My first OSINT CTF. Operation Runner.

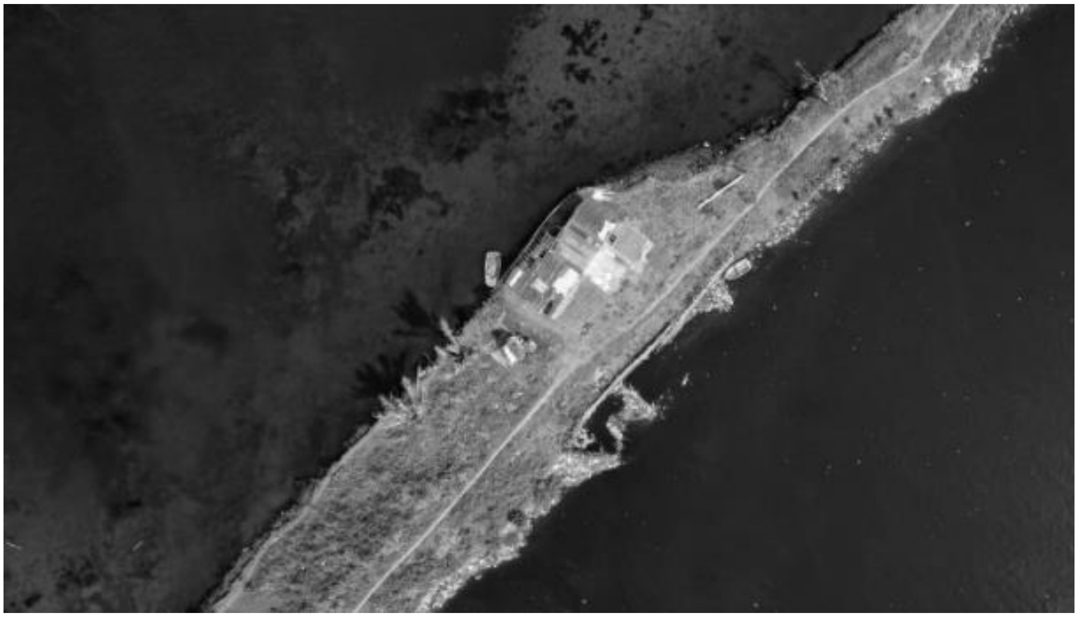
TABLE OF CONTENTS

I. Introduction.

In this monthly CTF organized by **Hacktoria** (https://hacktoria.com/monthly-ctf/operation-runner/), I had to find out the address where the Kotova family was located based on their daughter instagram profile. https://www.instagram.com/elenamkotova/

II. Step 1.

Firstly, I took a look at the CTF presentation image.



The picture seemed to be taken with a drone or directly from a satellite imagery provider. Reverse searching with **Google Lens** did not help me, but **Google Images** did. I got some pages that included similar images and all of them were posted between 2017 and 2019 on www.pexels.com, which is a website with free photos. I tried some combinations of keywords on that website, but nothing came out.

Reverse searching with **Yandex** helped me with the full coloured image.

Reverse searching again the full coloured image with **Google Images** and **Yandex** did not help me. That it where **Bing** came with an answer. It gave me the exact post on www.pexels.com. The image was posted by T.F. who is a (drone) photographer and it was taken in **Teluknaga, Indonesia**. I did not know if this would prove to be helpful in any way but I got it covered. It might be a hint that the Kotova Family lives on a coast or something like that.

III. Step 2.

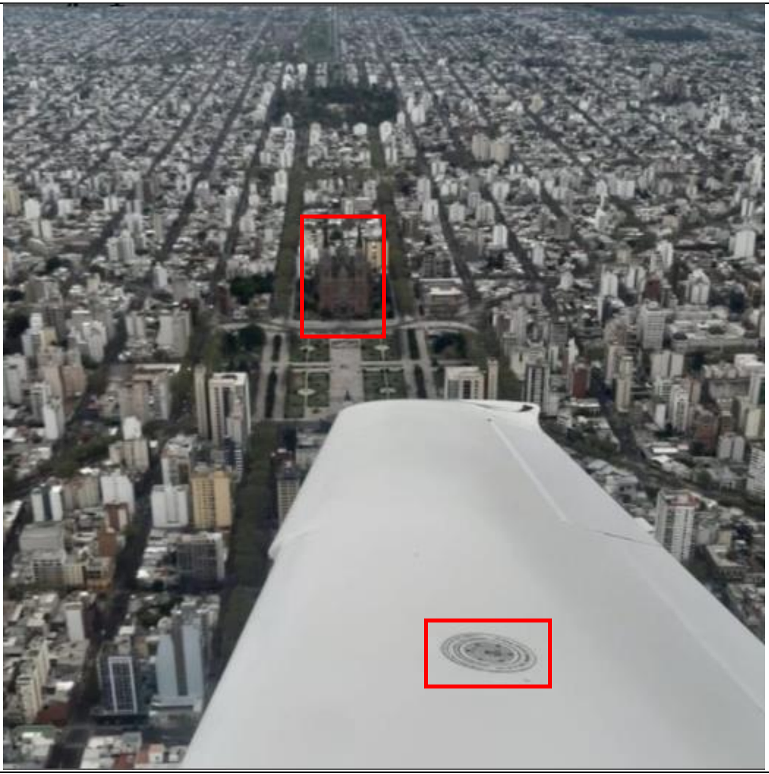
Back to the instagram, I saw that I was dealing with a teenage Russian girl. I started to analyze all her posts because the followers/following accounts did not give me any leads. The hashtags/profile picture did not indicate any location, so I had to rely only on GEOINT.

*The timestamps (GMT) of the posts were collected based on the JSON data that the instagram servers provide. Kudos to **@nixintel** blog post about this (the link the blog post can be found at the end of the write-up).*

Post no. 1

(Tuesday, January 18, 2022 9:53:46 PM)

Description: *"OMG **the landing with this tiny plane was so scary!** 😥😯 But the views were amazing and so **glad to spend time here with my family**. I will show you tomorrow **what this place looks like** ❤️"*



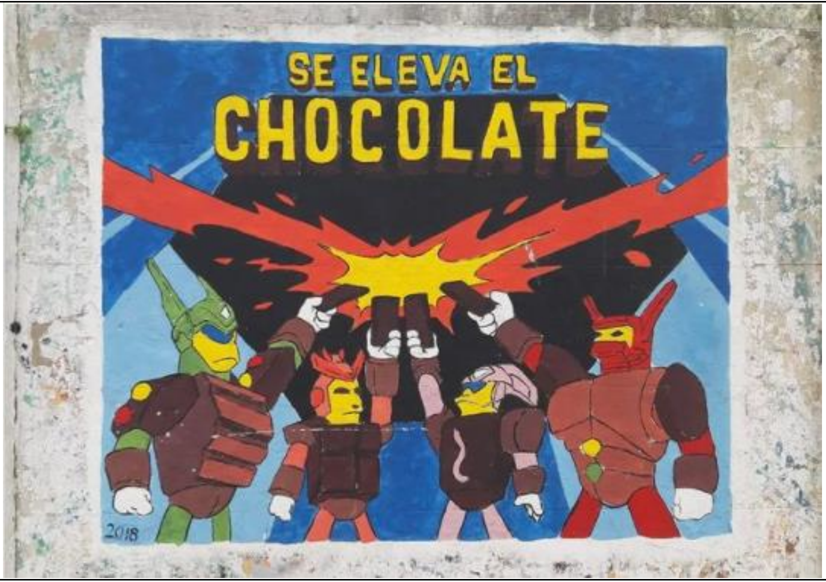
- From the bolded statements, I assumed that the Kotova family used a private plane (*"tiny plane")* and they landed in that city (*"what this place looks like"*).
- I saw the round-shaped symbol on the plane's wing, but I did not insist on that one (I did not find anything at first sight so I left it behind).
- The image indicated me that they were above the center of a big city and one obvious element was that gothic cathedral.

