Tracing more than a Billion Dollars: Using Geospatial/Location Intelligence to Combat Fraud and Corruption in Iraq

تعقّب أكثر من مليار دولار: استخدام تقنية تحليل الموقع الجغرافي المكاني لمكافحة الاحتيال والفساد في العراق

The Iraqi country's financial system has been plagued by corruption in the ministry of finance for many years. This insidious malpractice hindered economic growth, eroded public trust, and diverted crucial funds from their intended purposes. With fraudulent schemes and deceitful tactics coming to light, the need for a robust and dynamic approach to investigations has become more apparent than ever.

لقد استشرى الفساد في النظام المالي للدولة العراقية لسنوات عديدة بسبب الرشاوى في وزارة المالية. هذا السلوك المشين أدّى إلى إعاقة التقدم الاقتصادي، وزعزعة ثقة، حيث تمّ تحويل مبلغ مهم من الأموال العامة عن الاستخدامات اللازمة لها نتيجة لهذا الاحتيال الخبيث. مع كشف مخططات الاحتيال والتكتيكات الغادرة، أصبحت الحاجة لتحقيق قوي وديناميكي أكثر بروزاً من قبل مضى.

The fight against corruption in Iraq requires innovative solutions, such as leveraging advanced technologies like VALOORES Crowd Intelligence System to uncover hidden trails of embezzlement and ensure accountability within the ministry.

تتطلب مكافحة الفساد حلولاً مبتكرة، كالإستفادة من التقنيات المتقدمة مثل نظام *VCIS* للكشف عن المسارات الخفية للاختلاس والاحتيال والفساد وضمان المساءلة والمحاسبة داخل الوزارة.

Table of Contents

قائمة المحتويات

Introduction

After the occupation in 2003, the occupiers began to dismantle the Iraqi state and solve the Iraqi army and other security forces and create chaos in the country and dismantle the moral and social fabric of the country and spread sectarian, ethnic factors and destruction of social infrastructure and technical infrastructure, the absence of control fully. The reasons mentioned altogether occurred in Iraq, making the country lives in chaos unparalleled not only in ancient history and in the modern history, this chaos made it easier for the beneficiaries and thieves and traitors and warmongers and those who are in power to exploit this situation and exploit their influence in order to steal the whole of Iraq. The continuation of this will lead to economic and political security and social disasters.

In the heart of Iraq's financial system lies a web of corruption that has long plagued the nation's economic progress and trust in its government. The Ministry of Finance, tasked with managing crucial financial matters, has been grappling with the insidious presence of fraudulent activities and misappropriation of funds. This troubling revelation came to light in December 2022 when the ministry discovered a staggering four billion dollars fraudulently withdrawn from its official bank account.

مقدّمة

بعد احتلال دولة العراق في عام 2003، عمد المحتلون إلى تفكيك الدولة العراقية وحل الجيش العراقي والقوى الأمنية الأخرى وخلق الفوضى في البلاد وتفكيك النسيج الأخلاقي والاجتماعي ونشر العوامل الطائفية والعرقية وتدمير البنية التحتية الاجتماعية والبنية التحتية التقنية، مع غياب سيطرة الدولة بشكل تام. هذه الأسباب المنوه عنها، جعلت البلاد تعيش في فوضى لا مثيل لها ليس فقط في التاريخ القديم ولكن أيضًا حتى في التاريخ الحديث، مما سهل للمستفيدين واللصوص والخونة وهواة الحروب و لأولئك الذين يتمتعون بالسلطة بالاستفادة من هذا الوضع واستغلال تأثيرهم من أجل سرقة كامل مقدّرات الدولة العراقية. حيث إنّ استمرار هذا الوضع سيؤدي إلى كوارث اقتصادية وسياسية واجتماعية.

تتغلغل في قلب النظام المالي العراقي شبكة فساد أثرت بشكل كبير على تقدم البلاد اقتصاديًا وثقة المواطنين في حكومتهم. تكلفت وزارة المالية، الموكل إليها إدارة الشؤون المالية الحاسمة، بالتصدي للأنشطة الاحتيالية وسوء استخدام الأموال العامة. لقد ظهرت هذه المشاكل إلى العلن في ديسمبر 2022 عندما اكتشفت الوزارة عملية إختلاس اموال عامة بقيمة أربعة مليارات دولار بشكل احتيالي من حسابها البنكي الرسمي.

A sinister scheme unfolded as four seemingly legitimate companies, armed with authentic checks issued by the ministry, deceitfully claimed compensation for taxes they had paid in advance. Over a span of ten months, these fake entities orchestrated 10 check withdrawals, leaving the ministry in disarray and the culprits untraceable.

The modus operandi of the corruption was nothing short of organized, with swift actions taken to register the fake companies using falsified documents. An unknown broker acted as an intermediary, concealing the identities of the perpetrators, who used authentic passports with false information and VOIP applications to communicate anonymously.

In this document, we delve into the depths of this corruption and embark on a dynamic investigation, driven by the innovative VALOORES Crowd Intelligence System. Through intricate data analysis, location intelligence, and device history patterns, we seek to identify the masterminds behind this audacious "Heist of the Century" and expose their intricate network of deceit.

تمّ اكتشاف المخطّط الشرّير بعدما طالبت أربع شركات تبدو شرعية، بحوزتها شيكات أصلية صادرة عن الوزارة، باسترداد مبلغ كبير من الضرائب المدفوعة سلفاً بشكل مخادع ومغاير للواقع . حيث على مدى عشرة أشهر، قامت هذه الكيانات الوهمية بعشر عمليات سحب بواسطة هذه الشيكات، ممّا ترك الوزارة في حالة من الفوضى دون إمكانية تعقب الجناة.

لم تكن طريقة عمل الفساد أقل من منظّمة، حيث تم اتّخاذ إجراءات سريعة لتسجيل الشركات الوهمية باستخدام وثائق مزورة، وقام سمسار مجهول بدور الوسيط، لإخفاء هويّات الجناة، الذين استخدموا جوازات سفر أصلية تحتوي على معلومات مزيفة وتطبيقات VOIP للتواصل مع بعضهم البعض بشكل مجهول.

في هذه القضية، سنتعمّق في التحقيق حول أعمال الفساد الحاصلة من خلال مباشرة تحقيق ديناميكي، مدعوماً بنظام VALOORES Crowd Intelligence System المبتكر. حيث إننا من خلال تحليل البيانات المعقدة، والمواقع الجغرافية، وتاريخ أنماط حركة الأجهزة الخليوية، نسعى إلى تحديد العقول المدبرة التي تقف وراء "سرقة القرن" وكشف شبكة الإحتيال المعقدة الخاصة بهم.

Case Study

1. Elements

- The registry of companies
- The Ministry of Finance
- A Iraqi bank
- A politically influential person
- The general director of the ministry of finance
- The director of tax department
- A high-ranking employee in the department of passports
- Several brokers and smugglers

2. Story

The Iraqi government imposes on the petroleum companies that gain a contract the obligation to pay the tax in advance during the phase of registration. These taxes are deposited in the ministry of finance's official bank account at an Iraqi bank in Baghdad. Later, if the company doesn't succeed in its trade, it can apply for recompense for what it was paid.

During December 2022, the ministry of finance detected that more than a billion dollars were fraudulently withdrawn from its bank account to the benefit of four different companies. These companies had represented to the Iraqi bank checks issued from the ministry of finance in order to recompense taxes paid before. They were authentic checks.

دراسة الحالة

1. العناصر

- سجل تسجيل الشركات
- وزارة المالية
- بنك عراقي
- شخصية نافذة سياسياً
- المدير العام لوزارة المالية
- مدير مصلحة الضرائب
- موظف رفيع المستوى في دائرة الجوازات
- العديد من السماسرة والمهربين

2. قصة

تفرض الحكومة العراقية على شركات النفط الفائزة بالمناقصات، الالتزام بدفع الضريبة بشكل مسبق خلال مرحلة التسجيل، حيث يتمّ إيداع هذه الضرائب في الحساب البنكي الرسمي لوزارة المالية لدى أحد البنوك العراقية. لاحقاً، إذا لم تنجح الشركة في أعمالها التجارية، يمكنها التقدّم بطلب إسترداد الضرائب المدفوعة سلفاً.

كشفت وزارة المالية، خلال شهر ديسمبر 2022، عن سحب أكثر من مليار دولار بطريقة احتيالية من حسابها المصرفي لصالح أربع شركات مختلفة. حيث كانت هذه الشركات قد تقدمت لدى المصرف العراقي بشيكات صادرة عن وزارة المالية لاسترداد الضرائب المدفوعة من قبل. لقد كانت تلك الشيكات أصلية.

