|  |
| --- |
| Cyber Defenders |
| L’Espion |
| Threat Intelligence |

|  |
| --- |
| Abdallah Chbaro  09/04/2023 |

Table des matières

[Details 2](#_Toc131948330)

[Tools 2](#_Toc131948331)

[Write Up 3](#_Toc131948332)

[Txt File 3](#_Toc131948333)

[Instagram 6](#_Toc131948334)

[Office.jpg 12](#_Toc131948335)

[WebCam.png 14](#_Toc131948336)

# Details

You have been tasked by a client whose network was compromised and brought offline to investigate the incident and determine the attacker's identity.

Incident responders and digital forensic investigators are currently on the scene and have conducted a preliminary investigation. Their findings show that the attack originated from a single user account, probably, an insider.

Investigate the incident, find the insider, and uncover the attack actions

# Tools

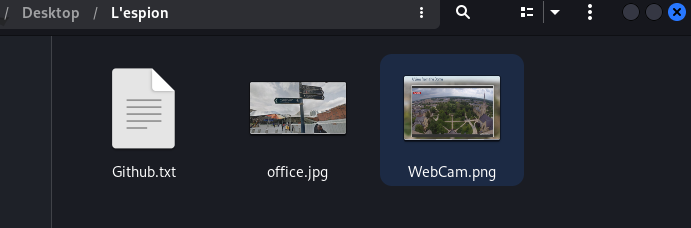
* Google Maps
* Google Image search
* Sherlock

# Write Up

The first thing we will do, is to gather as much information as possible from the given.

Extracting the zip file provided, we see three files:

1. A text file called ‘GitHub.txt’
2. An image called ‘office.png’
3. An image called ‘WebCam.png’

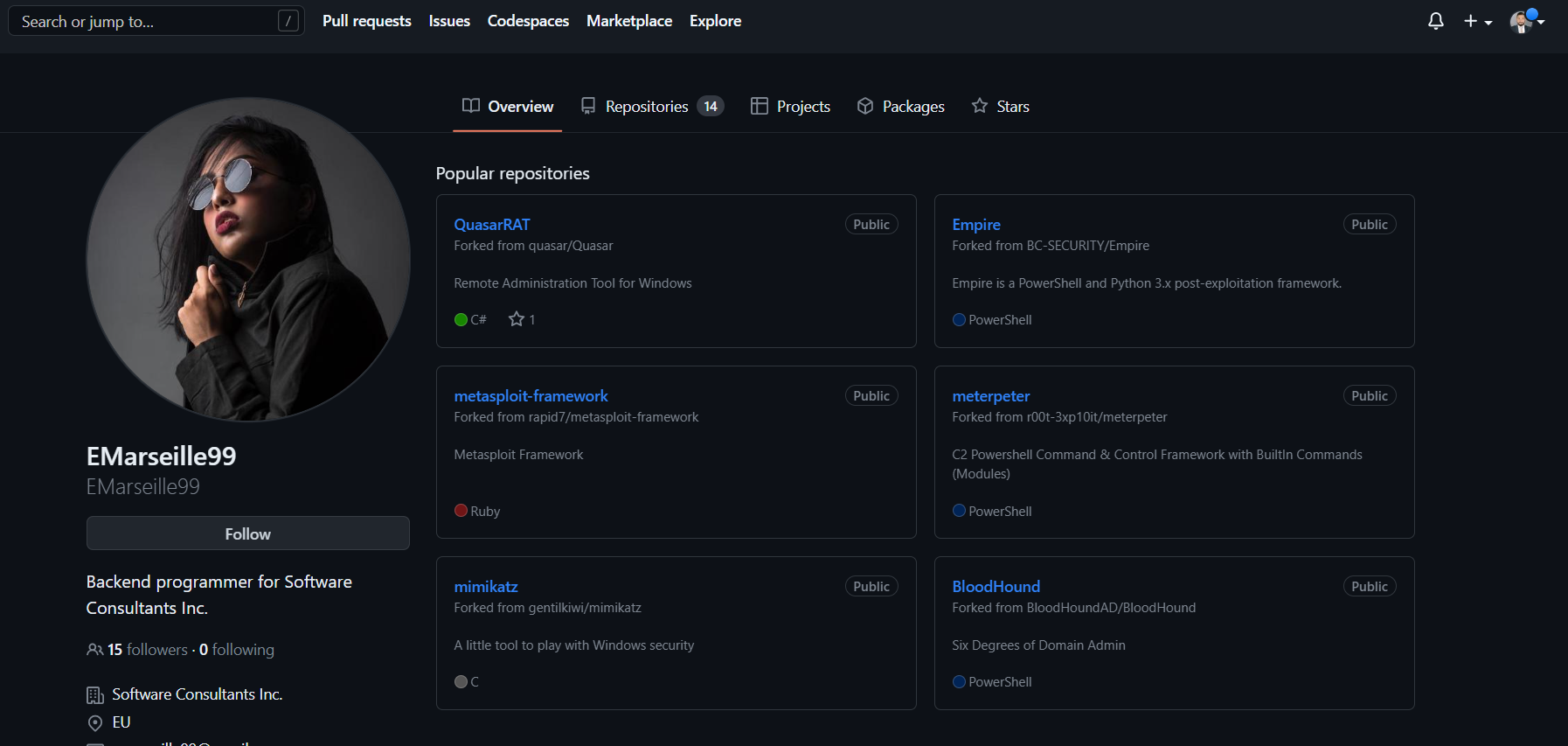


## Txt File

Looking at the Txt file, we find a url: ‘https://github.com/EMarseille99’



Visiting the link, we land on a profile on GitHub as shown below:

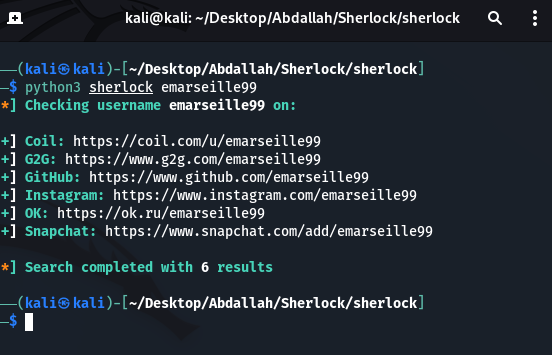


We can see on the profile that it is for a developer called ‘Emarseille99’ and working for ‘Software Consultants Inc.’, in Europe.

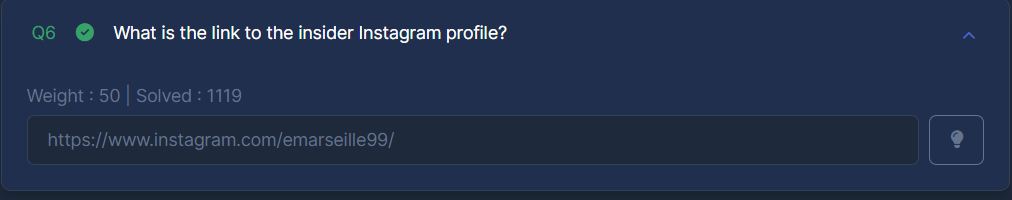
We see also an email address: ‘emarseille99@gmail.com’.

Doing a google search, we see that she is called Emilie Marseille. Visiting her profile on LinkedIn, we see that she studied at Sorbonne, in France.

Provided the username, we can use ‘Sherlock’ to hunt down social media accounts by username across social networks. After installing the tool, we run providing the username ‘Emarseille99’, as shown below:



Using the social media account found, we can answer question 6, as shown below:

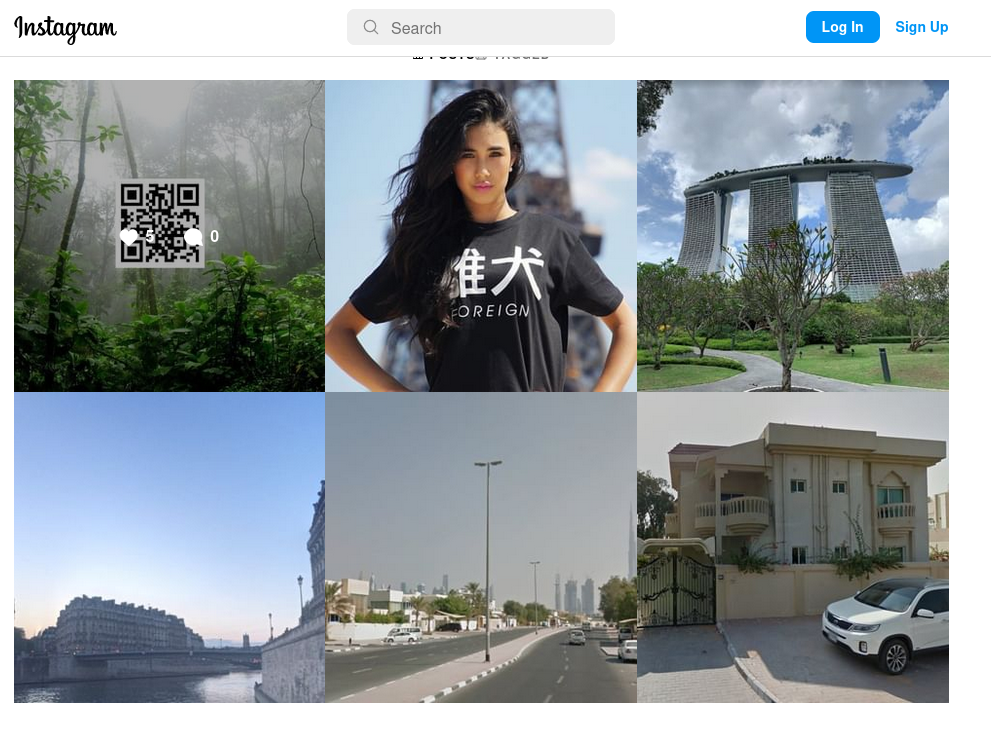


Next, we will check all the social media accounts, maybe we find something useful:

We find that only the GitHub account and the Instagram account are available (so nothing useful).

## Instagram

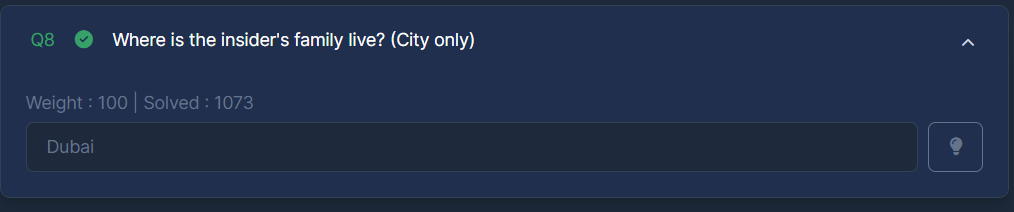
Visiting her Instagram account, we land on the following:



Opening each photo, we see that in her last photo she wrote: ‘nice to meet friends & family’.

The last 2 photos are taken from Dubai, as Burj Khalifa is shown and as the UAE flag is shown.

With the found information, we can answer question 8:



Looking for more picture in the Instagram profile, we see a photo with a comment: ‘Once in a lifetime holiday here, love me some slings x’, shown below:



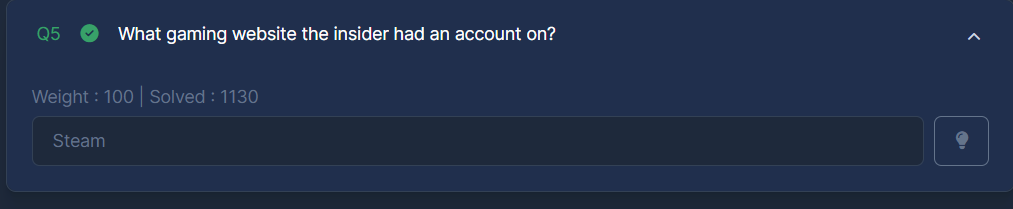
Doing an image search on google, we find that this photo is for Marina Bay Sands Hotel Tower 1 in Singapore. This information makes us answer question 7:



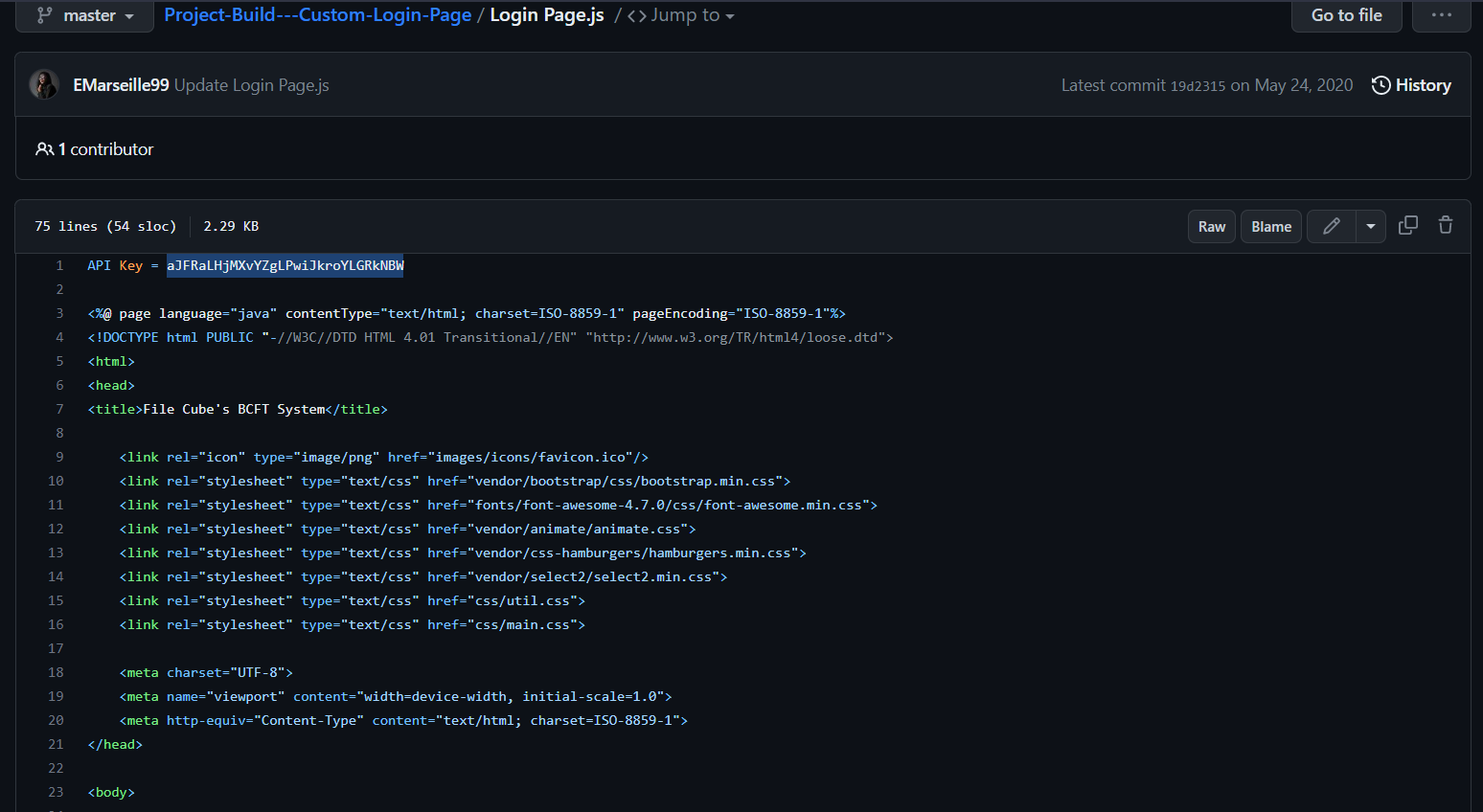
Looking at the first photo in the Instagram page, we see a QR code. Opening this QR code, we land on her account on Steam:



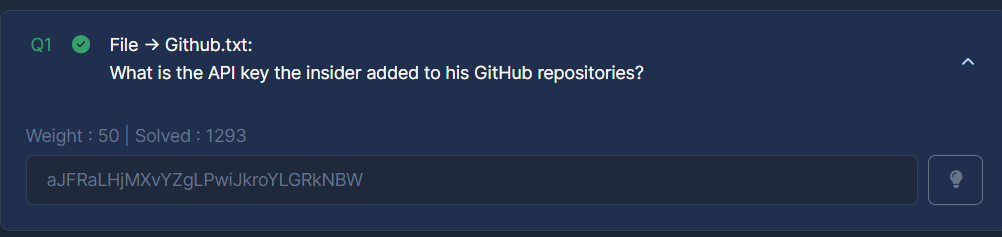
This information makes us answer question 5:



Scrolling through her GitHub page, we land on the following:



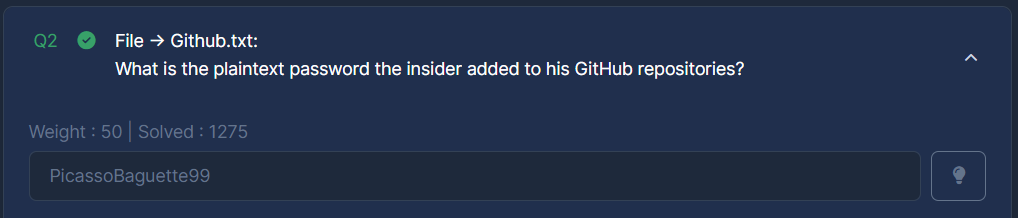
The first line contains an API, that makes us answer question 1:



Scrolling down, we see a base64 encoded password, as shown below:



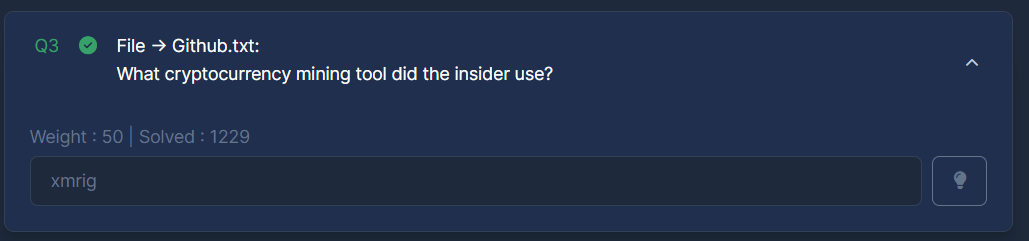
Decoding the password makes us answer question 2:



Scrolling through her repo, we see a crypto miner:

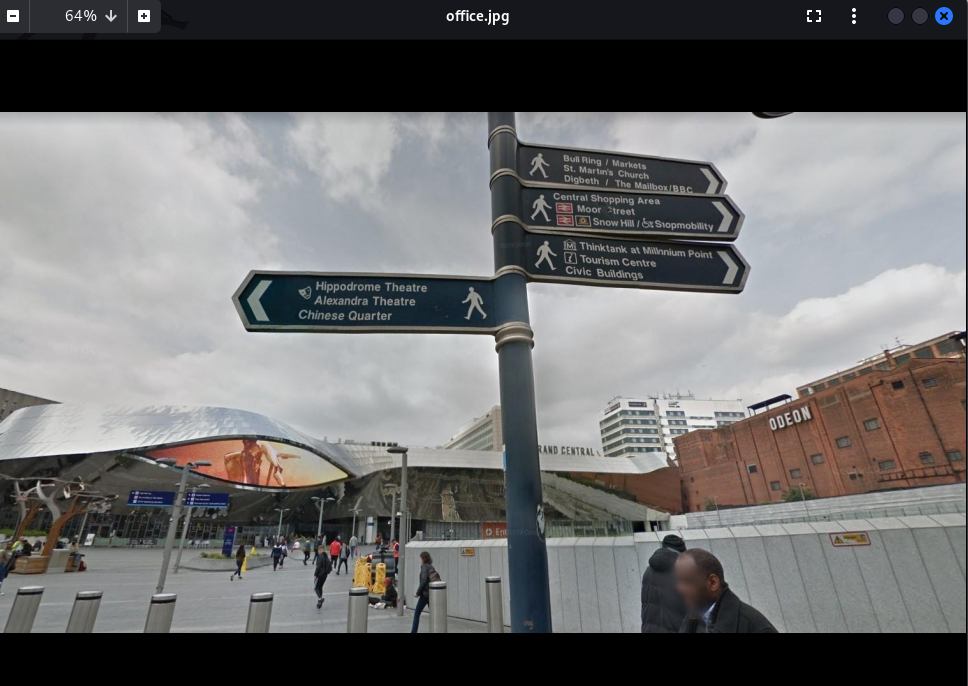


This information makes us answer question 3:

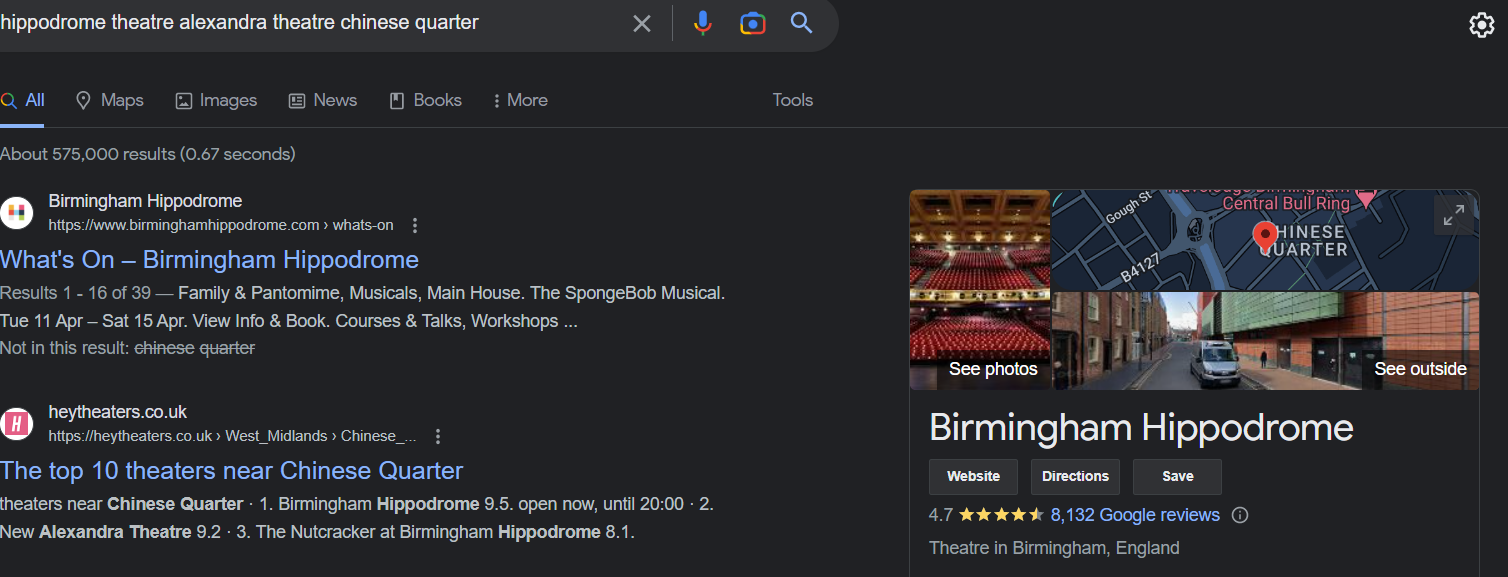


## Office.jpg

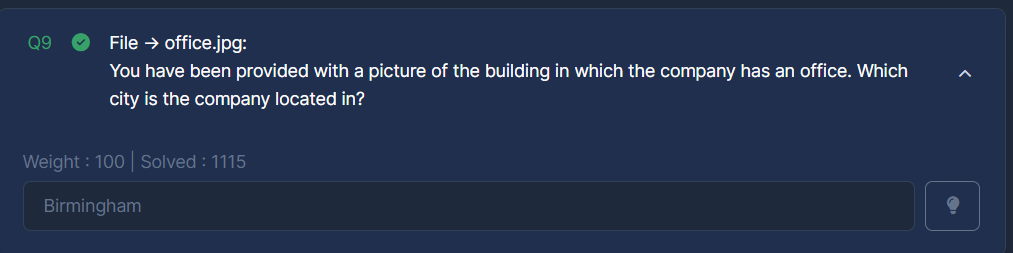
Opening the image ‘office.jpg’, we see the following:



Doing a google search on the Hippodrome Theatre, Alexandra Theatre and Chinese Quarter, we find that the location is in England Birmingham, as shown below:

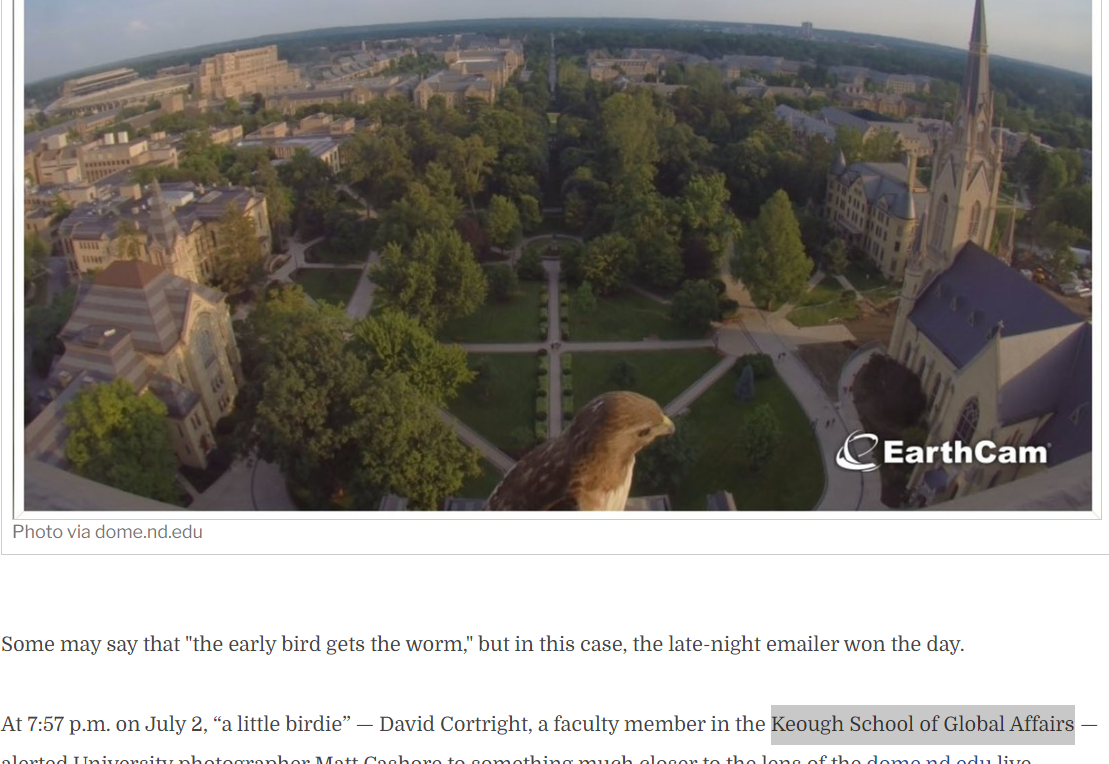


From this information, we can answer question 9, as shown below:



## WebCam.png

Uploading the image on google image search, we find that this image is for Keough School of Global Affairs



Doing a google search on the name of this university, we find that it is located in Indiana, United States. Which makes us answer the last question:

