Session #3 - OSINT

Cyber Security Uses-Cases Report

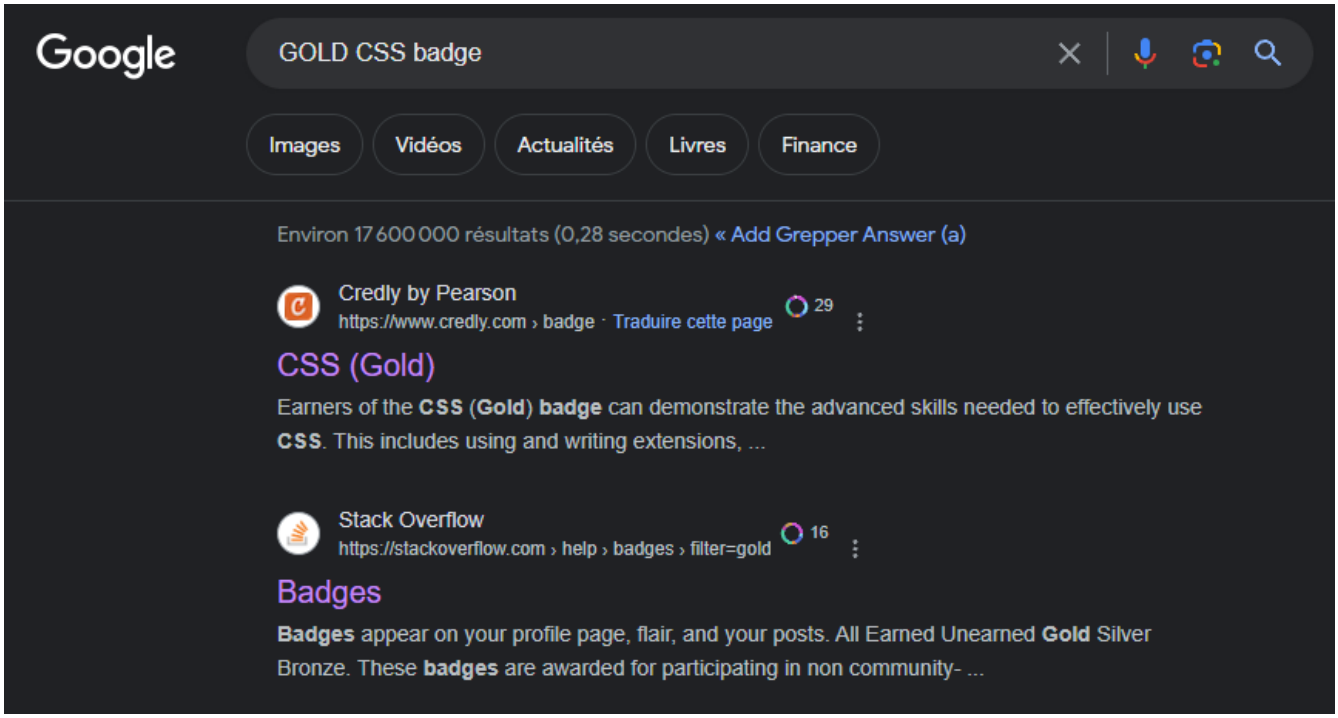
0. Table of Contents

1. Challenge 1

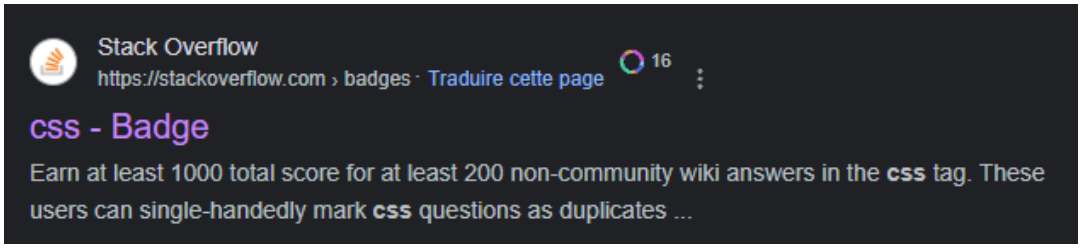
Challenge 1

I'm glad that the platform gived to me the GOLD CSS badge in 2011 April. Can you find which is my post code?
B.C.

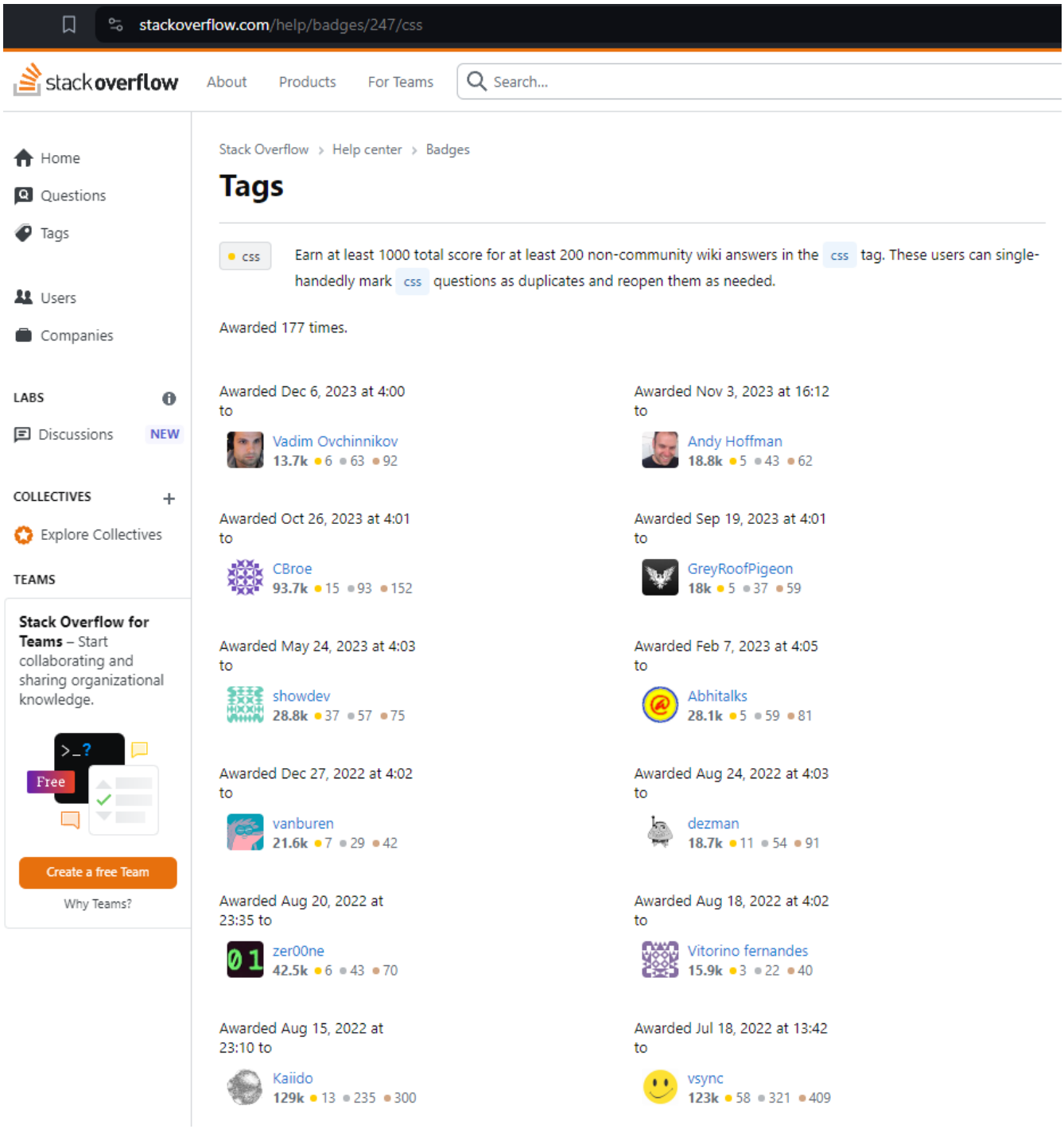
First we need to know what is a "GOLD CSS badge". A quick google search tells us that it is probably said in the context of a Stack Overflow badge.