These four companies used 10 checks to withdraw this huge amount of money from the ministry of finance's official bank account over the course of 10 months, between February and December 2022. The four fake companies were registered within a short time before the requests for compensation; all documents used for the registration were falsified. No phone numbers are related to those companies. There is no additional information at the registry of companies. All papers were presented to the Ministry of Finance indirectly through an unknown broker, and the checks were signed by several employees at the ministry.

Usually, the process of issuing checks from the ministry is a long, bureaucratic one. However, in this case, the checks were signed shortly after the requests were presented to the ministry, which reflects organized corruption. The perpetrators are unknown; they use authentic passports with fake information and operate with only VOIP applications through an internet hotspot to communicate between them without using SIMs to avoid being traceable by law enforcement authorities.

حيث استخدمت هذه الشركات، عشرة شيكات لسحب هذا المبلغ الضخم من الحساب البنكي الرسمي لوزارة المالية على مدار عشرة أشهر، بين شهري فبراير وديسمبر من العام 2022. وكان قد تمّ تسجيل الشركات الوهمية الأربع خلال فترة قصيرة قبل طلبات التعويض والإسترداد؛ بعد أن تمّ تزوير جميع المستندات المستخدمة في عملية التسجيل. لا توجد أرقام هواتف خليوية مرتبطة بتلك الشركات لدى التسجيل. لا توجد أي معلومات إضافية في سجل تسجيل الشركات. كان تمّ تقديم جميع الأوراق إلى وزارة المالية بشكل غير مباشر عبر وسيط مجهول، وتمّ توقيع الشيكات من قبل عدد من الموظفين في الوزارة.

عادةً ما تكون عملية إصدار الشيكات من الوزارة عملية طويلة وبيروقراطية. لكن في هذه الحالة، تمّ التوقيع على الشيكات بعد وقت قصير من تقديم الطلبات إلى الوزارة، وهو ما يعكس الفساد المنظم الحاصل. الجناة غير معروفين. يستخدمون جوازات سفر أصلية تحتوي على معلومات مزيفة ويستخدمون للتواصل فيما بينهم فقط تطبيقات التواصل من خلال عناوين بروتوكول الإنترنت VOIP عبر شبكة الإنترنت حصراً دون استخدام شرائح خطوط SIM لتجنّب تتبعهم من قبل سلطات إنفاذ القانون.

Scenario

Chapter 1: The beneficial owners of Fake Companies

A Device Travel Pattern **DTP** was executed in three areas of interest in order to identify the common devices that are the suspects in founding the fake companies, receiving the checks from the ministry of finance, and using them to withdraw the cash.

- the registry of the company's department (on the four different dates when the four companies are registered)
- the ministry of finance's department (on the period between the date of presenting the requests for compensation and the date of receiving the checks from the taxes department)
- the Iraqi Bank (on the period between the date of presenting the checks to the bank and the date of receiving the payment)

The results showed three devices that visited the three mentioned areas, as seen in the screenshots below;
(DTP: Ministry - Registry - Bank)

سيناريو

الفصل الأول: تحديد المستفيدون الحقيقيون من الشركات الوهمية

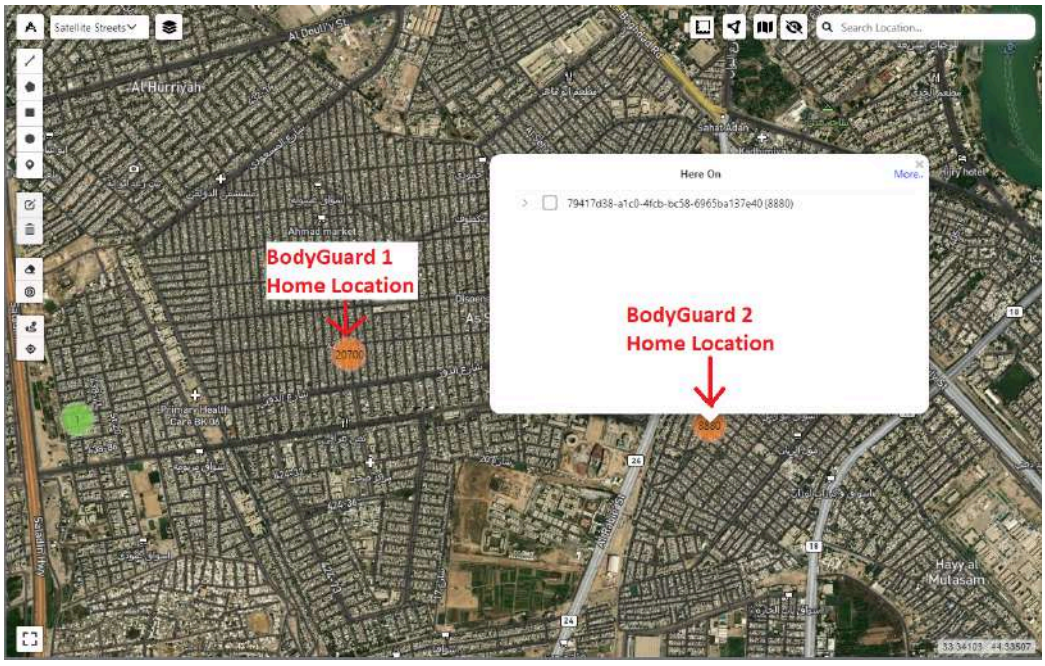
تم استخدام خاصية تحديد نمط حركة الجهاز **DTP** في ثلاث مناطق اهتمام بهدف التعرّف على الأجهزة المشتركة المشتبه بها بتأسيس الشركات الوهمية واستلام الشيكات من وزارة المالية واستخدامها لسحب الأموال.

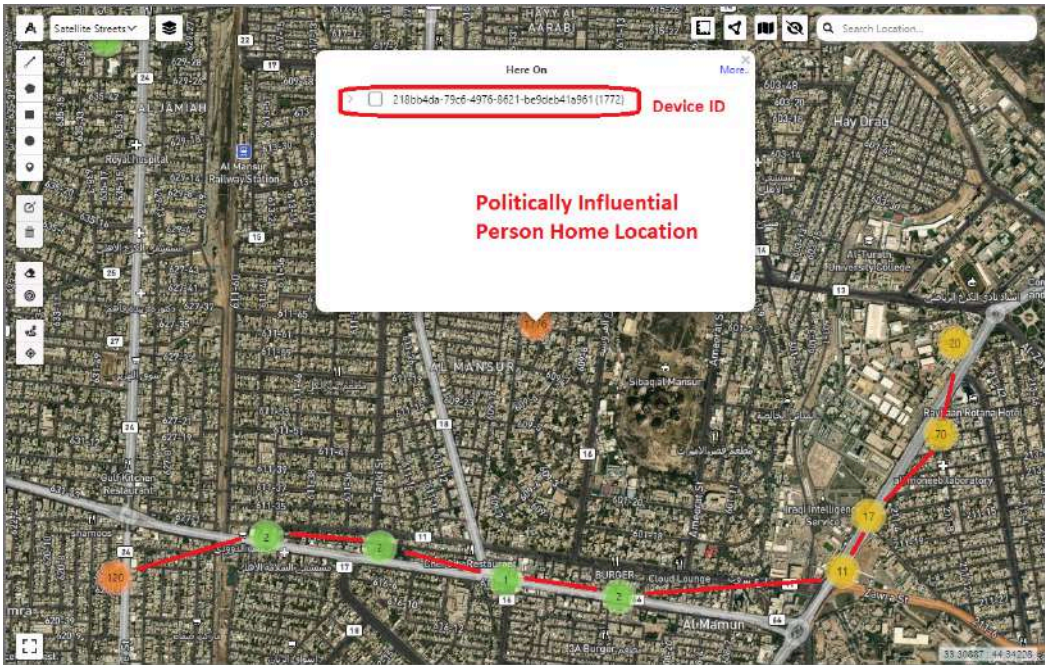
- سجل تسجيل الشركات (في التواريخ الأربعة المختلفة لدى تسجيل الشركات الأربع)
- دائرة وزارة المالية (في الفترة الزمنية ما بين تاريخ تقديم طلبات التعويض وتاريخ استلام الشيكات من دائرة الضرائب)
- البنك العراقي (في الفترة ما بين تاريخ تقديم الشيكات للبنك وتاريخ استلام الدفعات المالية)

وأظهرت النتائج تحديد ثلاثة أجهزة خليوية قامت بزيارة المناطق الثلاثة المذكورة، كما هو موضح في الصور أدناه؛
(DTP: Ministry - Registry - Bank)

Executing a Device History **DH** for each of these three suspects allowed us to discover their identity, home location, and behavior. The first one is a politically influential person with political connections, and the two other guys are his bodyguard and his driver.