- The image was taken above **La Plata, Argentina** based on **post no. 6** (*see details below*).
- I searched for some airports and aerodroms in **La Plata, Argentina** but I did not find anything.

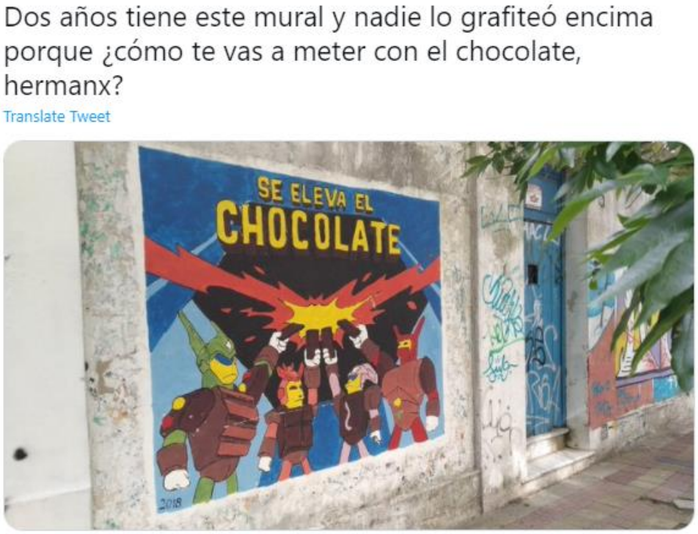
Post no. 6

(Thursday, January 20, 2022 4:31:50 PM)

Description: n/a

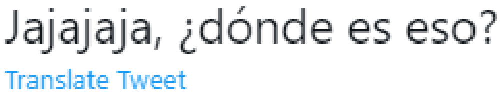


- This seemed to be a mural wall about some Simpsons cartoons.
- Reverse searching it on **Google Images** gave me a twitter post from a person **B.** which said that the mural had not been touched in the last 2 years.

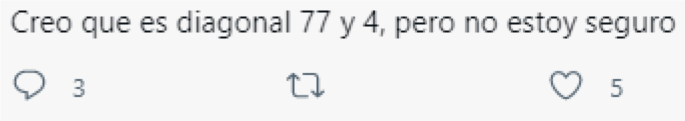


Dos años tiene este mural y nadie lo grafiteó encima porque ¿cómo te vas a meter con el chocolate, hermanx?

- From Mr. **B**'s twitter profile I observed that he declared his location being **La Plata, Argentina**.
- I always check the comments so my luck was that someone asked in the comments *"¿dónde es eso?"* and he got this response back *"Creo que es diagonal 77 y 4, pero no estoy seguro"*; as I come from a latin country, I could easily understood that without using any translation guide.

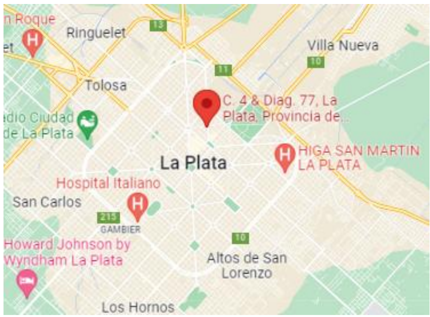


Jajajaja, ¿dónde es eso?

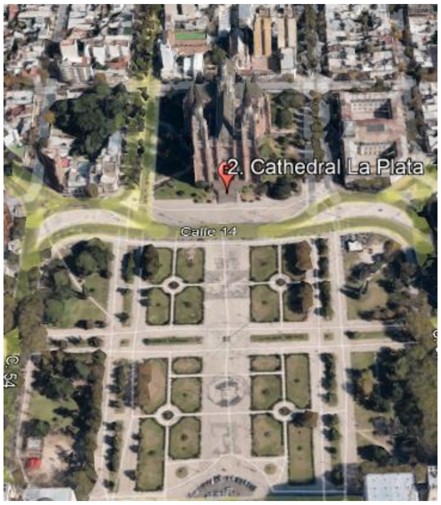


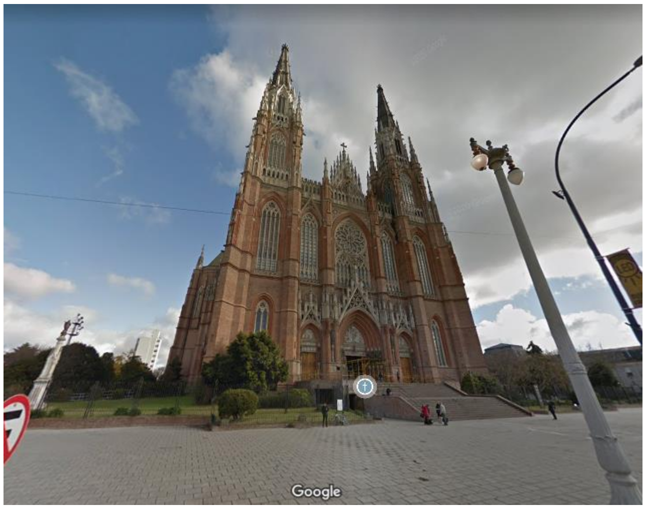
Creo que es diagonal 77 y 4, pero no estoy seguro

- I googled *"diagonal 77 y 4"* and I got a checkpoint in **La Plata, Provincia de Buenos Aires, Argentina**.



- Based on the **post no.1** I started to search around that area for a gothic cathedral and I found it right in the center of the city (**Cathedral de la Plata**).

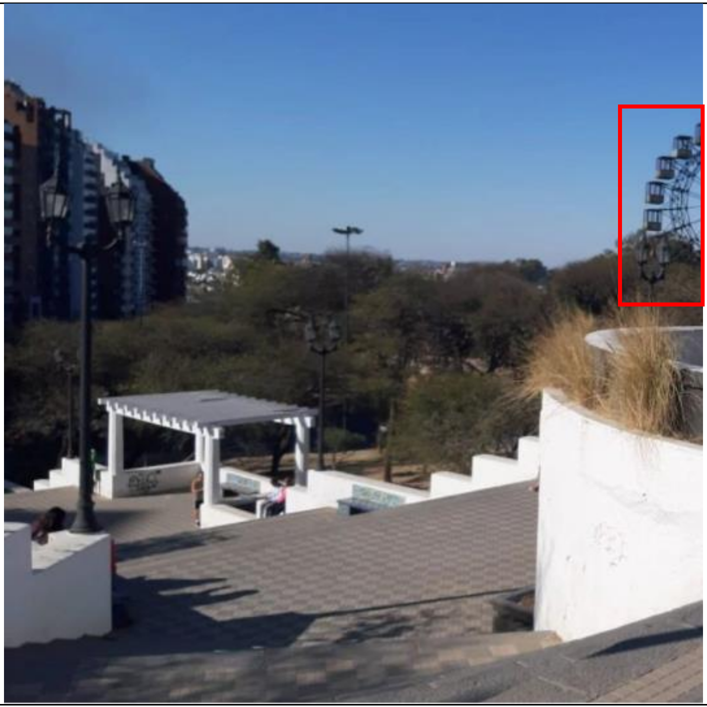




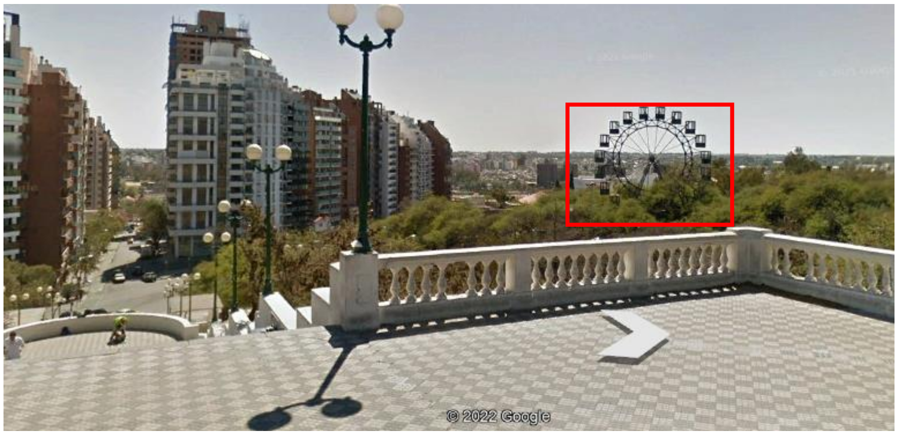
Post no. 9

(Sunday, January 23, 2022 1:18:29 PM)

