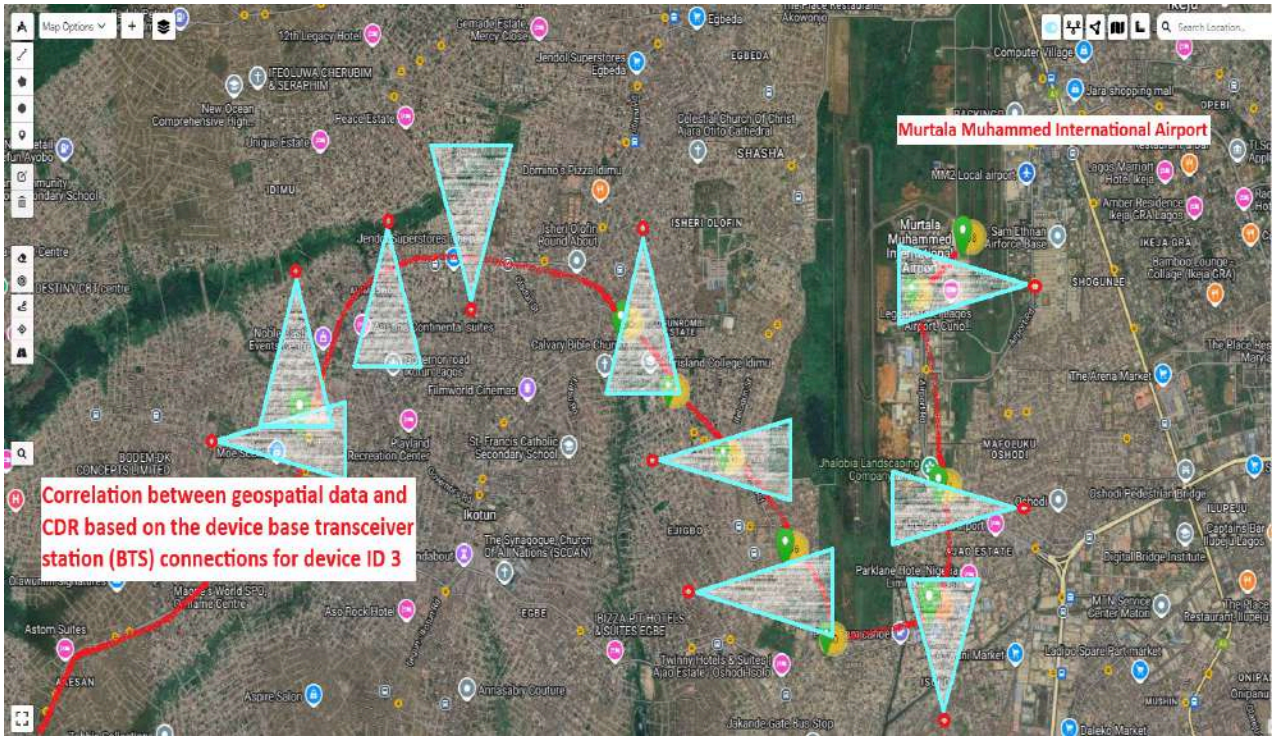
2. In contrast, Device ID3 exhibited a distinct pattern correlating with the suspected wallet address **TPyjXXXXXXXXXXXNan5**. Device ID3 visited the Crystal Star exchange store precisely during the times when transactions totaling 12 million dollars were sent to the VASP's wallet address. This observation strongly suggests that Device ID3 is the individual responsible for controlling the wallet address in question. They visited the exchange store to convert crypto assets into cash.
(DH - ID 3)

Moreover, an in-depth examination of Device ID3's history revealed that on February 10, 2024, at 14:30, Device ID3 arrived at Lagos International Airport (6.579516, 3.326987) from Istanbul.

