



OSINT



## Manhunt #1

My dad is pissed off! He was told by my mother NOT to buy ice cream but he did anyway when she wasn't looking.

Someone posted this picture on the internet and my mother saw it, man, he is in so much trouble!

I want to know WHO posted this picture, let's hunt this guy down!



# Exiftool

Es un software de código abierto que nos permite leer y manipular metadatos (datos EXIF) de imágenes, audios y vídeos.

```
(athanos@kali)-[~/osint]
```

```
$ exiftool icecream.jpg
```

```
ExifTool Version Number      : 12.12
File Name                    : icecream.jpg
Directory                    : .
File Size                    : 322 KiB
File Modification Date/Time   : 2021:10:06 19:12:47-04:00
File Access Date/Time        : 2021:10:06 19:16:14-04:00
File Inode Change Date/Time   : 2021:10:06 19:16:14-04:00
File Permissions              : rwxrw-rw-
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order               : Big-endian (Motorola, MM)
Resolution Unit               : inches
Y Cb Cr Positioning           : Centered
Exif Version                  : 0231
Components Configuration     : Y, Cb, Cr, -
Flashpix Version              : 0100
Owner Name                    : Johnny Dorfmeister
Image Width                   : 1536
Image Height                  : 2048
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:4:4 (1 1)
Image Size                    : 1536x2048
Megapixels                    : 3.1
```



## Munhunt #2

Ah, now you know his name, good. Can you tell me the name of his last employer?





Johnny Dorfmeister site:linkedin.com



 Todos

 Videos

 Imágenes

 Noticias

 Maps

 Más

Herramientas

Cerca de 22 resultados (0.35 segundos)

<https://be.linkedin.com › johnny-do...> · Traducir esta página

## Johnny Dorfmeister - Manager - Zelfstandige | LinkedIn

Limburg, Flemish Region, Belgium · Manager · Zelfstandige

View **Johnny Dorfmeister's** profile on LinkedIn, the world's largest professional community.

Johnny has 2 jobs listed on their profile.

## Google Dorks

Los dorks son códigos que al escribirlos en la caja de búsqueda de Google te permiten encontrar información de forma más específica.

[Connect](#)[Message](#)

## Johnny Dorfmeister

web 2.0 specialist

Limburg, Flemish Region, Belgium · [Contact info](#)



Zelfstandige

### Activity

15 followers

Posts Johnny created, shared, or commented on in the last 90 days are displayed here.

[See all activity](#)

### Experience



#### Manager

Zelfstandige

Jul 2011 – Present · 9 yrs 7 mos



#### Webontwikkelaar

pishapasha

May 2011 – Jun 2011 · 2 mos



# Social Searcher

Free Social Media Search Engine

MENTIONS

USERS

TRENDS

Johnny Dorfmeister







🔍 Johnny Dorfmeister



Johnny Dorfmeister

ManagerZelfstandige Johnny Dorfmeister - Manager - Zelfstandige |  
LinkedIn<https://be.linkedin.com › johnny-do...https://be.linkedin.com › johnny-do...> · Traducir esta página



John Dorfmeister

PartnerMax Dorfmeister & Co., LLP John Dorfmeister - Partner - Max Dorfmeister & Co., LLP<https://www.linkedin.com › john-d...https://www.linkedin.com › john-d...> · Traducir esta página



Johnny Meister

VigilanteAXA Johnny Meister - Vigilante - AXA |  
LinkedIn<https://pt.linkedin.com › johnny-me...https://pt.linkedin.com › johnny-me...> · Traducir esta página



Johnny Chen



Johnny Mar



Johnny Jane

🔊 3 followers



# Munhunt #3

Ah, now you know his name, good. Can you tell me his favorite food?



Johnny Dorfmeister



johnnydorfmeister  
Johnny Dorfmeister



johnnydorfmeister

Seguir



8 publicaciones

14 seguidores

0 seguidos

Johnny Dorfmeister

PUBLICACIONES

ETIQUETADAS







johnnydorfmeister • [Seguir](#)



johnnydorfmeister People use this to post about their food, right? I tried to make my favorite food macaroni in the microwave today. It did not go so well, but i'll enjoy it nevertheless!