Description: *"It feels here like that one time we went to Greece! It's so beautiful here 🤩"*



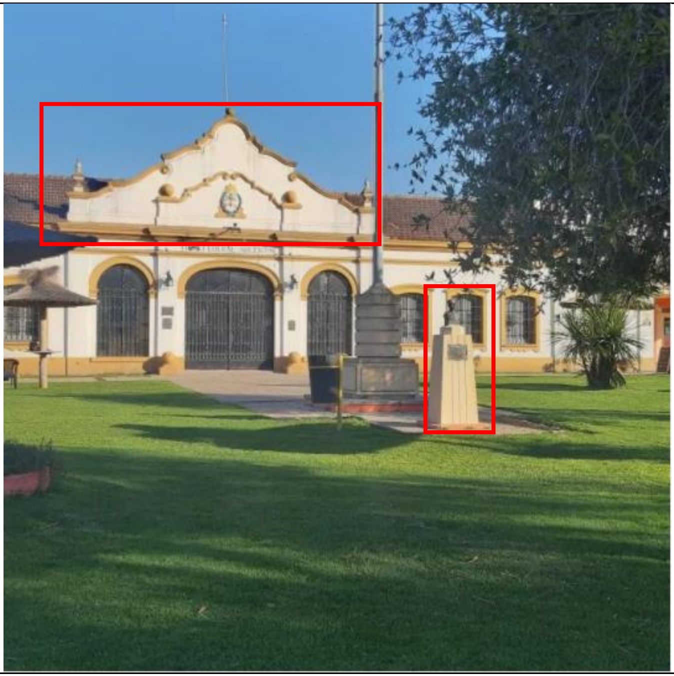
- This one was really easy. There can be seen that specific rolling wheel on the right.
- I searched for some fun parks with spinning wheels/carousels in Argentina and it did not take me long to find that the place was **Escaleras Parque Sarmiento (Mirador del Coniferal)** in **Cordoba, Argentina** – 8 hours drive from **La Plata, Argentina**.



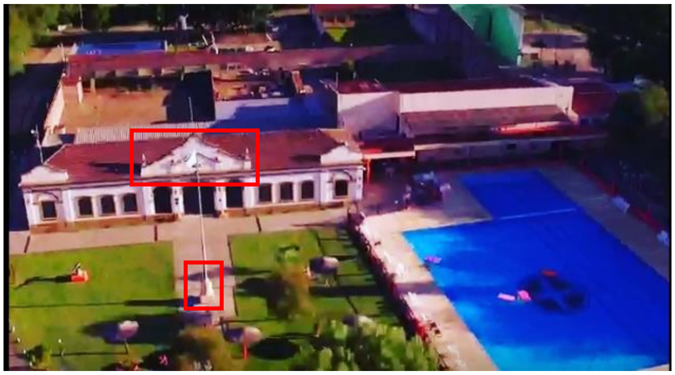
Post no. 12

(Monday, January 24, 2022 1:11:34 PM)

Description: *“More sightseeing, the buildings are so colorful here!* ❤️❤️❤️*”*



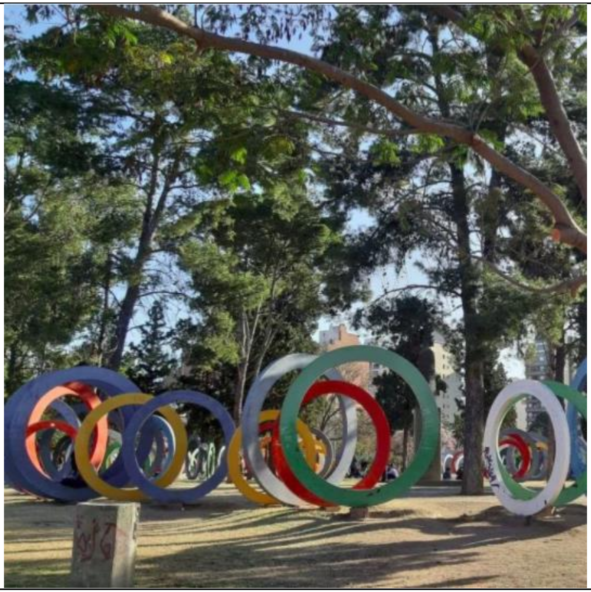
- I found the building pretty easy with reverse searching on **Google Images** and **Yandex.** The place was **Camping Tiro Federal** in **Baradero, Argentina** – around 3 hours from **La Plata, Argentina**.



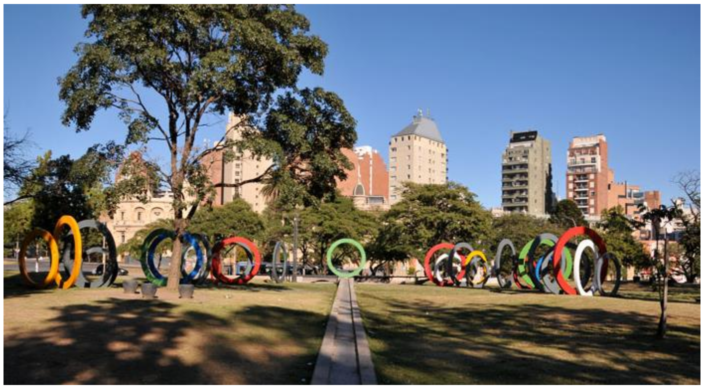
Post no. 13

(Monday, January 24, 2022 1:13:07 PM)

Description: *“Haha it looks like I work at google here, but no just more beautiful colors everywhere* ❤️*”*



- The same steps as fo the **post no. 12** (a little bit of **Google Images** and **Yandex**). The place was **Paseo del Bicentenario** in **Cordoba Argentina.**

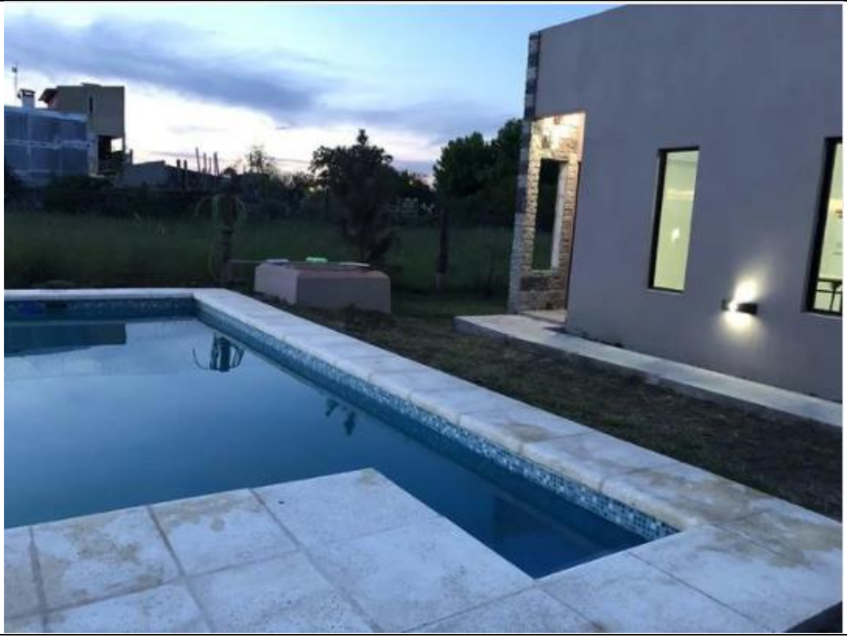


- Important fact: it was posted 2 minutes later than the **post no. 12** but the distance between the locations was about 6 hours so the posts' hours might not be helpful.

