Lespion_allunell --- CyberDefenders

Q1: File -> Github.txt: What API key did the insider add to his GitHub repositories?

```
aJFRaLHjMXvYZgLPwiJkroYLGRkNBW
```

Resolution:

I searched on the repositories, until I found on the first one 2 .js. Inspecting them, I found the API Key.

```
https://github.com/EMarseille99/Project-Build---Custom-Login-
Page/blob/master/Login%20Page.js
```

```
1     API Key = aJFRaLHjMXvYZgLPwiJkroYLGRkNBW
```

Q2: File -> Github.txt: What plaintext password did the insider add to his GitHub repositories?

```
PicassoBaguette99
```

Resolution:

In the same file, I found the password. It said it was in base64, so I decoded the password:

```
https://github.com/EMarseille99/Project-Build---Custom-Login-
Page/blob/master/Login%20Page.js
```

```
https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-
9%2B/%3D',true,false)&input=VUdsallYTnpiMEpoWjNWbGRHRlUmxPVGs9
```

```
Password: UGljYXNzb0JhZ3VldHRlOTk=
Password(base64)
```

Recipe	^ 🖫 ▭ 🗑	Input

Recipe   ^ 🖫 ▭ 🗑   **Input**

UGljYXNzb0JhZ3VldHRlOTk=

From Base64   ^ ⊘ ‖

Alphabet
A-Za-z0-9+/=   ▾   ☑ Remove non-alphabet chars

☐ Strict mode

ᴀʙᴄ 24   ☰ 1   ⸬ 22→23 (1 selected)

Output

PicassoBaguette99

Q3: File -> Github.txt: What cryptocurrency mining tool did the insider use?

    XMRig

Resolution:

Searching through the different repositories, checking the different descriptions, there was one it matches with a mining tool.

    https://github.com/EMarseille99/xmrig

Q4: On which gaming website did the insider have an account?

    steam

Resolution:

With a bit of OSINT, I found her instagram account:

``https://www.instagram.com/emarseille99/?hl=es

In her instagram, just in the feed there is a QR code:
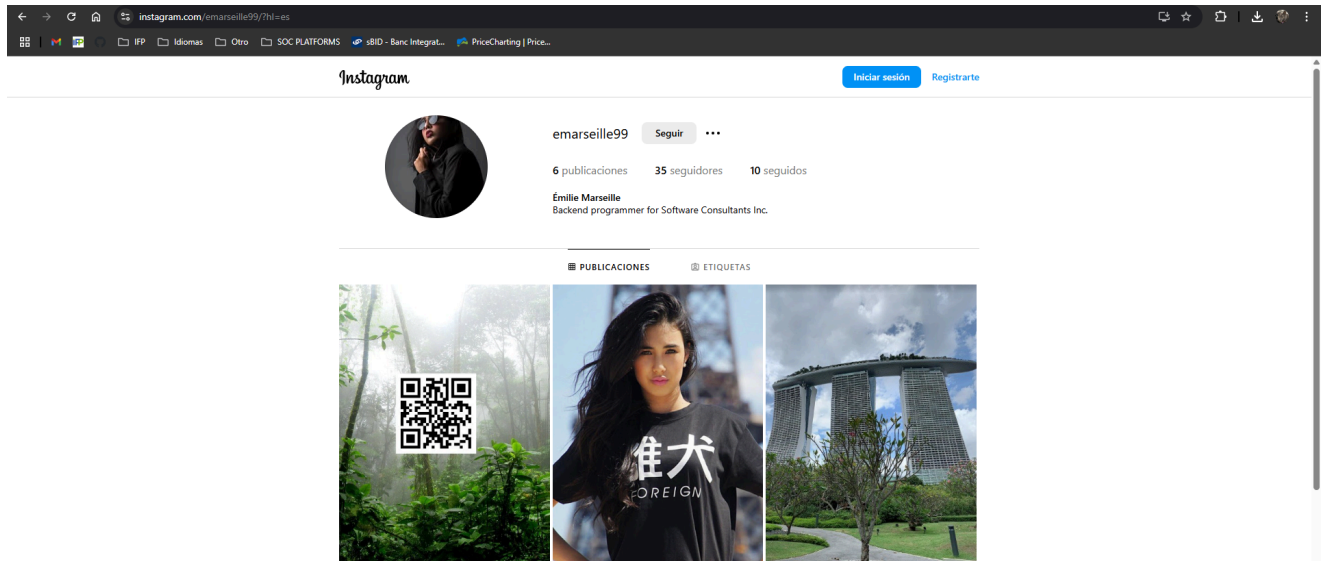
I screenshooted the QR code and went to a decoder website to retrieve the information:

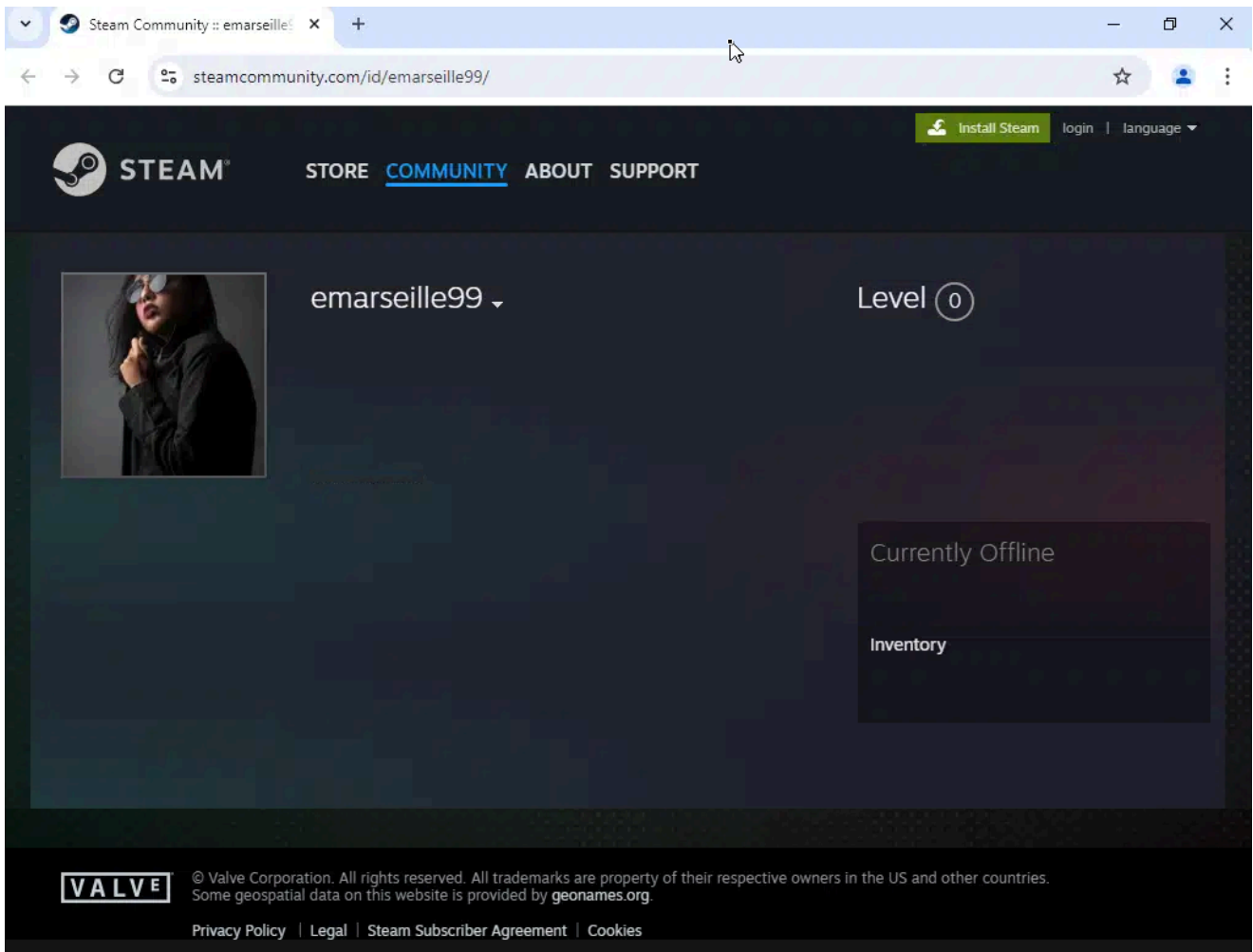Beep

↓ QR Code Result ↓

🔗 https://qrgo.page.link/4k9hH

📄 Copy   ⬀ Open Link

Later, in a sandbox for security measures, I opened the link and it showed the gaming site:

Q5: What is the link to the insider Instagram profile?