142 sem



im\_ezic looks really tasty bud



40 sem Responder



jobjoossen just keep on practicing



40 sem Responder



claarabarrios from today I love macaroni



40 sem Responder



6 Me gusta

14 DE ENERO DE 2019



Agrega un comentario

[Publicar](#)

# Munhunt #4

What is he talking about with that deleted page on his twitter account? can you retrieve it somehow?







johnny dorfmeister



Top

Latest

People

Photos

Videos



**johnny dorfmeister**

@johnnydorfmeis1

Webdeveloper / owner of [howitshould.be](https://howitshould.be)

Follow



**johnny dorfmeister**

6 Tweets




Follow

**johnny dorfmeister**

@johnnydorfmeis1

Webdeveloper / owner of [howitshould.be](https://howitshould.be)

 Joined January 2019

0 Following   **74** Followers

Not followed by anyone you're following



**johnny dorfmeister**

6 Tweets



Tweets

Tweets & replies

Media

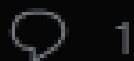
Likes



**johnny dorfmeister** @johnnydorfmeis1 · Jan 15, 2019



Does anyone know how to delete a page from a wordpress site? I created [howitshould.be/test-page](http://howitshould.be/test-page) but I can't seem to remove it now :-/



1



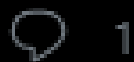
2



**johnny dorfmeister** @johnnydorfmeis1 · Jan 15, 2019



nevermind, found it! and in time too! it had some information on it that shouldn't be public... good thing the internet isn't archived, right? :D



1



Not followed by anyone you're following



Howitshould.be

Web Design  
AND CODING

## 404: Page not found

It looks like nothing was found at this location. Maybe try a search or one of the links below?



### Archives

Select Month ▼



# Wayback Machine

Nos permite tener acceso a versiones antiguas de webs, y en el caso de que estas hayan desaparecido o borrado de la WWW, siempre podemos encontrar una copia.

Además de ayudarnos a recuperar versiones antiguas, nos puede servir para añadir una url que queramos guardar por los motivos que sean.



**Calendar** · [Collections](#) <sup>beta</sup> · [Changes](#) <sup>beta</sup> · [Summary](#) · [Site Map](#) · [URLs](#)

Saved **2 times** between [January 15, 2019](#) and [December 28, 2020](#).



| JAN                  |                      |  |  |  |  |  | FEB         |                      |  |  |  |  |  | MAR           |                      |  |  |  |  |  | APR       |  |  |  |  |  |  |
|----------------------|----------------------|--|--|--|--|--|-------------|----------------------|--|--|--|--|--|---------------|----------------------|--|--|--|--|--|-----------|--|--|--|--|--|--|
| 1 2 3 4              |                      |  |  |  |  |  | 1           |                      |  |  |  |  |  | 1 2 3 4 5 6 7 |                      |  |  |  |  |  | 1 2 3 4   |  |  |  |  |  |  |
| 5 6 7 8 9 10 11      | 2 3 4 5 6 7 8        |  |  |  |  |  |             | 8 9 10 11 12 13 14   |  |  |  |  |  |               | 5 6 7 8 9 10 11      |  |  |  |  |  |           |  |  |  |  |  |  |
| 12 13 14 15 16 17 18 | 9 10 11 12 13 14 15  |  |  |  |  |  |             | 15 16 17 18 19 20 21 |  |  |  |  |  |               | 12 13 14 15 16 17 18 |  |  |  |  |  |           |  |  |  |  |  |  |
| 19 20 21 22 23 24 25 | 16 17 18 19 20 21 22 |  |  |  |  |  |             | 22 23 24 25 26 27 28 |  |  |  |  |  |               | 19 20 21 22 23 24 25 |  |  |  |  |  |           |  |  |  |  |  |  |
| 26 27 28 29 30 31    | 23 24 25 26 27 28 29 |  |  |  |  |  |             | 29 30 31             |  |  |  |  |  |               | 26 27 28 29 30       |  |  |  |  |  |           |  |  |  |  |  |  |
| MAY                  |                      |  |  |  |  |  | JUN         |                      |  |  |  |  |  | JUL           |                      |  |  |  |  |  | AUG       |  |  |  |  |  |  |
| 1 2                  |                      |  |  |  |  |  | 1 2 3 4 5 6 |                      |  |  |  |  |  | 1 2 3 4       |                      |  |  |  |  |  | 1         |  |  |  |  |  |  |
| 3 4 5 6 7 8 9        | 7 8 9 10 11 12 13    |  |  |  |  |  |             | 5 6 7 8 9 10 11      |  |  |  |  |  |               | 2 3 4 5 6 7 8        |  |  |  |  |  |           |  |  |  |  |  |  |
| 10 11 12 13 14 15 16 | 14 15 16 17 18 19 20 |  |  |  |  |  |             | 12 13 14 15 16 17 18 |  |  |  |  |  |               | 9 10 11 12 13 14 15  |  |  |  |  |  |           |  |  |  |  |  |  |
| 17 18 19 20 21 22 23 | 21 22 23 24 25 26 27 |  |  |  |  |  |             | 19 20 21 22 23 24 25 |  |  |  |  |  |               | 16 17 18 19 20 21 22 |  |  |  |  |  |           |  |  |  |  |  |  |
| 24 25 26 27 28 29 30 | 28 29 30             |  |  |  |  |  |             | 26 27 28 29 30 31    |  |  |  |  |  |               | 23 24 25 26 27 28 29 |  |  |  |  |  |           |  |  |  |  |  |  |
| 31                   |                      |  |  |  |  |  |             |                      |  |  |  |  |  |               | 30 31                |  |  |  |  |  |           |  |  |  |  |  |  |
| SEP                  |                      |  |  |  |  |  | OCT         |                      |  |  |  |  |  | NOV           |                      |  |  |  |  |  | DEC       |  |  |  |  |  |  |
| 1 2 3 4 5            |                      |  |  |  |  |  | 1 2 3       |                      |  |  |  |  |  | 1 2 3 4 5 6 7 |                      |  |  |  |  |  | 1 2 3 4 5 |  |  |  |  |  |  |
| 6 7 8 9 10 11 12     | 4 5 6 7 8 9 10       |  |  |  |  |  |             | 8 9 10 11 12 13 14   |  |  |  |  |  |               | 6 7 8 9 10 11 12     |  |  |  |  |  |           |  |  |  |  |  |  |
| 13 14 15 16 17 18 19 | 11 12 13 14 15 16 17 |  |  |  |  |  |             | 15 16 17 18 19 20 21 |  |  |  |  |  |               | 13 14 15 16 17 18 19 |  |  |  |  |  |           |  |  |  |  |  |  |
| 20 21 22 23 24 25 26 | 18 19 20 21 22 23 24 |  |  |  |  |  |             | 22 23 24 25 26 27 28 |  |  |  |  |  |               | 20 21 22 23 24 25 26 |  |  |  |  |  |           |  |  |  |  |  |  |
| 27 28 29 30          | 25 26 27 28 29 30 31 |  |  |  |  |  |             | 29 30                |  |  |  |  |  |               | 27 28 29 30 31       |  |  |  |  |  |           |  |  |  |  |  |  |

