STUDENT NAME: MUHAMMAD ANSAR RAZA

INSTRUCTOR NAME: SHAHZAIB ALI KHAN

PROJECT TITLE: OPEN SOURCE INTELLIGENCE (OSINT)

BATCH: COHORT-06

COURSE NAME: CYBER SECURITY

INSTITUTE OF EMERGING CAREERS IEC

Introduction to OSINT

A modern security professionals job is becoming more and more complex. In order to gain the information your security strategy must include a diverse, both predictive and reactive approach.

A major source of intelligence that cannot be overlooked is the vast amount of publicly available information (PAI) being produced by consumers, hackers, newsmakers, and bloggers every single day. Globally almost every person and organization is communicating across multiple platforms and networks, as well as handling personal and corporate needs virtually such as shopping, travel planning, and data management.

Finding like-minded communities and audiences online is the goal, wherever you have people congregating, especially if there is potential for monetary gain, the risk of nefarious behavior rises. This has created an increased need for open-source intelligence (OSINT) and OSINT platforms.

What is OSINT?

Open-source intelligence or OSINT refers to the process of gathering information from public, legal data sources to serve a specific function. Some open sources might include social media, blogs, news, and the dark web.

The concept of OSINT very basically works like this:

Public information exists → data is gathered → information is analyzed for intelligence.

It is a method of gathering information from the public or other open sources which can be used by security experts, national intelligence agencies or cyber criminals.

When used by cyber defenders the goal is to discover publicly available information related to their organization that could be used by attackers and take steps to prevent those future attacks.
Collecting data from public available resources. Like Yahoo, Google, Public databases etc.

If you have target email, domain, person and everything use OSINT.

OSINT in which reconnaissance is the first step in most of the cyber security things you do red teaming, penetration testing and find targets person, domain, IP or blue teaming whos attacking your system, researching phishing email.

It is like a puzzle you don’t know whats the picture is?

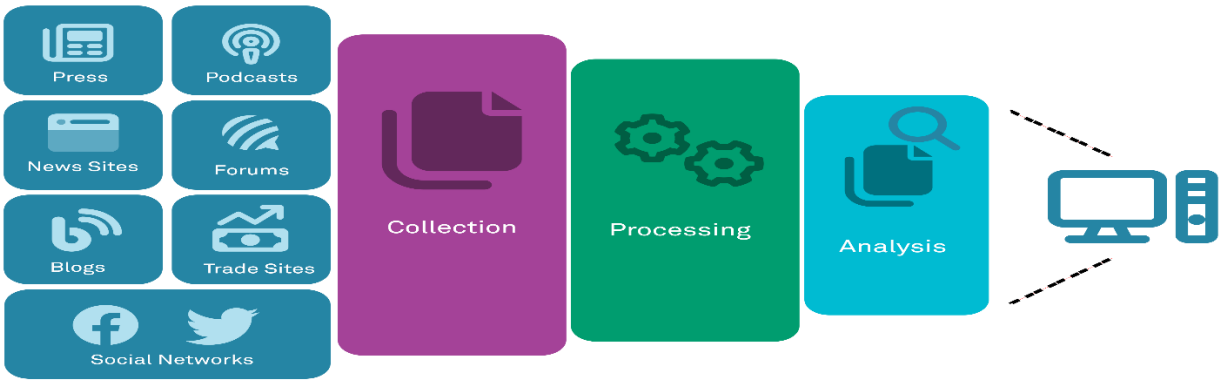
You got all of those data points together.

Assemble them.

Analyze them.

Now you can see the picture.

Analysis the things using twitter, read blogs learn something new in a short amount of time.



History of OSINT

The term OSINT was originally used by the military and intelligence community to denote intelligence activities that gather strategically important, publicly available information on national security issues.

In the cold war espionage focused on obtaining information via human sources or electronic signals and in the 1980s, OSINT gained prominence as an additional method of gathering intelligence.

The advent of the Internet, social media, digital services and open source intelligence grants access to numerous resources to gather intelligence about every aspect of an organization IT infrastructure and employees.

Security organizations are realizing that they must collect this publicly available information to stay one step ahead of attackers.

A CISOs primary goal is to find information that could pose a risk to the organization. This allows CISOs to reduce risk before an attacker exploits a threat.

OSINT should be used in combination with regular penetration testing in which information discovered via OSINT is used to simulate a breach of organizational systems.

OSINT Gathering Techniques

Three methods are commonly used to gain open intelligence data.

Passive Collection

This is the most commonly used way to gather OSINT intelligence. It involves scraping publicly available websites, retrieving data from open APIs such as the Twitter API or pulling data from deep web information sources.

Semi Passive Collection

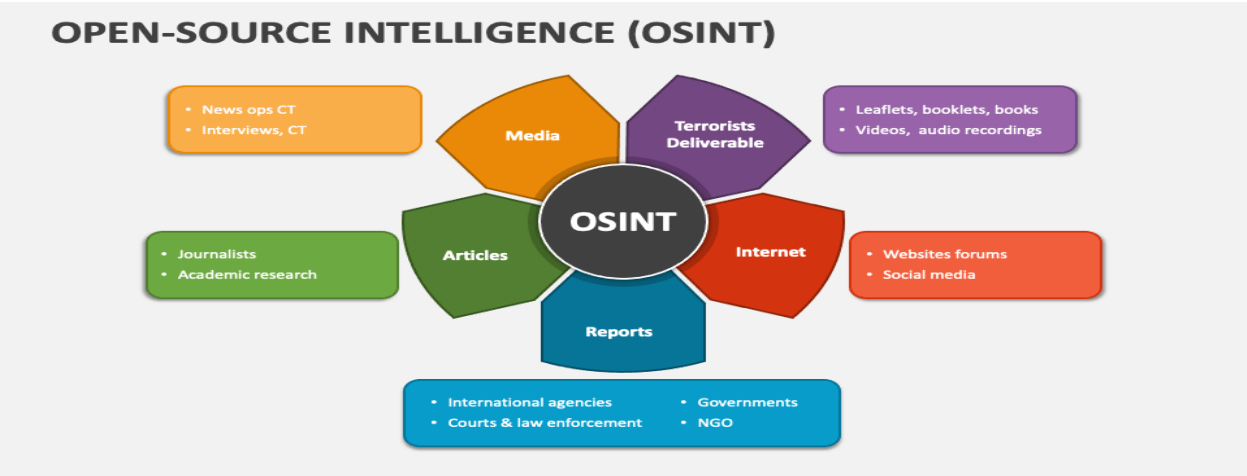
This type of collection requires more expertise. It directs traffic to a target server to obtain information about the server. Scanner traffic must be similar to normal Internet traffic to avoid detection.

Active Collection

This type of information collection interacts directly with a system to gather information about it. Active collection systems use advanced technologies to access open ports and scan servers or web applications for vulnerabilities.

This type of data collection can be detected by the target and reveals the reconnaissance process. It leaves a trail in the target firewall, Intrusion Detection System (IDS), or Intrusion Prevention System (IPS).

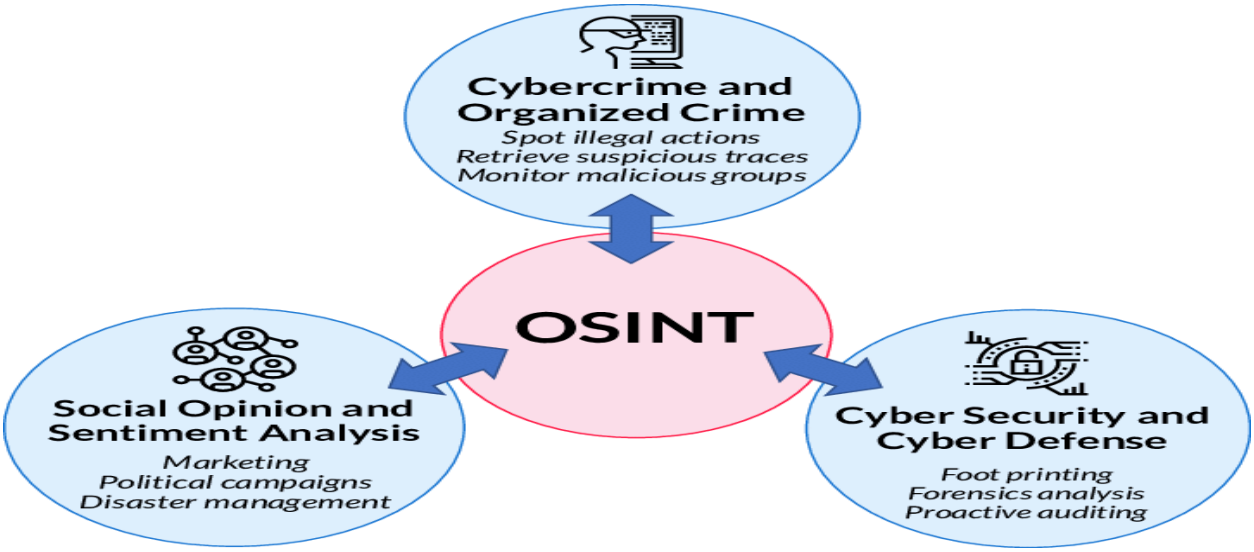
Social engineering attacks on targets are also considered a form of active intelligence gathering.



Artificial Intelligence: The Future of OSINT?

OSINT technology is advancing, and many are proposing the use of artificial intelligence and machine learning (AI/ML) to assist OSINT research.

According to public reports, government agencies and intelligence agencies are already using artificial intelligence to gather and analyze data from social media. Military organizations are using AI/ML to identify and combat terrorism, organized cybercrime, false propaganda and other national security concerns on social media channels.



OSINT Tools

Using OSINT tool for your organization can improve cyber security by helping to discover information about your company, employees, IT assets and other confidential or sensitive data that could be exploited by an attacker. Discover that information first and then hiding or removing it could reduce everything from phishing to DoS attacks.

Some of the tools used for OSINT:

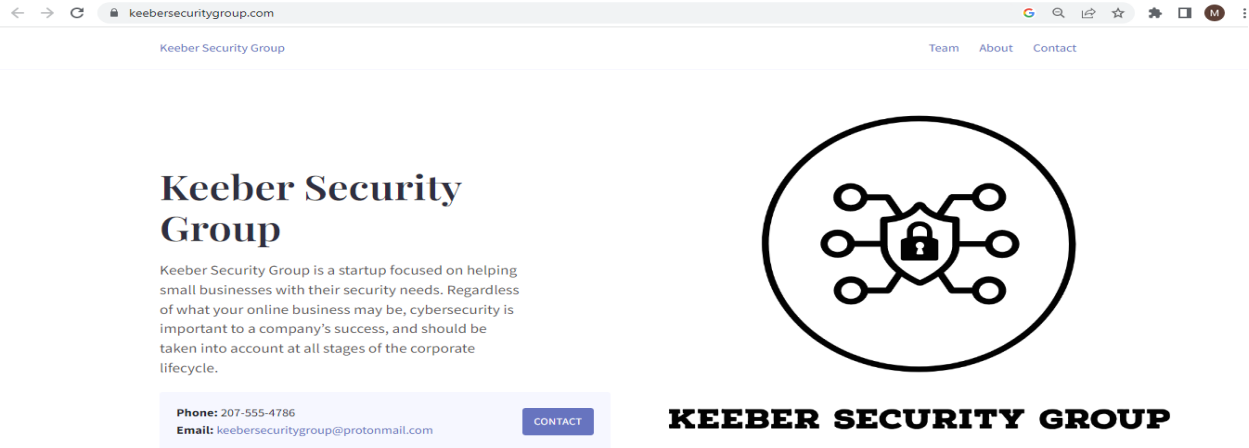
Maltego, Mitaka, SpiderFoot, Spyse, BuiltWith, Intelligence X, DarkSearch.io, Grep.app, TheHarvester, Shodan, Metagoofil, Searchcode, SpiderFoot, Babel X etc.

