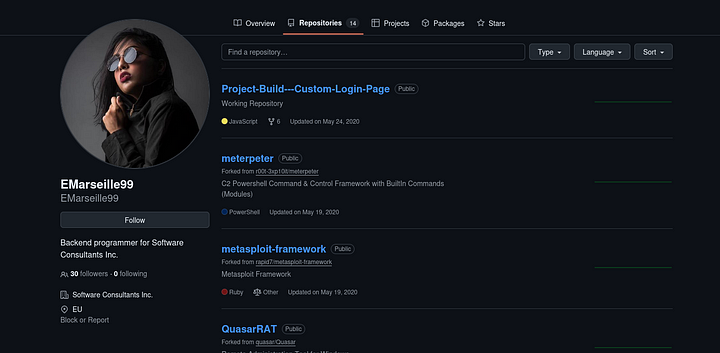
### **Lespion Lab — CyberDefenders**

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

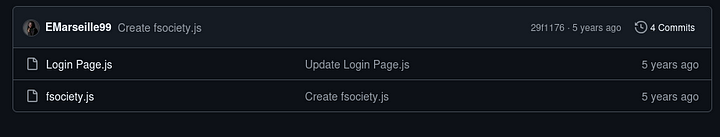
Incident responders and digital forensic investigators are currently on the scene and have conducted a preliminary investigation. Their findings show that the attack originated from a single user account, probably, an insider. Investigate the incident, find the insider, and uncover the attack actions.

#### **TASKS**

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

****

As we can see above, there are 14 repositories in the GitHub account. The first repository Project-Build — -Custom-Login-Page has two JavaScript files.



These are interesting as, usually, the front end JavaScript files will contain user authentication, calls to external services and more.

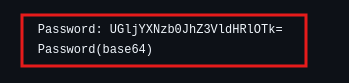


As we can see above, the Login Page.js has the API key.

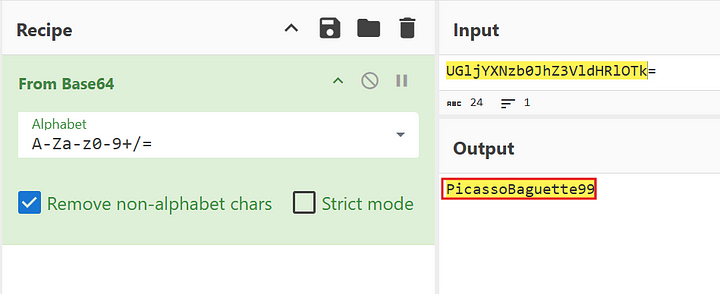
**Answer:** aJFRaLHjMXvYZgLPwiJkroYLGRkNBW

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

The same Login Page.js file has the password.



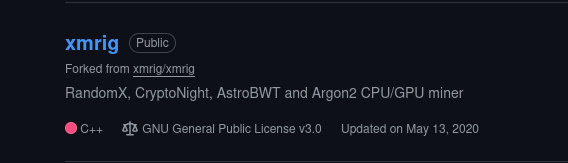
As we can see above, the password is stored in base64 encoding. We can decode this to get the password.



**Answer:** PicassoBaguette99

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

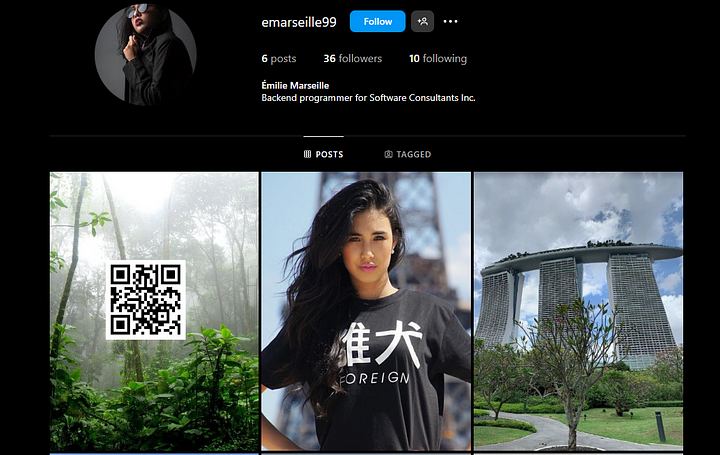
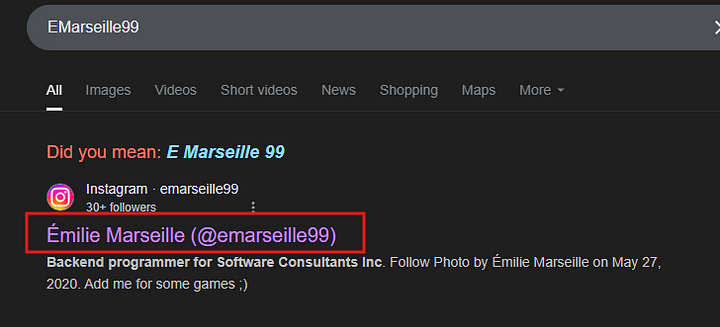
In the list of the repositories, we can find a repository named xmrig. In the description to this repository it is mentioned that it is a **RandomX, CryptoNight, AstroBWT and Argon2 CPU/GPU miner**.