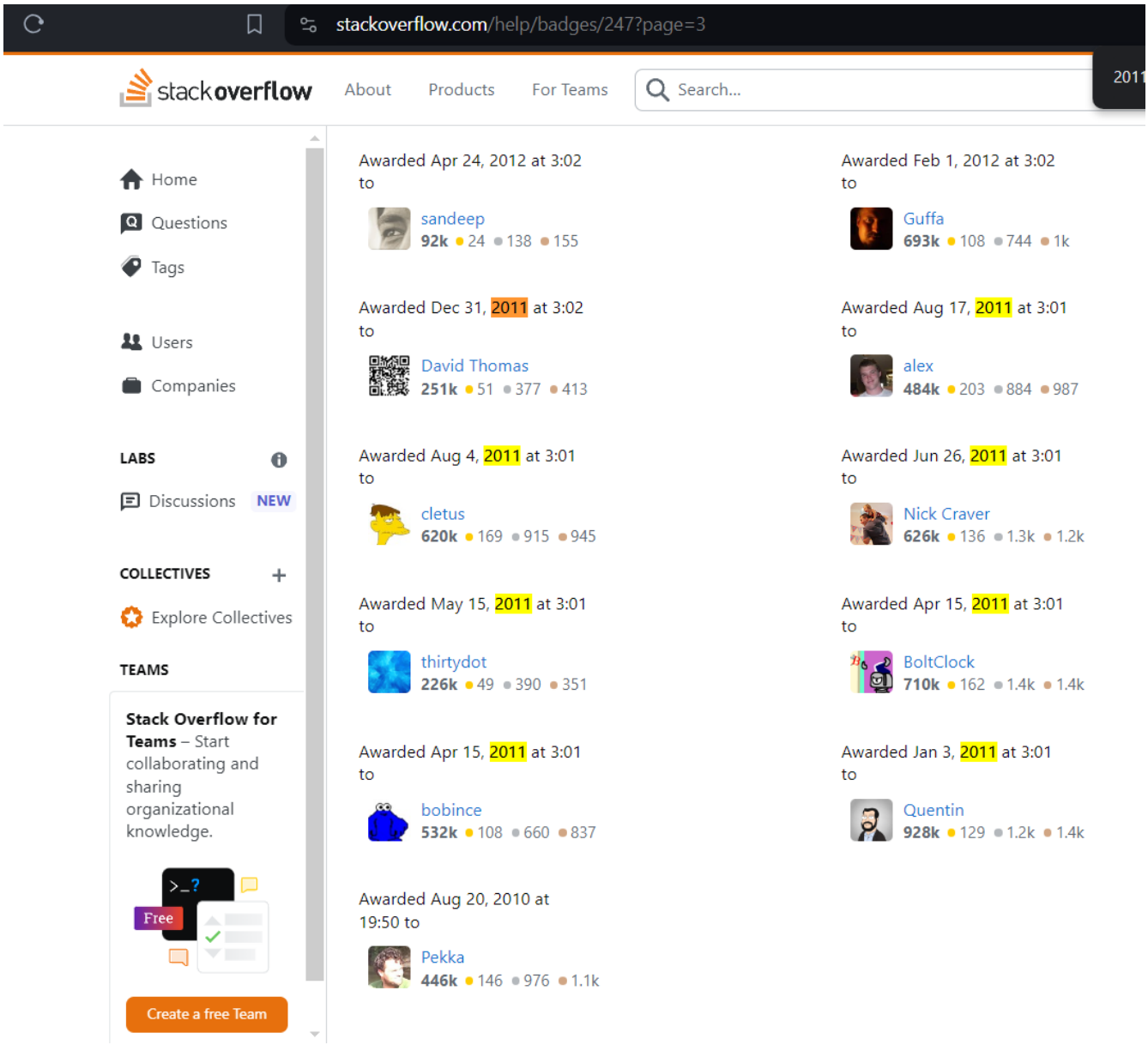
And a bit below we can confirm there is a css badge on Stack Overflow:



If we click on it we land on a page listing by date all the users who were awarded that badge:



We can just sort them until April 2011:

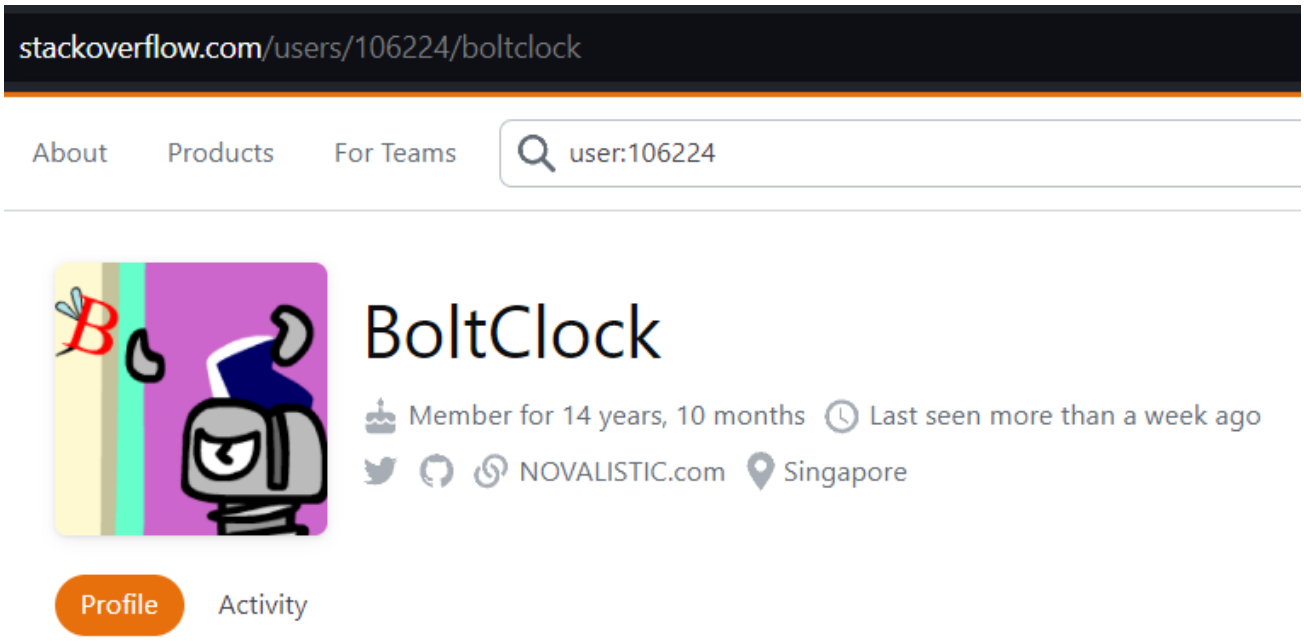


2 candidates:

- `bobince`
- `BoltClock`

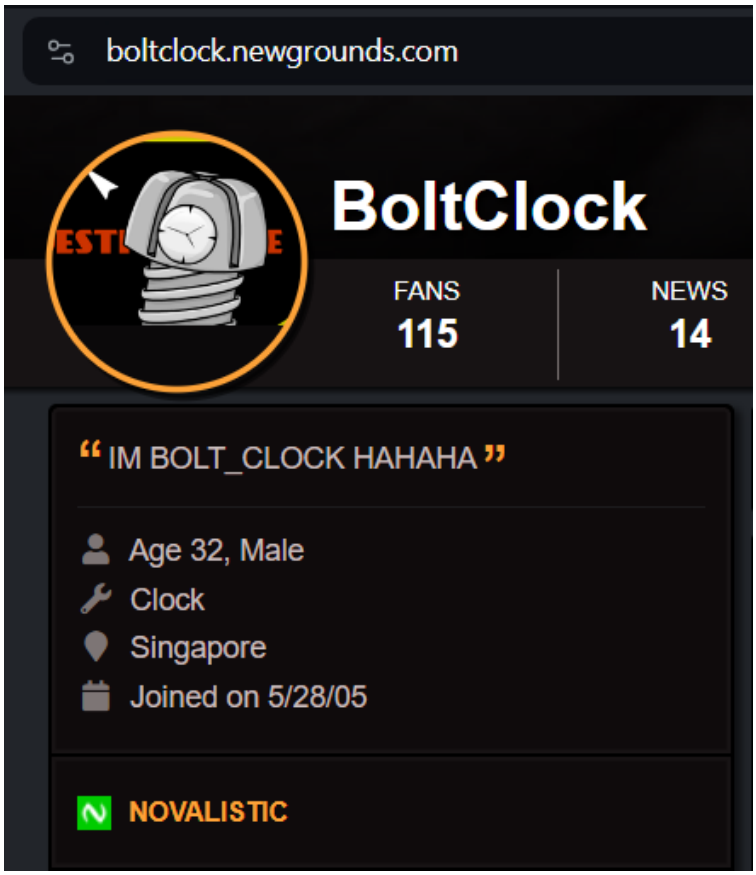
Because the note was signed "B.C." we can assume it is not `bobince`.

According to `BoltClock` public Stack Overflow profile he's located in Singapore but it may not be accurate.