ثم قمنا بإستخدام خاصية تاريخ حركة الجهاز **DH** لكل من الأجهزة الخليوية الثلاثة المشتبه بها مما سمح لنا باكتشاف هويتهم وتحديد مواقع منازلهم وسلوكهم الإعتيادي، فتبين أن الأول هو شخص ذو نفوذ سياسي وله علاقات سياسية، والرجلان الآخران هما حارسه الشخصي وسائقه.





Chapter 2: The links between the suspects and the public sector employees

Executing an activity scan query **AS** around the ministry of finance for a period of 6 months. After that, we applied the filter tool in order to narrow down the results to be limited to the devices of all employees and brokers who usually visit the site during official working hours only, which led us to identify 50 different devices.
(ministry of finance activity scan)

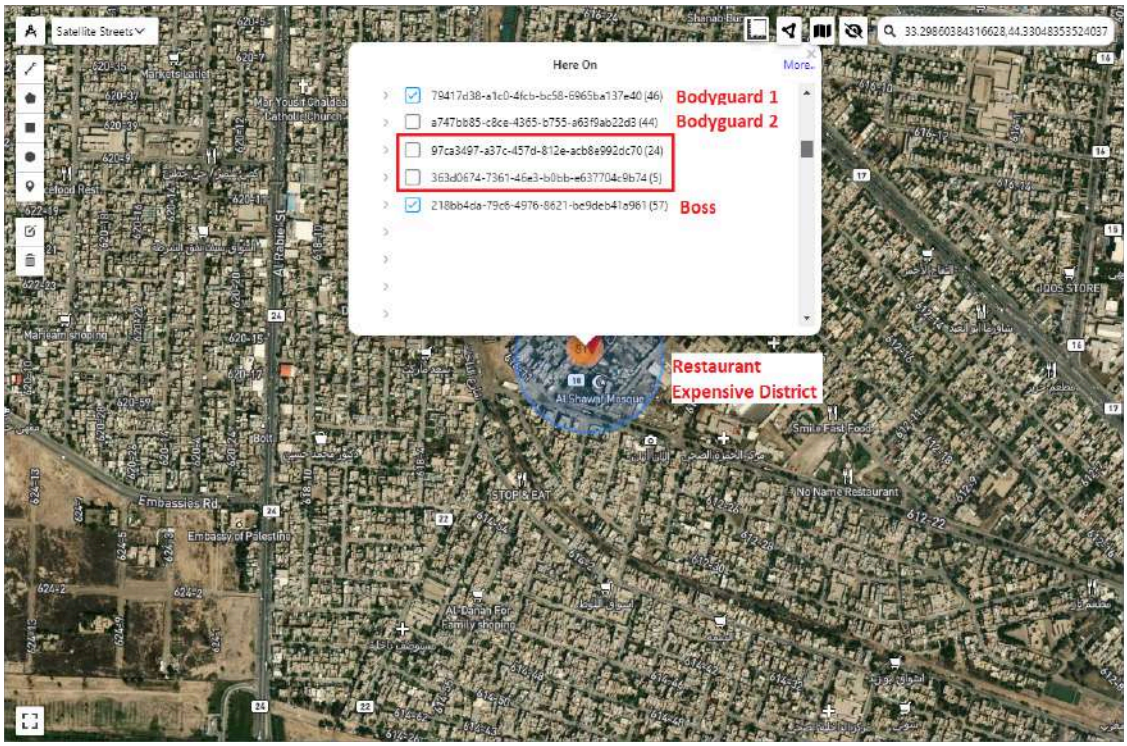
الفصل الثاني: تحديد الروابط بين المشتبه بهم الثلاثة وموظفي القطاع العام

قمنا بإستخدام خاصية مسح نشاط الأجهزة **AS** حول وزارة المالية لمدة 6 أشهر. بعد ذلك قمنا بتطبيق أداة التصفية من أجل تضييق النتائج لتقتصر على أجهزة جميع الموظفين والوسطاء الذين عادة ما يزورون الموقع خلال ساعات العمل الرسمية فقط، مما أدى بنا إلى تحديد 50 جهازاً مختلفاً.

(ministry of finance activity scan)

Executing a **POI** query for the Boss, his bodyguards, and the 50 devices detected through the previous activity scan led us to determine several encounters between the politically influential person, his bodyguards, and two other devices from the ministry of finance at a restaurant in an expensive district of Baghdad.
(POI: Boss & Bodyguards)

قمنا بإستخدام خاصية تحديد نقاط الإهتمام المشتركة **POI** فيما ما بين الشخص ذو النفوذ السياسي وحارسيه الشخصيين من جهة والأجهزة الخمسين التي تم اكتشافها من خلال الإستعلام السابق من جهة أخرى، مما سمح لنا من تحديد عدّة لقاءات بين الشخص النافذ وحراسه الشخصيين وجهازين آخرين من وزارة المالية في أحد المطاعم في حي راقٍ وثري من العاصمة بغداد. *(POI: Boss & Bodyguards)*



Executing a Device History **DH** for each of these two suspects from the ministry of finance allowed us to discover their identity, home location, and behavior. The first one is the general manager of the ministry of finance, and the second is the director of the tax department.
(General Manager HD- Director of the tax department DH)

ثم تم إستخدام خاصية تاريخ حركة الجهاز **DH** لكلّ من الجهازين المشتبه بهما من وزارة المالية الأمر الذي سمح لنا بتحديد هويتهما وموقع منزلهما وسلوكهما الإعتيادي. الأوّل هو مدير عام وزارة المالية، والثاني مدير دائرة الضرائب.
General Manager HD- Director of the tax) (department DH

This analysis allows us to identify the potential suspects in the ministry of finance who are involved in providing the politically influential person with checks for compensation for the fake companies and withdrawing the money from the ministry of finance's bank account.

لقد أتاح لنا هذا التحليل التعرّف على المشتبه بهم المحتملين في وزارة المالية المتورّطين في تزويد الشخص النافذ سياسياً بشيكات إسترجاع الضرائب للشركات الوهمية الأربع وسحب الأموال من الحساب البنكي لوزارة المالية.

الفصل الثالث: تحديد سلوكيات المشتبه بهم واصولهم محلياً ودولياً

باستخدام تقنية إستخبارات الموقع الجغرافي VCIS Location Intelligence، تمكّنّا من اكتشاف المنازل والعقارات للمشتبه بهم، لا سيما من خلال إستخدام خاصية تاريخ حركة الجهاز **DH**، والتي سمحت لنا أيضاً باكتشاف الوقت الدقيق الذين اشتروا فيه تلك الأصول وبالتالي تحديد متى بدأوا في غسل إيراداتهم غير المشروعة عن طريق شراء الأصول ومن ضمنها تلك غير المسجلة على أسمائهم.

لقد قمنا بإستخدام خاصية تاريخ حركة الجهاز **DH** بين عامي 2019-2022 لكل من أجهزة المشتبه بهم الخمسة، ممّا سمح لنا بمعرفة أنشطتهم وتحركاتهم الدولية، كالبلدان التي يترددون لزيارتها بشكل متكرر، أو أي مواقع أو عنوانين محددة اعتادوا على زيارتها. حيث قد تكون هذه العناوين المتكررة أصولاً مثل المنازل أو المتاجر أو العقارات أو مؤسسات مالية يستخدمونها لغسل أموالهم.
وقد أظهر التحليل الجغرافي:

1. يعيش السياسي النافذ في منطقة ثرية بالعاصمة بغداد، وعادة ما يسافر إلى عدّة دول أوروبية. كما يزور نفس المبنى في شارع باهظ الثمن في إسطنبول كما أحد البنوك التركية هناك، ممّا يدلّ على أن لديه عقارات وحساباً مصرفياً هناك. (*boss device history*)

