

Session #3 - OSINT

Cyber Security Uses-Cases Report



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

0. Table of Contents

- [Session #3 - OSINT](#)
 - [0. Table of Contents](#)
 - [1. Challenge 1](#)
 - [2. Challenge 2](#)
 - [3. Challenge 3](#)
 - [4. Challenge 4](#)

1. Challenge 1

⌚ Challenge 1

I'm glad that the platform gave 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.

Google search results for "GOLD CSS badge":

Environ 17 600 000 résultats (0,28 secondes) « Add Grepper Answer (a)

Credly by Pearson
https://www.credly.com › badge · Traduire cette page 29 :
CSS (Gold)
Earners of the **CSS (Gold) badge** can demonstrate the advanced skills needed to effectively use **CSS**. This includes using and writing extensions, ...

Stack Overflow
https://stackoverflow.com › help › badges › filter=gold 16 :
Badges
Badges appear on your profile page, flair, and your posts. All Earned Unearned **Gold** Silver Bronze. These **badges** are awarded for participating in non community- ...

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

Stack Overflow
https://stackoverflow.com › badges · Traduire cette page 16 :

css - Badge
Earn at least 1000 total score for at least 200 non-community wiki answers in the **css** tag. These users can single-handedly mark **css** questions as duplicates ...

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

stackoverflow.com/help/badges/247/css

Home Questions Tags Users Companies LABS Discussions NEW COLLECTIVES + Explore Collectives TEAMS

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

Create a free Team Why Teams?

Stack Overflow > Help center > Badges

Tags

css Earn at least 1000 total score for at least 200 non-community wiki answers in the `css` tag. These users can single-handedly mark `css` questions as duplicates and reopen them as needed.

Awarded 177 times.

Awarded Dec 6, 2023 at 4:00 to  Vadim Ovchinnikov 13.7k • 6 • 63 • 92

Awarded Nov 3, 2023 at 16:12 to  Andy Hoffman 18.8k • 5 • 43 • 62

Awarded Oct 26, 2023 at 4:01 to  CBroe 93.7k • 15 • 93 • 152

Awarded Sep 19, 2023 at 4:01 to  GreyRoofPigeon 18k • 5 • 37 • 59

Awarded May 24, 2023 at 4:03 to  showdev 28.8k • 37 • 57 • 75

Awarded Feb 7, 2023 at 4:05 to  Abhitalks 28.1k • 5 • 59 • 81

Awarded Dec 27, 2022 at 4:02 to  vanburen 21.6k • 7 • 29 • 42

Awarded Aug 24, 2022 at 4:03 to  dezman 18.7k • 11 • 54 • 91

Awarded Aug 20, 2022 at 23:35 to  zer00ne 42.5k • 6 • 43 • 70

Awarded Aug 18, 2022 at 4:02 to  Vitorino fernandes 15.9k • 3 • 22 • 40

Awarded Aug 15, 2022 at 23:10 to  Kaiido 129k • 13 • 235 • 300

Awarded Jul 18, 2022 at 13:42 to  vsync 123k • 58 • 321 • 409

We can just sort them until April 2011:

stackoverflow.com/help/badges/247?page=3

2011

 About Products For Teams Search...

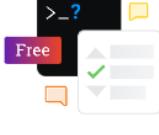
[Home](#) [Questions](#) [Tags](#) [Users](#) [Companies](#)

LABS [Discussions](#) **NEW**

COLLECTIVES [Explore Collectives](#)

TEAMS

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.



[Create a free Team](#)

Awarded Apr 24, 2012 at 3:02 to  **sandeep** 92k • 24 • 138 • 155

Awarded Feb 1, 2012 at 3:02 to  **Guffa** 693k • 108 • 744 • 1k

Awarded Dec 31, 2011 at 3:02 to  **David Thomas** 251k • 51 • 377 • 413

Awarded Aug 17, 2011 at 3:01 to  **alex** 484k • 203 • 884 • 987

Awarded Aug 4, 2011 at 3:01 to  **cletus** 620k • 169 • 915 • 945

Awarded Jun 26, 2011 at 3:01 to  **Nick Craver** 626k • 136 • 1.3k • 1.2k

Awarded May 15, 2011 at 3:01 to  **thirtydot** 226k • 49 • 390 • 351

Awarded Apr 15, 2011 at 3:01 to  **BoltClock** 710k • 162 • 1.4k • 1.4k

Awarded Apr 15, 2011 at 3:01 to  **bobince** 532k • 108 • 660 • 837

Awarded Jan 3, 2011 at 3:01 to  **Quentin** 928k • 129 • 1.2k • 1.4k

Awarded Aug 20, 2010 at 19:50 to  **Pekka** 446k • 146 • 976 • 1.1k

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.