TASK 01: 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?

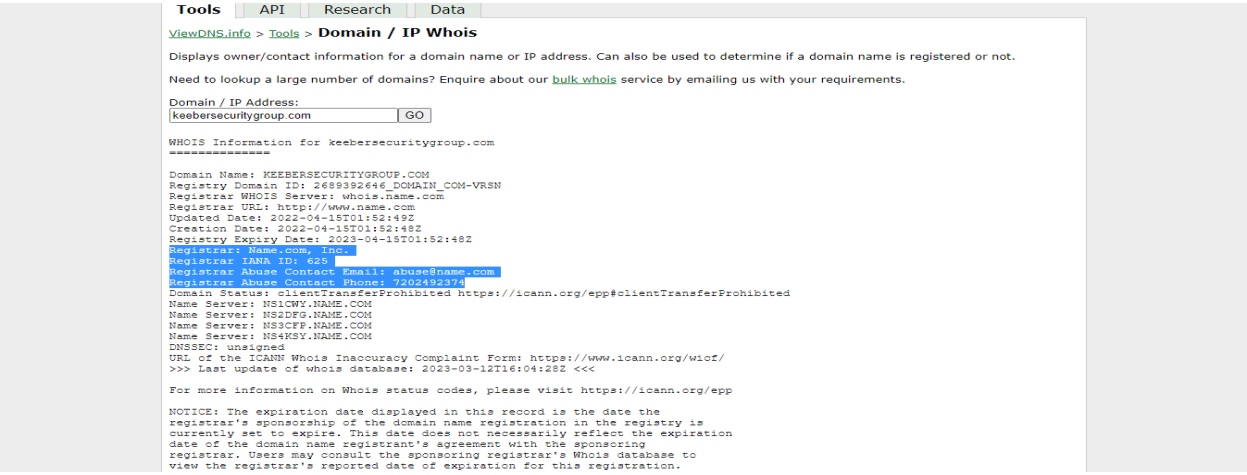
Answer:

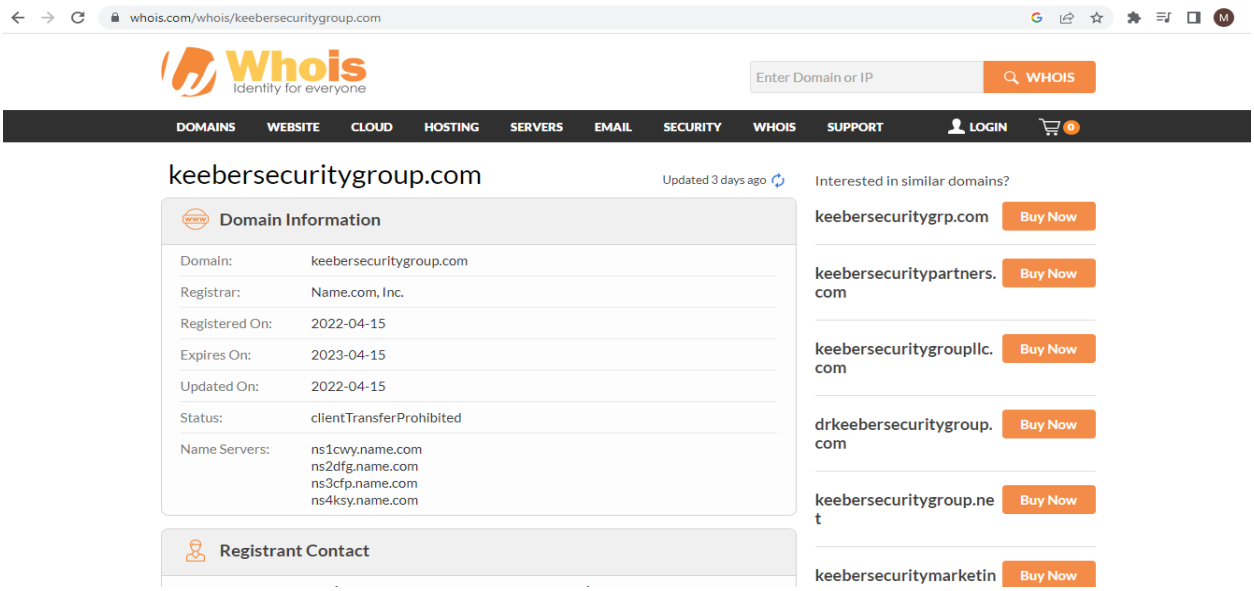
A simple google search for Keeber Security Group.

Website: keebersecuritygroup.com



To identify who registered the site, I used the whois.com or viewDNS.info which retrieves data about a given domain.

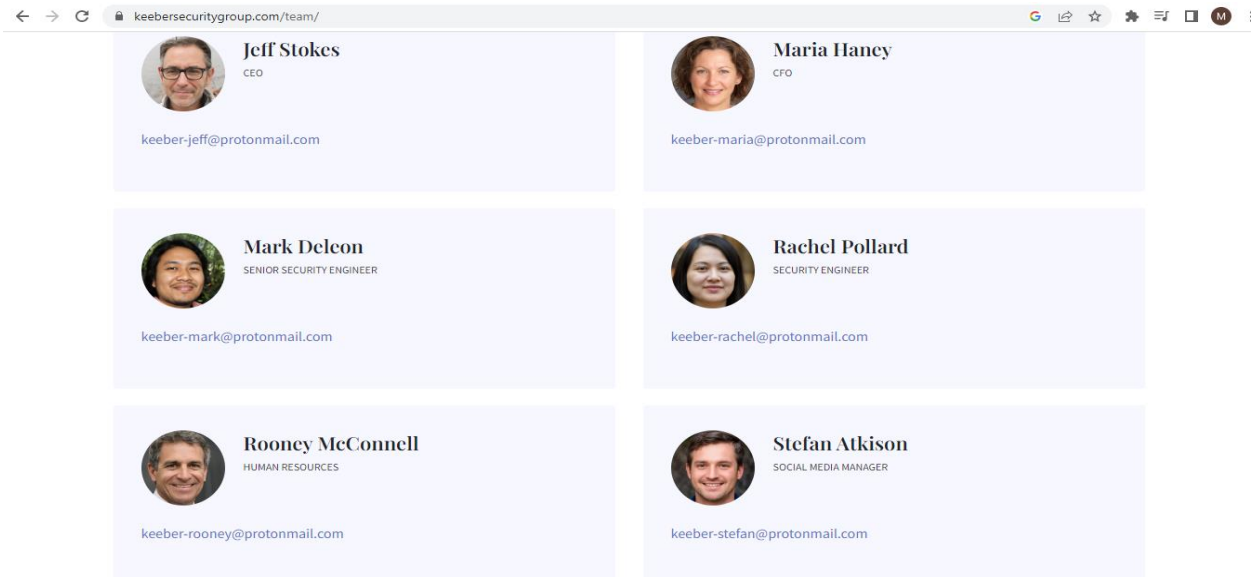




TASK 02: The Keeber Security Group is a new startup in its infant stages. The team is always changing and some people have left the company. The Keeber Security Group has been quick with changing its website to reflect these changes, but there must be some way to find ex-employees. Find an ex-employee through the website?

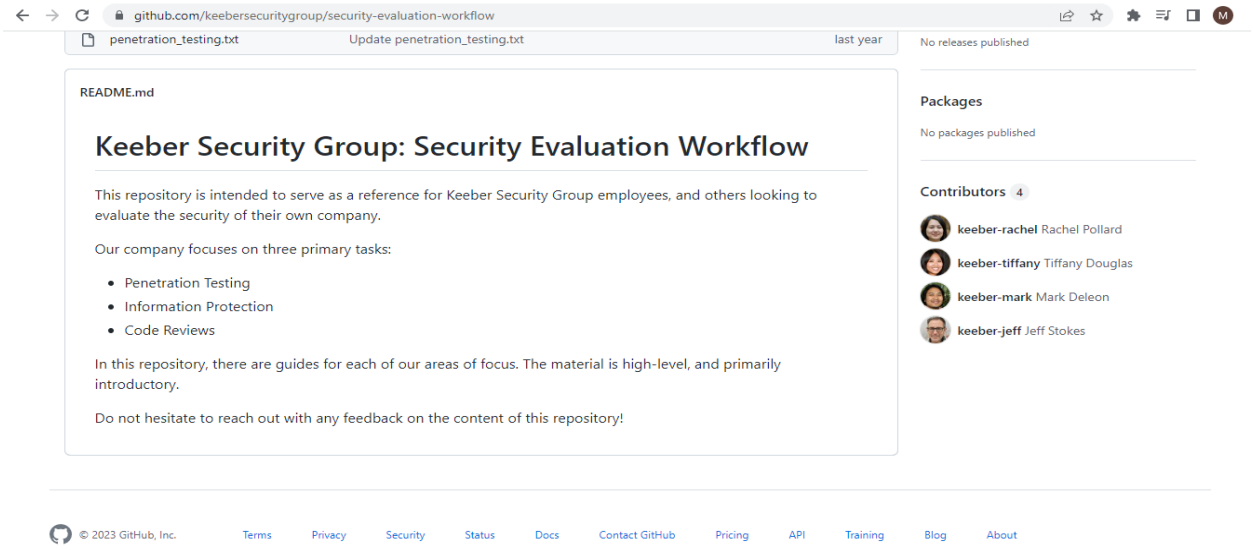
Answer:

Browsing to the team section on the Keeber Security Group company website reveals 6 employees.



Their website also has a link to their GitHub.

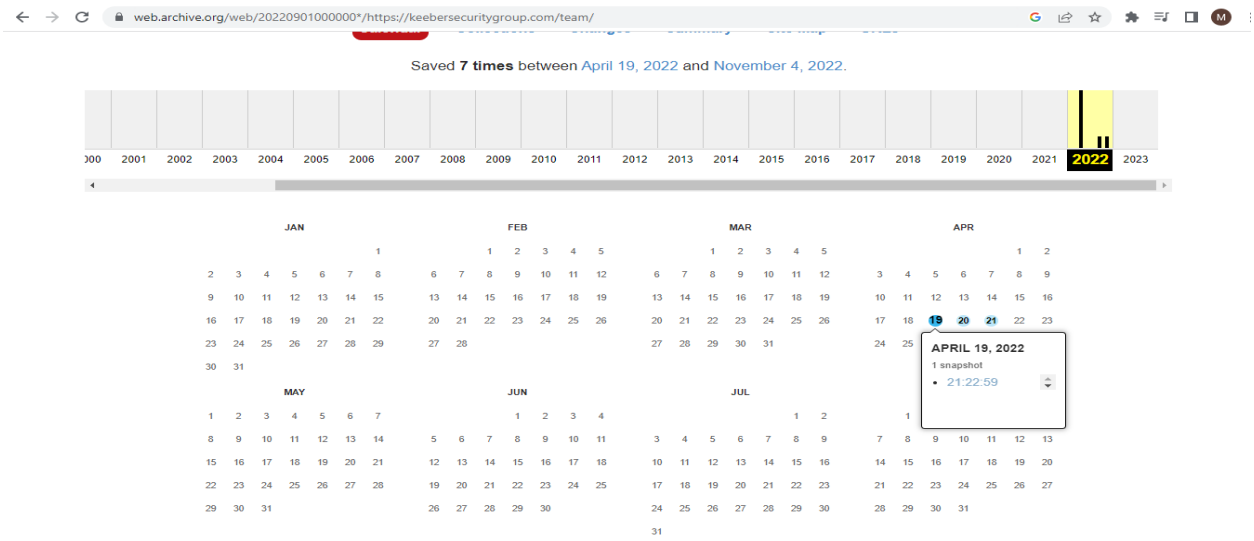
Searching their GitHub repositories did reveal something. In one of their repos, security-evaluation-workflow, the contributors list mentioned a name that was not in the list of employees at the website Tiffany Douglas.