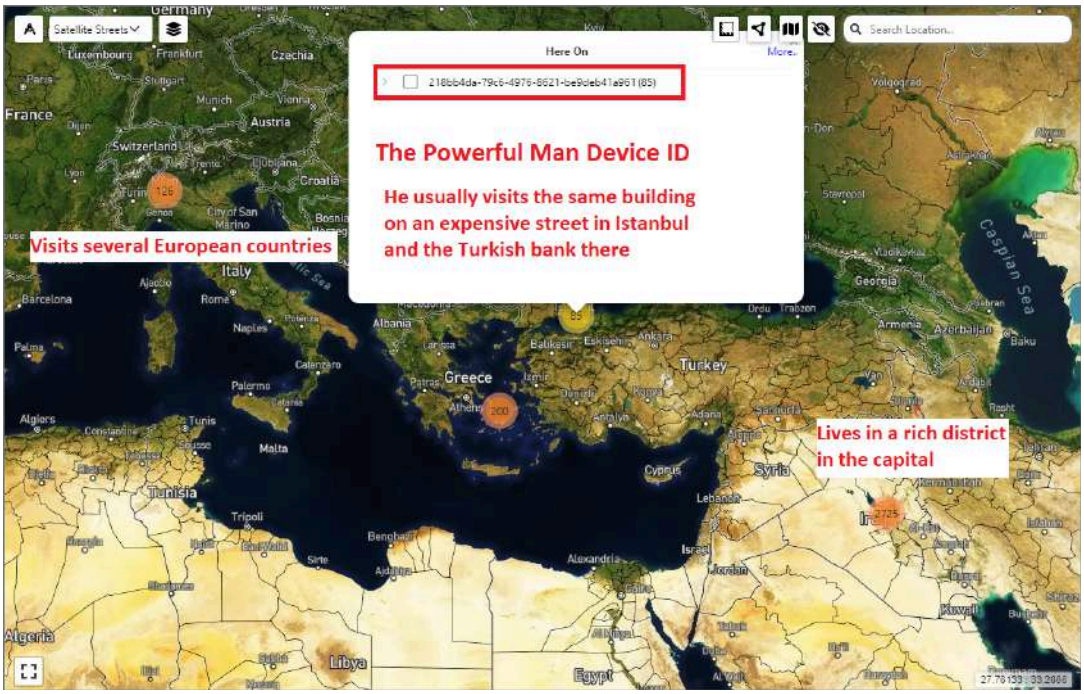
Chapter 3: The Suspects' behaviors and their Assets Locally and Internationally

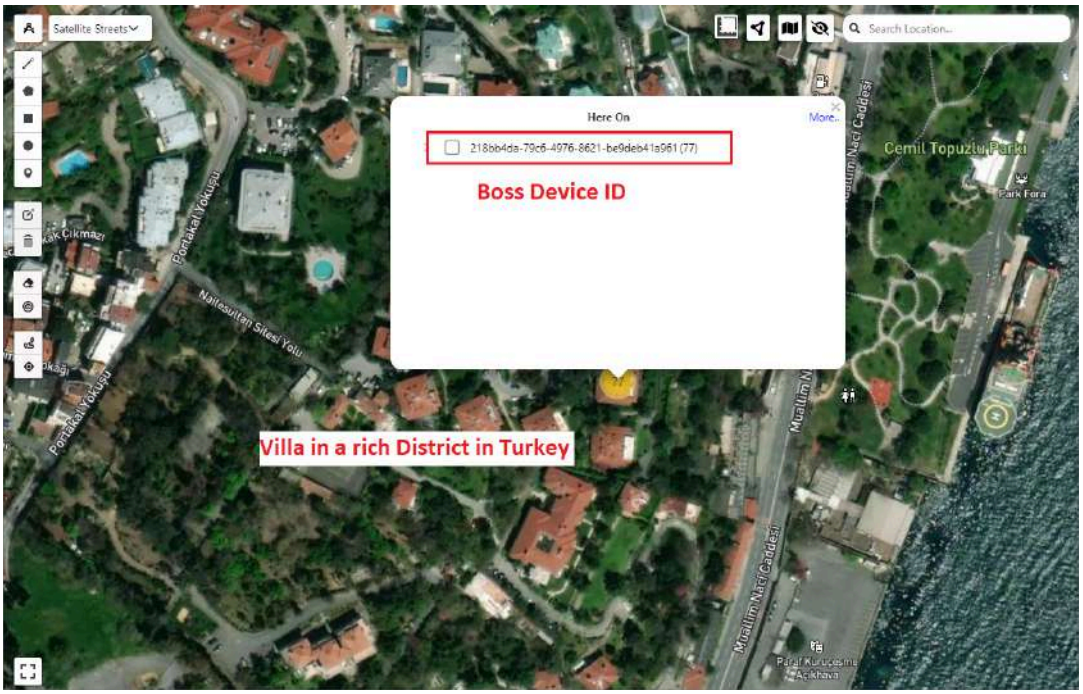
Using the VCIS Location Intelligence, we were able to detect suspects houses and real estate by executing a DH query, which allows us to also detect the exact time they bought those assets and thus identify when they started to use their money to launder their illicit revenues by buying assets that aren't registered in their names.

We executed a Device History **DH** query between 2019-2022 for each of the five suspects, which allowed us to see their international activities, like the frequent countries they frequented and if there was any specific location or address they used to visit. These frequent addresses might be assets like houses, shops, real estate, or a financial institution where they used to launder their money.

The geo-analysis showed:

1. The powerful man lives in a rich district in the capital, and he usually travels to several European countries. He usually visits the same building on an expensive street in Istanbul and the Turkish bank there, which indicates that he has real estate and a bank account there. *(boss device history)*



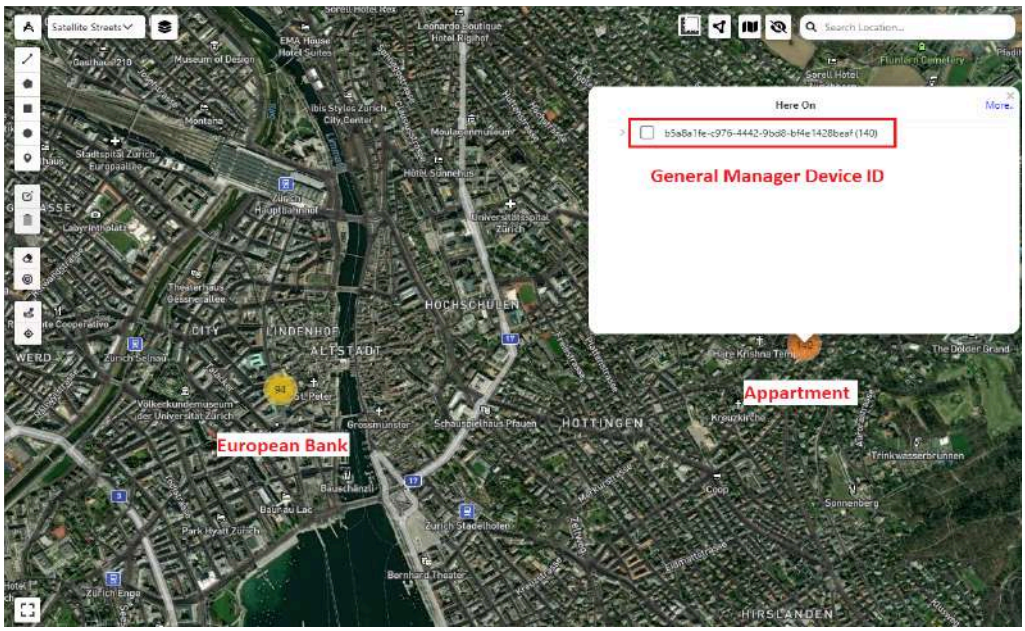


2. The two bodyguards live in the suburbs of the capital, and they travel from time to time with their boss to Turkey.
(bodyguards device history)

2. يعيش الحارسان الشخصيان في ضواحي العاصمة، ويسافران بين الحين والآخر مع رئيسهما إلى تركيا. *(bodyguards device history)*