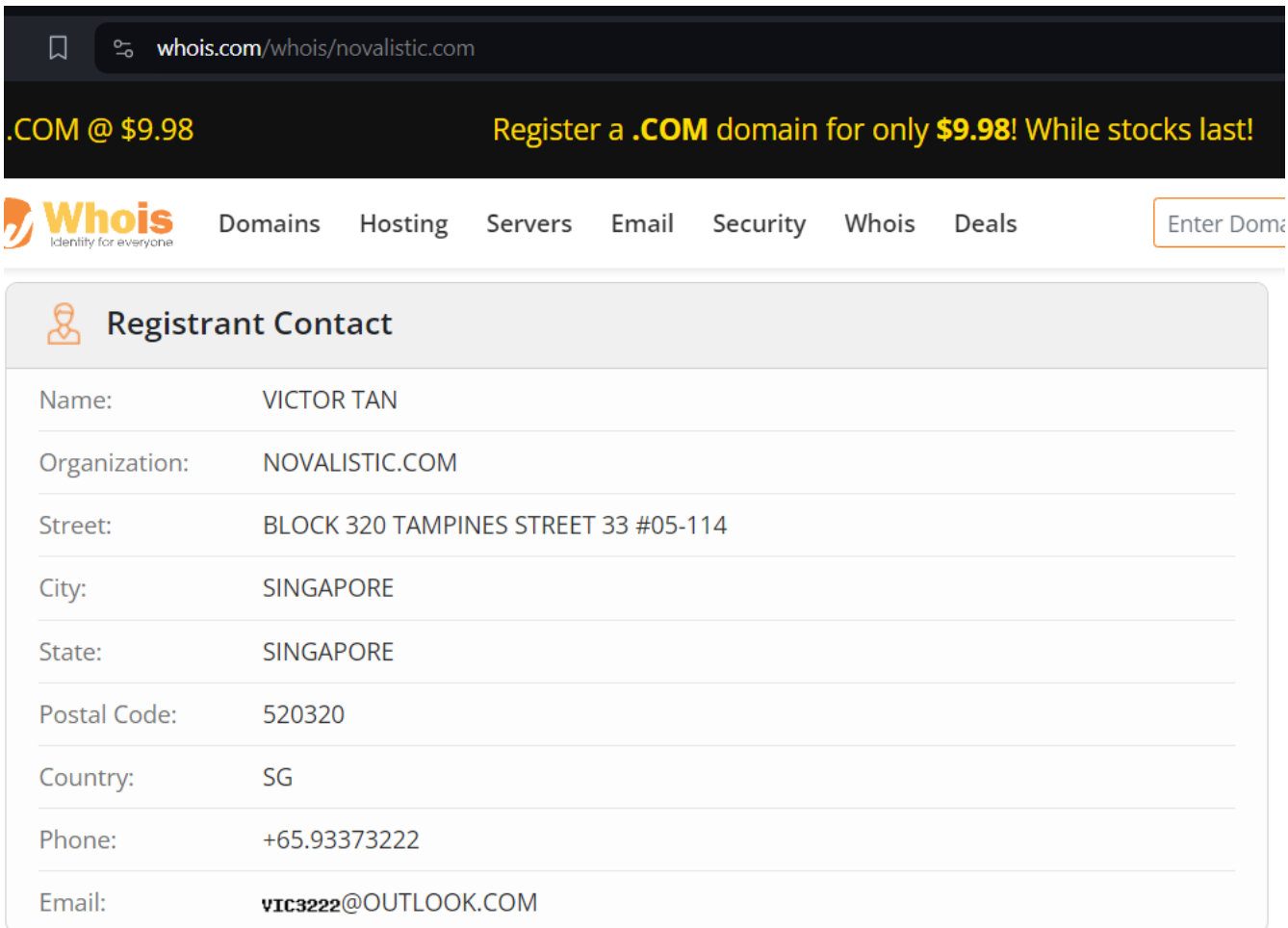


Checking his personal website NOVALISTIC.com I find a link to his `Newgrounds` profile:

And on this profile Singapore again:



When looking for information about the domain `novalistic.com` on *whois.com* we find a zip code related to Singapore:



And the same postal code on *whoisology.com*:

novalistic.com

This is Whoisology's most current historical whois lookup for the domain name novalistic.com. Click any of the records below (address, phone, email, etc) to perform a reverse lookup.

Admin Contact

The Admin Contact is the person or organization who controls the domain.

Name	VICTOR TAN (27) Changes: -1 ccTLD: 1
Org.	NOVALISTIC.COM (1) Changes: +0 ccTLD: 0
Email	VIC3222@OUTLOOK.COM (1) Changes: +0 ccTLD: 0
Street	BLOCK 320 TAMPINES STREET 33 #05-114 (1) Changes: +0 ccTLD: 0
Street 2	-
City	SINGAPORE (142,743) Changes: +2,658 ccTLD: 2,095
Region	SINGAPORE (116,246) Changes: +5,201 ccTLD: 1,371
Zip / Post	520320 (3) Changes: +0 ccTLD: 1

Other Details

These are technical details & related, connected to the domain.

Registrar Name	Dreamscape Networks International Pte Ltd(602,756) Changes: -21,984 ccTLD: 98,070
Created Date	2001-11-02(4,063) Changes: -60 ccTLD: 1,110
Whois Servers	whois.crazydomains.com(545,438) Changes: -21,278 ccTLD: 213
Updated Date	2023-08-05(647,780) Changes: +530,185 ccTLD: 186,366
Expires Date	2023-11-02(459,809) Changes: -49,632 ccTLD: 130,382
Name Servers	NS1.ASMALLORANGE.COM(23,878) Changes: -1,160 ccTLD: 2,171 NS2.ASMALLORANGE.COM(23,817) Changes: -1,160 ccTLD: 2,164 NS3.ASMALLORANGE.COM(566)