Post no. 15

(Tuesday, January 25, 2022 9:17:23 PM)

Description: *"Spent the whole day by the pool, tomorrow a good* ***3 hours drive to the capitol city****. Our* ***little home*** *here is really amazing, wish I could live here... 🏙"*

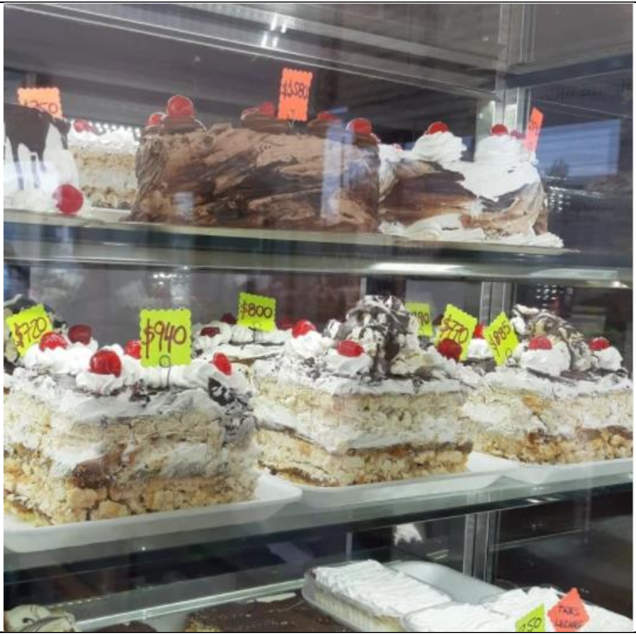


- The first post with the location. It looked like an image from a post about selling/renting places; it kind of seemed like a remote location, maybe with some lands around for sale; the pool seemed to have a specific shape which will be helpful for sure while searching through satellite imagery.
- Nothing from reverse searching with **Google Images/Yandex/Bing/TinEye**.
- Anyways, I also got the first hint about the position of the location – **3 hours drive to the capitol city** *(what does capitol city mean? Buenos Aires or La Plata? I assumed that she had not visited Buenos Aires unless she actually landed there, so maybe she thought that La Plata is the capital)*.
- The only place that she had visited was at a distance of 3 hours drive - **Camping Tiro Federal** from **Baradero, Argentina** identified based on **post no. 12**
- I searched for some houses with pool for sale/rent in **Baradero**, but did not find this one.
- I searched the same thing on several public groups from Facebook, but nothing.
- **Baradero** is located near two rivers called **Parana** and **Arrecifes** and the first thought I had was that maybe the CTF presentation image (the one from Indonesia) will prove to be helpful in some way, so I grid-searched images from satellites for a while, but nothing.
- *You can see at the end what I could have done better on this post.*

Post no. 17

(Thursday, January 27, 2022 7:53:36 AM)

Description: *"OMG 😳 More cake 🍰🍩 And they all taste so good! So much more flavor than Russian cake ❤️"*

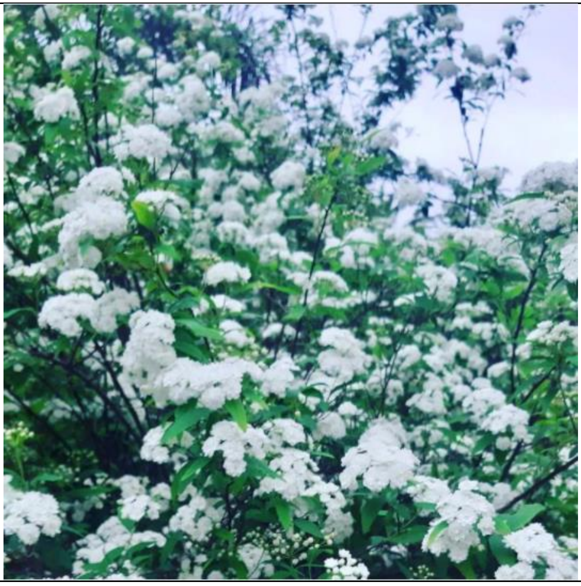


- Reverse searched the image and I found it on a reddit post where people asked the location of the Cake Shop; I thought this was set up by Hacktoria as a hint because some of the answers indicated **Rosario** (4 hours from **La Plata**) as being the city where one can find the Cake Shop with those products.
- I spent some time with Google Earth searching around **Rosario**, but nothing.

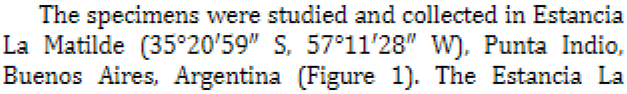
Post no. 19

(Thursday, January 27, 2022 9:57:43 PM)

Description: *"Flowers smell so good! But I do not like the insects here 😅"*



- I used **plant.id** to identify this plant which is *Crataegus monogyna* or *Crataegus laevigata. Kudos to* ***@gralhix*** *for her blog post that can be found at the end of the write-up.*
- Searching for *Crataegus monogyna* in **Argentina** led me to a scientific paper about the first record of this plant in **Buenos Aires province** and there were mentioned some coordinates.



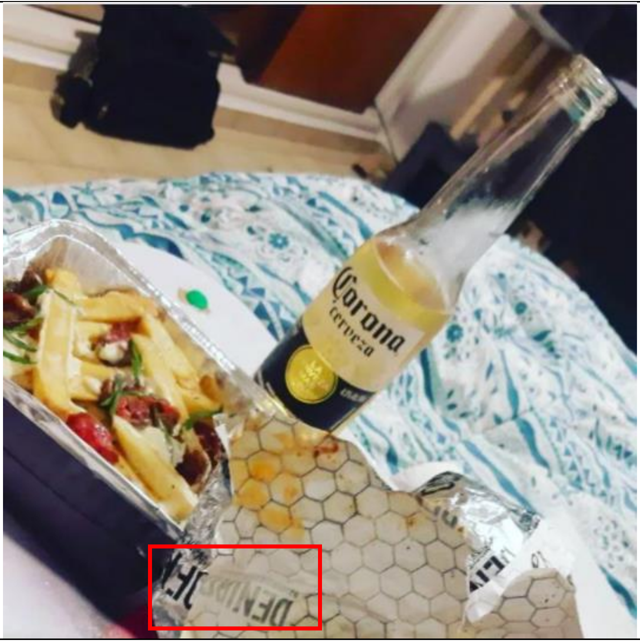
The specimens were studied and collected in Estancia
La Matilde (35°20′59″ S, 57°11′28″ W), Punta Indio,
Buenos Aires, Argentina (Figure 1). The Estancia La

- Of course, I thought that it was over and I simply found the place, but the coordinates sent me to an empty field. I searched for some cities around those coordinates (**Punta Indo, Pipinas, Veronica**), but nothing.