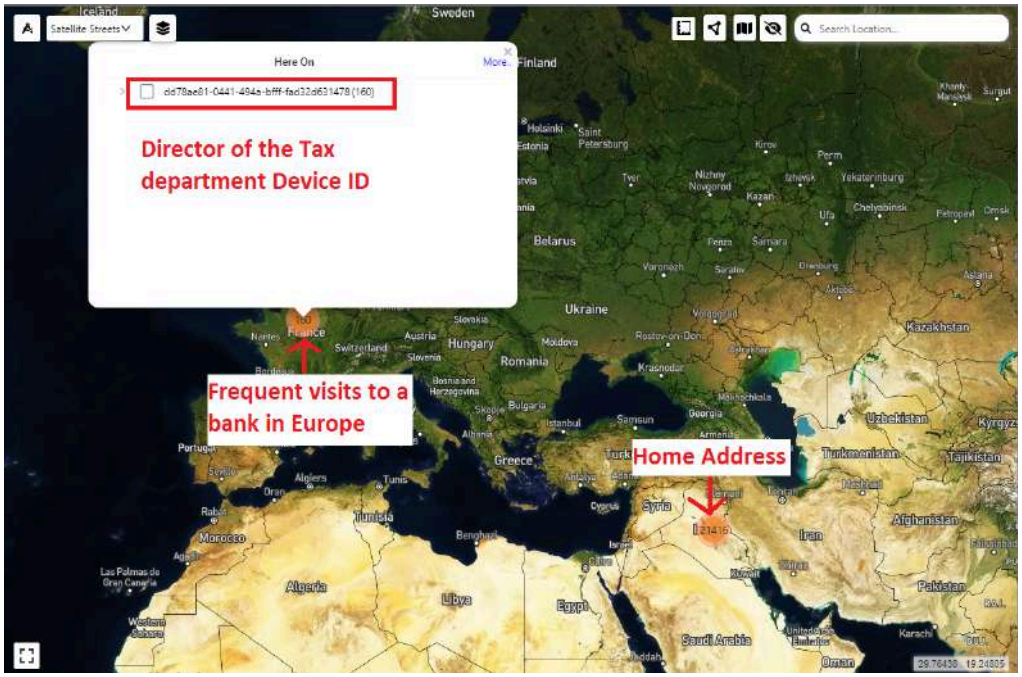
3. The general manager of the ministry of finance lives in the capital and he travels between the Gulf and European countries where he frequently visits a European bank and stays in an apartment; this probably indicates that he has a bank account there. *(general manager device history)*

3. مدير عام وزارة المالية يعيش في العاصمة ويتنقّل بين دول الخليج والدول الأوروبية حيث يزور أحد البنوك الأوروبية بشكل متكرر ويقيم في شقّة هناك؛ مما يشير هذا إلى أن لديه حساباً مصرفيّاً هناك.
(general manager device history)



4. The director of the tax department lives in Baghdad, usually travels to a city in Europe to stay in the same building and frequents a bank there, which indicates that he has an apartment and a bank account there. *(Director of the tax department)*

4. مدير مصلحة الضرائب يعيش في العاصمة بغداد، وعادة ما يسافر إلى إحدى مدن أوروبا للإقامة في مبنى واحد ويتردد إلى أحد البنوك هناك، ممّا يدل على أن لديه شقة وحساباً مصرفياً هناك.
(Director of the tax department)



Chapter 4: The money - smuggling tactic and its final destination

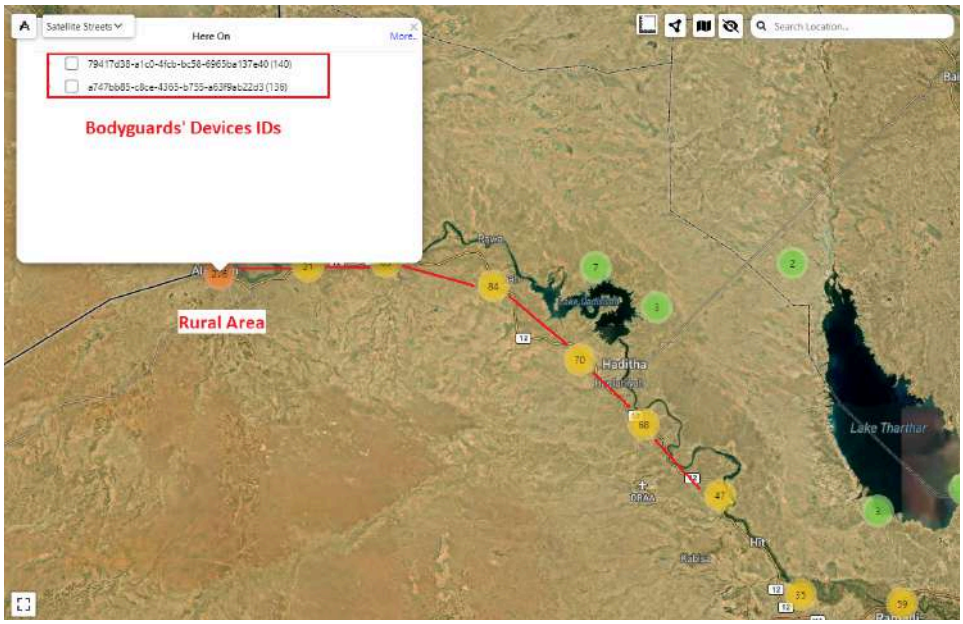
Executing a Device History query **DH** for the three main suspects led us to map that the two bodyguards, after being located at the Iraqi bank in the capital:

1. They are moving several times north to the borders between Syria and Iraq and staying at a house located in a rural area, as seen in the screenshot below. (*Bodyguards DH 2018-2019)*

الفصل الرابع: الأموال – تكتيك التهريب ووجهتها النهائية

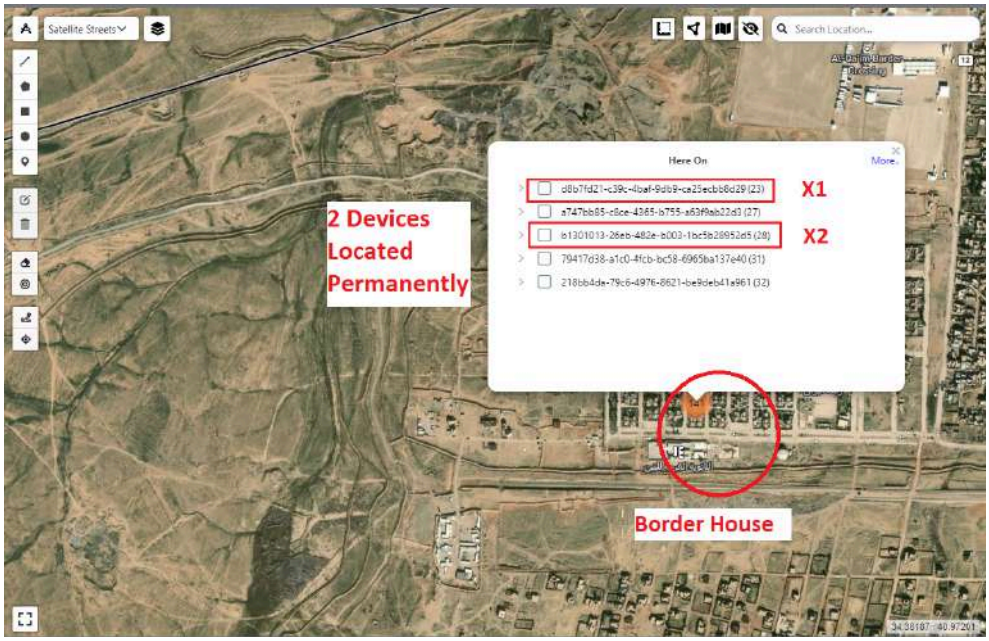
من خلال تنفيذ خاصية تاريخ حركة الجهاز **DH** للمشتبه بهم الثلاثة الرئيسيين قادتنا إلى تتبّع مسار الحارسين الشخصيين، حيث بعد تواجدهما في محيط البنك العراقي في العاصمة وقبض الاموال:

1. كانا قد انتقلا عدّة مرات شمالاً إلى منطقة حدودية بين العراق وسوريا وأقاما في منزل يقع في منطقة ريفية، كما هو موضح في لقطة الشاشة أدناه.
(*Bodyguards DH 2018-2019*)



من خلال إستخدام خاصية مسح نشاط الأجهزة **AS** حول المنزل الريفي الأخير، تمكنا من تحديد جهازين موجودين بشكل دائم هناك، وهما X1 وX2 .
(Border home activity scan)

Using the activity scan around the latter house, we recognized two devices located permanently there, named X1 & X2.
(Border home activity scan)