https://www.instagram.com/emarseille99/

Resolution:

Previous this task, we already found the instagram profile:
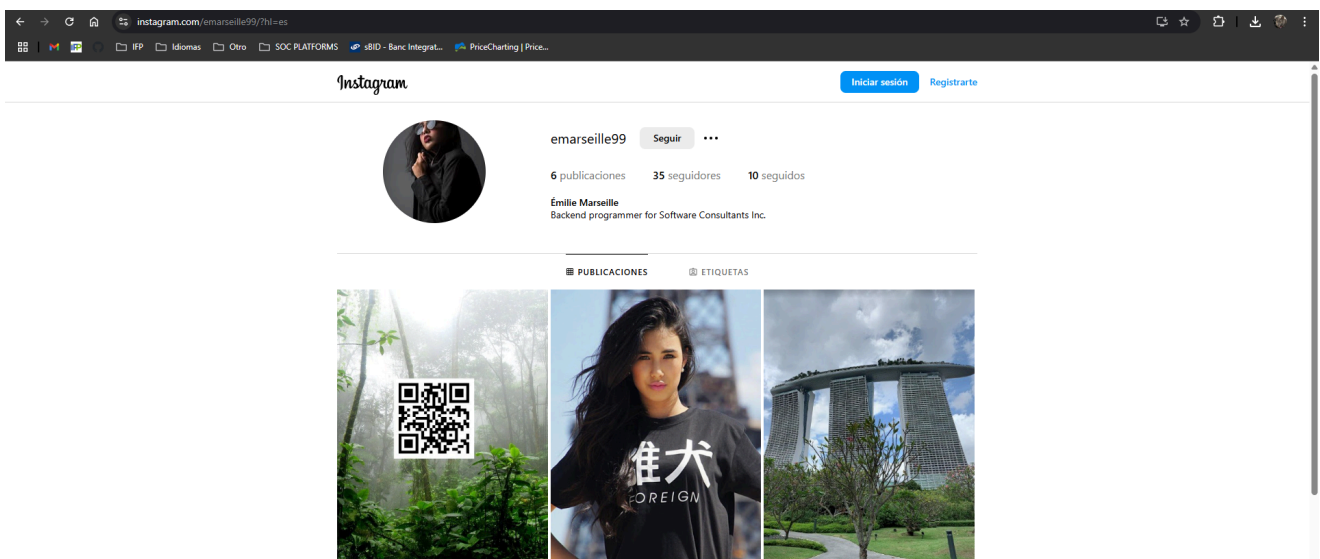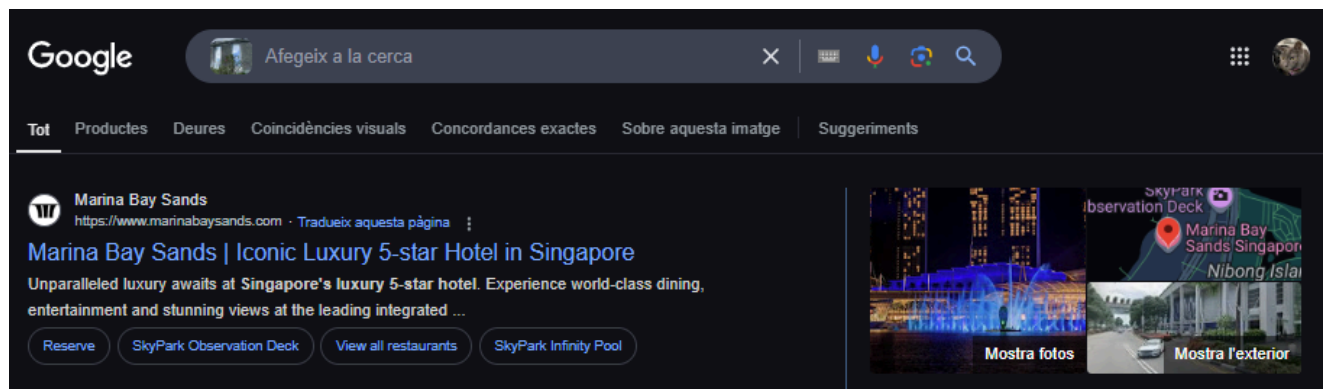
Q6: Which country did the insider visit on her holiday?

