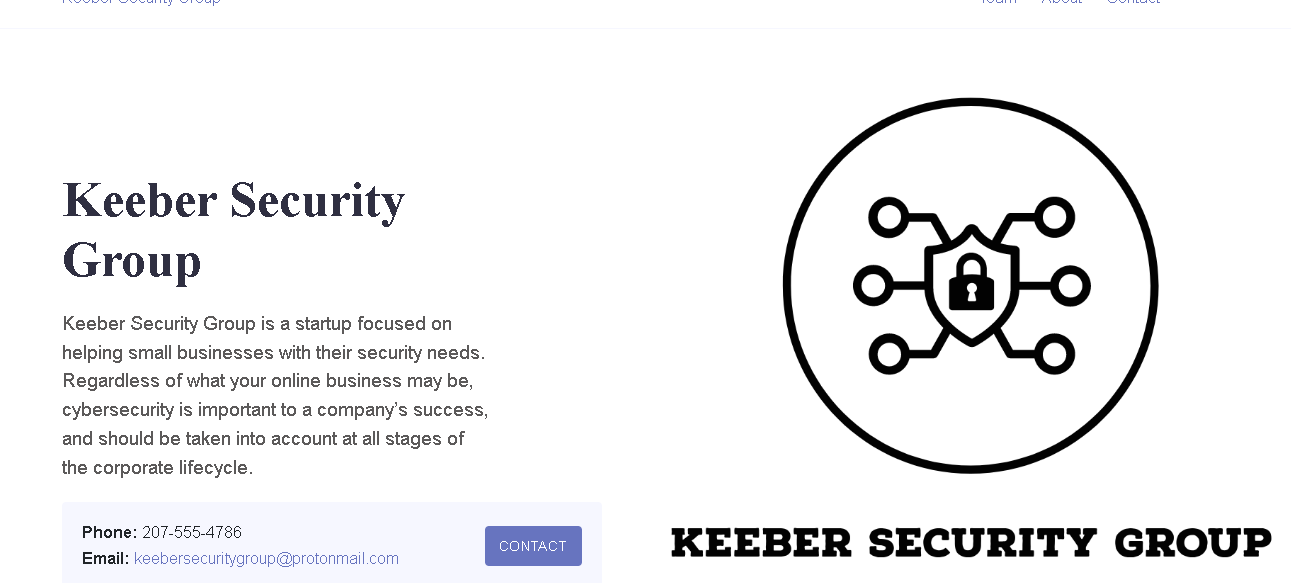
**Name hasnain muavia**

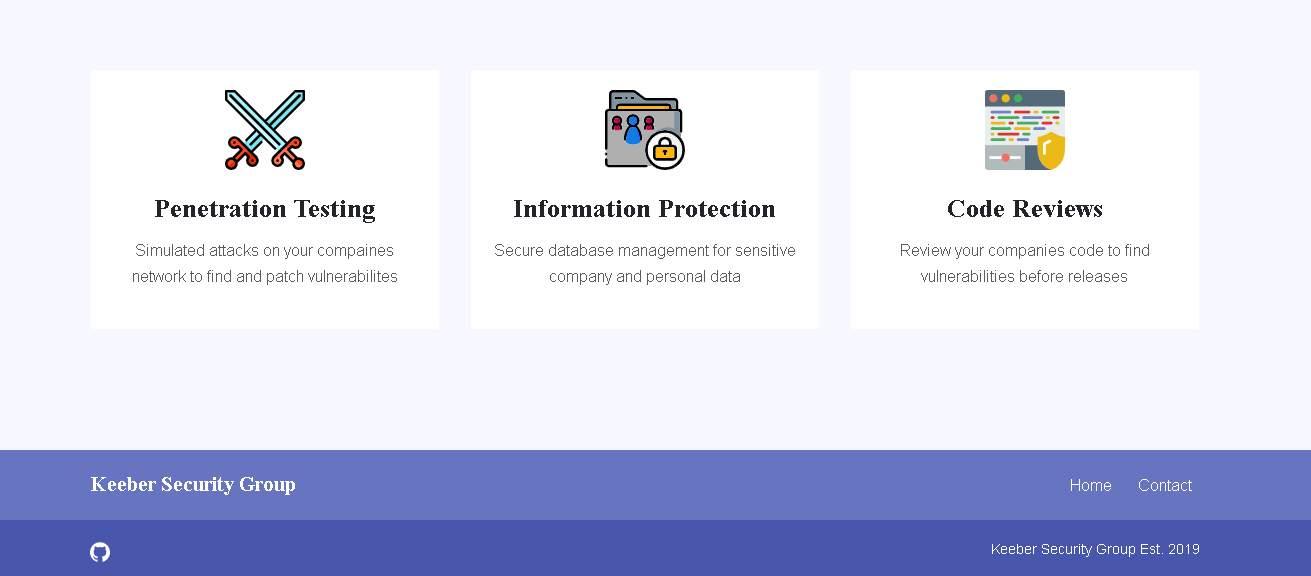
**Email hk3116320@gmail.com**

**TASK 1: You have been applying for entry-level cybersecurity jobs. You got an interview with the Keeber Security Group. They want to test your skills through a series of challenges oriented around investigating the Keeber Security Group. The first step in your investigation is to find more information about the company itself. All we know is that the company is named Keeber Security Group