**DECEMBER 28, 2020**  
1 snapshot  
• 07:18:46

Calendar view maps the number of times <http://www.howitshould.be/test-page/> was crawled by the Wayback Machine, *not* how often it was actually updated. More info in the

howitshouldbe.be

[CONTACT](#)

[HOW THE WEB SHOULD BE!](#)

[TEST PAGE](#)



Howitshould.be  
Web Design  
AND CODING

## test page

Howdy! the flag is: w@yb@ck!

# Munhunt #5

So he's a webdesigner huh? I wonder what his customers have to say about his work. In english please!



# How the web should be!

Trust me, I've been on the web since 1995, I know webdesign!

So if you need a website that looks good, [contact me!](#)

But if you don't believe me, check out these stunning reviews:

*I've been using howitshould.be for over 15 years now! It's a pleasure working with Johnny and my website looks fabulous!*

— Ling – sells cars on her website

*Stor webdesigner, vil anbefale! Hjalp meg masse med mitt fantastiske nettsted.*

— arngren

*Есть свободный флаг: поэзия*

*In one word: stunning*

—

переведите меня

If you order a webdesign for more than 1 website, I'll throw in a selection of animated GIF's to place on your site!

Ruso detectado



Inglés

Есть свободный  
флаг: поэзия



Yest' svobodnyy flag: poeziya

There is a free flag:  
poetry



[Abrir en Google Traductor](#) • [Compartir](#)



# Munhunt #6

Can you tell me where he  
lives? Then I can drop  
some kind words in his  
mailbox!





# Howitshould.be

## Web Design

AND CODING

## contact

### Contact Me

Fields marked with an \* are required

**Name \***

**Email \***

**Message \***

# contact

Thanks for contacting me, an e-mail is on the way with more details.

It might happen that the mail server is broken again, if so, please send a letter with the job description to:

*Johnny Dorfmeister  
Melkvoetstraat 48  
3500 Hasselt*

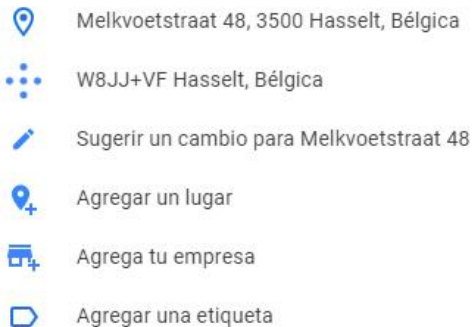
*Seriously, don't send anything to these people, I don't know them, it's only for the CTF!*