Singapore

Resolution:

With the image in the instagram profile, we did a fast research on google photos.

Q7: Which city does the insider family live in?

Dubai

Resolution:

I found in the image, in the long distance, the distintive Burj Khalifa builidng, set on Dubai.

emarseille99 • Seguir

emarseille99 photo 2/2
254 sem

7 Me gusta
24 de mayo de 2020

Inicia sesión para indicar que te gusta o comentar.

Q8: File -> office.jpg: You have been provided with a picture of the building in which the company has an office. Which city is the company located in?

```
Birmingham
```

Resolution:

With **yandex**, I did the image research. In the section "About the image", the first result is "birmingham new street railway station".

```
https://yandex.com/images/search?
cbir_id=215549%2FauewGjGB2pOYUSIXRfNBXQ467&rpt=imageview&url=https%3A%2F%2Fa
vatars.mds.yandex.net%2Fget-images-
cbir%2F215549%2FauewGjGB2pOYUSIXRfNBXQ467%2Forig
```
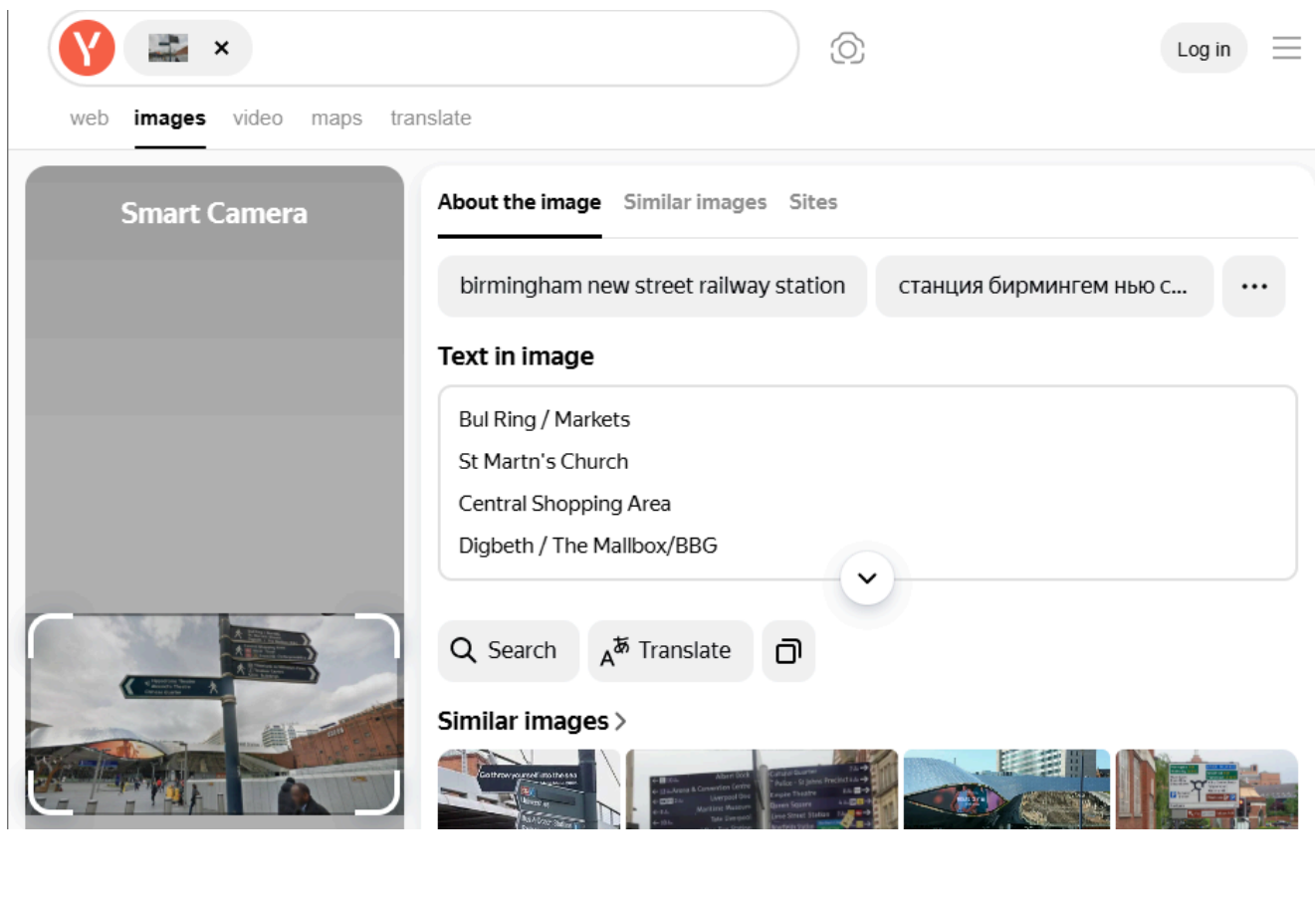