and they are a cybersecurity startup. To start, help us find the person who registered their domain.**

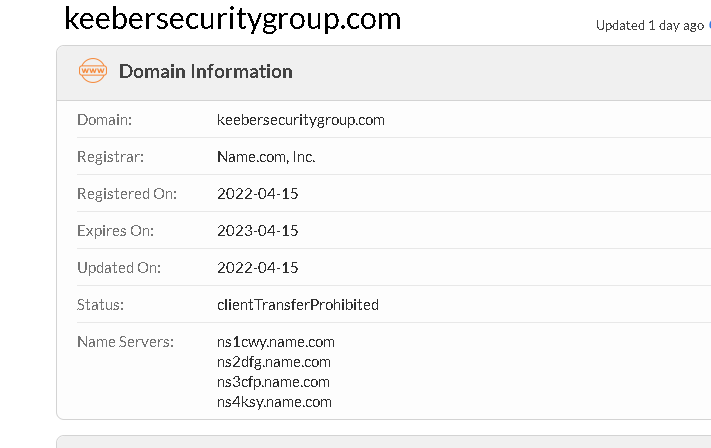
**Answer:**

**A simple google search for: Keeber Security Group gets us to the company’s website: keebersecuritygroup.com**

****

****

**To identify who registered the site, I used the whois lookup website which retrieves various metadata about a given domain.**

****

****

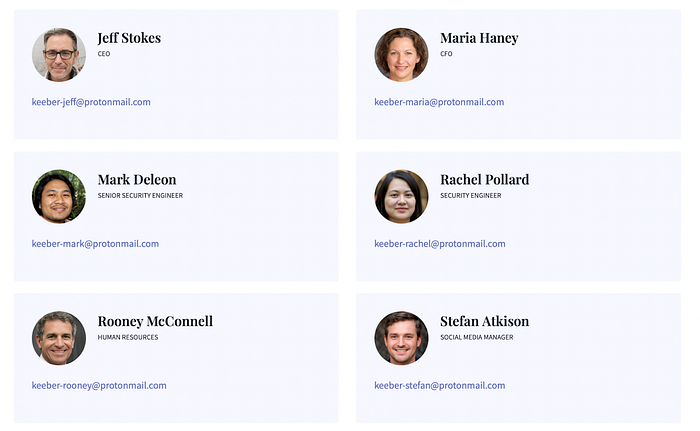
**By running: whois keebersecuritygroup.com, we get the flag:**