# Munhunt #7

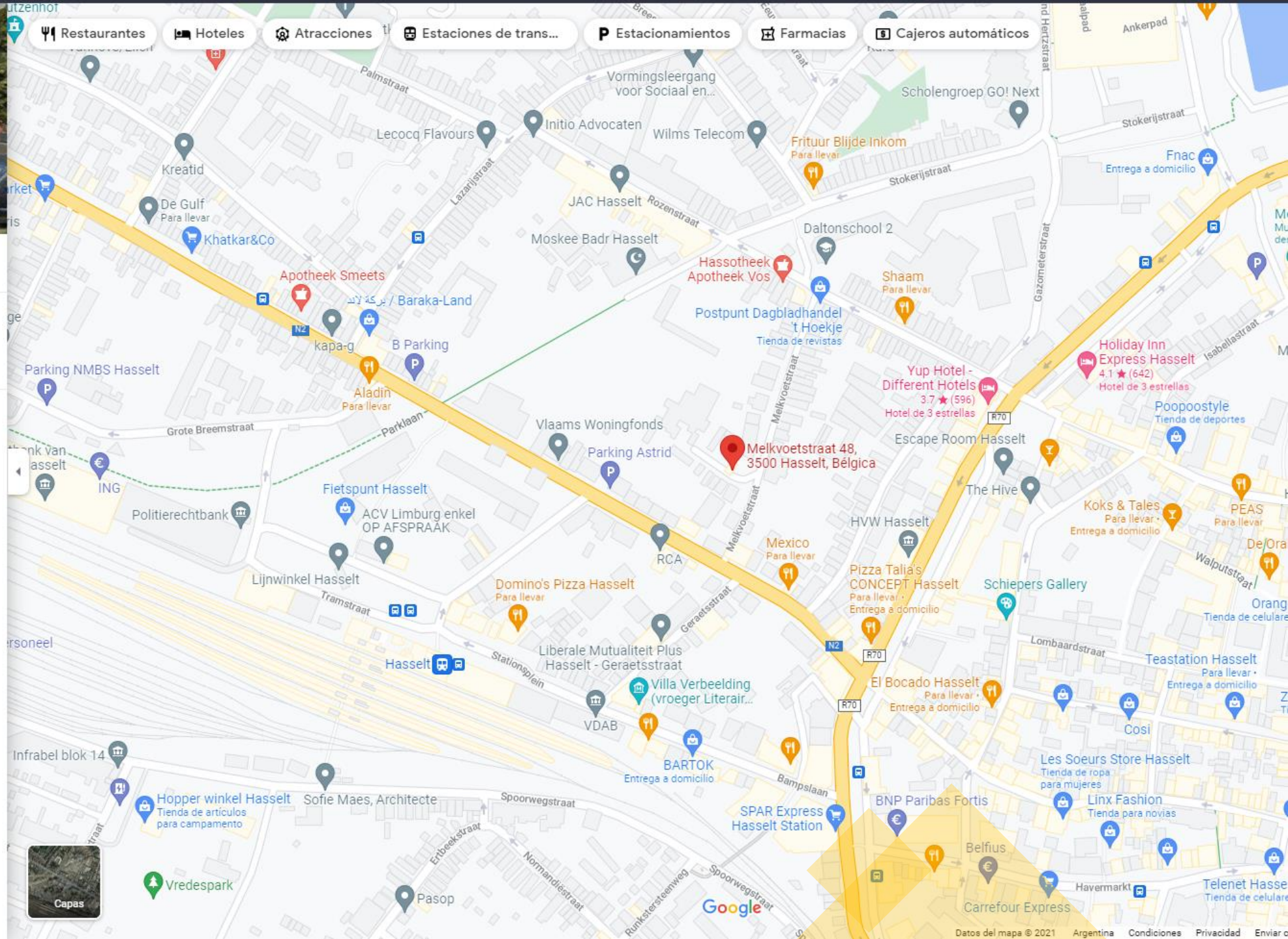
So now you know where he lives, can you tell me what was written on his wall in 2013?







## Fotos







Melkvoetstraat 48

Todo

Street View y 360°



**14 Melkvoetstraat**  
Hasselt, Región Flamenca

Google

🕒 Street View - jun. 2018



Google





Street View - jun. 2018



ago. 2009



2009



2018



4 Melkvoetstraat  
asselt, Región Flamenca

Google

Street View - jul. 2013



Actualmente se muestra: jul. 2013

2009

2018





# Munhunt #8



If you order a webdesign for more then 1 website, I'll throw in a selection of animated GIF's to place on your site!