BoltClock

Member for 14 years, 10 months Last seen more than a week ago
 NOVALISTIC.com Singapore

[Profile](#)

[Activity](#)

Checking his personal website NOVALISTIC.com I find a link to his [Newgrounds profile](#):

about products stuff dev blog contact

2. A personal site showcasing... well, a variety of *other* hobbies of mine (2.0, 2006–2007). Believe it or not, I did not learn CSS until I started developing this *second* iteration of the site from the ground up.
3. An attempt at creating an online resource for web developers, with tutorials, assets, and even a discussion forum. Codenamed "Oltanis", I spent months implementing version 3.0 between 2007 and 2008 before finally deciding not to launch it as I realized it was too large of a commitment for myself.
4. My first venture into the world of freelancing (4.0, 2010–2012). While I did launch my portfolio under the codename "Sarathos", I ultimately decided that freelancing wasn't for me for personal reasons, and so I doubled back not long afterward.

Astute readers will note that NOVALISTIC has spent basically *half* of its lifetime lost in space. So I've set out to change that. Today, NOVALISTIC 5.0, codenamed "Veldin" brings the site back to its roots: a showcase of websites and software that I've created as well as a collection of mini-sites based on my other interests. Just an online avenue for self-expression; no more, no less. Ten-year-old me would be amazed. Read more about it in this [blog post](#).

If you have any questions or feedback about the site, feel free to [reach out!](#)

me answering questions on Stack Overflow about Internet Explorer and Microsoft Edge, as well as Windows app development on WPF and UWP.

Fans of the Ratchet & Clank video game franchise may have noticed that the more recent versions of my site have been codenamed after various locations in the series. That's right: I'm a fan too! In fact, I'm planning to start a Ratchet & Clank fansite of my own, so watch this space!¹

You may know me elsewhere online as **BoltClock**, and you may be wondering how I came up with that name. That's a good question that comes up a lot; it comes from my roots in an Internet community known as the **Clock Crew**. I hope to elaborate on it with my Origins series of Flash animations, which you can find on my [Newgrounds profile](#).

1. This cosmic pun was brought to you by former Galactic President Copernicus L. Qwark. ↪

And on this profile Singapore again:

“ IM BOLT_CLOCK HAHAHA ”

Age 32, Male
Clock
Singapore
Joined on 5/28/05

NOVALISTIC

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

.COM @ \$9.98 Register a .COM domain for only \$9.98! While stocks last!

Whois Identity for everyone Domains Hosting Servers Email Security Whois Deals Enter Domain

Registrant Contact

Name:	VICTOR TAN
Organization:	NOVALISTIC.COM
Street:	BLOCK 320 TAMPINES STREET 33 #05-114
City:	SINGAPORE
State:	SINGAPORE
Postal Code:	520320
Country:	SG
Phone:	+65.93373222
Email:	vic3222@OUTLOOK.COM

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

Other Details

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

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



TOTAL RESULTS

314

TOP COUNTRIES



China	303
Germany	2
United Kingdom	2
United States	2
Canada	1

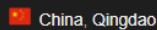
[More...](#)

TOP ORGANIZATIONS

Aliyun Computing Co., LTD	259
Aliyun Computing Co.LTD	17
China Mobile Communications Corpo...	5
DigitalOcean, LLC	5

[View Report](#)[View on Map](#)**Access Granted:** Want to get more out of your existing Shodan account?**47.104.36.86**

Aliyun Computing Co., LTD



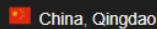
China, Qingdao

[eol-product](#)[eol-os](#)

```
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:636cde3b5c7a3923
redis_mode:standalone
os:Linux 5.11.105-16.1.al8.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtins
gcc_version:9.2.1
process_id:1
run_id:d21728347b1bbf34...
```

47.104.37.1

Aliyun Computing Co., LTD



China, Qingdao

[eol-product](#)

```
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:636cde3b5c7a3923
redis_mode:standalone
os:Linux 5.10.109-16.1.al8.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtins
```

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.