Post no. 20

(Sunday, January 30, 2022 1:05:32 AM)

Description: *“Ow no I came here and caught corona!* 😂*”*

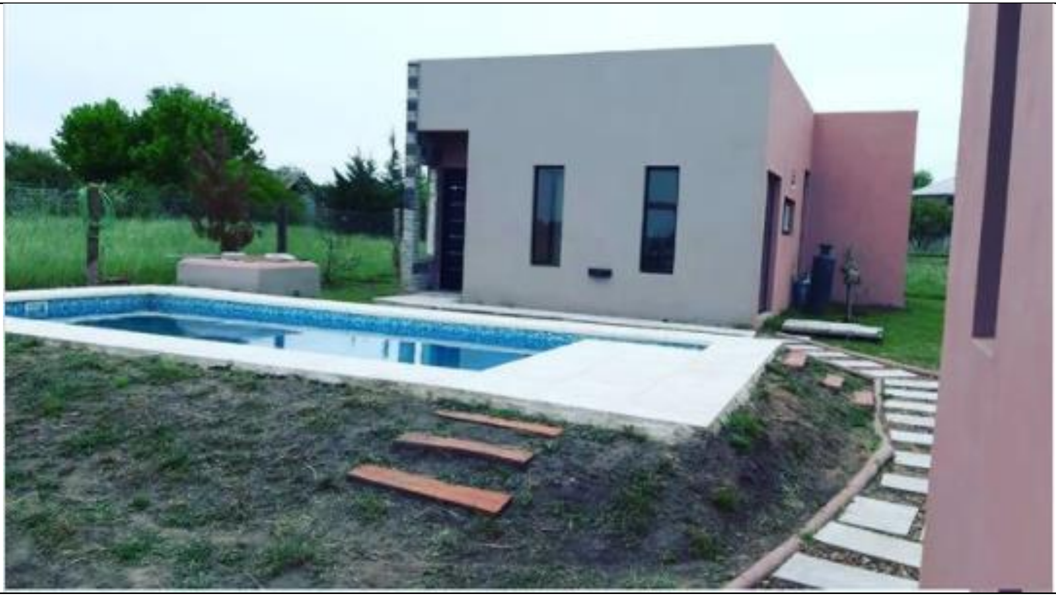


- Based on the text from that wrapper I found the **Deniro Hamburgueseria** which was located only in **Buenos Aires** and **Cordoba**, so that meant nothing as I had already searched around those areas.

Post no. 21

(Wednesday, February 2, 2022 3:34:25 PM)

Description: *“I wish our home back in Russia had a pool! Only downside here its* ***three hours south to the capital city*** *where all the fun stuff is ⍰”*

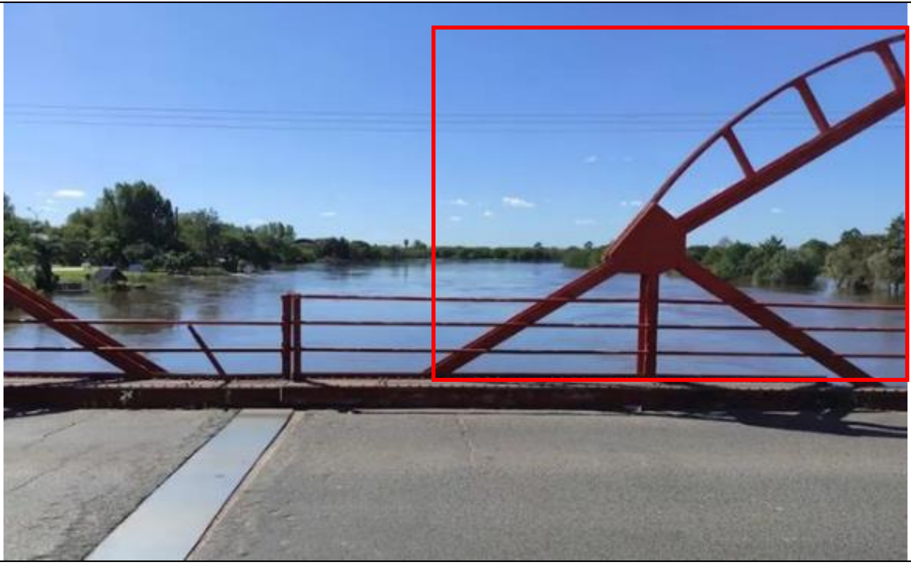


- The second post with the location. Based on the description (*“three hours south to the capital city”*), I knew that the place was located **north to the capital**, be it Buenos Aires or La Plata.
- I tried several methods to find the place: real estate brokers ads, pool *“construccion”* ads, but nothing.
- I used **withinhours.com** to find the places located at around 3 hours north to Buenos Aires/La Plata, but there were approximately 30 locations (I had to find o solution to narrow down this number).
- I spent some time on this one and I got very frustrated at one moment because Hacktoria announced that there were already 2 players who had already found the location (how did they do it?).

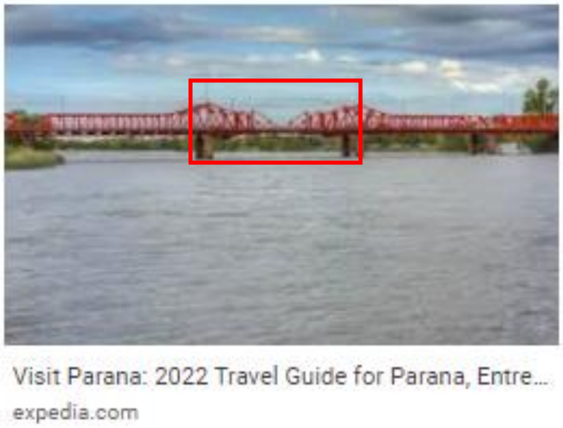
Post no. 22 (extra hint)

(February 13 2022, no time was collected as it proved not to be helpful)

Description: *“Went for a nice* ***bicycle ride*** *to the* ***nearest city today,*** *just* ***15 minutes*** *and the weather was amazing. Also the view from the* ***bridge going to the*** *city was wonderful!* 🌅*”*



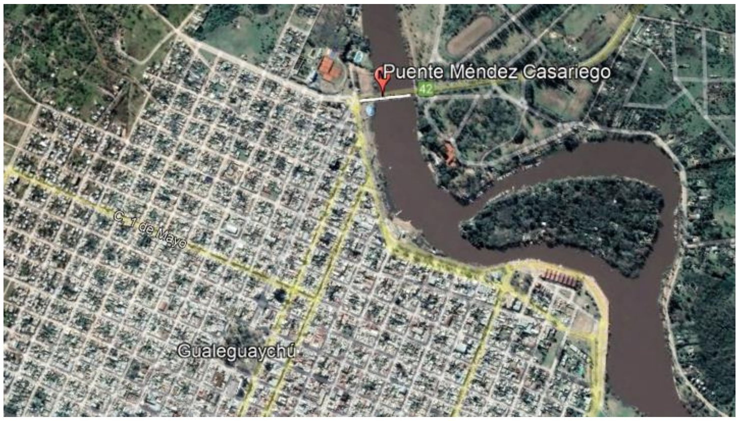
- From the description I had: (i) a bicycle ride, (ii) 15 minutes to the city and (iii) a bridge that connects the nearest city to the family’s location (at this moment I got the confirmation that the first step I did (with the CTF presentation image) was not in vain).
- I searched the bridge with **Google Images/Lens/Yandex/Bing/TinEye**, but nothing.
- I started to search for all the rivers located near Buenos Aires and I combined their name with the word “puento” (which means bridge in spanish).
- When I searched for *“puento Parana”*, along all the resulted images I found this particular one which kind of resembled.



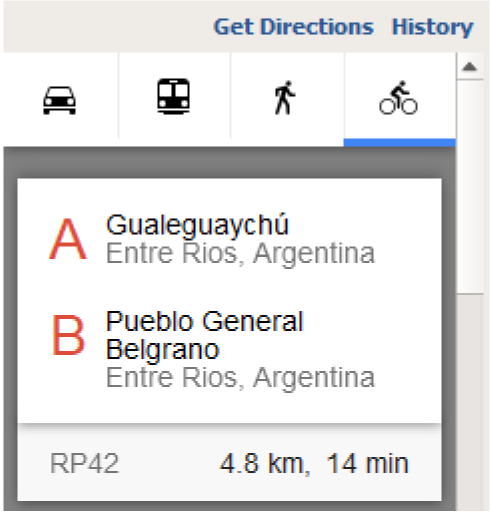
Visit Parana: 2022 Travel Guide for Parana, Entre...

expedia.com

- I used **Google Lens** on this image and *Voila!*, I found the **Puente Méndez Casariego** which was located near the city **Gualeguaychú, Argentina** which, in turn, was located at 3 hours north to the capital city.