[Auth](#)


<http://authentication.howitshould.be/auth.php>

## 1 capture

27 Dec 2020

Eat shit and die...



 | Elements Console Sources Network Performance Memory Application Security Lighthouse

```
<html>
  <head>...</head>
  <body>
    <!-- BEGIN WAYBACK TOOLBAR INSERT -->
    <style type="text/css">...</style>
    <script>__wm.rw(0);</script>
    <div id="wm-ipp-base" lang="en" style="display: block; direction: ltr;">...</div>
    <div id="wm-ipp-print">...</div>
    <div id="donato" style="position: relative; width: 100%;">...</div>
    <script type="text/javascript">...</script>
    <!-- END WAYBACK TOOLBAR INSERT -->
    <title>Auth</title>
    <!-- Authentication script by Johnny Dorfmeister. https://github.com/JohnnyDorfmeister/authentication-requests !--> == $0
    " Eat shit and die..."
  </body>
</html>
```

JohnnyDorfmeister / authentication-requests Public

< > Code

Issues

Pull requests

Actions

Projects

Wiki

Security

Insights

master

1 branch

0 tags

Go to file

Add file

Code



JohnnyDorfmeister Update auth.php ...

391b2e5 on 17 Jan 2019

2 commits



auth.php

Update auth.php

3 years ago

1 contributor

26 lines (26 sloc) | 749 Bytes

Raw

Blame



```
1 <html>
2 <body>
3 <title>Auth</title>
4 <?php
5 if(!isset($_POST['username']))
6 {
7     die("Eat shit and die...");
8 }
9 if($_POST['username'] == "johnny" && $_POST['password'] == removed for security reasons)
10 {
11     $_SESSION["loggedin"] = "true";
12     include("flag.php");
13     die();
14 }else{
15     echo "<form method=\"POST\" action=\"\" . $_SERVER['PHP_SELF'] . \">\n";
16     echo "<table align=\"center\">\n";
17     echo "  <tr><td>Username:&nbsp;<td><input type=\"text\" name=\"username\"></tr>\n";
18     echo "  <tr><td>Password:&nbsp;<td><input type=\"password\" name=\"password\"></tr>\n";
19     echo "  <tr><td colspan=2 align=\"right\"><input type=\"submit\" name=\"submit\" value=\"log in\"></tr>\n";
20     echo "</table>\n";
21     echo "</form>\n";
22     die();
23 }
24 ?>
25 </body>
26 </html>
```

 master ▾

 Commits on Jan 17, 2019

Update auth.php ...



JohnnyDorfmeister committed on 17 Jan 2019

Add files via upload



JohnnyDorfmeister committed on 17 Jan 2019

Newer

Older



Showing 1 changed file with 26 additions and 0 deletions.

Unified

Split

26 auth.php

...

@@ -0,0 +1,26 @@

```
1 + <html>
2 + <body>
3 + <title>Auth</title>
4 + <?php
5 + if(!isset($_POST['username']))
6 + {
7 +     die("Eat shit and die...");
8 + }
9 + if($_POST['username'] == "johnny" && $_POST['password'] == "letmein")
10 + {
11 +     $_SESSION["loggedin"] = "true";
12 +     include("flag.php");
13 +     die();
14 + }else{
15 +     echo "<form method=\"POST\" action=\"http://authentication.howitshould.be/auth.php\">\n";
16 +     echo "<table align=\"center\">\n";
17 +     echo "  <tr><td>Username:&nbsp;<td><input type=\"text\" name=\"username\"></tr>\n";
18 +     echo "  <tr><td>Password:&nbsp;<td><input type=\"password\" name=\"password\"></tr>\n";
19 +     echo "  <tr><td colspan=2 align=\"right\"><input type=\"submit\" name=\"submit\" value=\"log in\"></tr>\n";
20 +     echo "</table>\n";
21 +     echo "</form>\n";
22 +     die();
23 + }
24 + ?>
25 + </body>
```



```
6 + {
7 +     die("Eat shit and die...");
8 + }
9 + if($_POST['username'] == "johnny" && $_POST['password'] == "letmein")
10 + {
11 +     $_SESSION["loggedin"] = "true";
12 +     include("flag.php");
13 +     die();
14 + }else{
15 +     echo "<form method=\"POST\" action=\"http://authentication.howitshould.be/auth.php\">\n";
16 +     echo "<table align=\"center\">\n";
```

Untitled Request

BUILD

POST http://authentication.howitshould.be/auth.php

Send

Save

ParamsAuthorizationHeaders (9)BodyPre-request ScriptTestsSettings

none

form-data

x-www-form-urlencoded

raw


binary

GraphQL

|                                     | KEY      | VALUE   | DESCRIPTION | ... | Bulk Edit |
|-------------------------------------|----------|---------|-------------|-----|-----------|
| <input checked="" type="checkbox"/> | username | johnny  |             |     |           |
| <input checked="" type="checkbox"/> | password | letmein |             |     |           |
|                                     | Key      | Value   | Description |     |           |

PrettyRawPreviewVisualizeHTML

```
1 <html>
2
3 <body>
4   <title>Auth</title>
5   <!-- Authentication script by Johnny Dorfmeister. https://github.com/JohnnyDorfmeister/authentication-requests !-->
6   congratulations, the flag is glittern00b
```



Dudas y  
preguntas



Extra!