The screenshots below show the journey of Device ID3 from Istanbul international Airport to Lagos and onwards to the B&C Dyamond Hotel & SUITES (6.528894311636171,3.215514999376401) *(DH - ID 3)*

D. Correlation between geospatial data and call detail record (CDR)

Furthermore, leveraging the correlation feature between geospatial data and CDR, we executed a query for device ID3 between Lagos International Airport and the B&C Dyamond Hotel & Suites to compare its geospatial activities on the road to its CDR activities based on the device base transceiver station (BTS) connections.



The previous query allowed us to identify significant associations tied to ID3:

1. Device ID3 utilized a Nigerian SIM card associated with the IMSI number: 6548xxxxxxxx13453.
2. This IMSI is linked to the IMEI number: 3554xxxxxxxxx1239.
3. This IMSI corresponds to the phone number: +234 201 XXX XXX registered to a Turkish resident with the ID number : RG3 xxxx 70

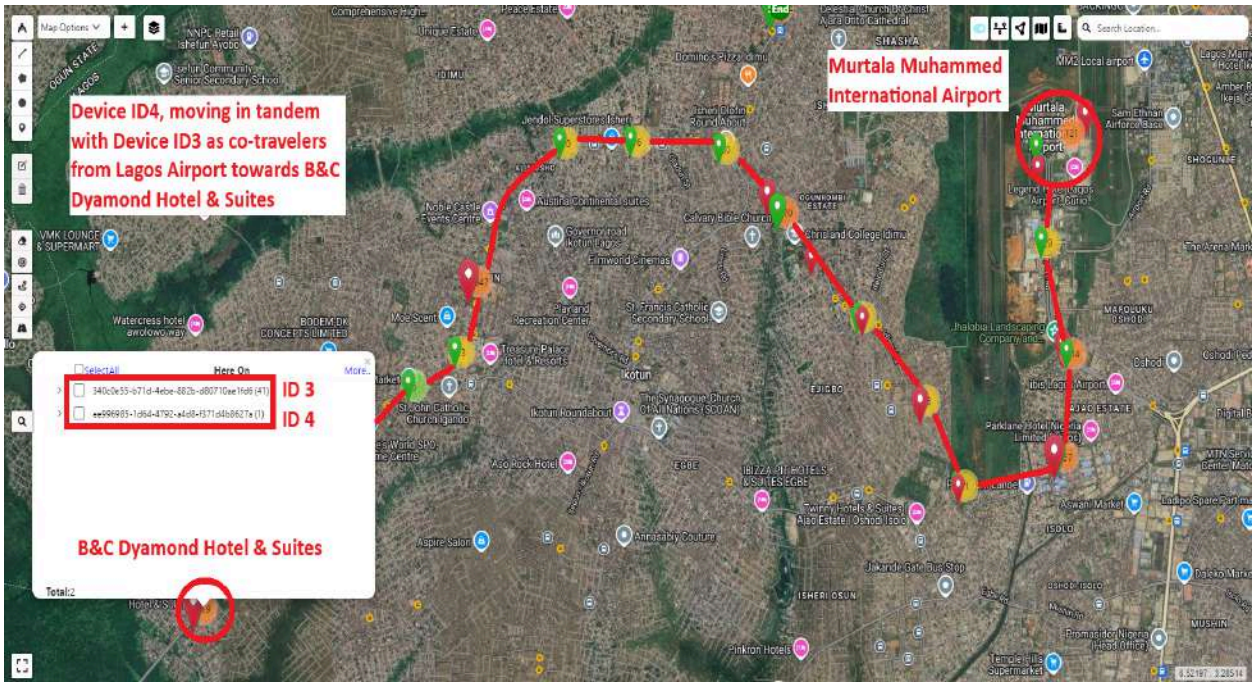
Accumulatively, these findings corroborate the identification of the owner of the wallet address **TPyjXXXXXXXXXXXNan5** as a Turkish individual who travels between Istanbul and Lagos. The integrated capabilities of VCIS enabled the synthesis of geospatial, CDR, blockchain database, and transactional data to uncover vital details crucial to this investigative case. Attached are relevant screenshots and data visualizations, providing comprehensive documentation of these critical findings within the investigative process.This robust analysis strengthens our understanding of the individuals and activities tied to the flow of illicit cryptocurrency transactions.