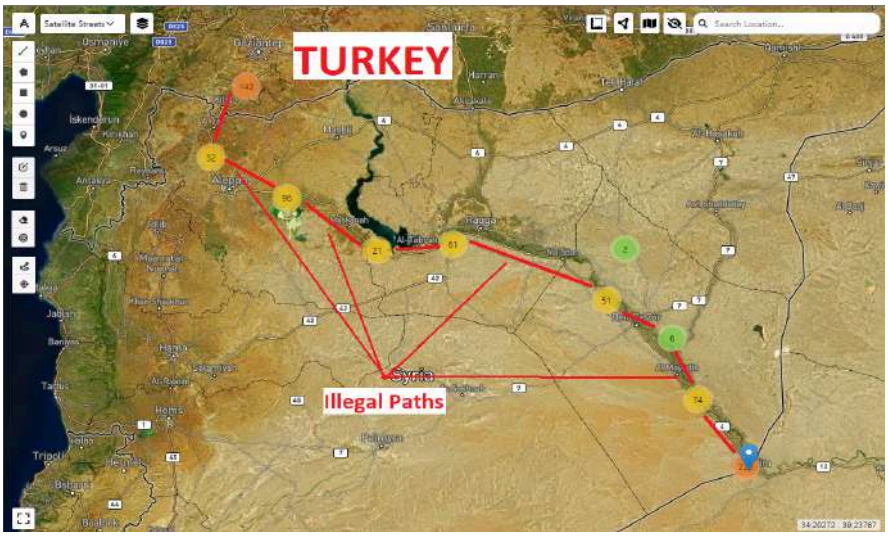


ثم إنّ تنفيذ خاصية تاريخ حركة الجهاز **DH** عن X1 وX2 أظهرت لنا أنهما يتنقلان بين منزلهما الحدودي وتركيا عبر مسارات غير شرعية، مما يدل على أنّهما متورّطان في التهرّيب عبر الحدود،

Executing a device history query **DH** for X1 and X2 showed us that they are moving between their border house and Turkey using illegal paths between them, which indicates that they are involved in

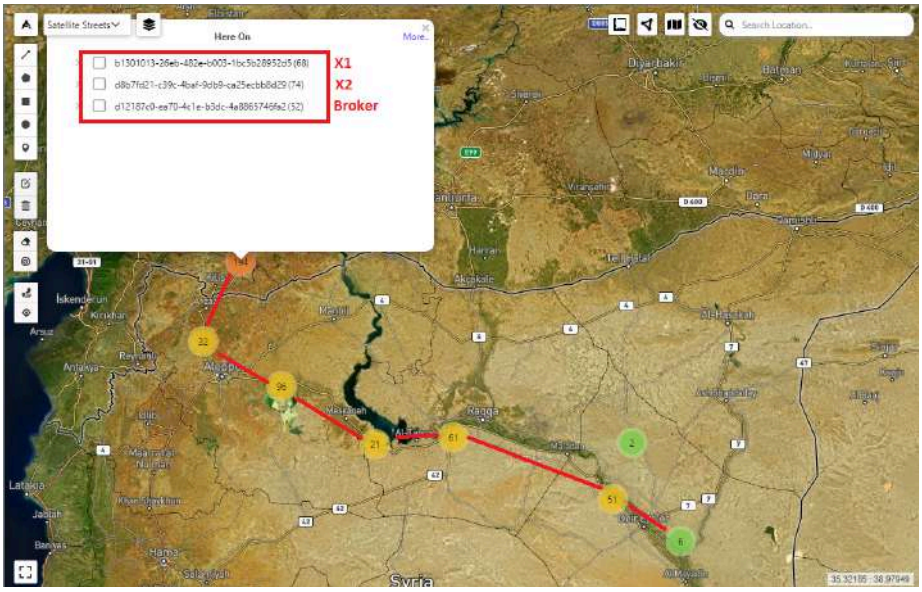
smuggling through the borders and that the sums of money are exported outside towards the Turkish territories.
(Smugglers X1-X2 DH)

وأن المبالغ المالية المقبوضة كان يتم تهريبها إلى الخارج باتجاه الأراضي التركية.
(Smugglers X1-X2 DH)



We executed a **Co-traveler** query for X1 and X2 devices that led us to identify a device that is moving simultaneously with them from the Turkish border to Gaziantep village, which designates that there are those who are involved in using and laundering money there.
(Co-Traveler X!, X2 & Broker)

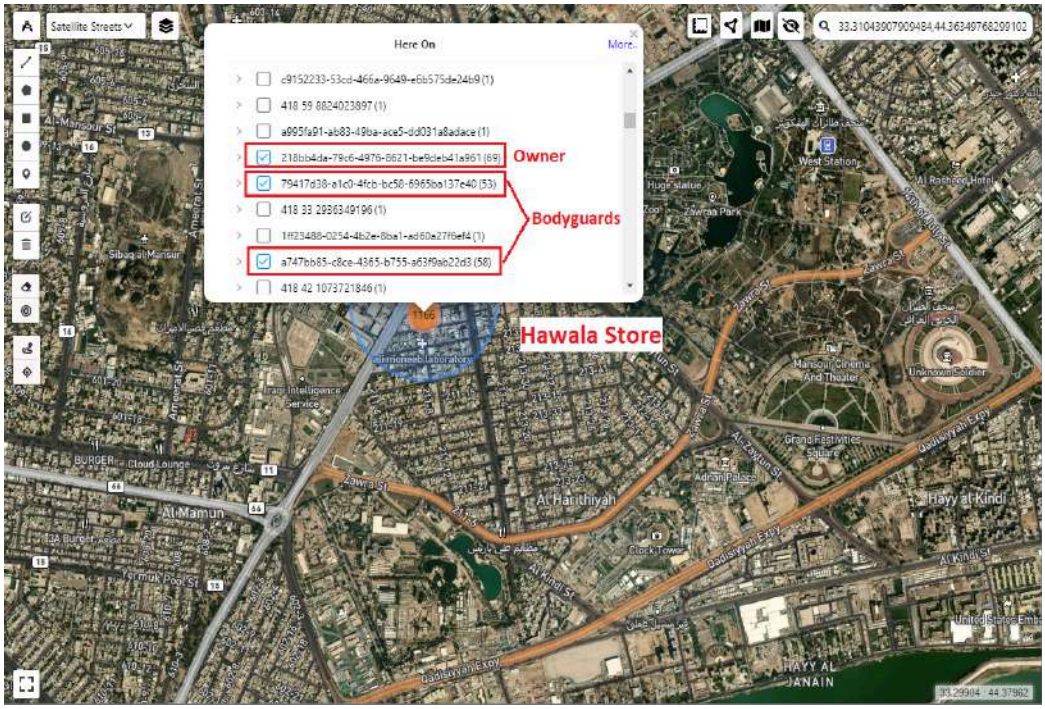
لقد نفذنا خاصية الاستعلام عن المسافر المرافق بالنسبة لجهازي X1 وX2 خلال انتقالهما على مسالك التهريب قادتنا إلى التعرف على جهاز يتحرك بشكل متزامن معهما من الحدود التركية إلى قرية غازي عنتاب، وهو ما يعني أنّ هناك من هو متورط في استخدام الأموال وتبييضها هناك. *(Co-Traveler X!, X2 & Broker)*



2. كانا X1 وX2 قد انتقلا عدة مرات إلى مكتب حوالة غير شرعية بالقرب من العاصمة بغداد، حيث تبين هناك وجود دائم لجهاز خليوي خلال ساعات العمل (حيث من المحتمل جداً أن يكون مالك المكتب)، حيث كانت تجتمع هذه الأجهزة الثلاثة معاً في نفس الموقع الجغرافي لمدة حوالي الساعة، كما نرى في لقطة الشاشة أدناه، ممّا يقودنا إلى تحديد أن الرجل السياسي النافذ يستخدم القطاع المالي غير الرسمي لتحويل الأموال إلى الخارج لتجنب تعقبه من قبل السلطات الوطنية. ومن المحتمل أنه يتم تحويل الأموال إلى إسطنبول، حيث يوجد نشاط كبير للحوالات غير الرسمية وحيث كان الرجل النافذ وعائلته يسافرون بشكل متكرر.