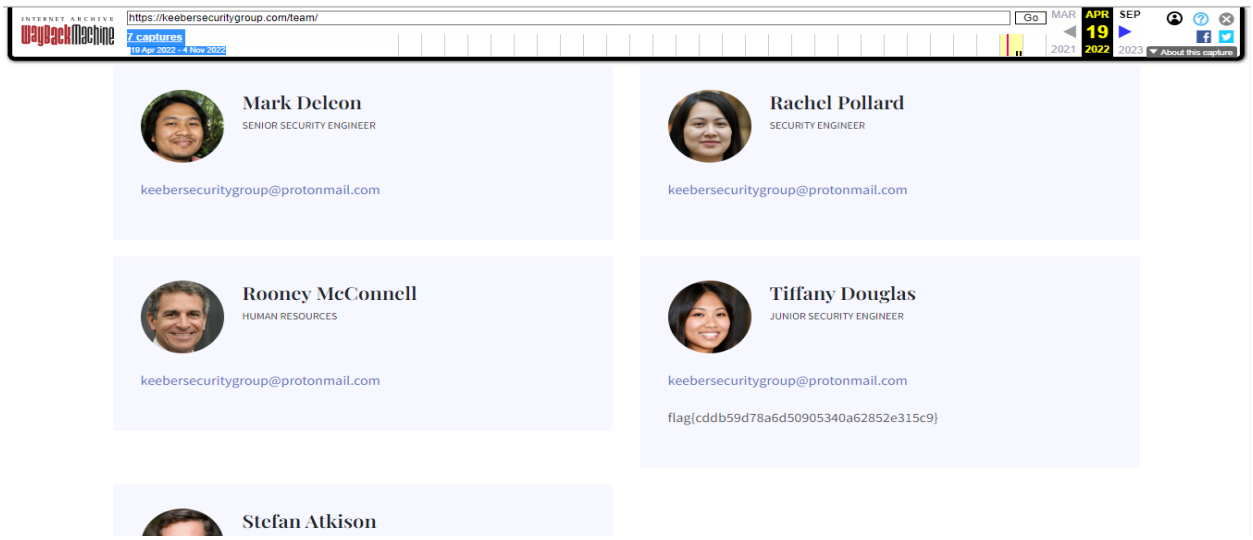
Now we can use the Wayback Machine.

The Wayback Machine is a digital archive of the World Wide Web that stores archived copies of obsolete web pages.

When looking for the team page we see that the oldest copy present is from April 19th:



Archived version of the page and scrolling down will get us the ex-employee Tiffany Douglas.

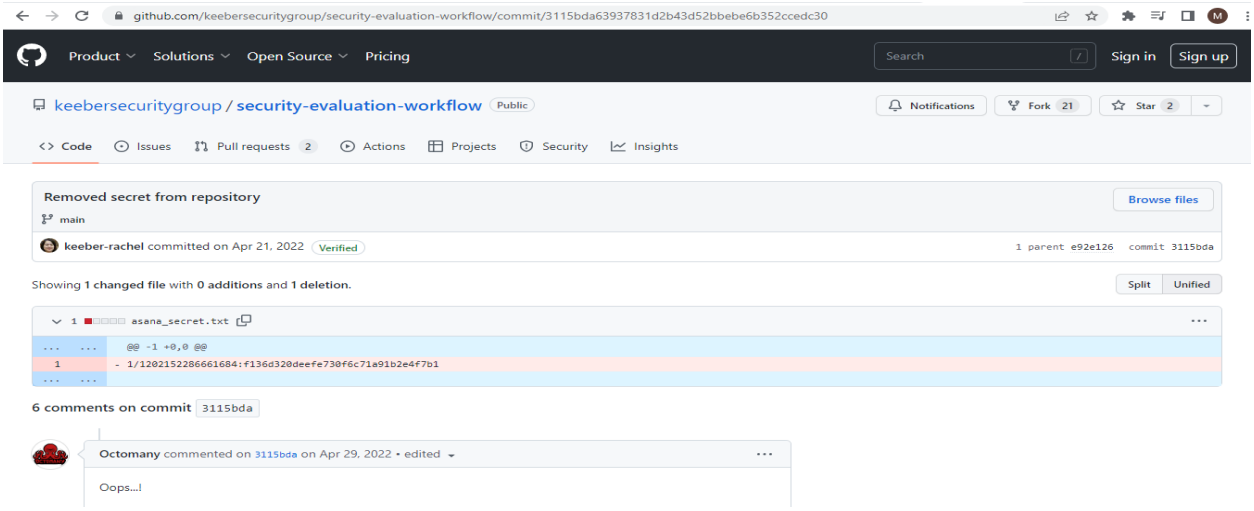


TASK 03: The ex-employee you found was fired for "committing a secret to public GitHub repositories". Find the committed secret, and use that to find confidential company information. Also, find more information regarding the secret file?

Answer:

During searching through GitHub.

In the commits of the security evaluation workflow repo, one commit reads Removed secret from repository.

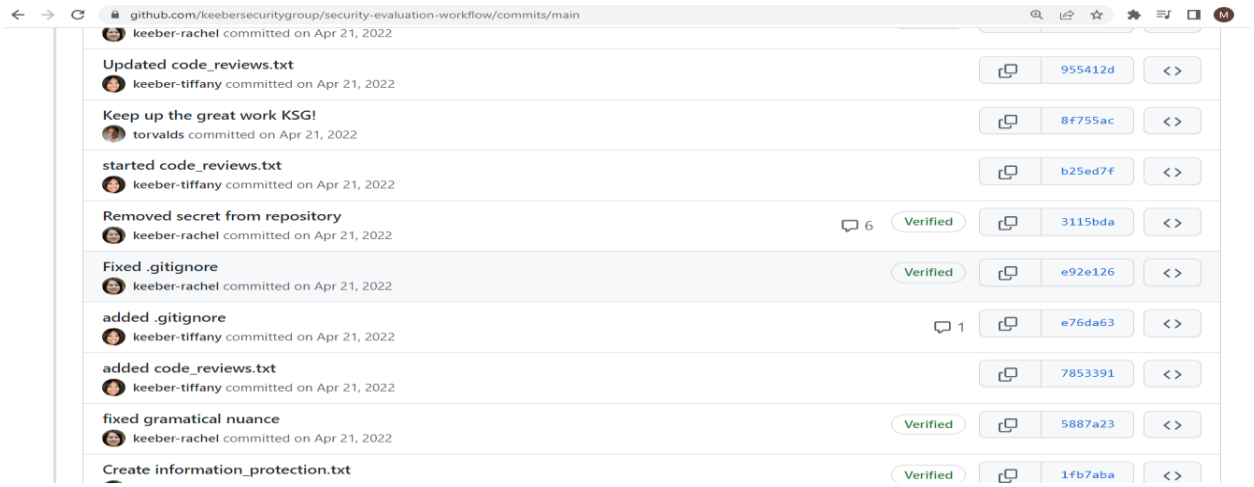


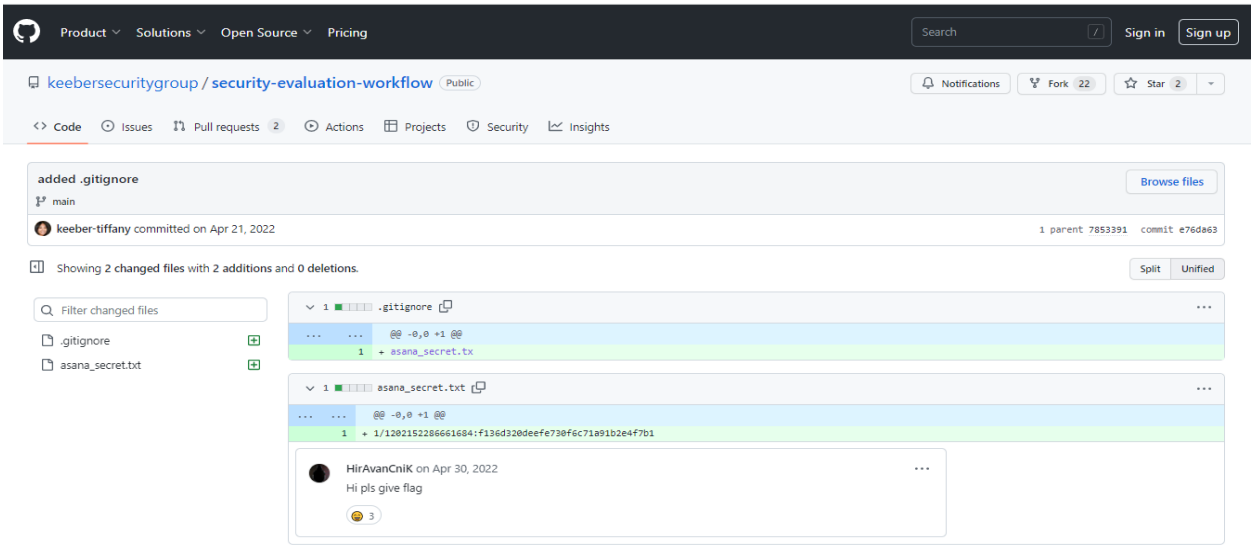
We know file name secret token to Asana.

Asana helps companies track and manage their work.

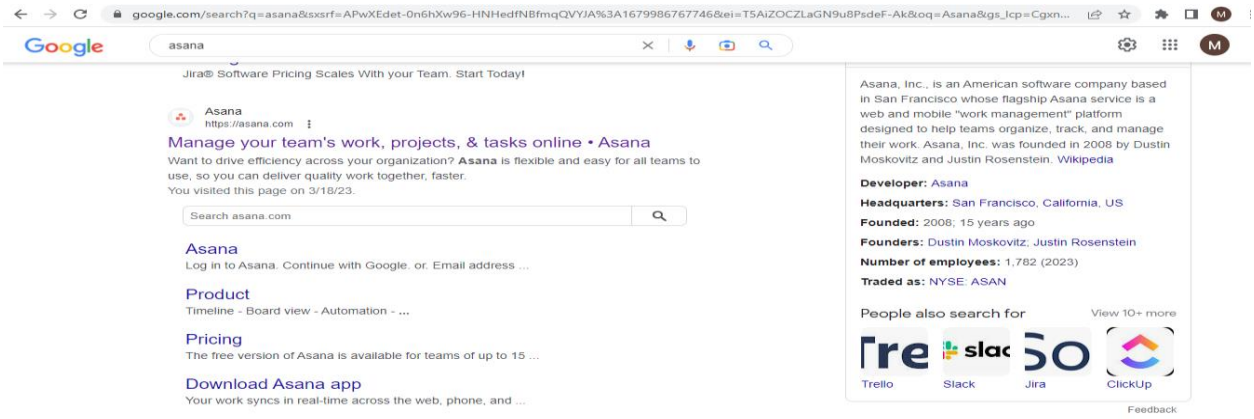
Find the commit in which the secret was added. It is added in just a few commits prior added .gitignore.