Chapter 2: Suspects and their Suspicious Activities

Continuing our investigation, we employed advanced queries and analyses within the VCIS tool to uncover the suspicious activities of the identified suspects, focusing on Device ID3.

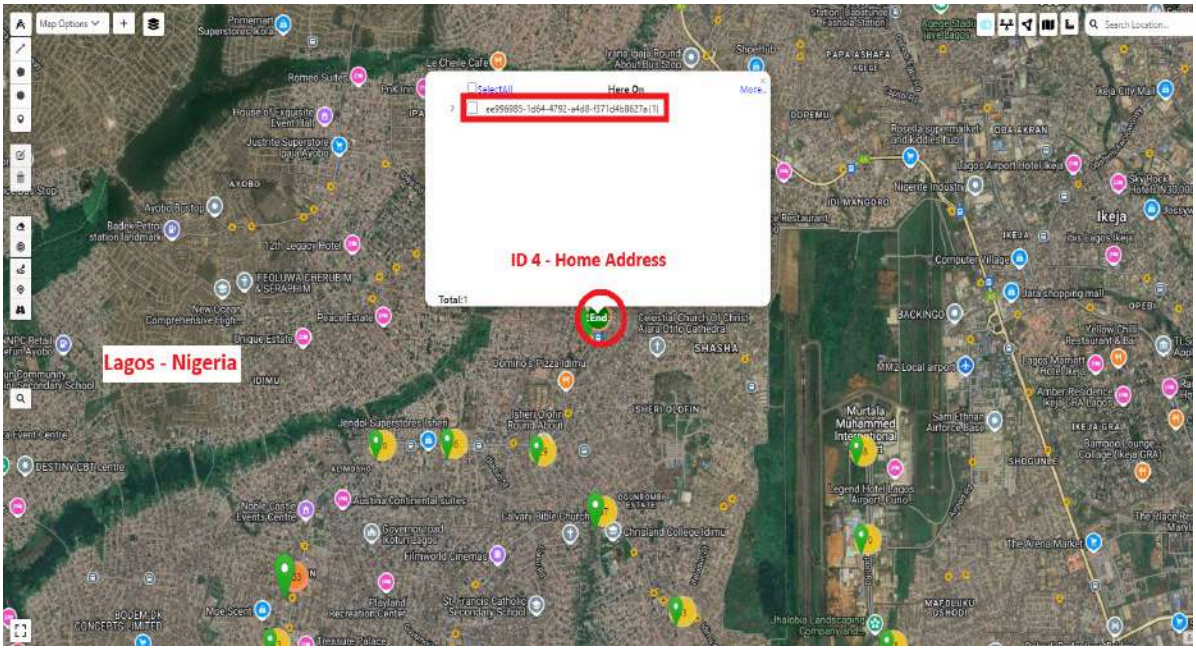
A. Co-Traveler Query

Applying a co-traveler query for Device ID3 from Lagos Airport to “B&C Dyamond Hotel & Suites” revealed the presence of a new device, Device ID4, which moved in tandem with Device ID3 during this journey. The screenshot detailing this co-traveler scenario provides critical evidence of their association.