**flag{ef67b2243b195eba43c7dc797b75d75b}**

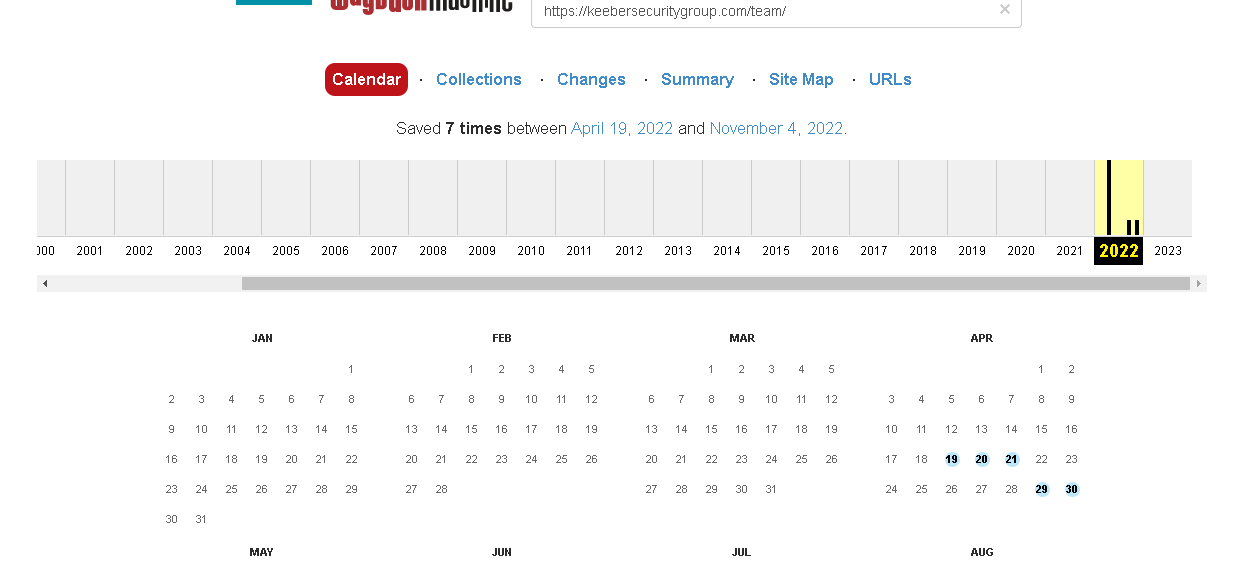
**TASK 2:   The Keeber Security Group is a new startup in its infant stages. The team is always changing and some people have left the company. The Keeber Security Group has been quick with changing its website to reflect these changes, but there must be some way to find ex-employees. Find an ex-employee through the website.**