# Visit Limburg

I'm supposed to meet up with my buddy who supplies me with Twilight cd's but he's very cryptic about the meeting location.

He told me he will meet under a bridge that sits in the middle of a triangle of 3 locations.

The first two locations are the two mineshafts of the coalmines in the province that are the furthest appart from each other.

The third location is where the provided (hazy) picture was taken

Please provide the date that was written under the bridge in 2013





genk



mine shafts



limburg belgium



belgium stock



at eisen



netherlands



1945 location



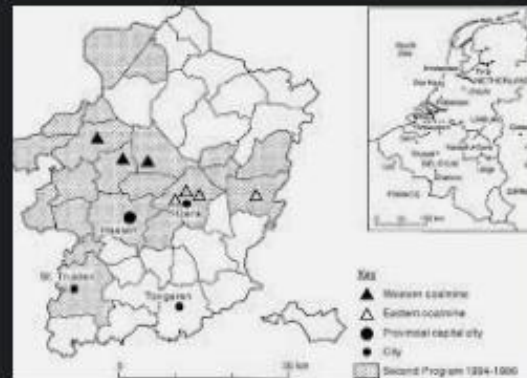
duto

**Quisiste decir:** limburg *coal mines*

South Limburg coal mi...  
en.wikipedia.org



This is Belgium: Coal mines in Limburg  
whatisbelgium.blogspot.com



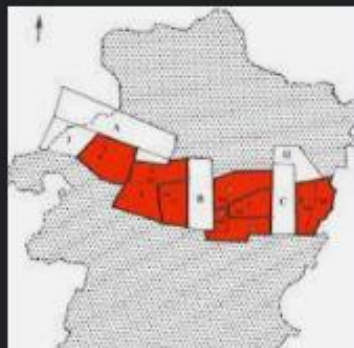
Limburg's former coal mines, the Objective...  
researchgate.net