B. Device ID4 Home Address

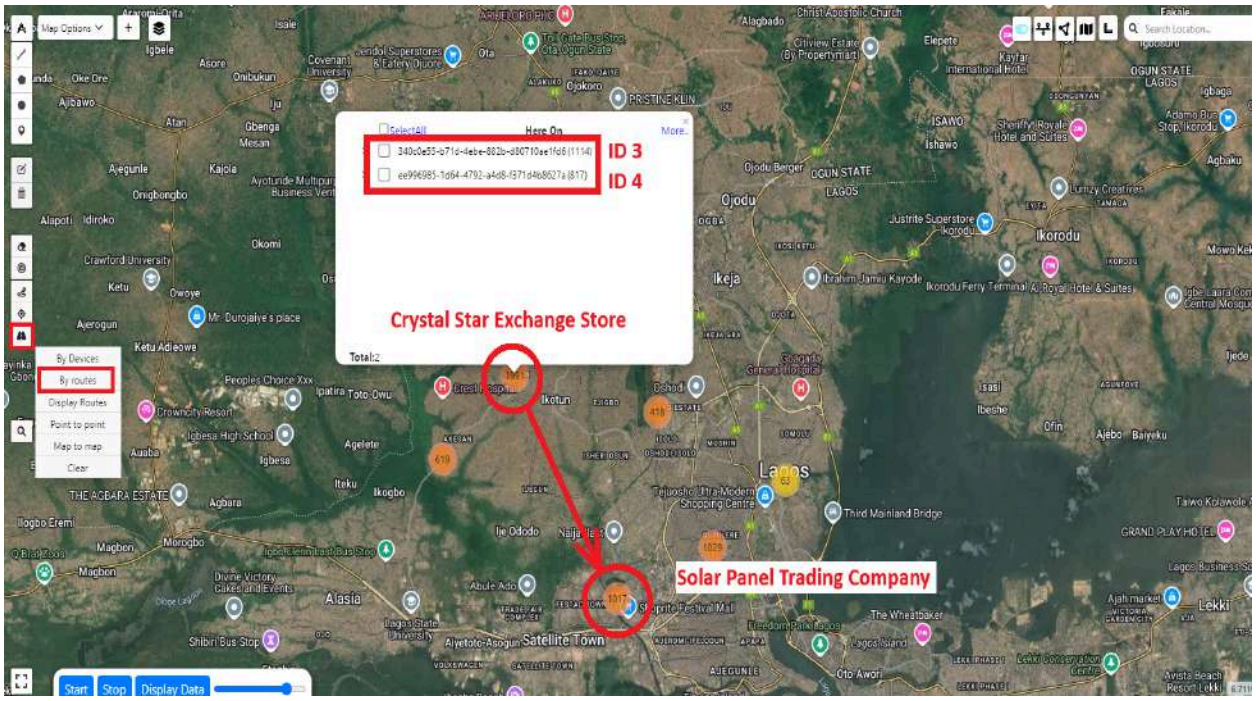
Subsequent analysis through a device history query for Device ID4 allowed us to identify their residential address and identity. The screenshot capturing Device ID4's home address strengthens our understanding of their background and potential involvement in the suspicious activities. (*DH - ID4)*



C. Activities of Devices ID3 and ID4

Further examination of the device histories of ID3 and ID4 revealed compelling patterns. They were observed moving together to the Crystal Star exchange location to facilitate the cash-out of cryptocurrency transactions.

Following this, they proceeded to a solar panel trading company working between Lagos and Turkey. This company's operations suggest potential involvement in trade-based money laundering schemes. *(DH - ID3 and ID4)*



D. Identification of Employees

An activity scan conducted around the trade company (6.470216, 3.300636) during working hours for one week led to the identification of 13 device IDs belonging to employees of this company. The screenshot around the company's area sheds light on the network of individuals associated with this enterprise. *(AS - Trade Company)*

E. Encounters and Points of Interest (POI)

By executing POI query between Devices ID3, ID4, and the identified employees, several encounters were identified, particularly with Device ID28, at various locations in Lagos, notably two different Locations. *(DH - ID3 ID4 ID28)*

1. "Festac 3"

2. “Adetayo” Cafe

These encounters suggest potential meetings or transactions occurring between the suspects and key individuals within the network.