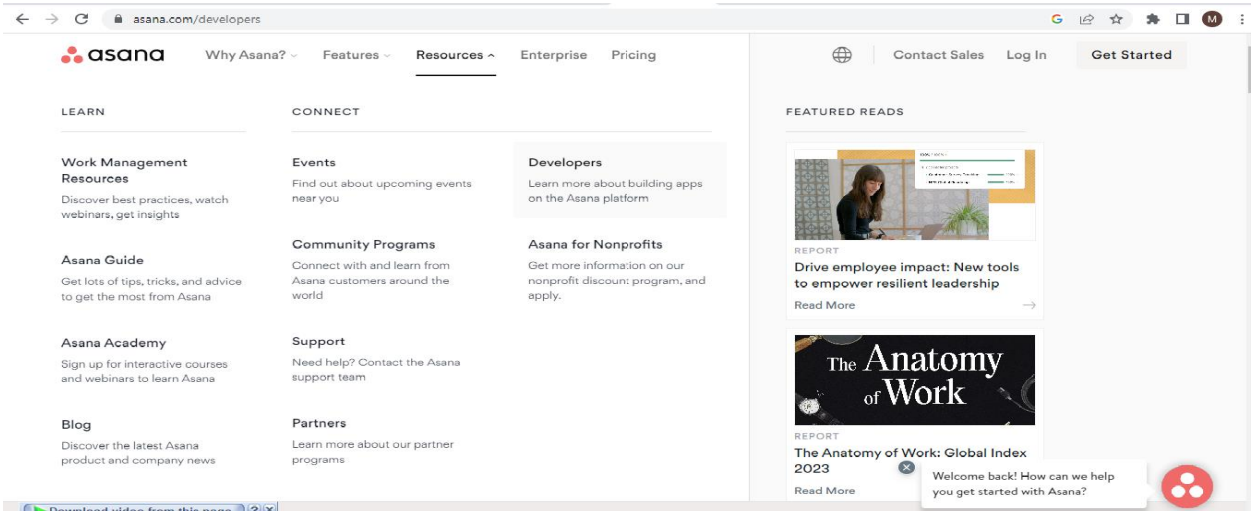
A gitignore file specifies intentionally untracked files that Git should ignore. This includes files that contain confidential information, like passwords and secret keys.

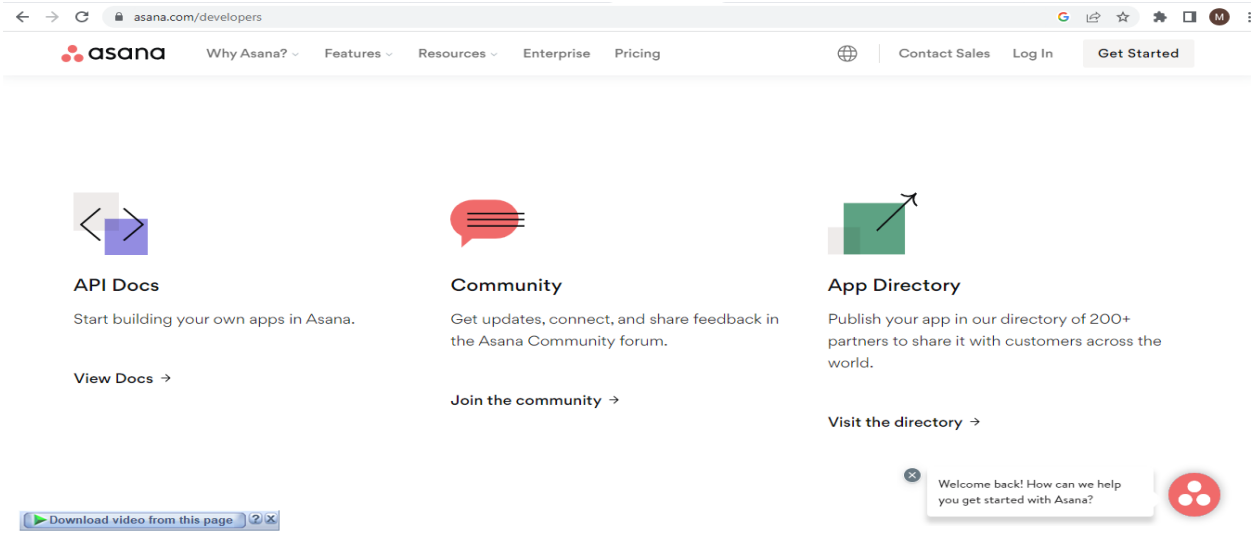


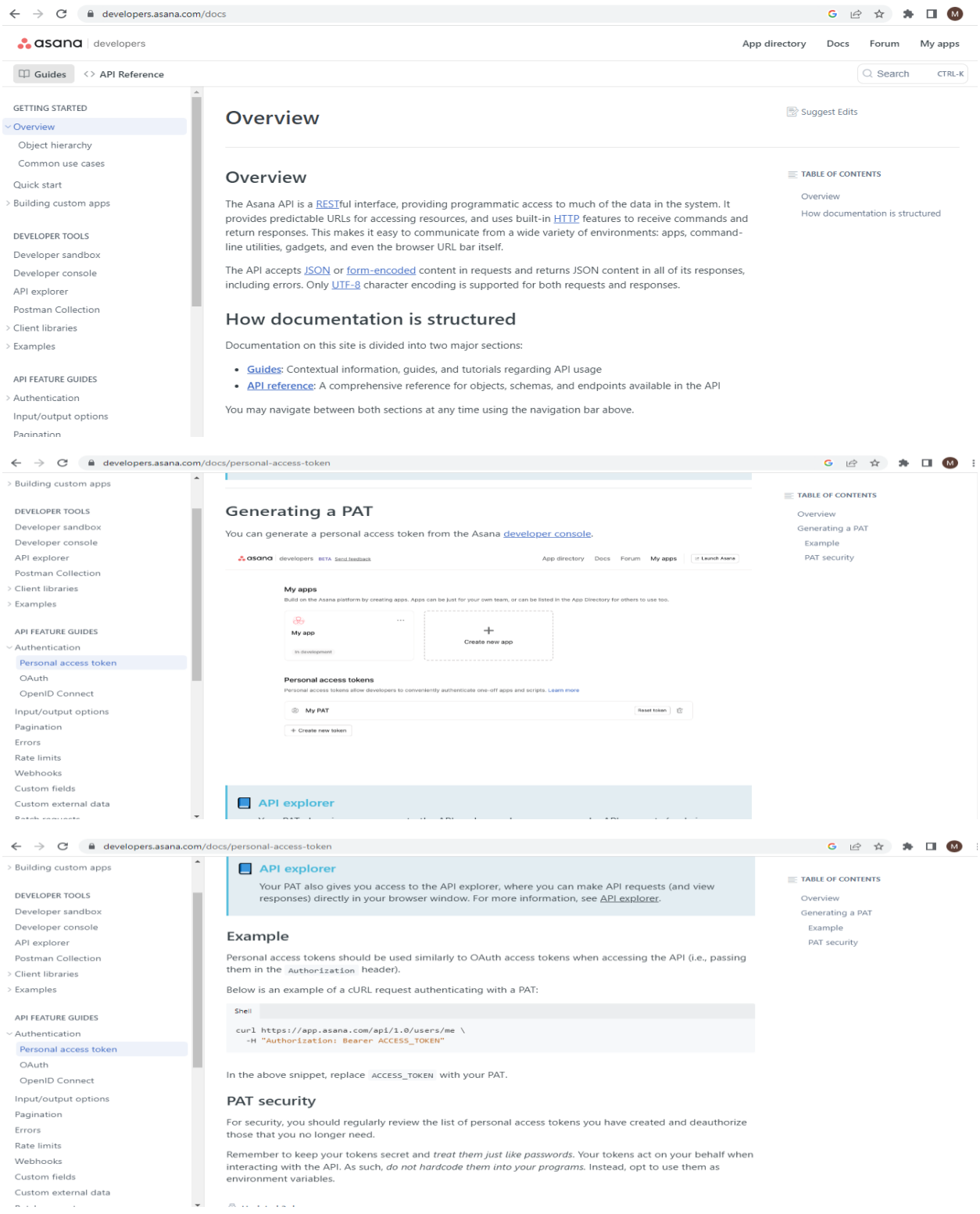


Google to find out what Asana is and how this can be used.


google.com/search?q=asana&sxsrf=APwXEdet-0n6hXw96-HNHedfNBfmqQVYJA%3A1679986767746&ei=T5AiZOCZLaGN9u8PsdeF-Ak&oq=Asana&gs_lcp=Cgxn...
Google
asana
Jira® Software Pricing Scales With your Team. Start Today!
Asana
https://asana.com
Manage your team's work, projects, & tasks online • Asana
Want to drive efficiency across your organization? Asana is flexible and easy for all teams to use, so you can deliver quality work together, faster.
You visited this page on 3/18/23.
Search asana.com
Asana
Log in to Asana. Continue with Google. or. Email address ...
Product
Timeline - Board view - Automation - ...
Pricing
The free version of Asana is available for teams of up to 15 ...
Download Asana app
Your work syncs in real-time across the web, phone, and ...
People also ask
Asana, Inc., is an American software company based in San Francisco whose flagship Asana service is a web and mobile "work management" platform designed to help teams organize, track, and manage their work. Asana, Inc. was founded in 2008 by Dustin Moskovitz and Justin Rosenstein. Wikipedia
Developer: Asana
Headquarters: San Francisco, California, US
Founded: 2008; 15 years ago
Founders: Dustin Moskovitz, Justin Rosenstein
Number of employees: 1,782 (2023)
Traded as: NYSE: ASAN
People also search for
View 10+ more
Trello
Slack
Jira
ClickUp
Feedback


asana.com/developers
asana
Why Asana?
Features
Resources
Enterprise
Pricing
Contact Sales
Log In
Get Started
LEARN
Work Management Resources
Discover best practices, watch webinars, get insights
Asana Guide
Get lots of tips, tricks, and advice to get the most from Asana
Asana Academy
Sign up for interactive courses and webinars to learn Asana
Blog
Discover the latest Asana product and company news
CONNECT
Events
Find out about upcoming events near you
Community Programs
Connect with and learn from Asana customers around the world
Support
Need help? Contact the Asana support team
Partners
Learn more about our partner programs
Developers
Learn more about building apps on the Asana platform
Asana for Nonprofits
Get more information on our nonprofit discoun: program, and apply.
FEATURED READS
REPORT
Drive employee impact: New tools to empower resilient leadership
Read More
The Anatomy of Work
REPORT
The Anatomy of Work: Global Index 2023
Read More
Welcome back! How can we help you get started with Asana?


asana.com/developers
asana
Why Asana?
Features
Resources
Enterprise
Pricing
Contact Sales
Log In
Get Started
API Docs
Start building your own apps in Asana.
View Docs →
Community
Get updates, connect, and share feedback in the Asana Community forum.
Join the community →
App Directory
Publish your app in our directory of 200+ partners to share it with customers across the world.
Visit the directory →
Welcome back! How can we help you get started with Asana?
Download video from this page



After digging around the Asana documentation, I came across this Curl can be used in order to query the Asana API.