The screenshot shows a Shodan search result for the IP address 147.182.145.61. The search query used was "636cde3b5c7a3923 country:'CA'". The results page includes navigation links for "View Report", "Download Results", "Historical Trend", and "View on Map". A prominent message "Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to!" is displayed. The main card for the IP shows the following details:

147.182.145.61

DigitalOcean, LLC
Canada, Toronto

eol-product cloud

```
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:636cde3b5c7a3923
redis_mode:standalone
os:linux 6.1.0-0.deb11.7-amd64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.2.1
process_id:1
run_id:2ffc608fd83822ff9ab7becb1c44bd98b42687ab...
```

The screenshot shows the detailed host information for the IP 147.182.145.61. The host is identified as "Ubuntu". On port // 6379 / TCP, a Redis service is running. The service details are as follows:

// 6379 / TCP

run_id 1/1

Redis key-value store 5.0.7

```
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:636cde3b5c7a3923
redis_mode:standalone
os:Linux 6.1.0-0.deb11.7-amd64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtin
gcc_version:9.2.1
process_id:1
run_id:2ffc608fd83822ff9ab7becb1c44bd98b42687ab
tcp_port:6379
uptime_in_seconds:293
```

✓ 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:

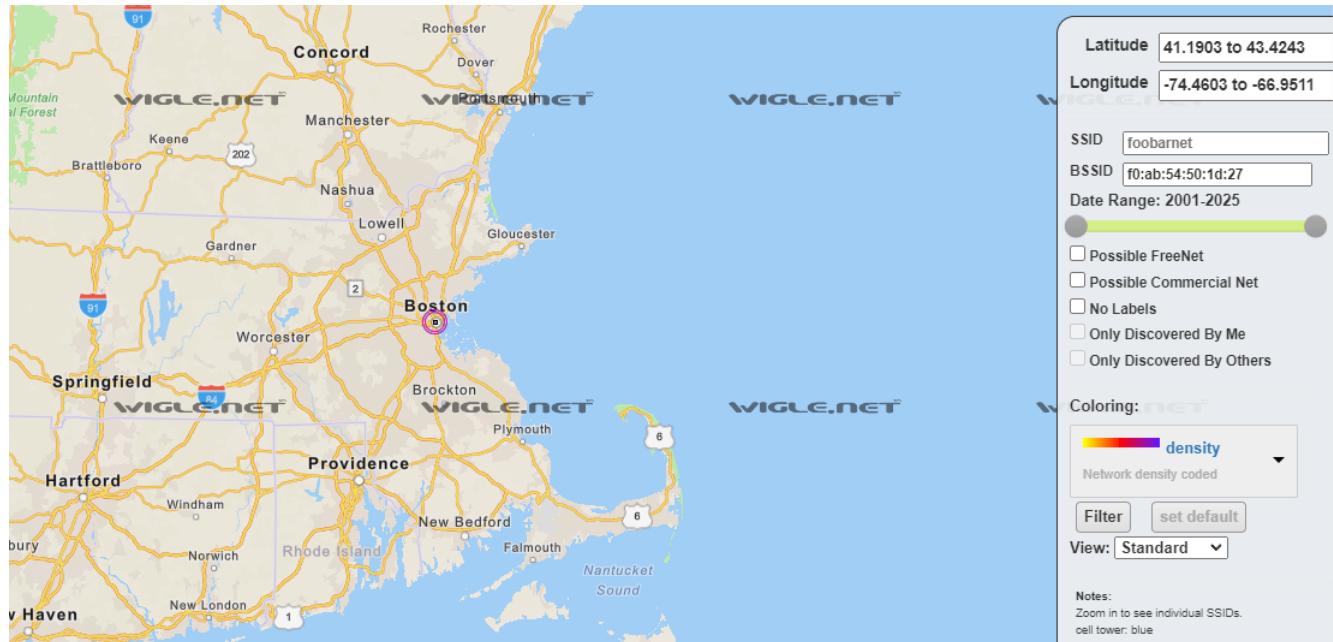
```
print  
ip = "130.41.35.56"  
port = 4444
```

And a MAC address:

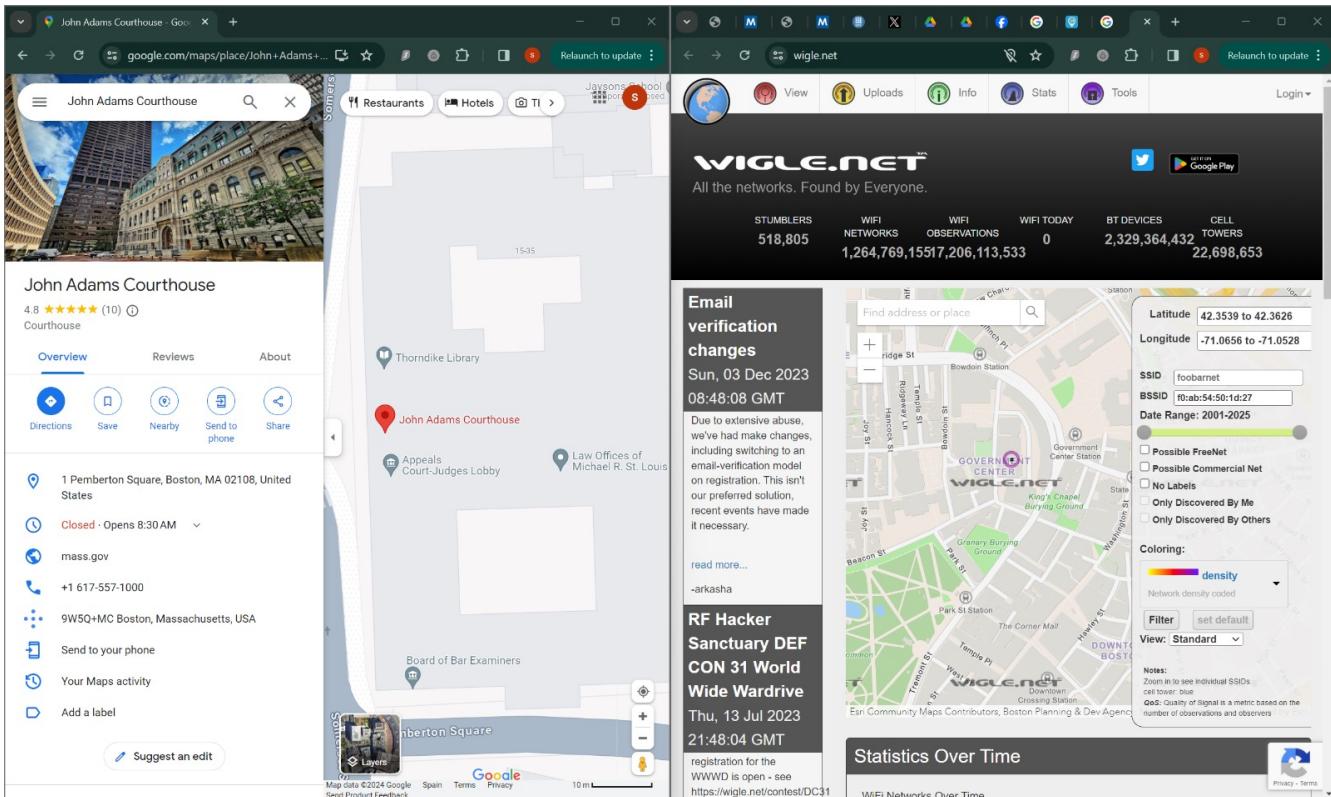
```
0.1 0:00.01 /usr/bin/VBoxClient --draganddrop  
0.1 0:00.00 /usr/bin/VBoxClient --seamless  
0.1 0:00.00 /usr/bin/VBoxClient --seamless  
0.1 0:00.00 /usr/bin/VBoxClient --seamless  
0.4 0:00.59 /usr/sbin/haveged --Foreground --verbose=1 -w 1024  
0.1 0:00.00 /sbin/getty -o -p -- \u --noclear tty1 linux  
0.1 0:00.20 xcape -e Super_L Control_L Escape  
0.1 0:00.00 xcape -e Super_L Control_L Escape  
0.0 0:00.00 ./airodump-ng -c 11 --bssid f0:ab:54:50:1d:27 -w dump wlan0mon  
ByF7Nice + F8Nice + F9Kill F10Quit
```

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:

< Tous

Maps

Images

Actualités

Vidéos

Plus



thinking mu



colmado



pep guardiola



charcutería



cristina s



serra-claret-woman.business...
Serra Claret Barcelona - Bot...



Time Out
Queviures Serra



serra-claret-woman.bus...
Serra Claret Barcelona ...



serra-claret-w...
Serra Claret Ba



VilaWeb
Queviures Serra: la botiga centenària on...



serra-claret-woman.business.s...
Serra Claret Barcelona - Bot...



regio7
Serra Claret tanca la botiga del Borr

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

Detalles

Girona, 13
Barcelona
08010

Contacto

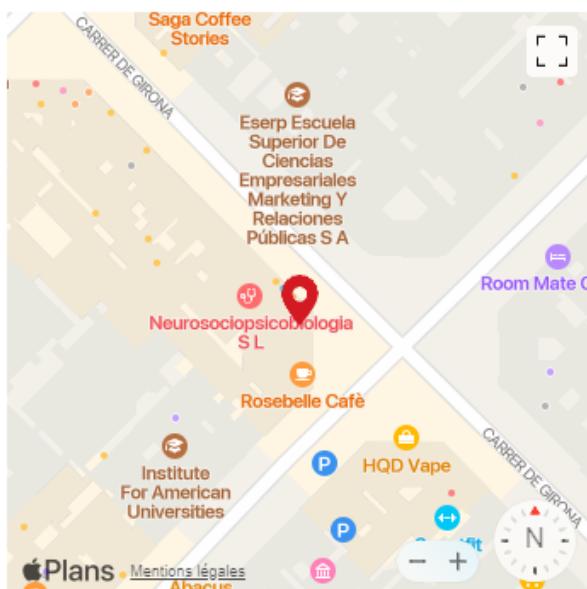
933 17 76 88

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:

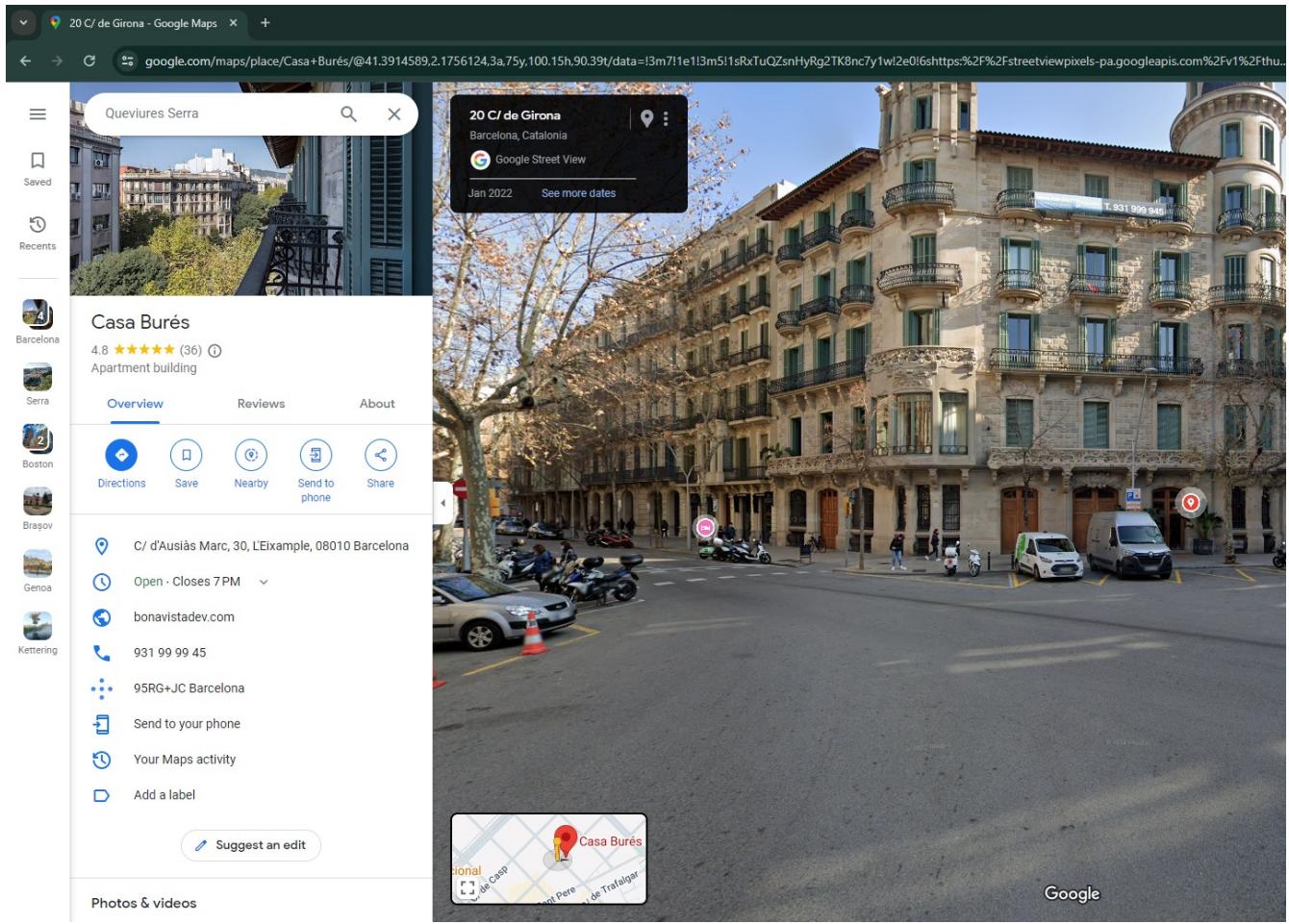


And in front of the shop there is building with the same balcony as one the photo:



The balcony is located here:





✓ Address found

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