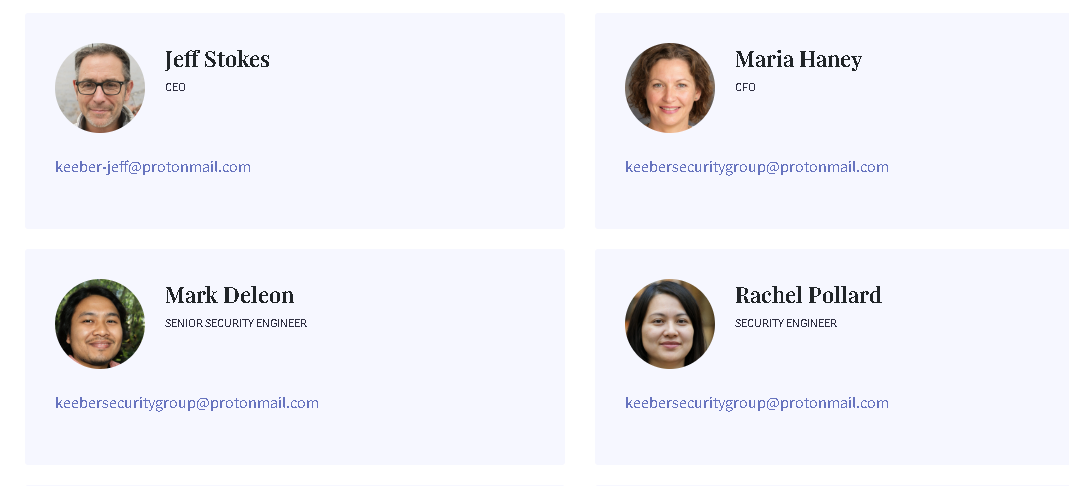
**Answer:**

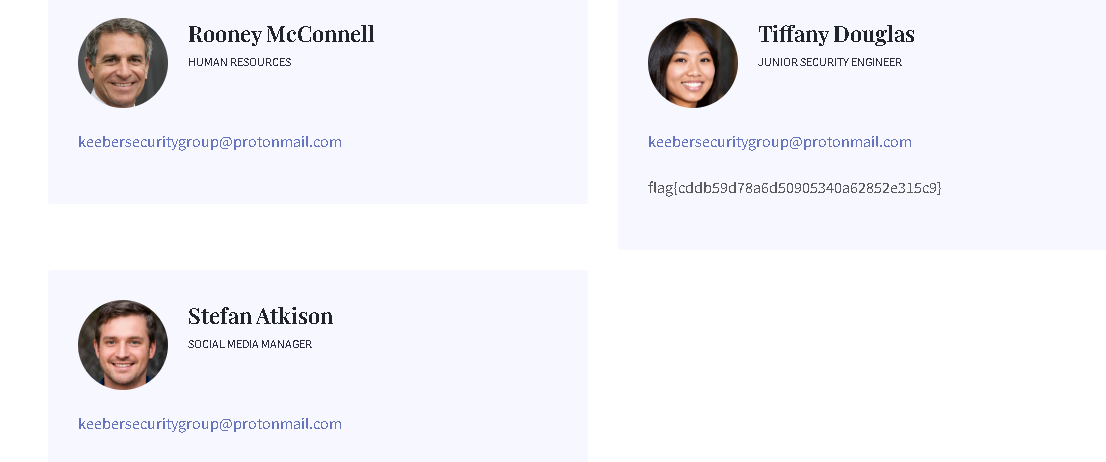
**Browsing to the Team section on the Keeber Security Group company website reveals 6 employees:**

****

**If you need to access information about an ex-employee on the Keeber Security Group website, you can use the Wayback Machine, which is an online archive of web pages. By searching for the team page, you can access previous versions of the website and find the desired information. To begin, you can check the oldest archived version available, which is from April 19th. From there, you can scroll down the page and locate the details about the ex-employee, Tiffany Douglas, and retrieve any necessary information. By utilizing this method, you can access valuable information that may no longer be available on the current version of the website.**

****

****

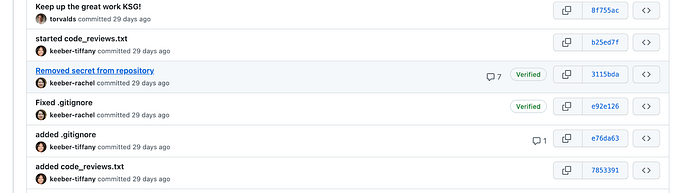
****

**flag{cddb59d78a6d50905340a62852e315c9}**

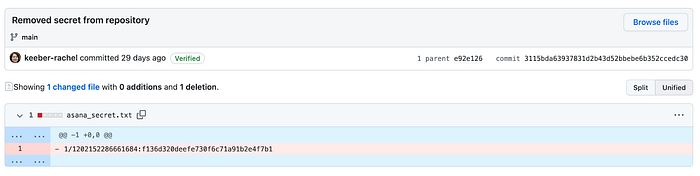
**TASK 3:  The ex-employee you found was fired for “committing a secret to public GitHub repositories”. Find the committed secret, and use that to find confidential company information. Also, find more information regarding the secret file.**

**Answer:**

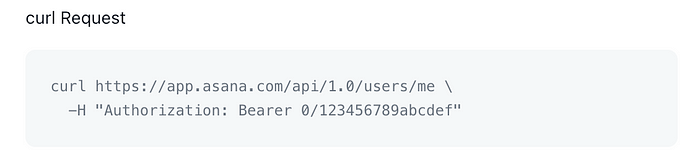
**The Keeber Security Group website contained a link to their Github account. By examining the commit history for the security-evaluation-workflow repository, we can see a suspicious commit message stating “Removed Secret from repository”**

****

**By clicking on the above-mentioned commit and looking at the diff we can see the actual secret in a file called asana\_secret.txt.**

****

**Upon initial inspection, the given information appeared to be limited. Therefore, I conducted an online search to gather more information about Asana and the potential usage of the provided string. After thorough research of the Asana documentation, I discovered a useful text box that explained how Curl could be utilized to access the Asana API.**