Q9: File -> Webcam.png: With the intel, you have provided, our ground surveillance unit is now overlooking the person of interest suspected address. They saw them leaving their apartment and followed them to the airport. Their plane took off and landed in another country. Our intelligence team spotted the target with this IP camera. Which state is this camera in?

```
Indiana
```

Resolution:

With the image research, I found the building: The Golden Dome atop. With some research, I found is from the University of Notre Dame, in Indiana, US.

```
https://yandex.com/images/search?
cbir_id=10235469%2FUyo8IJD5YYWzZME2i8e5Ig959&lr=10429&rpt=imageview&url=http
s%3A%2F%2Favatars.mds.yandex.net%2Fget-images-
cbir%2F10235469%2FUyo8IJD5YYWzZME2i8e5Ig959%2Forig
```
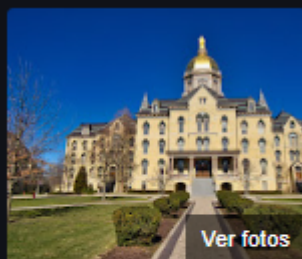
The Golden Dome atop the MaIn Building at th…
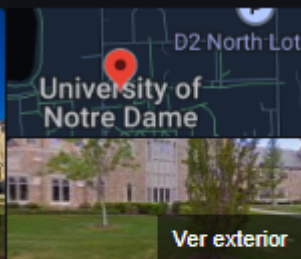
Universidad de Notre Dame

4,7 ★★★★☆ 1.410 reseñas ⓘ

Universidad en Notre Dame, Indiana