- Based on these pieces of information, I searched the places that were located at approximately 15 minutes distance with a bicycle and I found **Pueblo General Belgrano**.

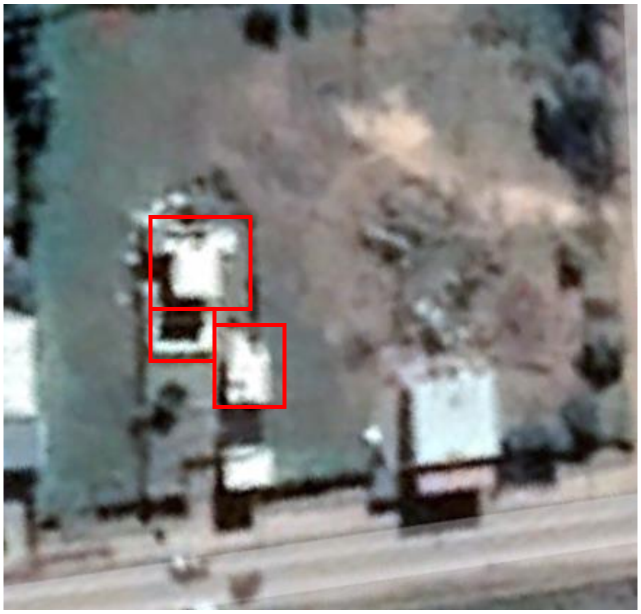


A Gualeguaychú
Entre Rios, Argentina

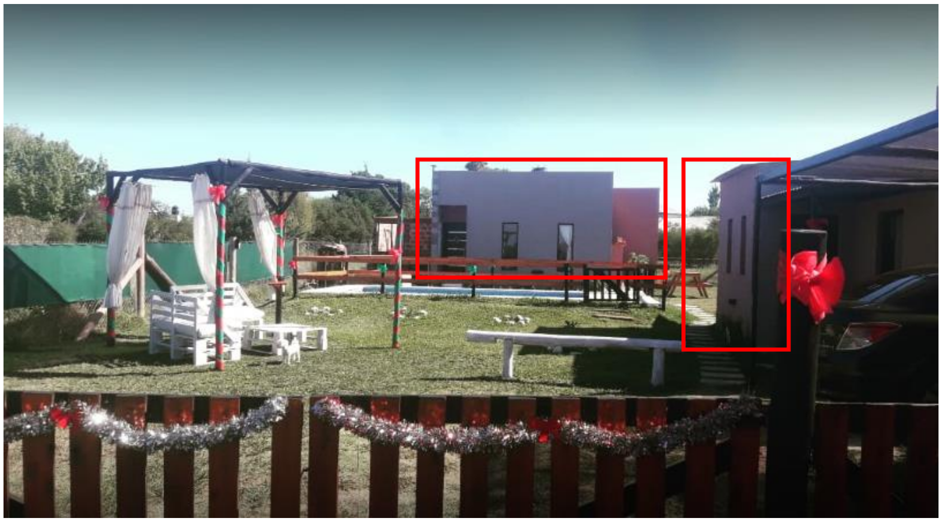
B Pueblo General Belgrano
Entre Rios, Argentina

RP42 4.8 km, 14 min

- Being sure that was the place, I started to scan every inch of Google Earth's images collected by satellites and that is how in the middle of the night I found the location - **El Ensueño** (I mostly searched for two buildings (as we can see from the **post no. 21**) that had a lot of free space around them and also had a pool with that specific shape).



- A cabin accommodation… who would have thought? I should… as I searched only for real estate ads for renting/selling houses.



IV. Step 3.

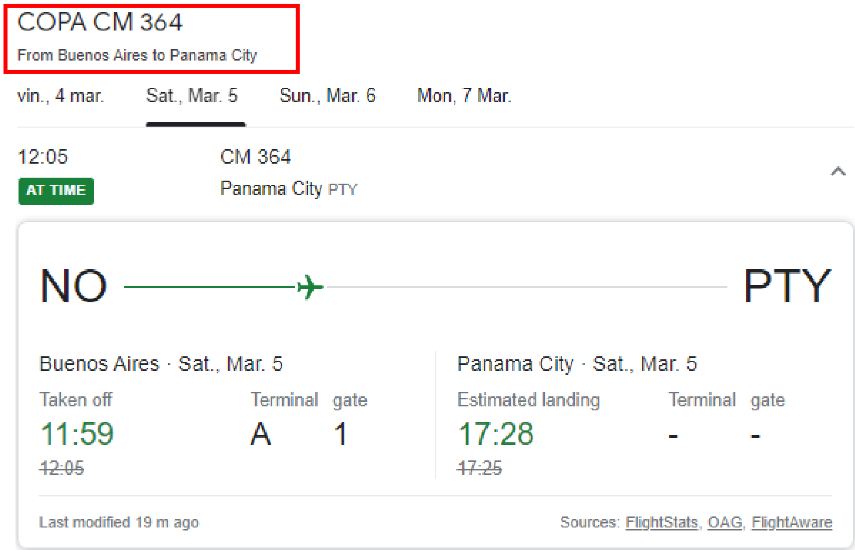
I sent the location to Hacktoria Agents and surprise… the Kotova family had already left and the only thing left behind was a notepad with an imprint of the previous writing on it. Based on some letters and blanks I had to find out where did they go.

COC_ _ _ _   _ ODG _

C_ _ _ S _ _ _ NO

CM 364

Well, I started with what I could understood, so I searched for **CM 364** combined with the word "Argentina" on Google and I found that it was a code for a flight between Argentina and **Panama**.



COPA CM 364
From Buenos Aires to Panama City

vin., 4 mar. | Sat., Mar. 5 | Sun., Mar. 6 | Mon, 7 Mar.

12:05 AT TIME | CM 364 Panama City PTY

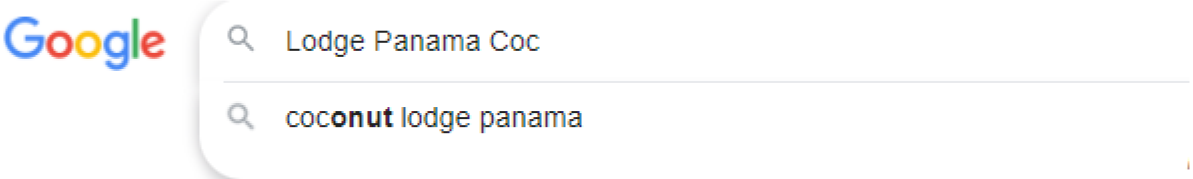
NO → PTY

Buenos Aires · Sat., Mar. 5
Taken off 11:59 ~~12:05~~ | Terminal A | gate 1

Panama City · Sat., Mar. 5
Estimated landing 17:28 ~~17:25~~ | Terminal - | gate -

Last modified 19 m ago
Sources: FlightStats, OAG, FlightAware

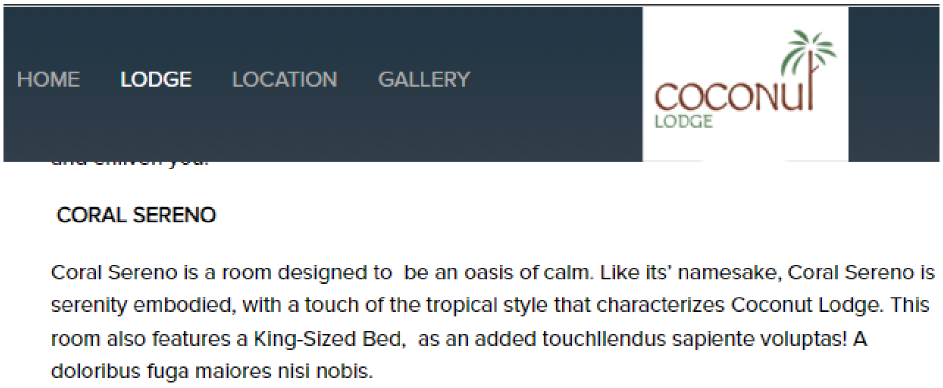
Presuming that they fled to Panama and based on those blank letters I had to do some deductions. The only word that popped out in my head for "_ODG_" was LODGE, so I searched for *"Lodge Panama Coc…"* and directly in suggestions there was **Coconut Lodge**, a resort located right near **Ciudad de Panama**.