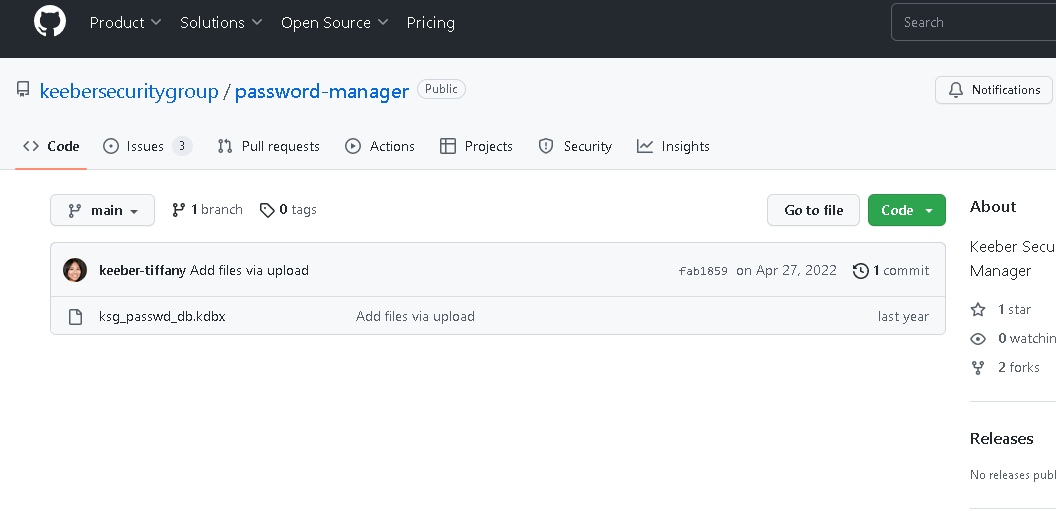
****

**As can be seen, the last parameter in the curl command resembles the secret we have identified in Git. This must be the API token**.

**TASK 4: The ex-employee also left the company password database exposed to the public through GitHub. Since the password is shared throughout the company, it must be easy for employees to remember. Find and open the password database and extract the flag. The password of the file is: craccurrelss**

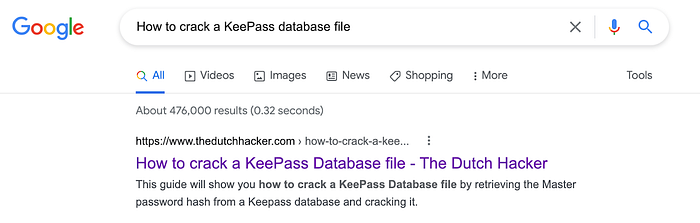
**Answer:**

**first, we need to find the password database. We return to the company Github page and specifically examine the**[**password-manager**](https://github.com/keebersecuritygroup/password-manager)**repository to find the desired database file:**

****

**Answer:**

**If you come across a .kdbx file and are unfamiliar with its meaning, a quick Google search will inform you that it is typically associated with data files created by the KeePass Password Safe application. However, if you need to crack this file, you may require additional guidance. A thorough search engine query led to an excellent guide that provides a comprehensive walkthrough on how to crack .kdbx files using popular tools like John the Ripper or Hashcat. Following this guide can offer valuable insight and assistance to those who may be unfamiliar with this process.**

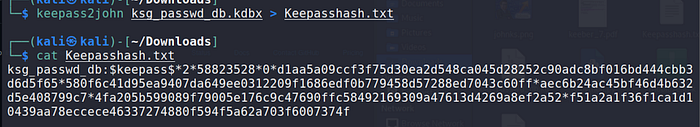
****

**According to the guide (and the challenge description), there are 3 stages we need to go through to crack the database file:**

1. **Extract the password hash from the database file**
2. **Generate a custom wordlist**
3. **Use john-the-ripper to crack the password hash using the generated wordlist**

**To extract the hash, we run the following command:**

**keepass2john ksg\_passwd\_db.kdbx > Keepasshash.txt**

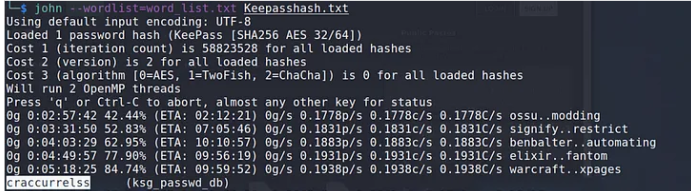
****

**Now that we have the password hash, in order to generate the wordlist, we will use**[**Custom Word List generator**](https://digi.ninja/projects/cewl.php)**(Cewl) and provide it with the company’s Github page:**

**cewl** [**https://github.com/keebersecuritygroup/security-evaluation-workflow**](https://github.com/keebersecuritygroup/security-evaluation-workflow) **-w word\_list.txt — lowercase -d 1**