✓ **Flag found!**

BoltClock's postal code is `520320`, Singapore

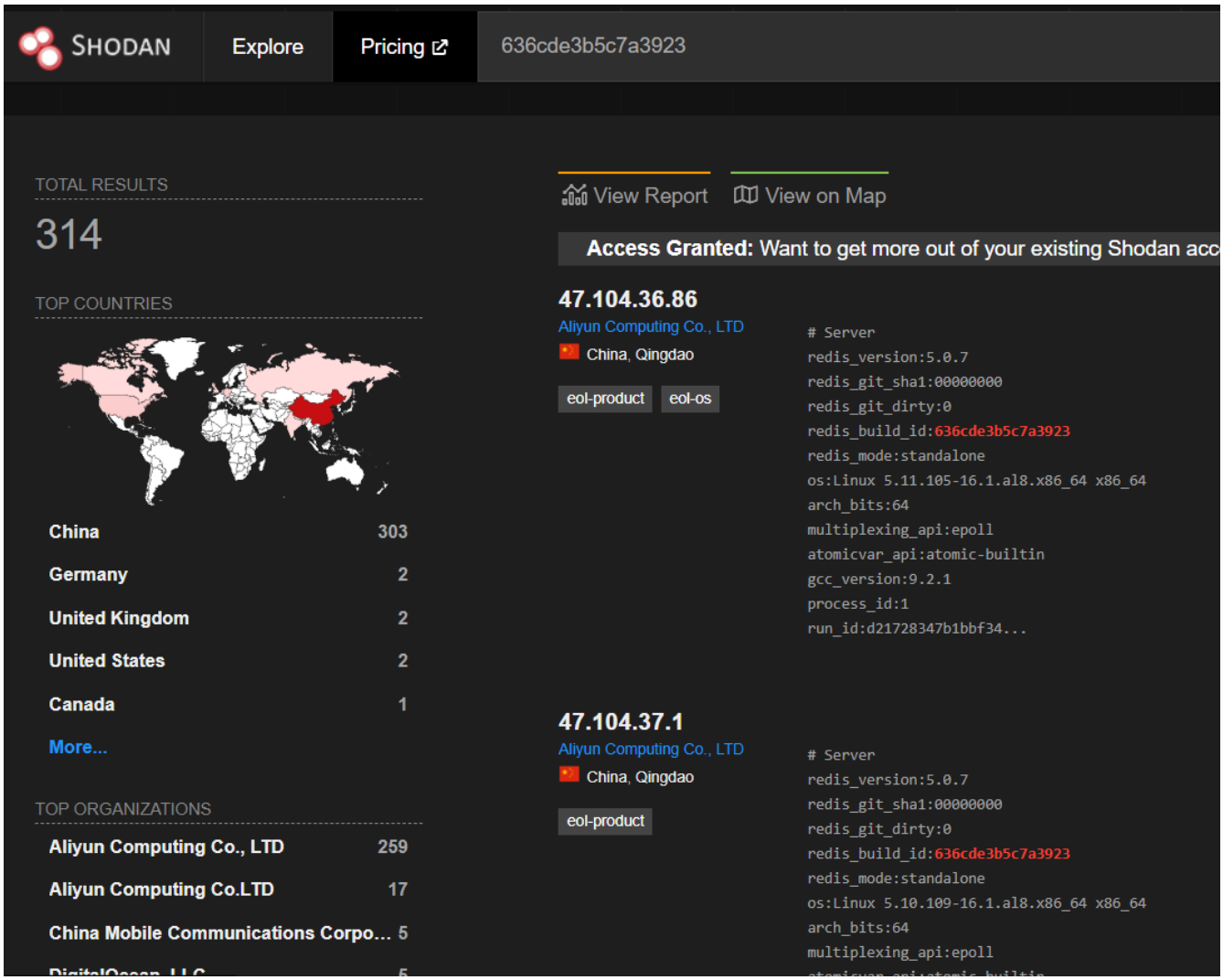
2. Challenge 2

Challenge 2

The Red Team of INCIDE is doing a pentest for a company in Canada. They find the redis build id, i.e. `636cde3b5c7a3923`. Can you find the '`run_id`' of this server?

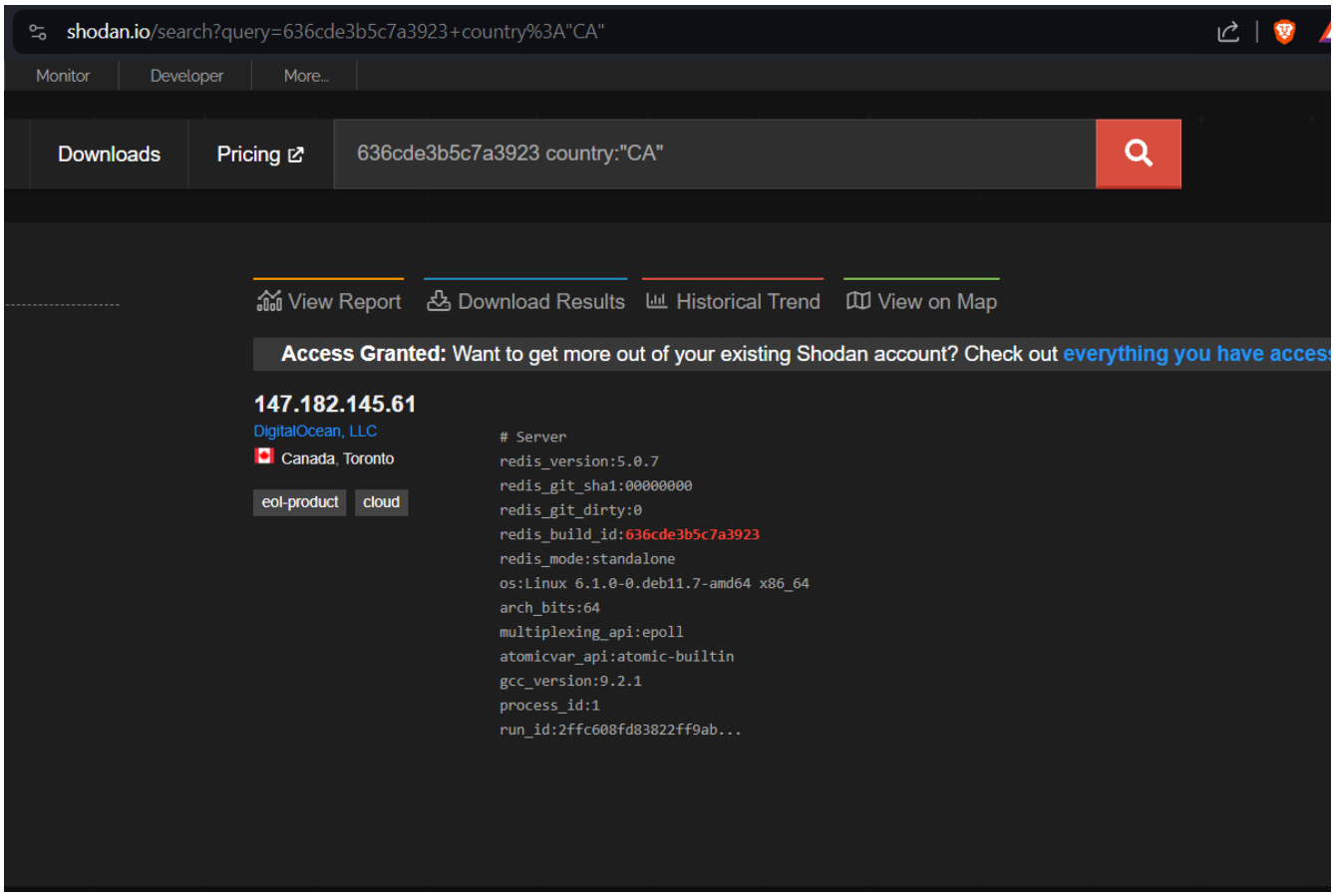
Basic google searches of "*incide canada*", "*incide redis*", "*redis 636cde3b5c7a3923*" or "*build_id 636cde3b5c7a3923*" don't give any information.