Lodge Panama Coc

coconut lodge panama

Now, what could be the next two words? Well, maybe a room? I went to the **Coconut Lodge**'s site and I started to search through their rooms. A little bit of scrolling and there it was… **CORAL SERENO** room.



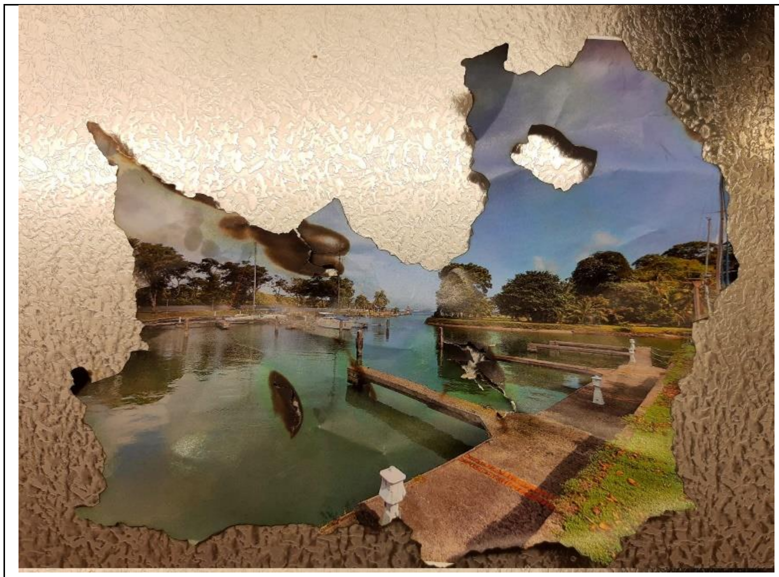
and enliven you.

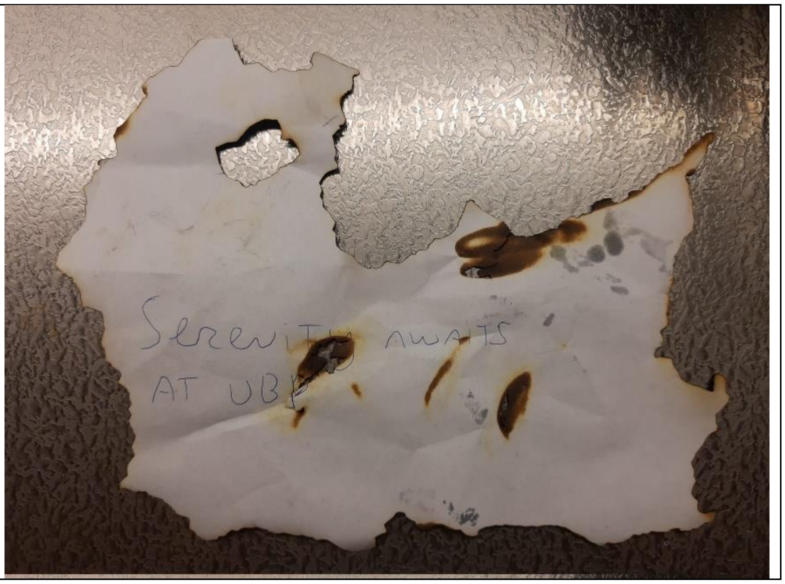
CORAL SERENO

Coral Sereno is a room designed to be an oasis of calm. Like its' namesake, Coral Sereno is serenity embodied, with a touch of the tropical style that characterizes Coconut Lodge. This room also features a King-Sized Bed, as an added touchllendus sapiente voluptas! A doloribus fuga maiores nisi nobis.

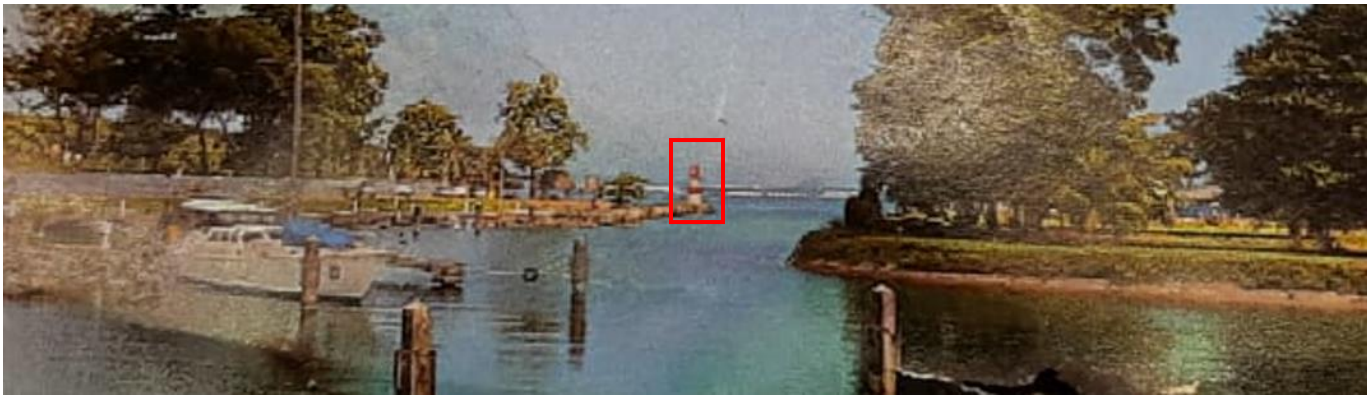
V. **Step 4.**

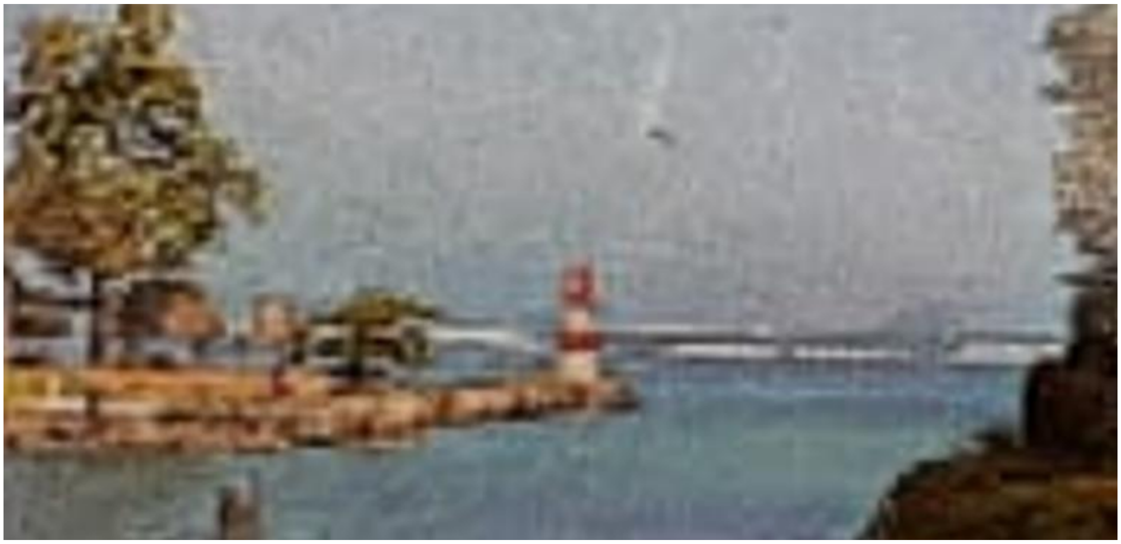
I sent the information to Hacktoria Agents and surprise again… the Kotova family had already left and nothing could be found at that location except for two burned photos: one with a harbor and another one with the text *"Serenity awaits at UBP"*.