**Lastly, we will run john-the-ripper using the generated wordlist in order to crack the password hash:**

**All that is left is to wait patiently for the results and we get our password:**

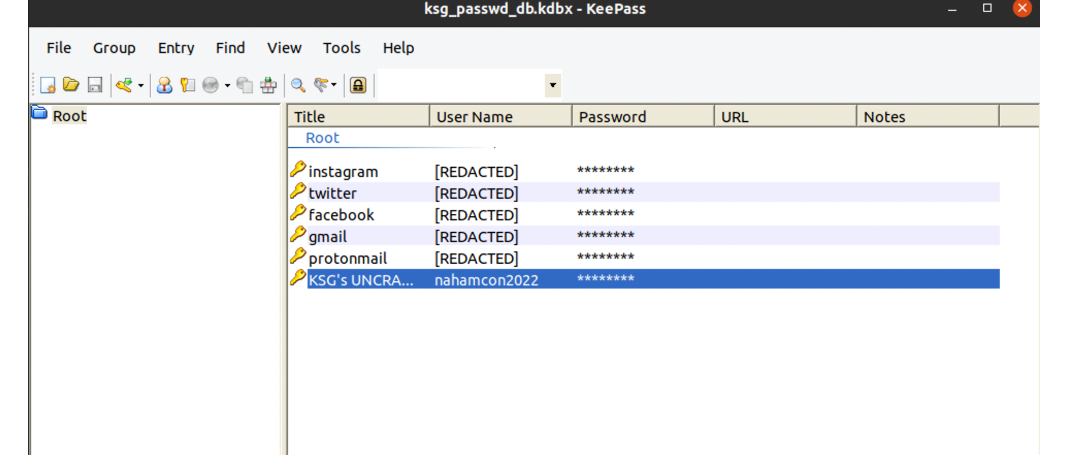
****

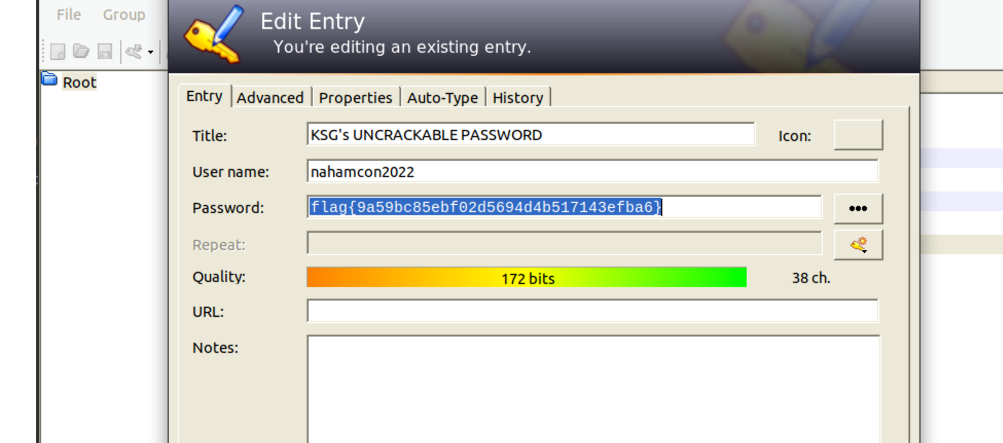
* **I found the password database when solving Keeber 2, in the password-manager**

**If you come across a .kdbx file and are unfamiliar with its meaning, a quick Google search will inform you that it is typically associated with data files created by the KeePass Password Safe application**

* **On further searching, I found that this is a password database file for an application called KeePass, an open source password manager. To get the flag, we're required to get the password to this database file.**

**Before opening the password file, ensure that you have KeePass installed on your system. Then open the file, and enter the password**