F. Background of Device ID28 - CEO of Solar Panel Trading Company

Executing a device history query of Device ID28, we discovered that they reside in DXB3173 building, AL Karama Street (6.4958823815,3.31767120329), serving as the CEO of the solar panel trading company associated with the suspicious activities. The screenshot capturing Device ID28's home address further solidifies their pivotal role in this investigation. *(DH - CEO Chinese Company)*

G. Previous Activities of Device ID3 in Istanbul

Tracing back through the device history query of Device ID3, we uncovered their visits to a Turkish solar Panel company located in Istanbul before their arrival to Lagos. This historical connection raises concerns regarding potential links between the suspects and the trade-based money laundering scheme through two different solar panel trading companies. *(DH - ID3)*

In summary, leveraging the capabilities of the VCIS tool, we have unveiled a suspicious nexus between the suspects and a Chinese company engaged in exporting solar panels to Europe through a Turkish intermediary company. This operation appears to disguise illicit funds through cryptocurrency transfers in Lagos, subsequently converting them into fiat currency for purchasing solar panels destined for the European market. These panels are then sold, integrating the laundered money into legitimate bank accounts under the guise of trading revenues. This sophisticated scheme underscores the significance of our ongoing investigation and the imperative need for further scrutiny by all involved parties.

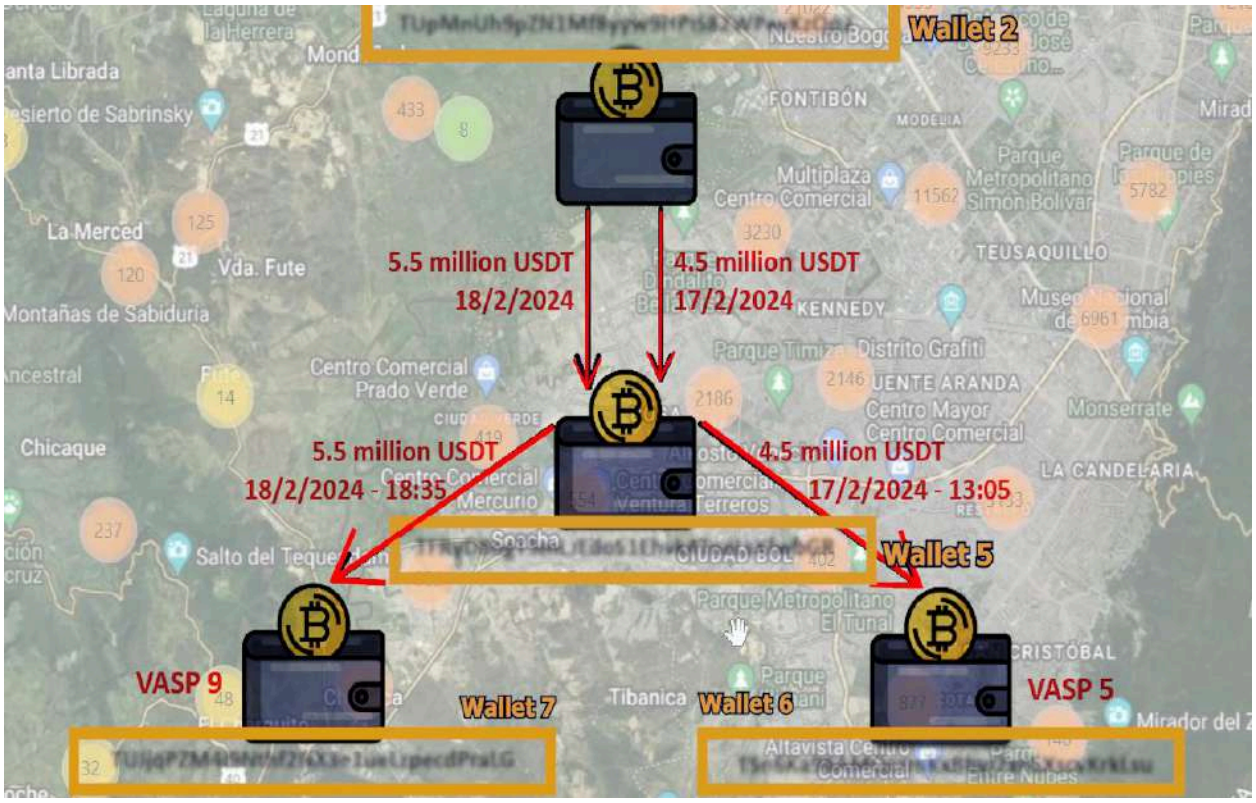
Chapter 3: New wallets' addresses involved in the money laundering