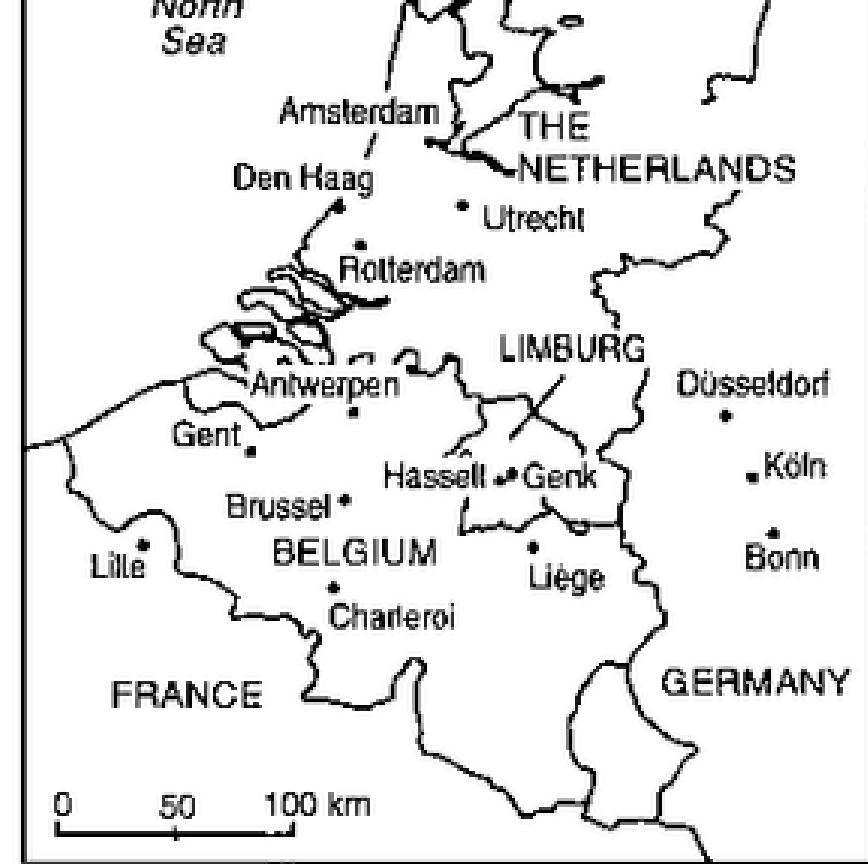
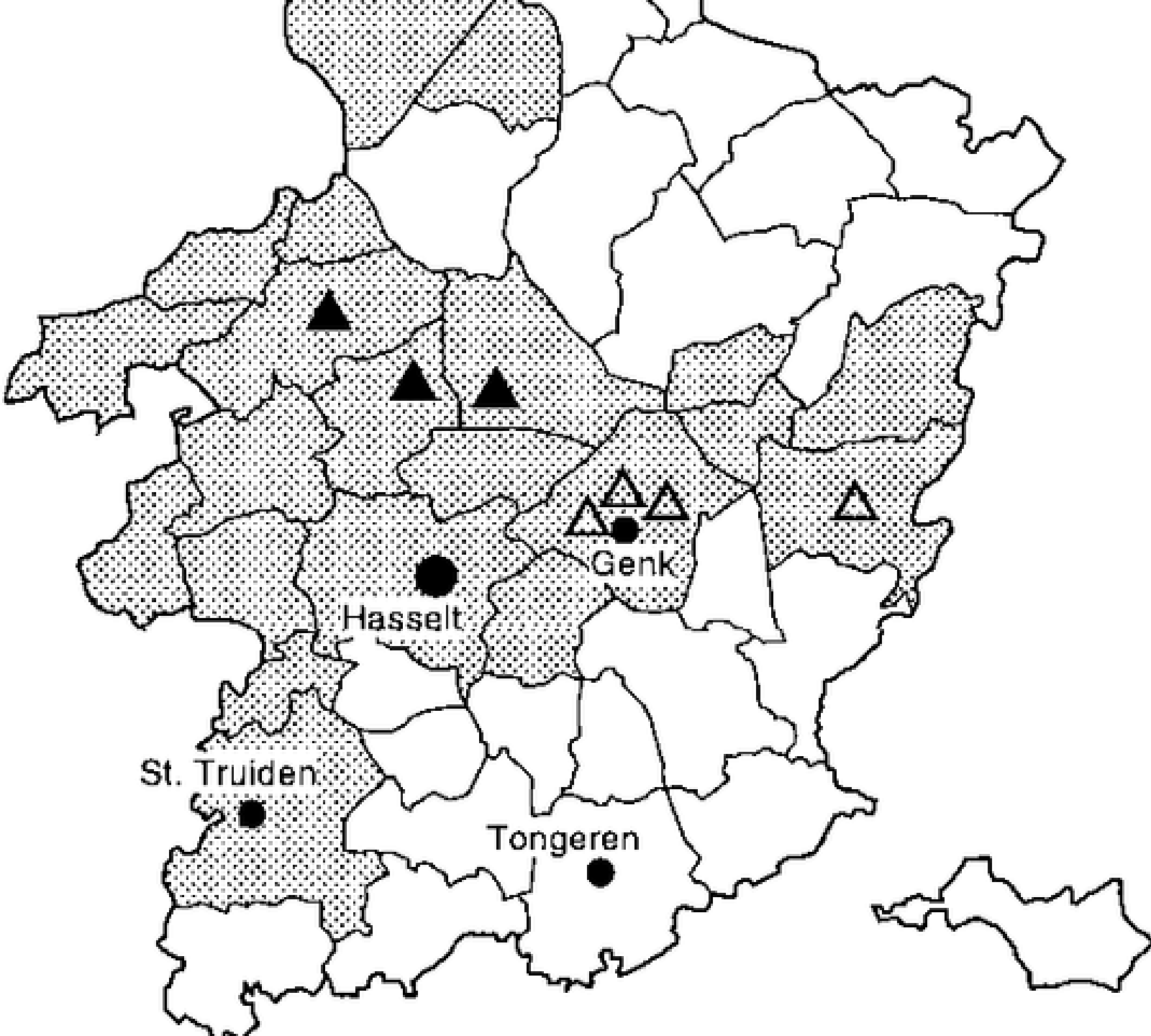