****

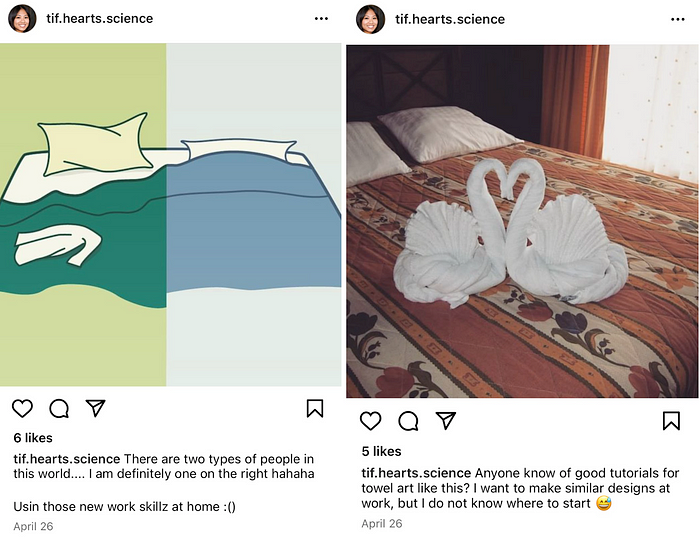
****

**TASK 5: After all of the damage the ex-employees mistakes caused to the company, the Keeber Security Group is suing them for negligence! In order to file a proper lawsuit, we need to know where they are so someone can go and serve them. Can you find the ex-employee's new workplace? Her Instagram profile is:**[**https://www.instagram.com/tif.hearts.science/**](https://www.instagram.com/tif.hearts.science/)**What is the name of her new work which is in the Maine area?**

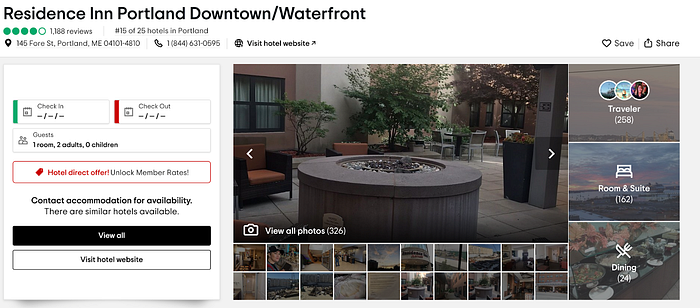
**Answer:**

**Her Instagram account only contains 6 posts,**

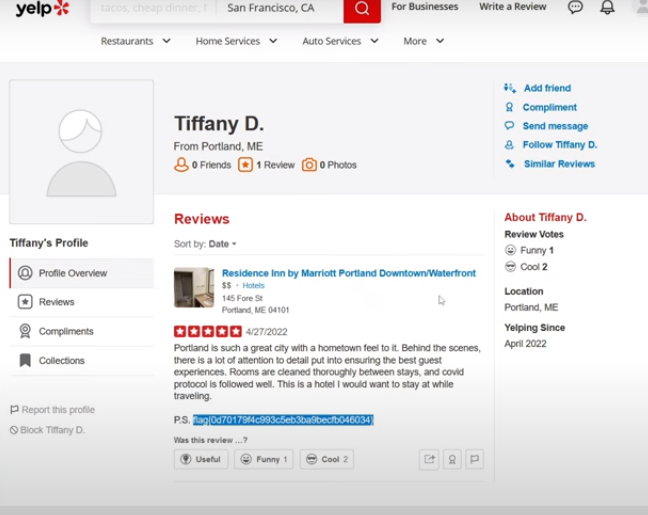
**For example:**

****

**I went over to TripAdvisor and started going over hotels in the Maine Area that have an indoor pool, until I came across Residence Inn or more specifically, these images:**