**Answer:** xmrig

**4. On which gaming website did the insider have an account?**

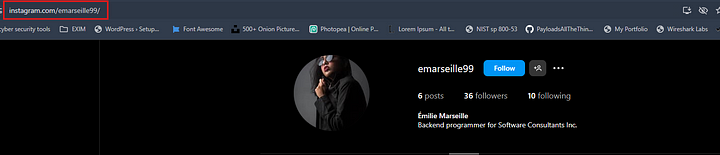
The hint suggests to look at her instagram profile.



As we can see above, there is a QR code in the profile. Scanning this with google lens took to the gaming site.

**Answer:** Steam

**5.What is the link to the insider Instagram profile?**

****

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

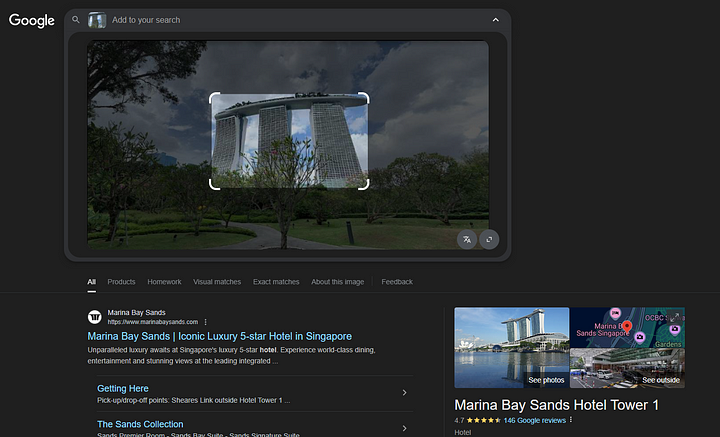
**6. Which country did the insider visit on her holiday?**

The third photo on the Instagram profile has the following caption

“Once in a lifetime holiday here, love me some slings x”



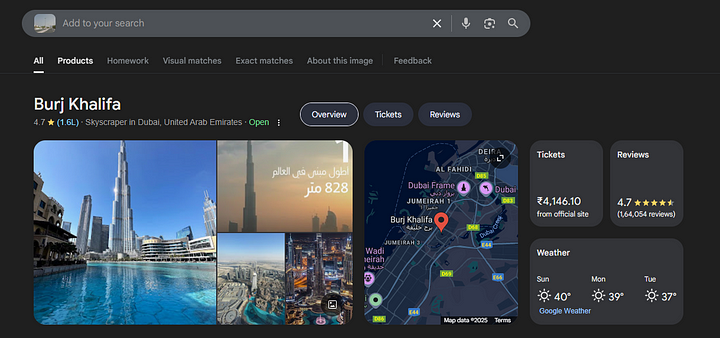
The landmark above is in Singapore. Confirmed by google image search.



**Answer:** Singapore

**7. Which city does the insider family live in?**

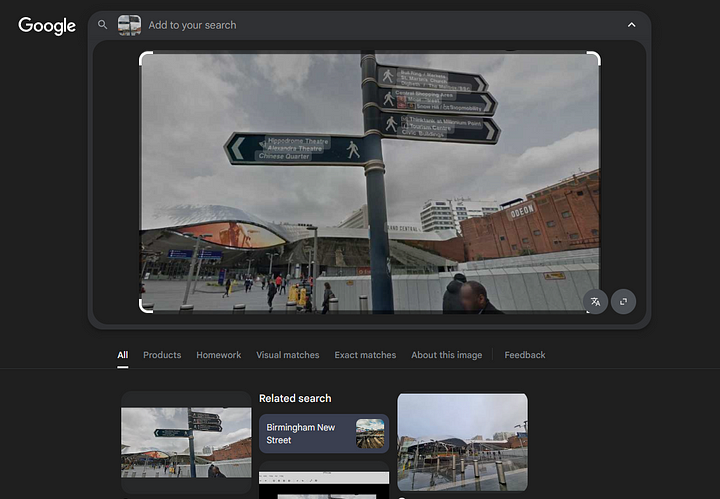
One of the images in the profile had Burj Khalifa in it.



**Answer:** Dubai

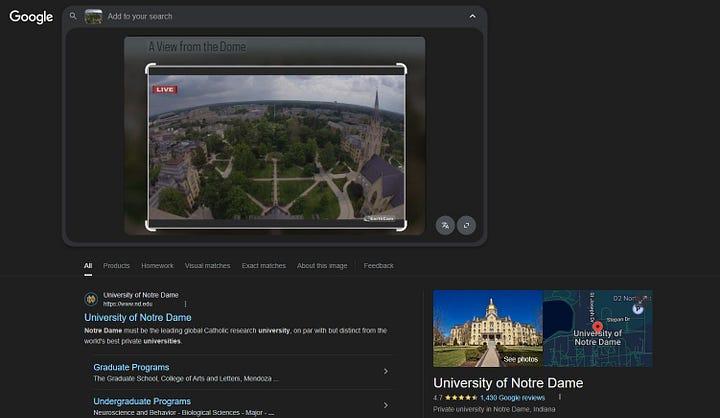
**8. File -> office.jpg: You have been provided with a picture of the building in which the company has an office. Which city is the company located in?**

Google Image search to the rescue again.



**Answer:** Birmingham

**9. 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?**

****

**Answer:** Indiana