*https://app.asana.com/api/1.0/users/me *
-H"Authorization: Bearer 0/123456789abcdef"

The curl command resembles the secret we have identified in Git.

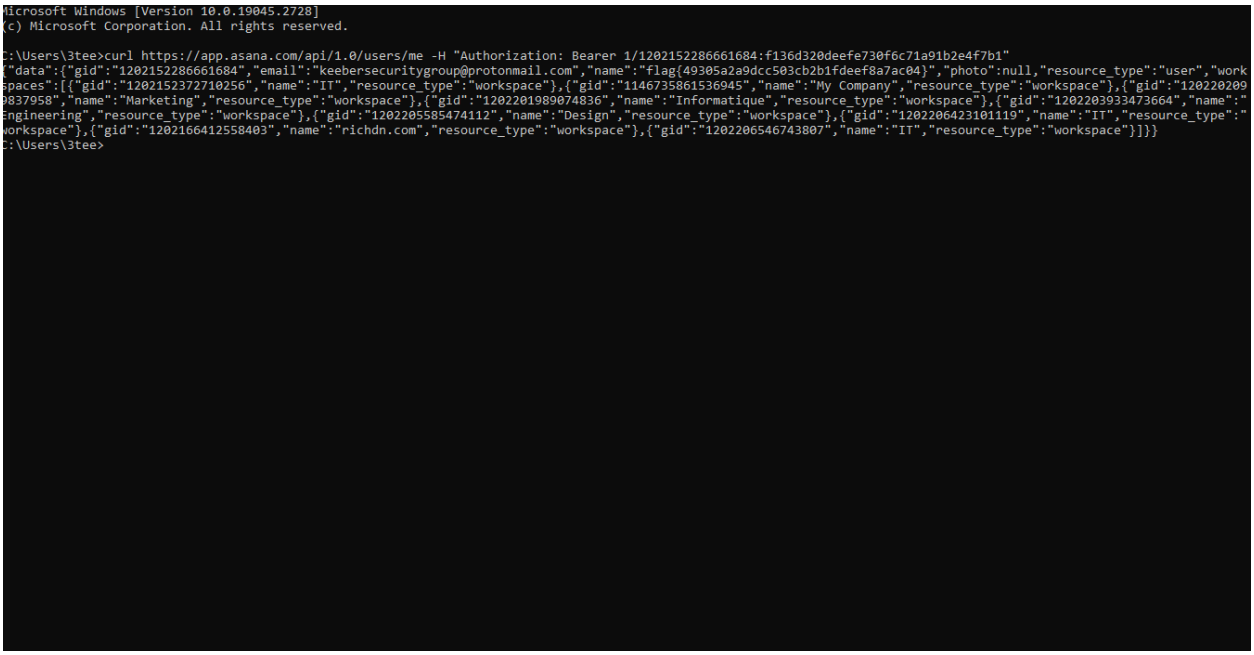
This must be the API token.

Run the following curl command in Command Prompt (cmd):

https://app.asana.com/api/1.0/users/me

-H"Authorization: Bearer 1/1202152286661684:f136d320deefe730f6c71a91b2e4f7b1"

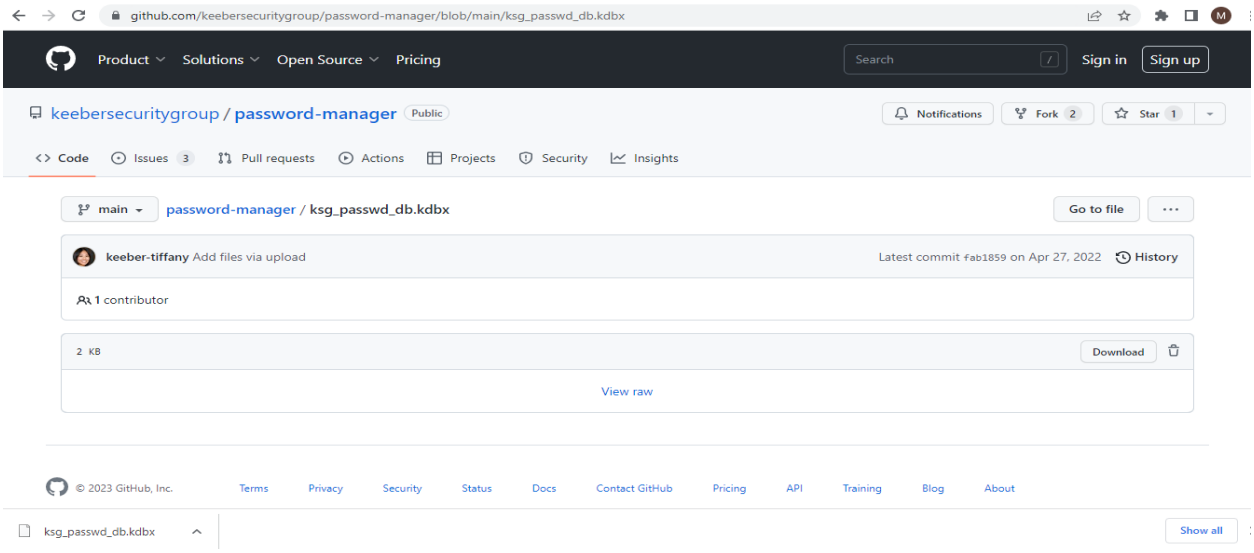
We get response:



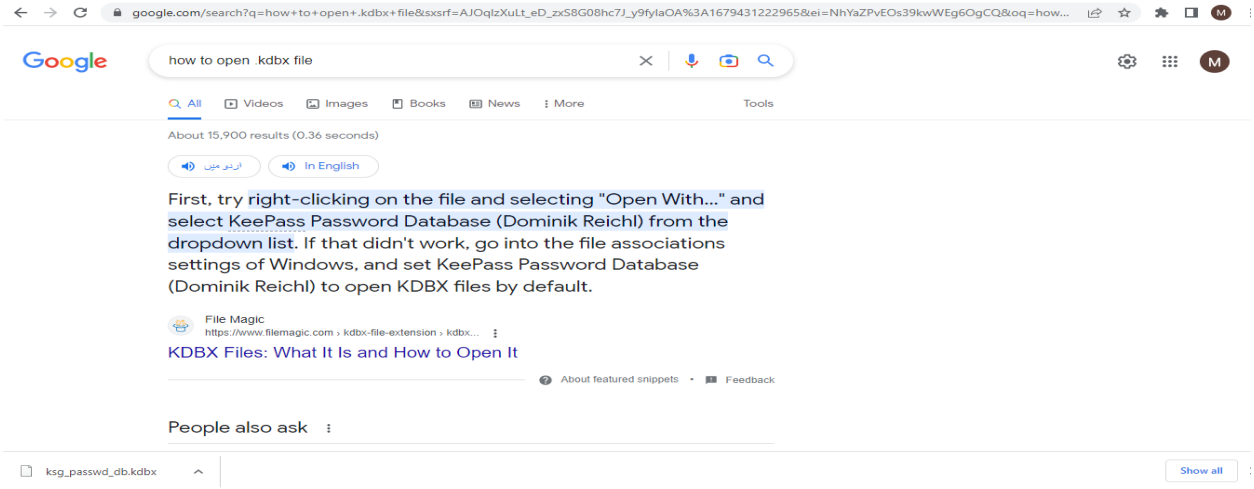
TASK 04: The ex-employee also left the company password database exposed to the public through GitHub. Since the password is shared throughout the company, it must be easy for employees to remember. Find and open the password database and extract the flag. The password of the file is: craccurrelss

Answer:

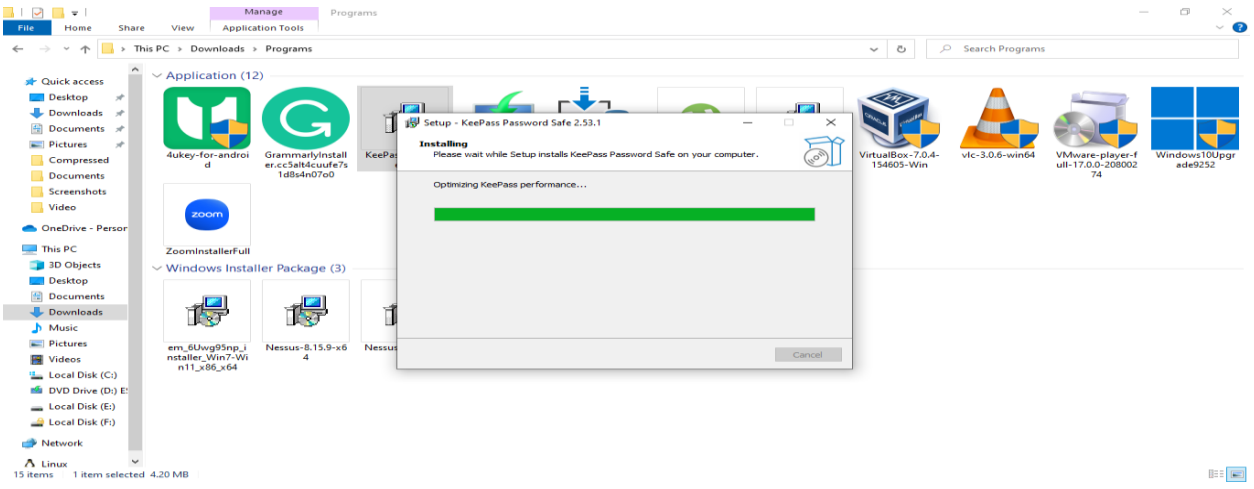
We thoroughly check company GitHub page and specifically examine the password manager repository to find the database file:

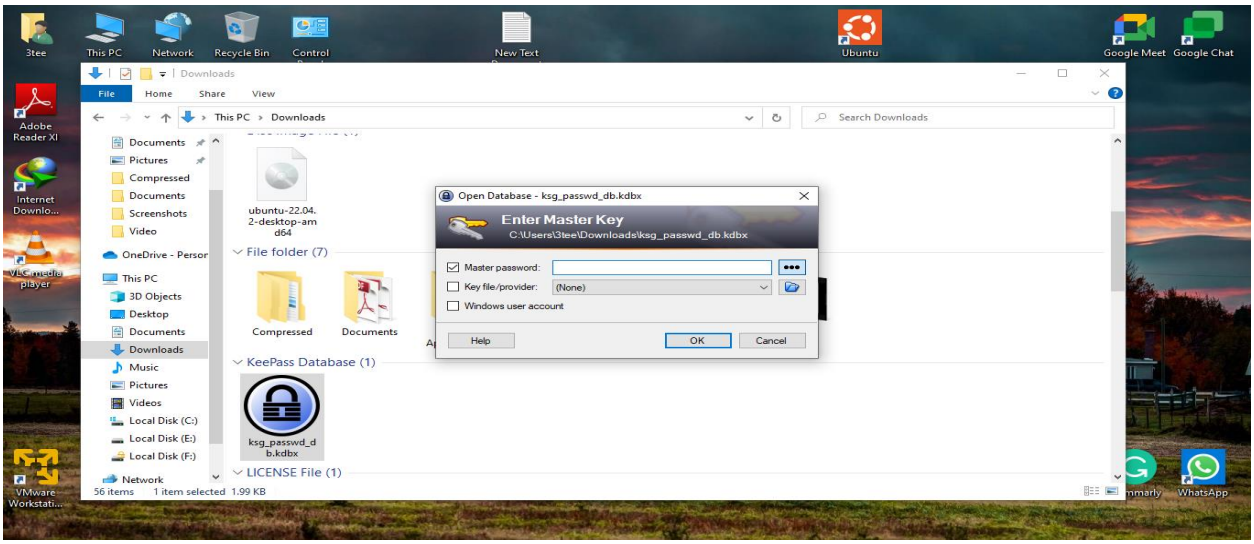


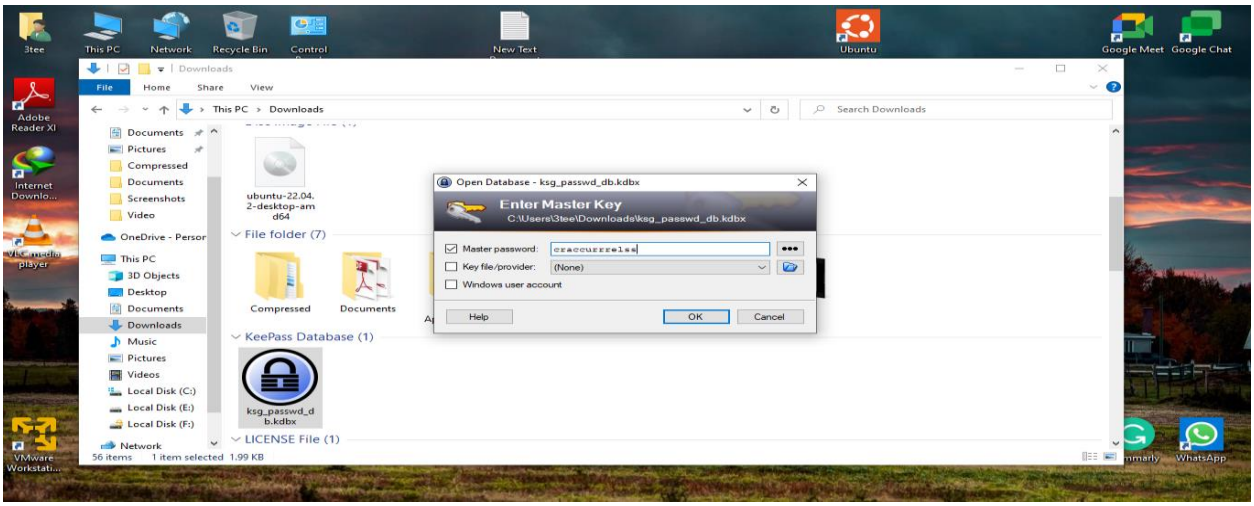
What is a .kdbx file? How to crack such a .kdbx file?

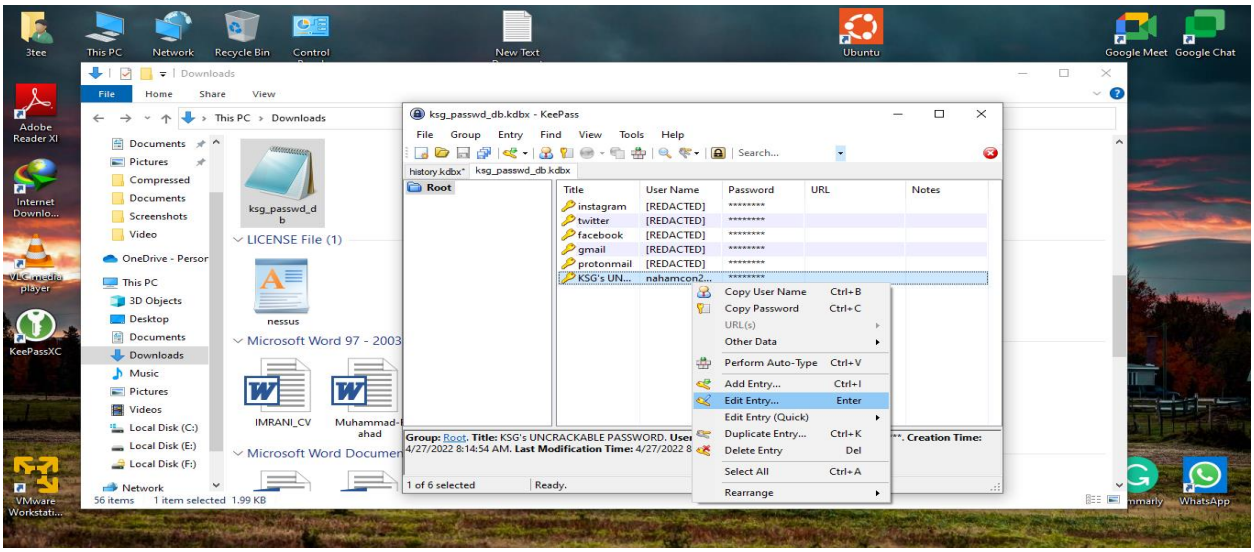


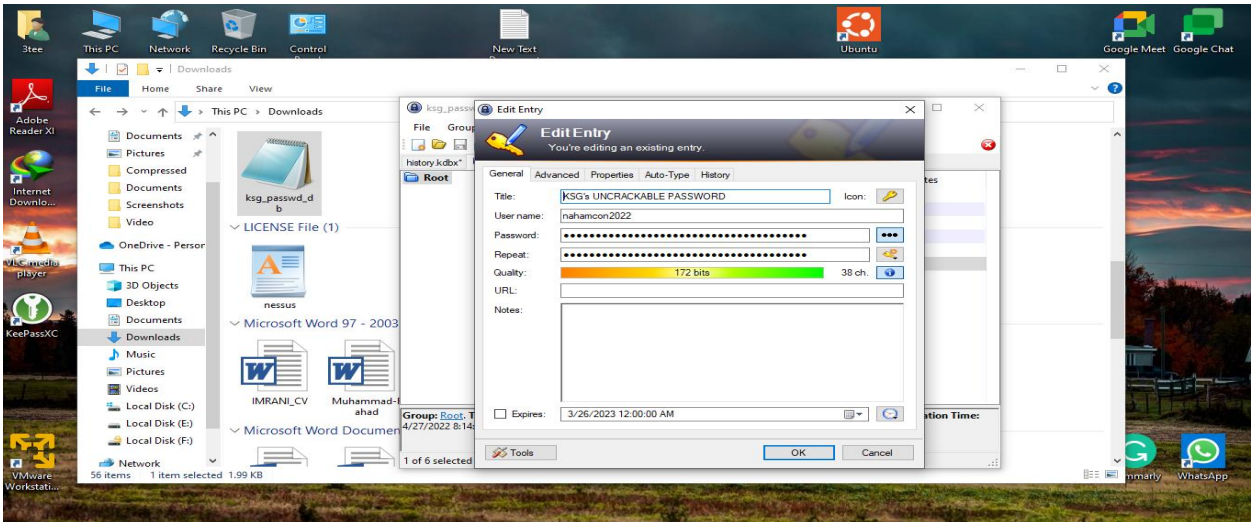
Downloaded and install Keepass software and open .kdbx file from keepass software. The password is given we crack this particular file.

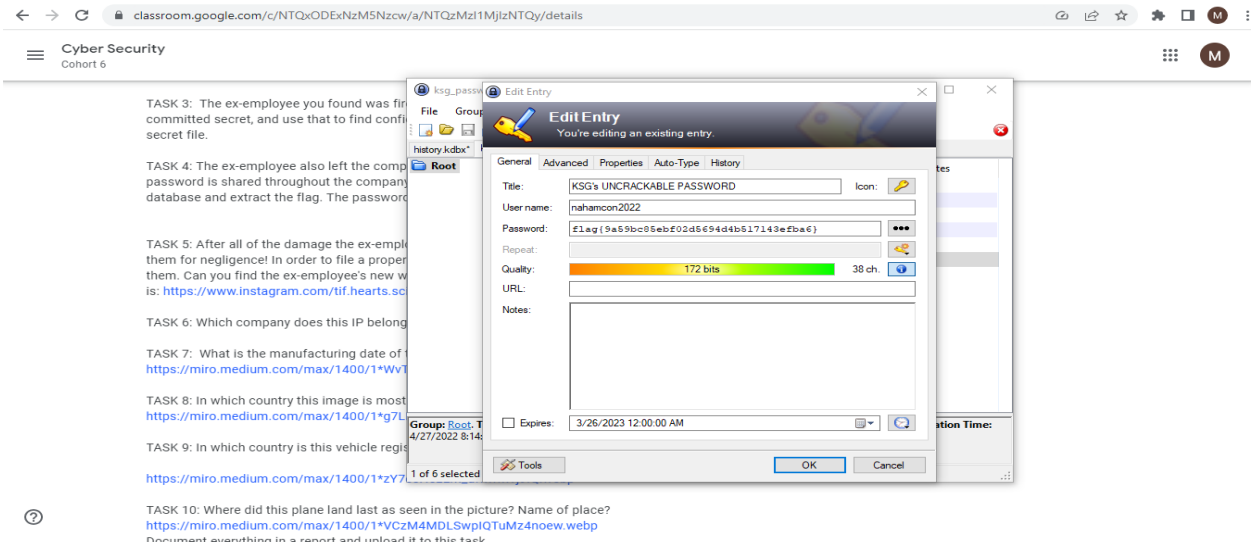



Open Database - ksg_passwd_db.kdbx
Enter Master Key
C:\Users\3tee\Downloads\ksg_passwd_db.kdbx
Master password:
Key file/provider:
(None)
Windows user account
Help
OK
Cancel
File folder (7)
KeePass Database (1)
LICENSE File (1)


Open Database - ksg_passwd_db.kdbx
Enter Master Key
C:\Users\3tee\Downloads\ksg_passwd_db.kdbx
Master password:
Key file/provider:
(None)
Windows user account
Help
OK
Cancel
File folder (7)
KeePass Database (1)
LICENSE File (1)


ksg_passwd_db.kdbx - KeePass
File Group Entry Find View Tools Help
Root
Title User Name Password URL Notes
instagram [REDACTED]
twitter [REDACTED]
facebook [REDACTED]
gmail [REDACTED]
protonmail [REDACTED]
KSG's UN... nahamcon2...
Copy User Name Ctrl+B
Copy Password Ctrl+C
URL(s)
Other Data
Perform Auto-Type Ctrl+V
Add Entry... Ctrl+I
Edit Entry... Enter
Edit Entry (Quick)
Duplicate Entry... Ctrl+K
Delete Entry Del
Select All Ctrl+A
Rearrange
1 of 6 selected
Ready.
LICENSE File (1)
nessus
Microsoft Word 97 - 2003
IMRANI_CV