****

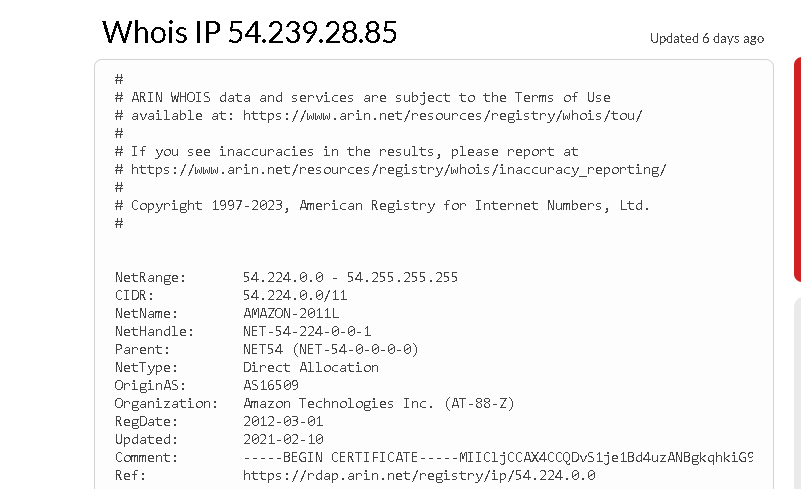


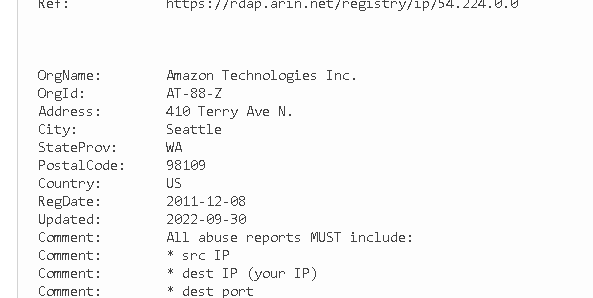
****

**The name of her new work is Portland which is in the maine area .**

**TASK 6: Which company does this IP belong 54.239.28.85?**

**Answer:**

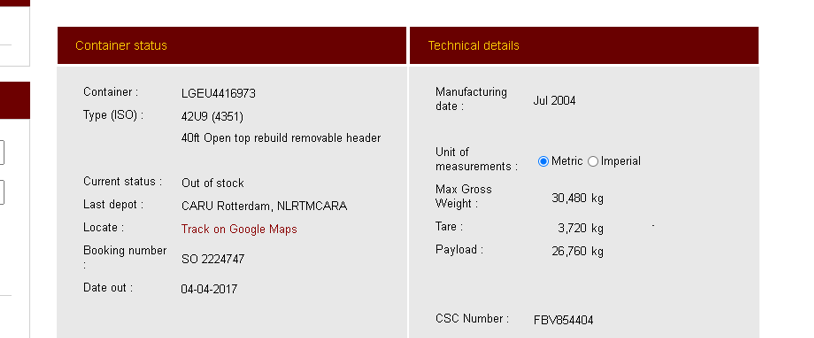
****

****

**Company is amazon technologies inc.**

**TASK 7:  What is the manufacturing date of this container? (Month and year only)**

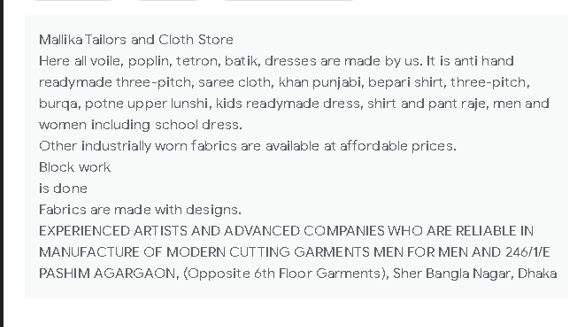
**Answer:**

****

**Manufacturing date of the container is jul 2004.**

**TASK 8: In which country this image is most likely taken?**

**Answer:**

****

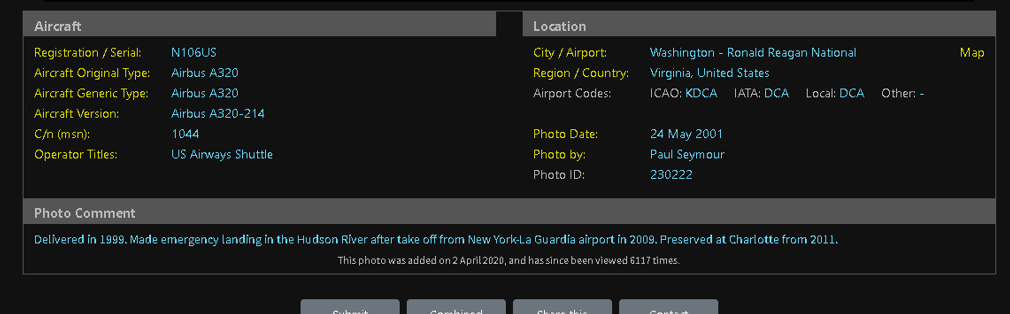
**This image is taken in sher bangla nagar , dhaka**

**TASK 9: In which country is this vehicle registered?** **Answer:**

**The Dacia Dokker is a**[**panel van**](https://en.wikipedia.org/wiki/Panel_van)**and**[**leisure activity vehicle**](https://en.wikipedia.org/wiki/Leisure_activity_vehicle)**(LAV) built at the**[**Renault**](https://en.wikipedia.org/wiki/Renault)**factory in**[**Tangier**](https://en.wikipedia.org/wiki/Tangier)**, Morocco.**

**TASK 10: Where did this plane land last as seen in the picture? Name of place?**

 **Answer:**

****

**Delivered in 1999, made an emergency landing in the Hudson river after take off from new york la gurdia airport in 2009.**