A. Illicit Money New Destinations

In this phase of our investigation, we leveraged the VCIS knowledge graph to analyze all transactions linked to the wallet address **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2**, source of illicit money, and its final destinations. Two new transactions were sent from this wallet to a new suspected address **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR**. The transactions flow is the following:

1. From **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** towards the wallet address **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR**
- On 17/2/2024, a transfer of $4.5 million
- On 18/2/2024, a transfer of $5.5 million

2. From **TFRyD8ogT5mLJEdoS1Ehvk4TnaLsXfwbGR** towards two new wallets
- **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsu** at 13:05 on 17/2/2024
- **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG** at 18:35 on 18/2/2024



B. VASPs Locations as Fixed Elements

We integrated fixed elements into our analysis, specifically the geo locations of known VASPs (Virtual Asset Service Providers) operating as exchange stores within Nigeria.

C. New Suspicious Wallet Address

We conducted an activity scan in proximity to these VASP locations within a 30-minute timeframe surrounding the aforementioned two transactions to identify which device ID moved to any of their locations in the same dates and times to exchange the cryptocurrencies into Fiat.

By comparing the transactions recorded on the Tron blockchain database through an AI engine to our geospatial database resulting from these activity scans around the VASPs' exchange stores , we conclusively identified that the common device located at two different virtual asset service providers locations on the same date and time of each one of these two transactions is device ID 4.

This device ID4 was consistently present at:

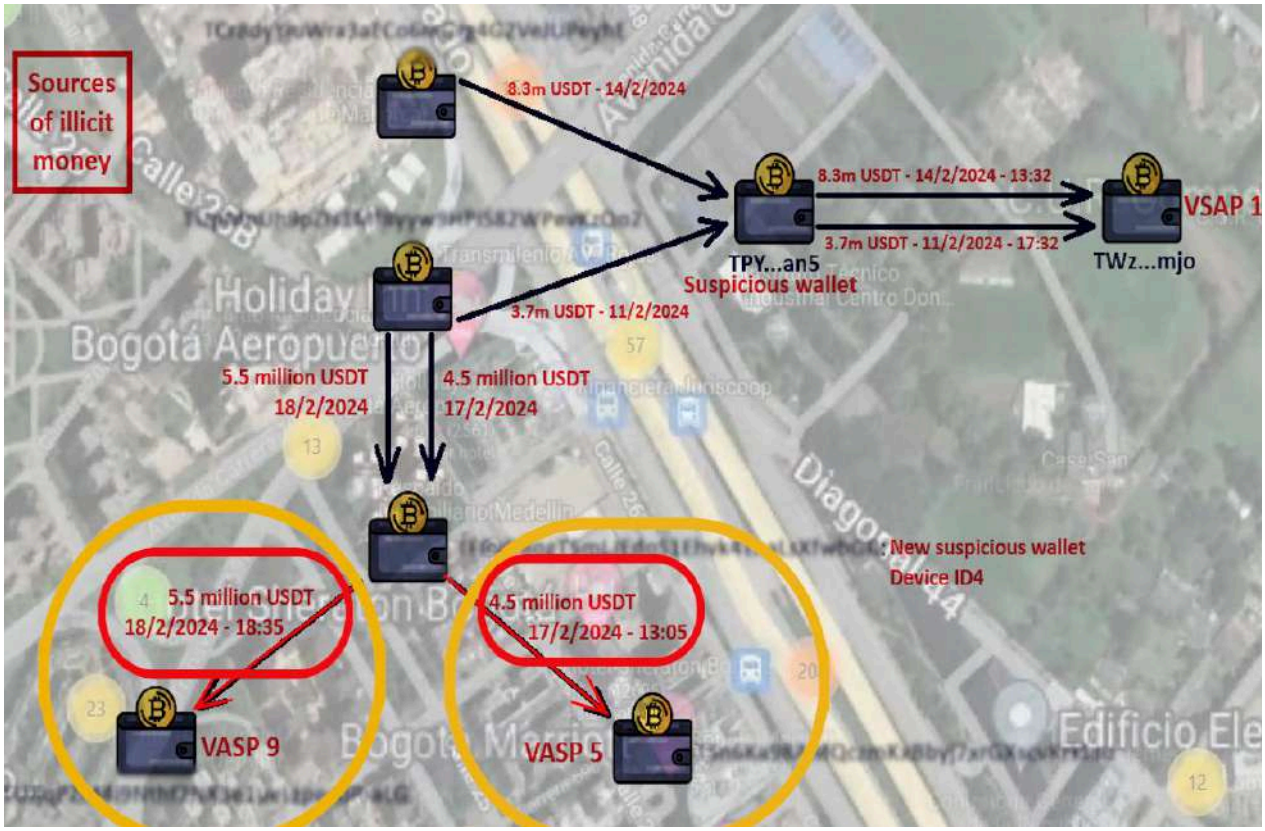
1. **VASP 5** (6.4906403656548495,3.3454441026910735) exchange store location while the first transaction was made at 13:05 on 17/2/2024 *(AS - VASP 5.)*

2. **VASP 9** (6.520315310442519,3.3800412080020497) exchange store location while the second transaction was made at 18:35 on 18/2/2024. (*AS - VAPS 9)*

Based on the previous findings, device ID4 is the owner of the wallet address **TFRyD8ogT5mLJEdS1Ehvk4TnaLsXfwbGR** who received funds from **TUpMnUh9pZN1Mf8yyw9HPiS82WPevKzQo2** and sent them to the VASP 5's wallet address **TSn6Ka98AMQczmKxBbyj7xrGXscvKrkLsu**, and the VASP 9's wallet address, **TUJjqPZM4i9Nthf2NX3e1ueLzpecdPraLG**, to cash them out.

In summary, our comprehensive analysis of the transactions involving these new wallet addresses unveils intricate connections within the money laundering network. By linking blockchain databases with geospatial insights and leveraging AI-powered analytics, we continue to unravel the complex web of illicit financial activities. The integrated use of VCIS tools and data visualization techniques provides compelling evidence to support ongoing investigative efforts and uncover additional layers of the laundering operation. Attached screenshots and detailed findings further document these critical advancements in our investigation and regulatory compliance measures.

Money Laundering Schema



Conclusion

This case study illustrates the multifaceted challenges posed by illicit financial activities within the realm of virtual assets.

The investigation outlined in this study exemplifies the pivotal role of advanced technological solutions like the VCIS in uncovering and dismantling sophisticated money laundering schemes. By leveraging geospatial data, telecommunication records, and transactional insights, law enforcement agencies can identify key actors, trace illicit funds, and disrupt criminal networks operating across borders.

The case also underscores the need for an advanced investigation tool to address the evolving tactics of financial criminals effectively.

Extrapolating to the UAE´s vision in the realm of virtual assets, and as the country continues to position itself as a leading hub for blockchain innovation, it is imperative to enhance investigation oversight and enforcement mechanisms to mitigate the risks associated with virtual asset activities. By harnessing the power of technology and collaboration, stakeholders can safeguard the integrity of the financial system and uphold the principles of transparency, security, and trust in the digital era.