(Hawala Activity Scan)

2. X1 and X2 are moving several times at a Hawala store near Baghdad, where we detect a permanent presence of a device in the working hour (which probably belongs to the owner), and all these three devices met together at almost the same time for one hour, as we can see in the screenshot below, which leads us to identify that the powerful man is using the informal financial sector to transfer money abroad to avoid being tracked by the national authorities. Probably the funds are transferred to Istanbul, where there is a large activity of informal hawala and where the powerful man and his family used to travel frequently. (*Hawala Activity Scan)*

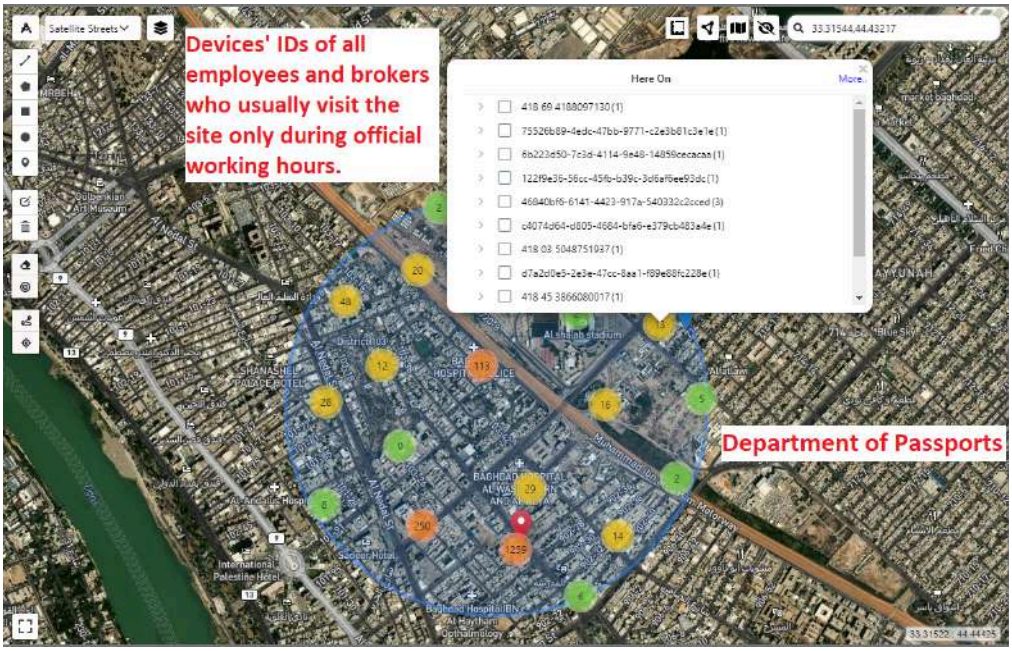


Chapter 5: The source of fake passports

Executing an **Activity Scan** query around the Department of Passports for the period between June and December 2022. After that we apply the filter tool in order to narrow down the results to be limited to the devices of all employees and brokers who usually visit the site during official working hours only.
(30 devices detected - employees)
(*Department of Passports AS)*

الفصل الخامس: مصدر جوازات السفر المزورة

قمنا تنفيذ خاصية مسح نشاط الأجهزة **AS** حول دائرة الجوازات للفترة ما بين يونيو وديسمبر 2022. بعد ذلك، قمنا باستخدام أداة التصفية لتضييق نطاق النتائج لتقتصر على أجهزة جميع الموظفين والوسطاء الذين عادة ما يزورون الموقع خلال ساعات العمل الرسمية فقط، حيث تم الكشف عن 30 جهاز عائدين للموظفين.
(Department of Passports AS)



Going back in time to 2021, we executed a **POI** query for the three suspected devices and the 30 devices that resulted from the previous query. We identified a continuous meeting with one of the 30 devices in a location south of Baghdad.
(POI: Boss - Bodyguards- Passports Officier)

وبالعودة إلى عام 2021، قمنا بتنفيذ خاصية تحديد نقاط الإهتمام المشتركة **POI** فيما بين الأجهزة الثلاثة المشتبه بها (الشخص النافذ ومرافقيه) والـ 30 جهازاً الناتجة عن الاستعلام السابق، حيث تمكنا من تحديد اجتماعاً مستمرّاً مع أحد الأجهزة الخليوية من الأجهزة الثلاثون.
(POI: Boss - Bodyguards- Passports Officier)

قمنا بتنفيذ خاصية تاريخ حركة الجهاز **DH**، ممّا دفعنا إلى التعرّف على عنوان منزله وهويته، وتبين أنّه ضابط رفيع المستوى من إدارة الجوازات. لذلك اكتشفنا أنه هو من كان يزود المشتبه بهم بجوازات سفر أصلية تتضمن معلومات مزيّفة تستخدم في عملية تسجيل الشركات الوهمية.

(passport officer device history)

We executed a Device History query **DH,** which led us to identify his home address and identity. He is a high ranking officer from the Department of Passports; therefore, we discovered that he was providing the suspects with authentic passports with fake information used in the companies' registration process.

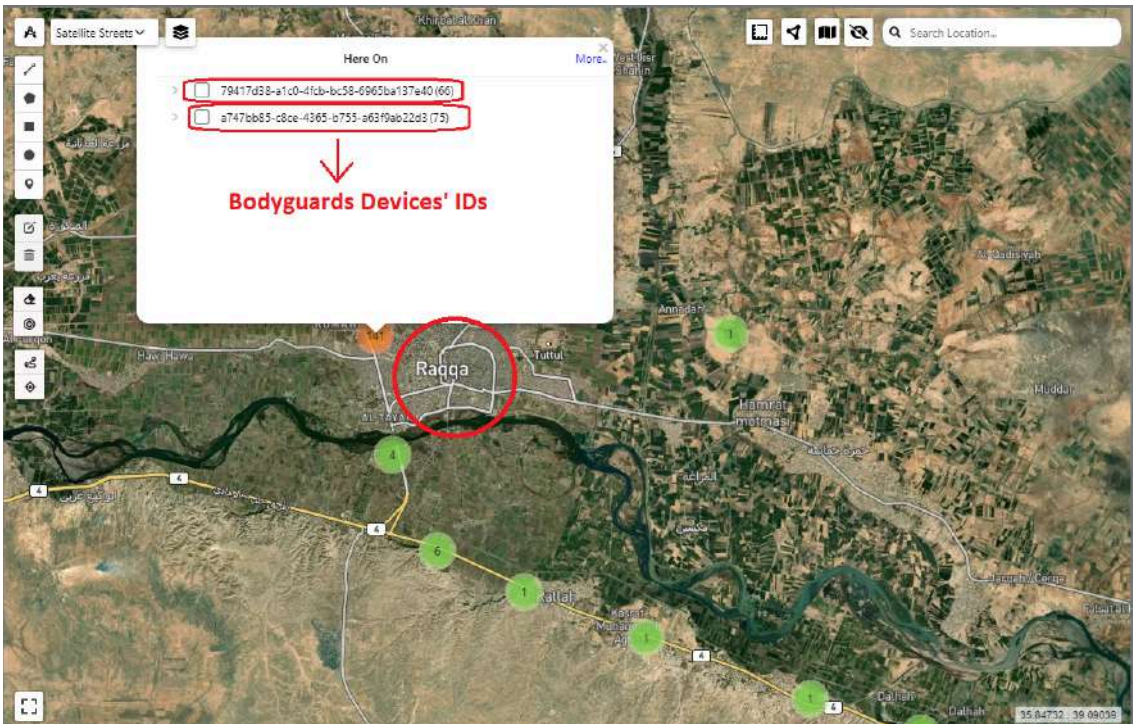
(passport officer device history)

Chapter 6: Other criminal links

Going back in time between 2019 and 2020, we executed a Device History query **DH** for the devices of the two bodyguards; therefore, we identified their location in an area that was under the control of the ISIS group.
(Bodyguards DH 2018-2019)

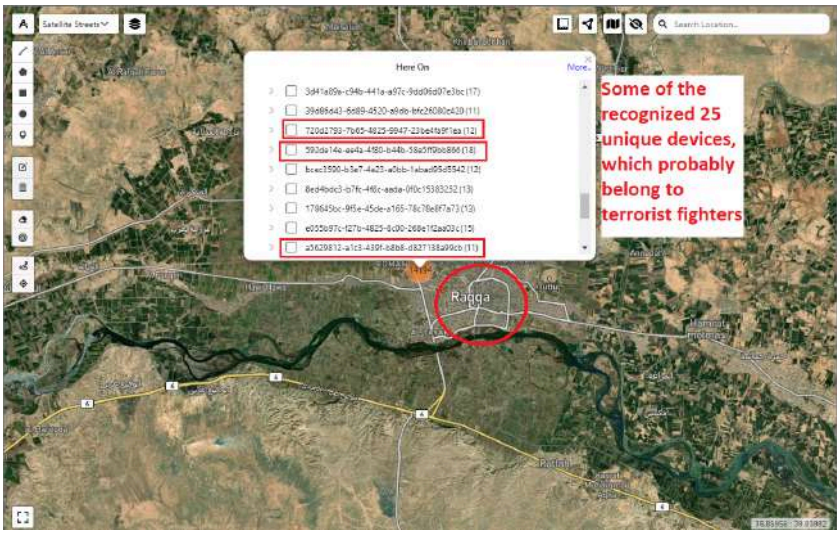
الفصل السادس: الروابط الإجرامية الأخرى

وبالعودة بالزمن إلى ما بين عامي 2019 و2020، قمنا باستخدام خاصية تاريخ حركة الجهاز **DH** لأجهزة الحارسين الشخصيين؛ مما مكّننا من رصد موقعهما في منطقة كانت تحت سيطرة تنظيم داعش.
(Bodyguards DH 2018-2019)