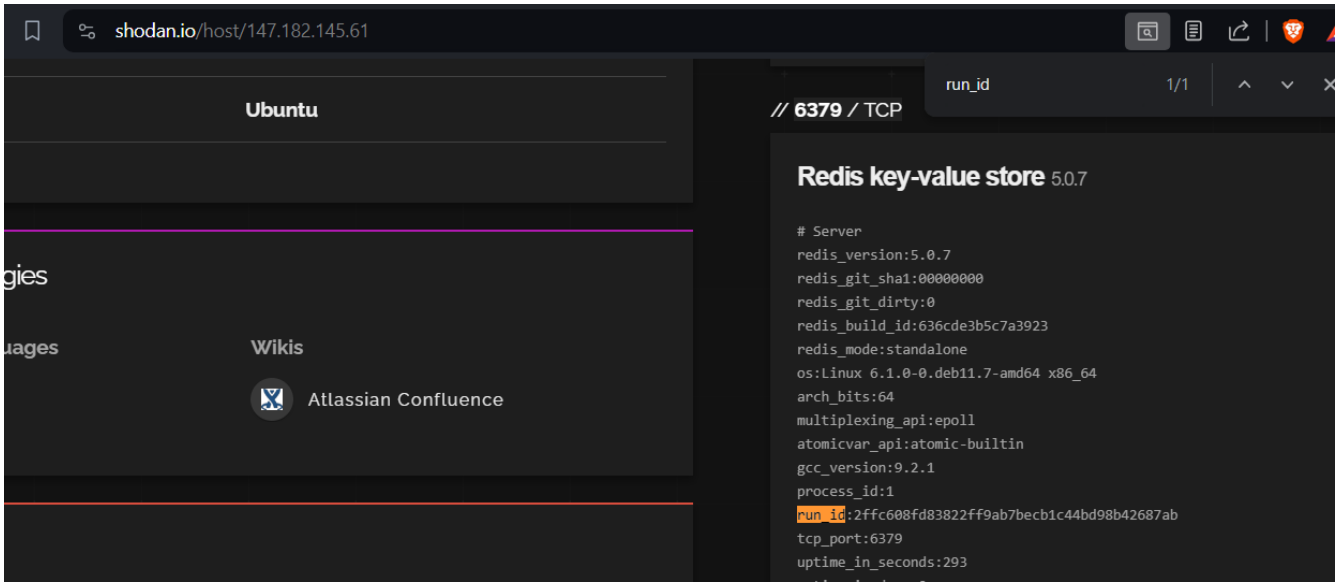
I know Shodan is a search engine for Internet-connected devices. Maybe we will have more luck there:



Out of the 314 results only 1 is in Canada!

To directly be able to see it you need an account, if not you will have to go through every page one by one.





✓ **Find run_id**

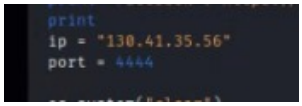
The run_id is `2ffc608fd83822ff9ab7becb1c44bd98b42687ab`

3. Challenge 3

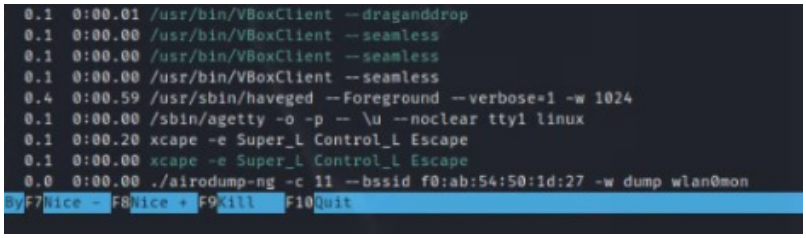
Challenge 2

Can you find my City? This gif was taken from my PC: https://drive.google.com/file/d/1S2s1-NodXhndfOzQ9_QaYu7CJi2l01nX/view?usp=share_link

We can identify an IP address:

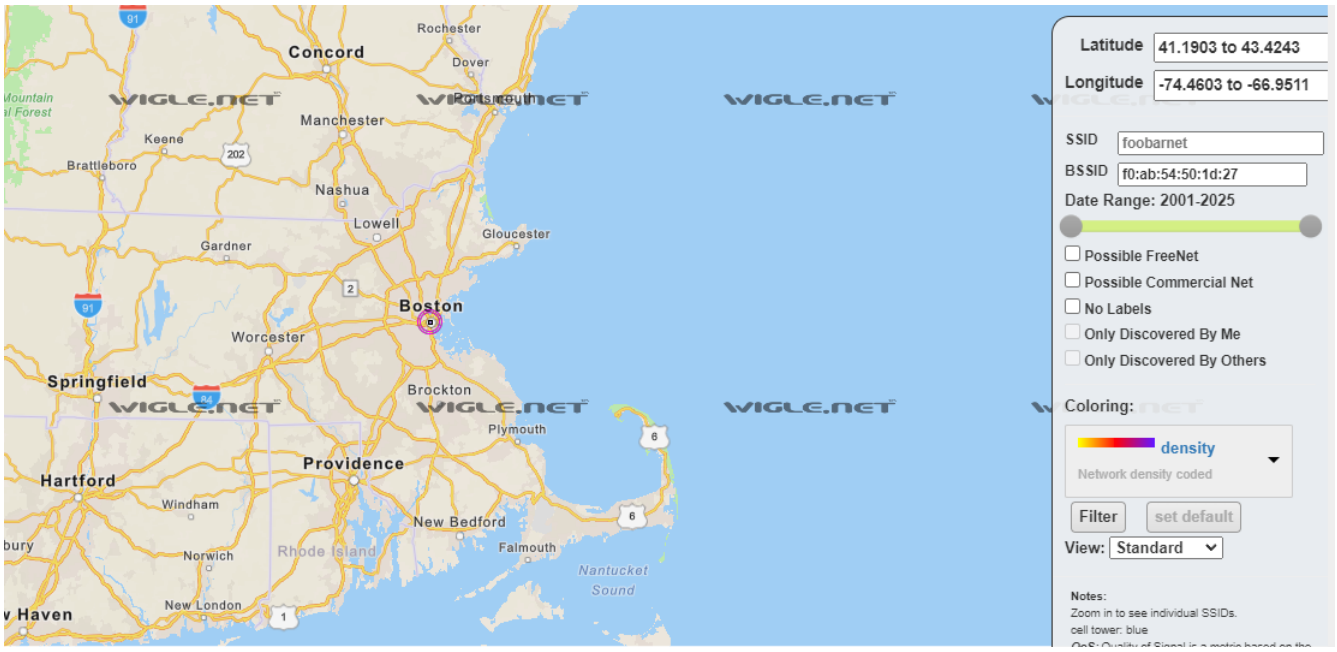


And a MAC address:

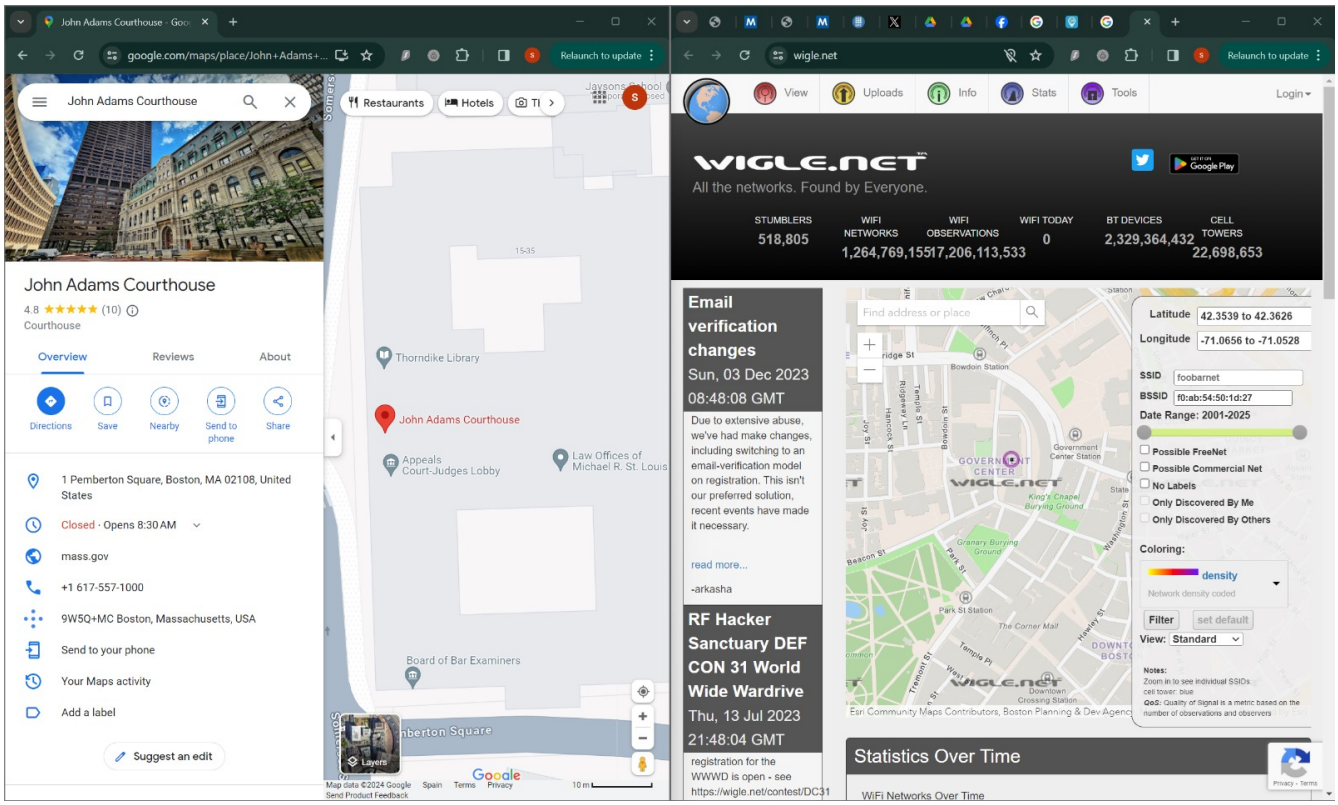


The IP address is located in Saudi Arabia, but the real location can be hidden behind a VPN.

We can use the website *wiggle.net*, a website for collecting information about the different wireless hotspots around the world, to try to locate the router using its MAC address:



And we find him in Boston!



✓ **Address found!**

The gif was taken from a computer located in Boston.

4. Challenge 4

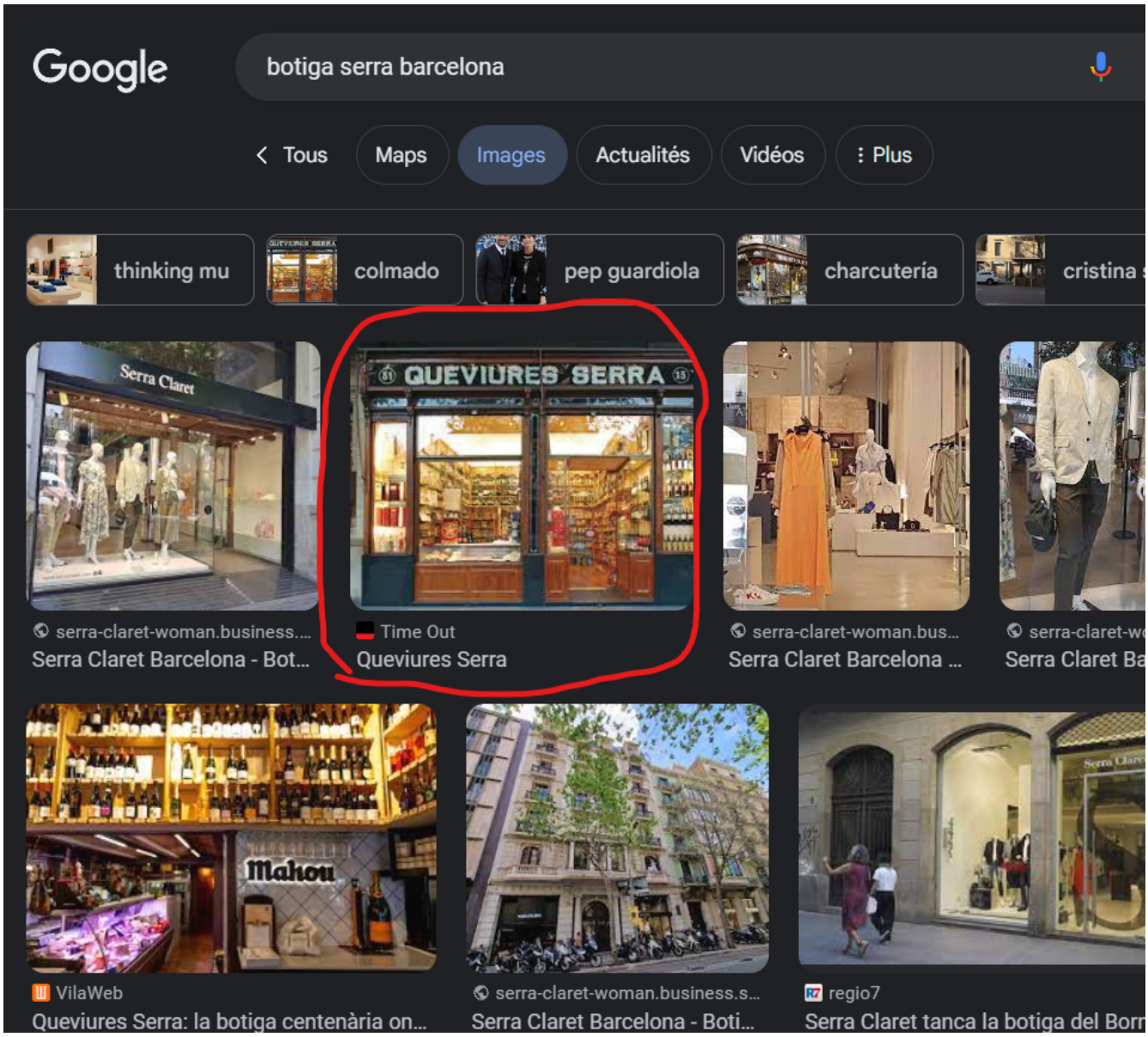
Challenge 4

The Spanish singer Rosalía published a post on Instagram on March 15, 2023. This post was part of a marketing campaign for a special F.C. Barcelona T-shirt. Find the address of the building where Rosalía was located.
https://www.instagram.com/p/Cpzmwl-MdbG/?igsh=MXhqa3JkZ3F6dXM0

The best photo is this one:

On the right we can see right up her arm something like a shop called "... SERRA".