Coal Mines, a photo from Limburg, FI...  
treearth.com



Headframes / lift towers of abandone...  
alamy.com









Key

- ▲ Western coalmine
- △ Eastern coalmine
- Provincial capital city
- City





 Todos **Imágenes** Maps Noticias Videos Más

Herramientas



arquitectura



bélgica



reading between



borgloon



iglesia abandonada



arquitectos belgas



gij



Una iglesia transparente en Bélgica de Gijs Van Vaer...  
anticcolonial.com



Una Iglesia Transparente...  
rinconabstracto.com



Arquitectura y Escultura: La iglesia transparen...  
lamparadecarton.com



La 'iglesia transparente' ...  
latrotamundos.com



Arquitectura y Escultura: L...  
lamparadecarton.com



Conéctate con la naturaleza en esta igl...  
elcomercio.pe



Iglesia Transparente - yalosabes.com  
yalosabes.com



Arquitectura y Escultur...  
lamparadecarton.com



Iglesia transparente... - Curiosidades univer...  
facebook.com



Parece una iglesia aba...  
coyotitos.com






## Doorkijkerk Borgloon

4.6 ★★★★★ 76 opiniones

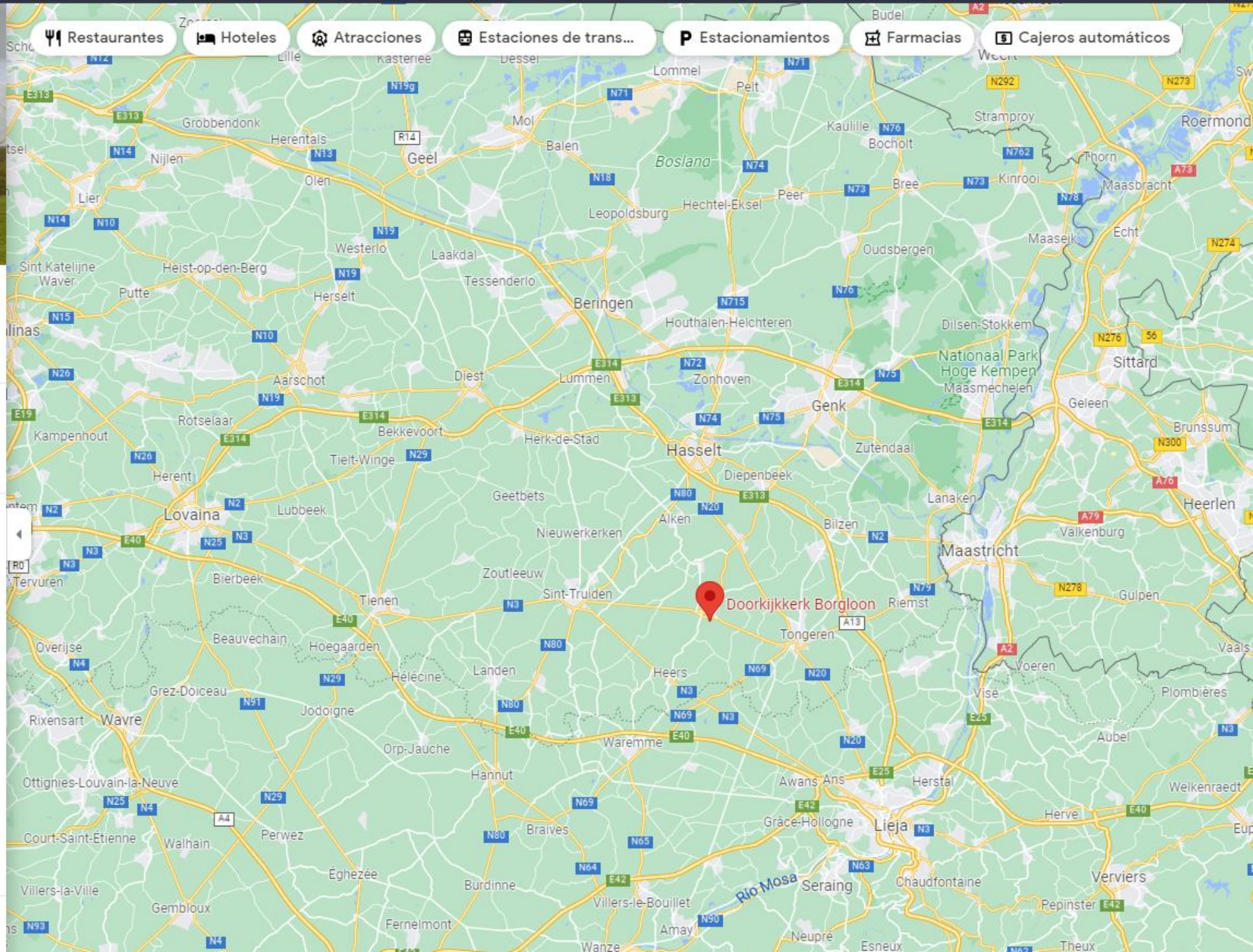
Atracción turística

-  Indicaciones
-  Guardar
-  Cerca
-  Enviar al teléfono
-  Compartir

-  3840 Borgloon, Bélgica
-  Abierto ahora: Abierto las 24 horas ▾
-  borgloon.be
-  +32 12 67 36 53
-  Q9V2+JQ Borgloon, Bélgica
-  Reclamar este negocio
-  Agregar una etiqueta

 Sugerir una edición

Horarios populares **miércoles** ⓘ



















009 • 2019



Mirando los CTFs ahora,  
parecen muy fáciles,  
pero créanme, durante  
el CTF no lo fueron.