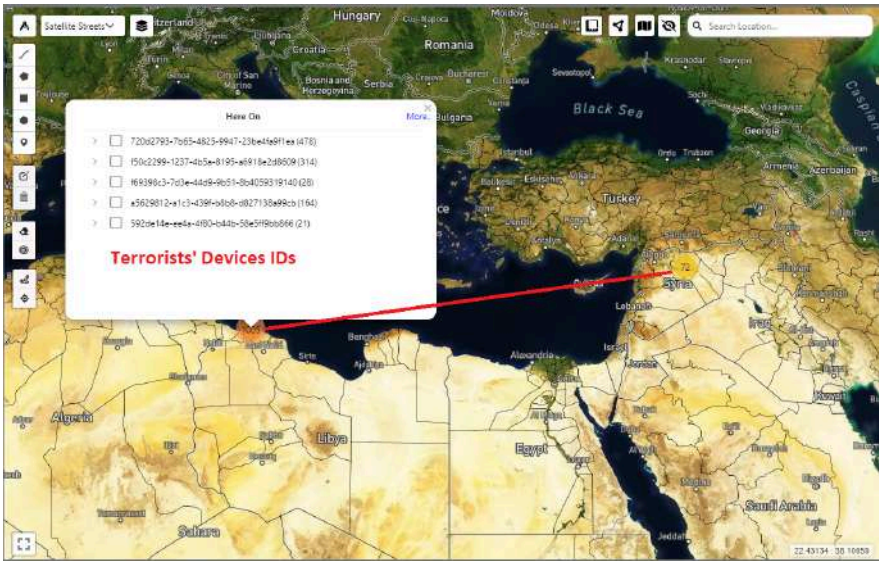
By executing an **AS** around this area, we recognized twenty-five unique devices, which probably belonged to fighters with this terrorist group. *(Raqqa activity scan)*

عبر تنفيذ خاصية مسح نشاط الأجهزة **AS** في هذه المنطقة، تمكنا من تحديد 25 جهازاً فريداً، يرجح أنها كانت مستخدمة لمقاتلين مع هذه المجموعة الإرهابية. *(Raqqa activity scan)*



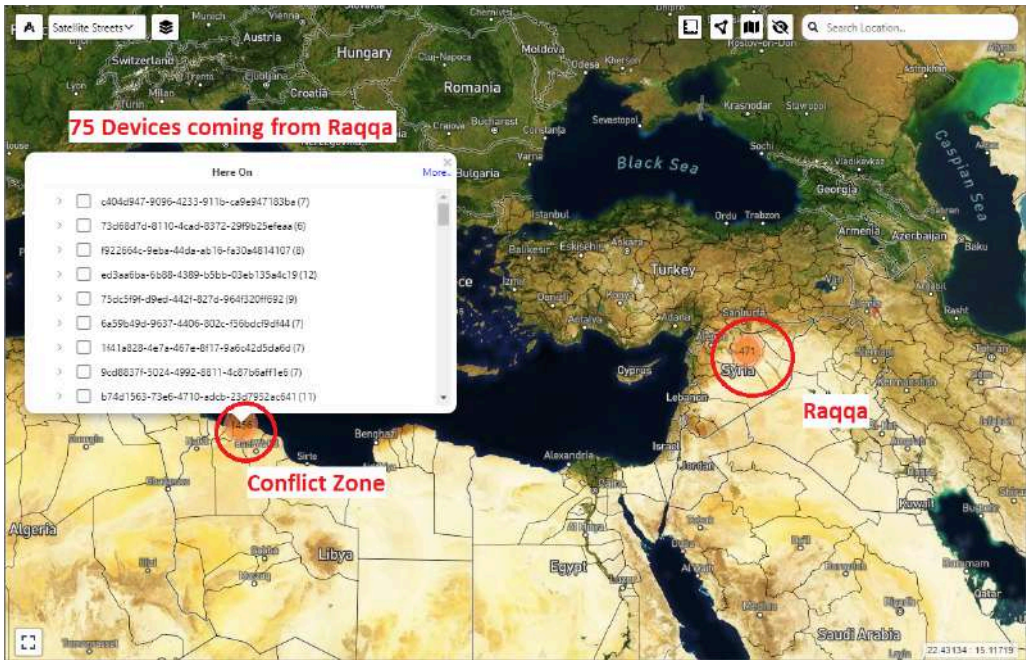
بعد تنفيذ خاصية تاريخ حركة الجهاز **DH** تبين أن هناك خمسة أجهزة انتقلت من سوريا إلى منطقة نزاع في شمال أفريقيا.
(terrorists device history)

Executing the device history **DH**, it became evident that five devices moved from Syria to a conflict zone in North Africa. *(terrorists device history)*



ثم من خلال تنفيذ خاصية تحديد نمط حركة الجهاز **DTP** بين منطقة الرقة ومنطقة النزاع، تمكنا من تحديد 75 جهازاً انتقلوا أيضاً من الرقة إلى منطقة النزاع.
(conflict zone and Raqqa hits)

Executing the **DTP** functionality between two areas *(Raqqa zone and Conflict zone)* allows us to detect 75 devices that were also moved from Raqqa to the conflict zone. *(conflict zone and Raqqa hits)*



خاتمة

تسلط النتائج الاستنتاجية لهذه الدراسة على فعالية VALOORES Crowd Intelligence System في معالجة الاحتيال المالي المعقد والشبكات الإجرامية. النجاح الذي تمّ تحقيقه في فك لغز تعقيدات السيناريو المستقصى يشهد على فعالية النظام في تحليل اللحظات الزمنية وإقامة الروابط بين نقاط البيانات المتنوعة. لعب VCIS دوراً حيوياً في الكشف عن الحقيقة المخفية في طبقات التضليل للسحب الاحتيالية، كاشفاً شبكة دقيقة من الغش التي ظلّت خفيّة.

وكان من الأمور الأساسية لهذا النجاح النشر الحكيم لمعلومات الموقع المتقدمة والاستعلامات المعقدة والتحليل المستنير لأنماط الأجهزة. ساهمت هذه العناصر مجتمعة في التعرف على المشتبه بهم، وفك تكتيكات تهريب الأموال، وشرح الروابط المعقدة داخل الشبكة الإجرامية. تعتبر هذه الدراسة حالة مثلى، تعرض كيف يظهر VCIS كقوة فعّالة في مواجهة الأنشطة

Conclusion

The conclusive findings of this case study underscore the remarkable efficacy of the VALOORES Crowd Intelligence System (VCIS) in addressing intricate financial fraud and criminal networks. The success achieved in unraveling the complexities of the investigated scenario attests to the system's potency in parsing through temporal nuances and establishing connections among diverse data points. VCIS played a pivotal role in unveiling the truth concealed within the deceptive layers of fraudulent withdrawals, exposing an intricate web of deceit that had remained veiled.

Central to this success was the judicious deployment of advanced location intelligence, intricate queries, and insightful analysis of device patterns. These elements collectively contributed to the identification of suspects, unraveled money-smuggling tactics, and elucidated

الإجرامية المعقدة. يُسلط الضوء على قدرته على حماية نزاهة الأنظمة المالية وتعزيز السلامة العامة من خلال استخدامه العاقل في هذا البحث. قصة نجاح VCIS في هذا السياق تسلط الضوء على إمكانياته كحليف قوي في الحرب المستمرة ضد أشكال الجريمة المتزايدة تعقيداً. تؤكد الدروس المستفادة من هذه الحالة على أهمية الاستفادة من التكنولوجيا المتقدمة والأنظمة الذكية لتعزيز الدفاع ضد الاحتيال المالي، مساهمةً في نهاية المطاف في تحقيق هدف الحفاظ على نزاهة الهياكل المالية وضمان سلامة الجمهور.

the intricate links within the criminal network.

This case study serves as an exemplar, showcasing how VCIS emerges as a formidable force in combating sophisticated criminal activities. Its capacity to safeguard the integrity of financial systems and bolster public safety is underscored by its adept utilization in this investigation. The success story of VCIS in this context highlights its potential as a robust ally in the ongoing battle against increasingly sophisticated forms of criminality. The lessons drawn from this case emphasize the significance of leveraging cutting-edge technologies and intelligent systems to fortify defenses against financial malfeasance, ultimately contributing to the overarching goal of upholding the integrity of financial structures and ensuring the safety of the public.