A simple search on google returns a shop that looks very similar:



If we click on the image link we arrive on a website where the location is given:

Detalles

Girona, 13
Barcelona
08010

Contacto

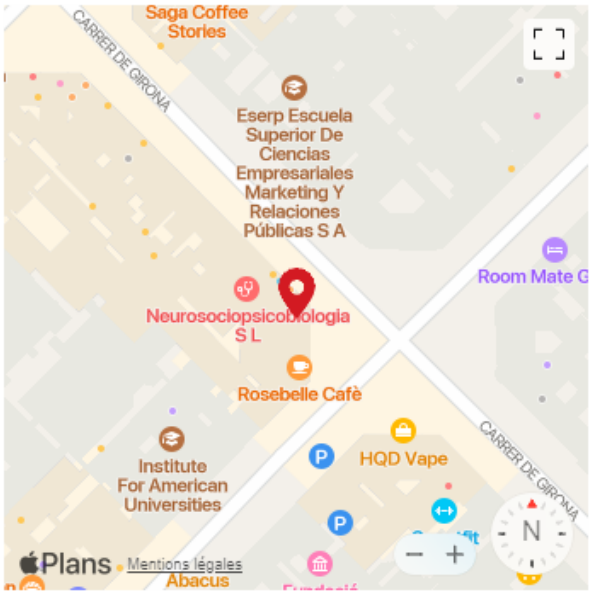
933 17 76 88

Transporte

Girona (M: L4)

Horas de apertura

De dl. a dv. de 9 h a 15 h i de 17 h a 21 h. Ds. de 9 h a 14 h

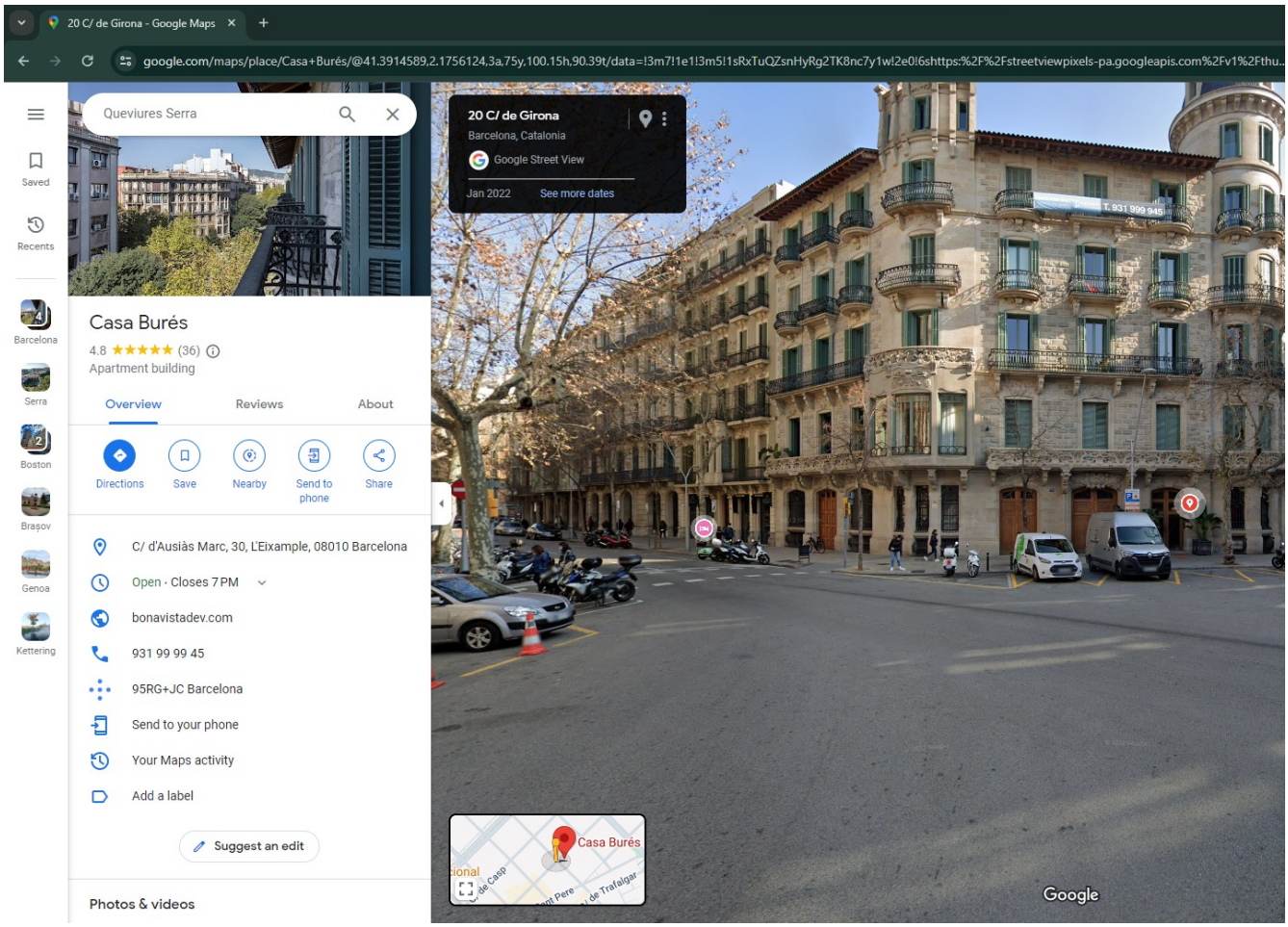


When we go there in street view we can confirm it is the shop of the photo:

And in front of the shop there is building with the same balcony as one the photo:

The balcony is located here:


Institut Europeu
de la Mediterrània
Casa Burés
Queviures Serra
Novela
Brunch · €€
Grupo Premium
Fermé temporairement
Clínica de Fisioteràpia
i Osteopatia Enric...



✓ Address found

The photo was taken in `C/ d'Ausiàs Marc, 30`