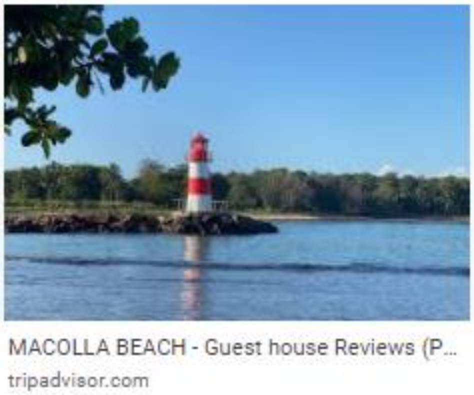


I spent some time searching for Serenity, which I thought was a boat name and for UBP which I thought was an acronym for a harbor name, but I was not able to find anything relevant. So I spent more time on the image with the harbor. The first thing about it was that it didn't look as a harbor in a proper sense, but more like a marina… a pier or a boathouse. Of course, no image reversing search tool helped me so I had to rely on other methods. One of it, as **@Bendobrown** says in his youtube series OSINT at Home (link at the end) is that, when you are trying to geolocate an image and there are no obvious elements, you should try to identify something particular that either alone or corroborated with other elements could give some leads. I looked at every inch of that image, searching for something special and I found this:



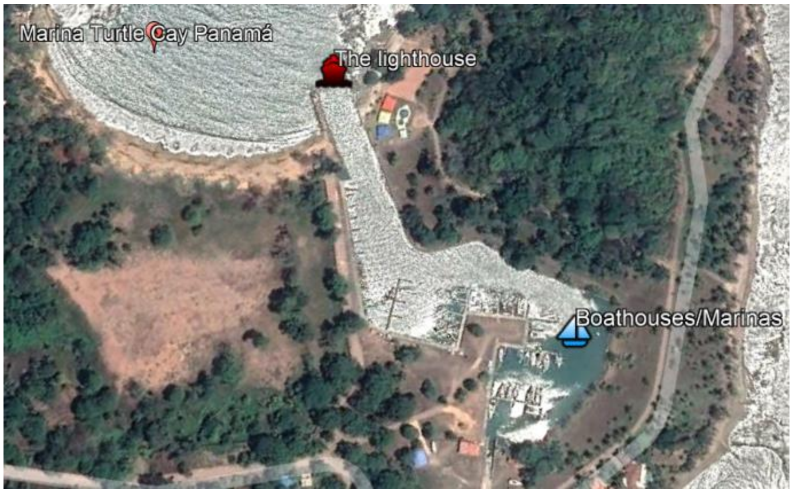


A lighthouse coloured in a combination of white-red-white-red. If I was able to find it, the final location would be a piece of cake. If you use search engines to search for lighthouses in Panama, you will not find this one. Trust me, I tried with *"faro"* and a lot of other combinations, but absolutely nothing came out. Scrolling, scrolling, frustrating, frustrating. That is when, in the middle of the night I searched the this combination of keywords *"panama marina lighthouse"* and the 120th result was this particular one:

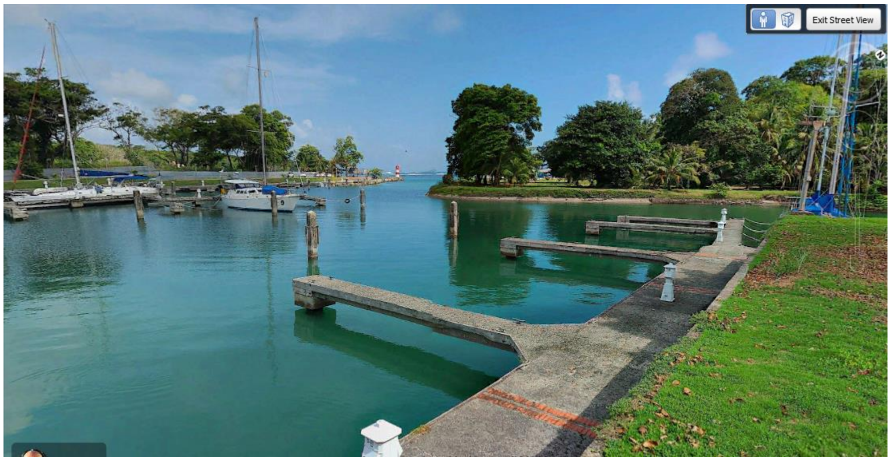


MACOLLA BEACH - Guest house Reviews (P...
tripadvisor.com

The image was from a tripadvisor post about **Macolla Beach** located in **Green Turtle Cay, Nombre de Dios 0301 Panama**. Searched the location on Google Earth and took a look around to see if there were marinas/boathouses. Sure thing, there were some.



Using street view functionality I was able to find the real, full and unburned picture posted by a contributor on Google Maps.



And that was it. I finished on the fourth place and I was awarded the **Badge Finisher Operation Runner**. Quite an experience, both fun and frustrating, but finding the final location was totally worth it.

VI. What I could have done better:

- From the **post no. 15** I found that the location was at a distance of 3 hours drive from the capital city. The only thing that I did (besides looking for real estate ads) was concentrating on the location found from the **post no. 12** (Camping Tiro Federal from Baradero, Argentina) because it was the only one that had been already visited and it was approximately 3 hours away from the capital city. I should have searched for (1) the average speed limit per hour in that area, (2) multiply the speed limit with 3 (hours) and (3) use Circle Generator provided by https://www.scottmurray.me/kml/circle/index.php which, based on some coordinates, radius and a measurement unit, gives a circle using **KML** (an XML notation for expressing geographic annotation and visualization within two-dimensional maps and three-dimensional Earth browsers; more about KML here: https://en.wikipedia.org/wiki/Keyhole_Markup_Language). My guess is that this would have narrowed the number of cities/locations compared to what I got from withinhours.com.
- I should have searched for cabin accommodation locations near Buenos Aires, but it did not cross my mind at that time. I spent a lot of time analyzing advertisements on real estate websites; made some lists with popular brokers from that area and stalked their social media profiles; scrolled through a lot of pictures posted on public facebook groups from different areas around the capital city, but nothing.

VII. Lessons learned:

- If you feel that you do not reach endpoints, take breaks, but do not stop (by breaks I mean chilling, work-out, meditate, anything that has a destressing effect). The best ideas that I had happened during relaxing moments.
- Do not rely on one tool and validate your findings. Be careful with those cognitive biases.
- Be creative. The OSINT field requires a lot of improvisation, out-of-the box thinking and creativity.
- Learn, read, connect with or follow people that are already in the business. There is always something new to learn.

Finally, I cannot wait to read the winner’s write-up and I encourage anyone who is interested in OSINT CTFs to take part in the next Hacktoria’s challenge. (https://hacktoria.com/monthly-ctf/operation-brutus/)

Kudos to Hacktoria for their work! 😎

@praetorius

***Disclaimer:** any mention of real locations, people, countries, organizations and such, are not affiliated with me or Hacktoria; they are incorporated into the stories to make them more immersive and relatable.*

VIII. Resources:

- Google Lens, Google Images, Yandex, Bing, TinEye (for reverse image searching)
- https://nixintel.info/osint/how-to-find-timestamps-for-verification/ (for timestamps of instagram posts)
- https://plant.id/ (for plants/trees identification) + gralhix’s post where I found about this tool (https://gralhix.medium.com/walkthrough-hacktoria-geolocation-02-a987eef13dbe)
- https://withinhours.com/ (for places around a location based on flight/drive time)
- https://www.youtube.com/watch?v=qW96515QG6Y&list=PLrFPX1Vfqk3ehZKSFeb9pVIHqxqrNW8Sy (OSINT at Home playlist by BenDoBrown)
- https://www.scottmurray.me/kml/circle/index.php (for circle displaying on digital maps)