Flag is: 9a59bc85ebf02d5694d4b517143efba6

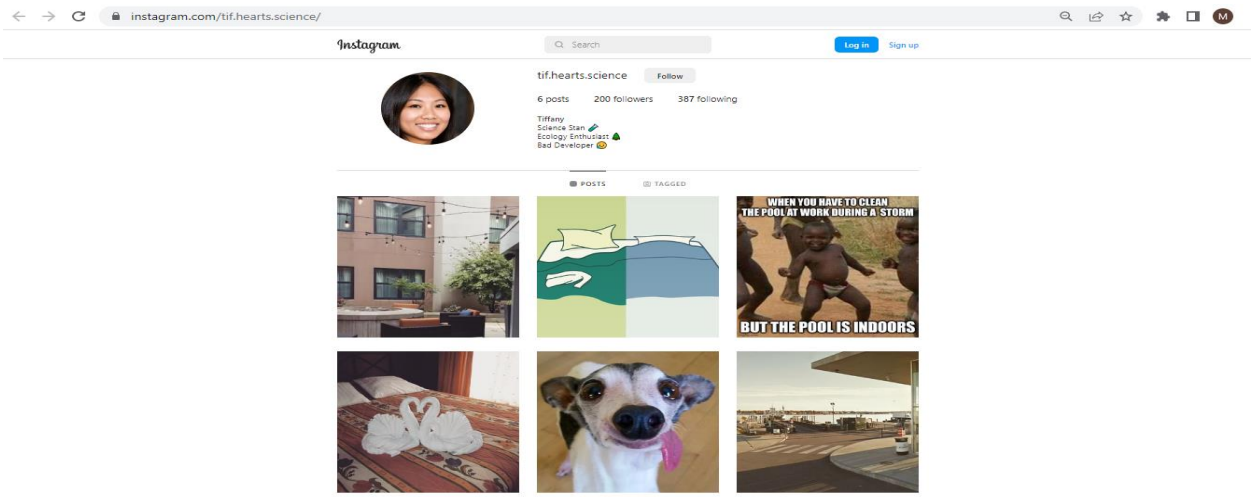
TASK 05: After all of the damage the ex-employees mistakes caused to the company, the Keeber Security Group is suing them for negligence! In order to file a proper lawsuit, we need to know where they are so someone can go and serve them. Can you find the ex-employee's new workplace? Her Instagram profile is:

https://www.instagram.com/tif.hearts.science/

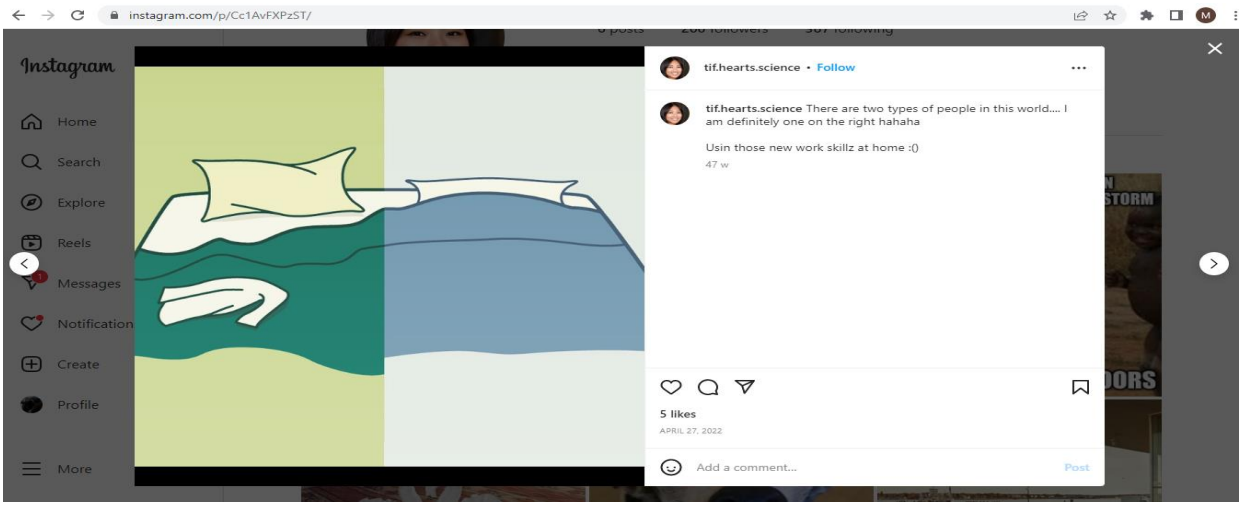
What is the name of her new work which is in the Maine area?

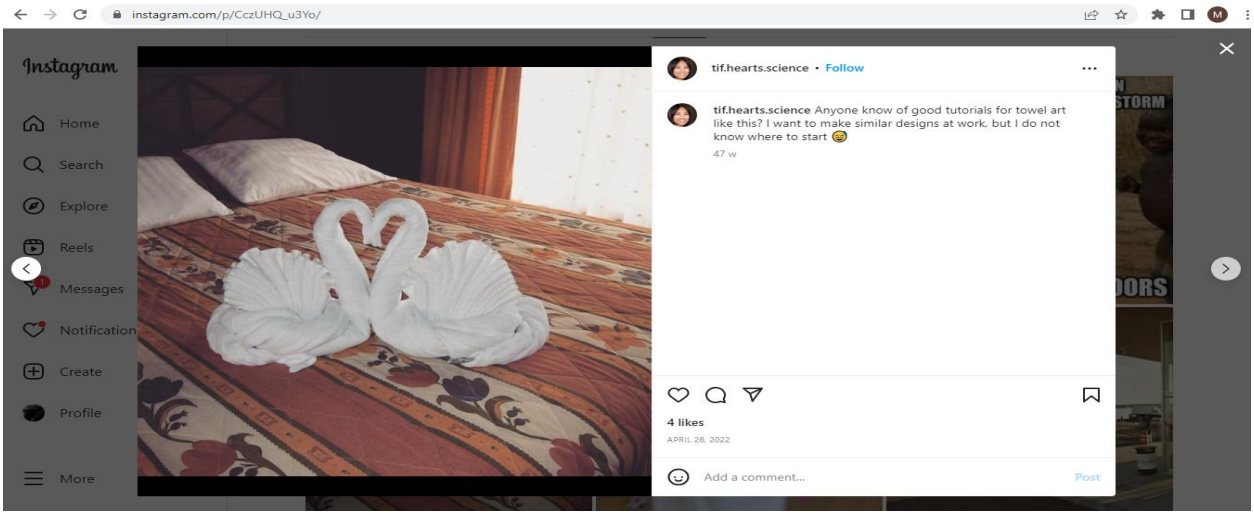
Answer:

Tiffany Instagram account only contains 6 posts with some useful information.



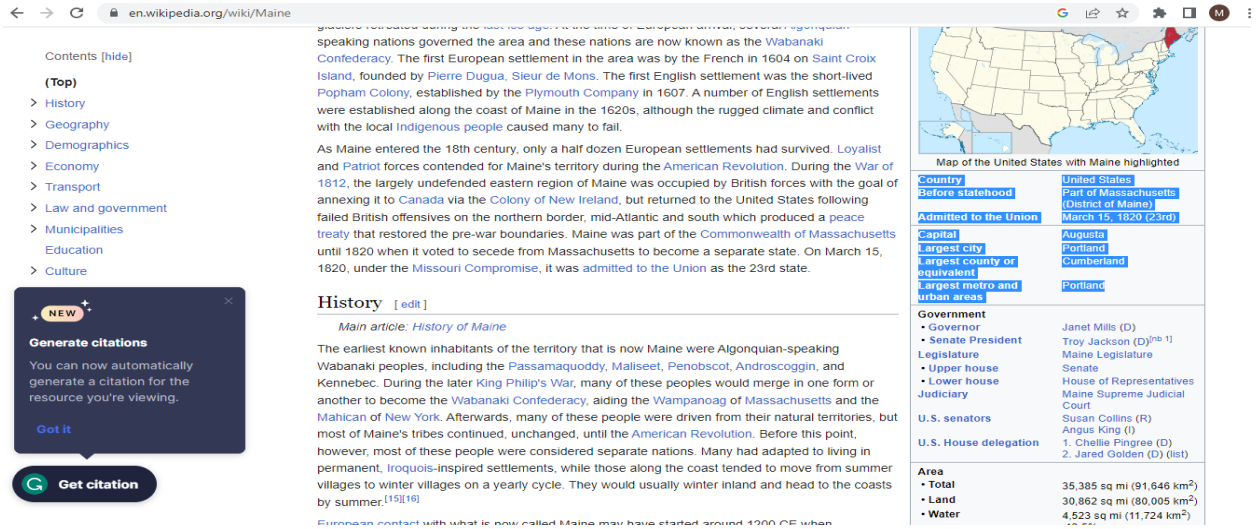
Below two images make clear that Tiffany has abandoned her career in software field and interested in Art that found in a hotel. Like Towel art etc.



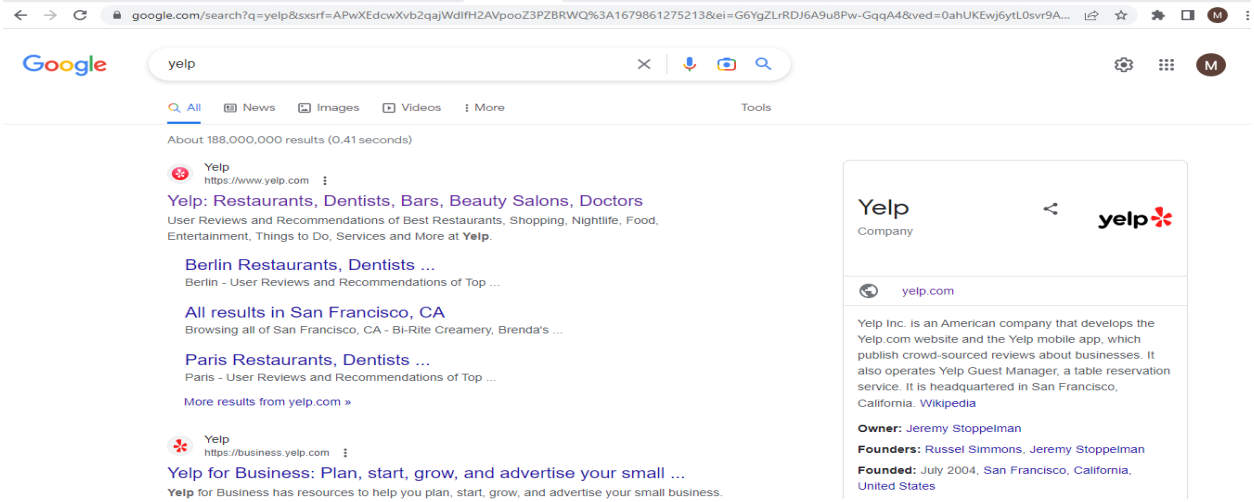


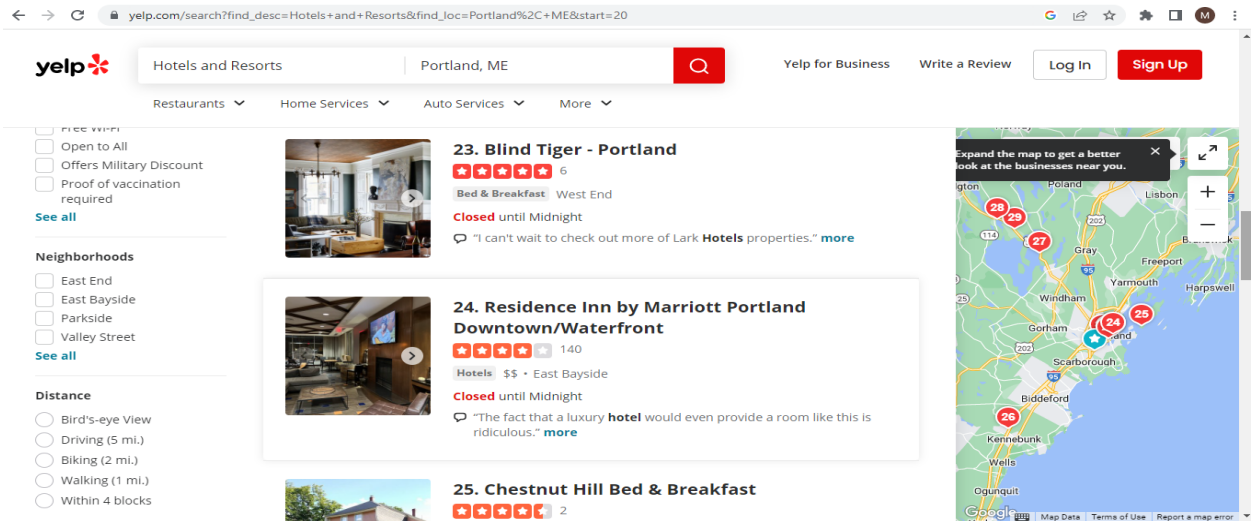
The hotel has an indoor pool.

Her new workplace is in Maine area. The Maine is in United States.

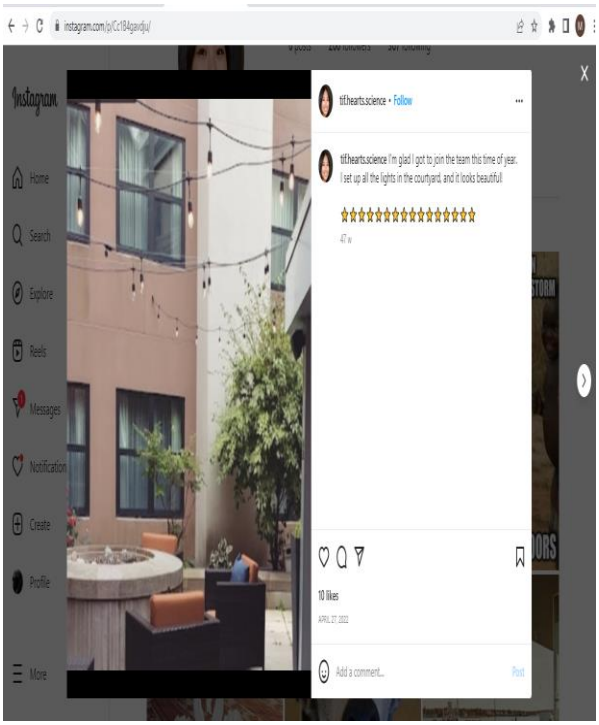


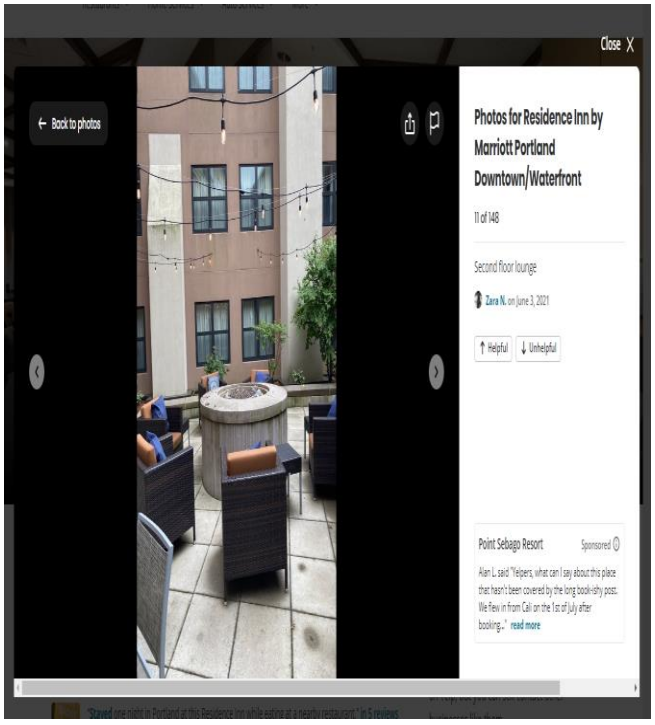
Only way I could find hotel was to search all hotels in Portland, Maine on yelp or TripAdvisor.

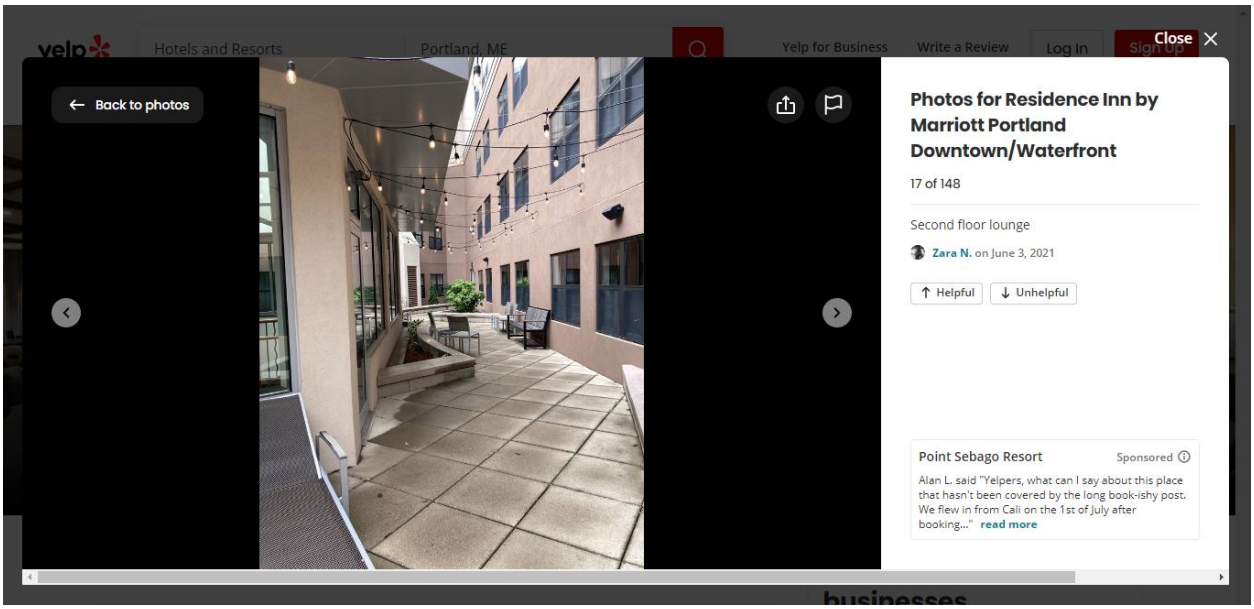




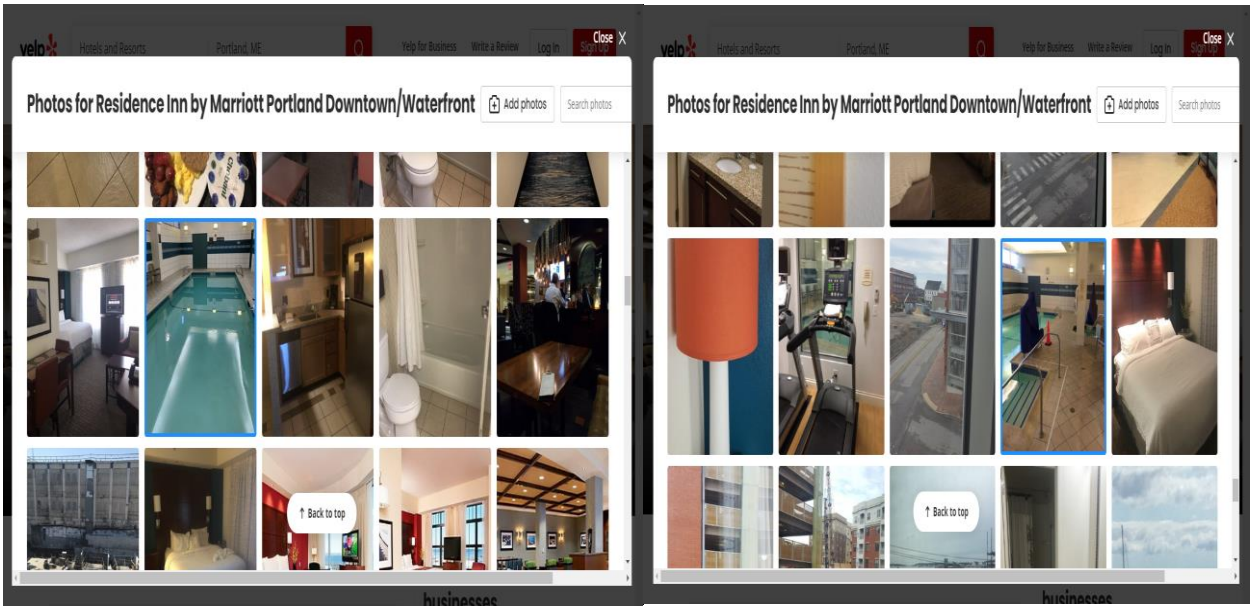
There are many resemblance points on Tiffany Instagram pictures and this hotel.

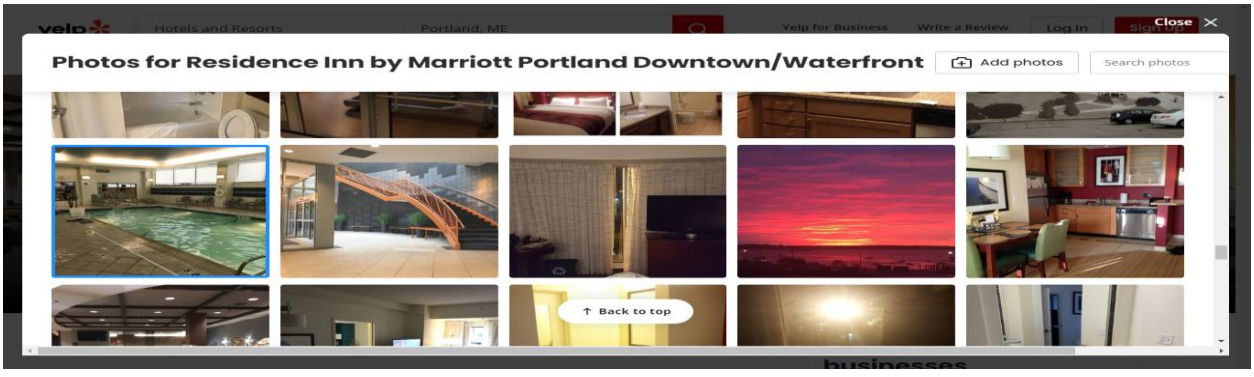






Discussed above hotel has indoor pool.



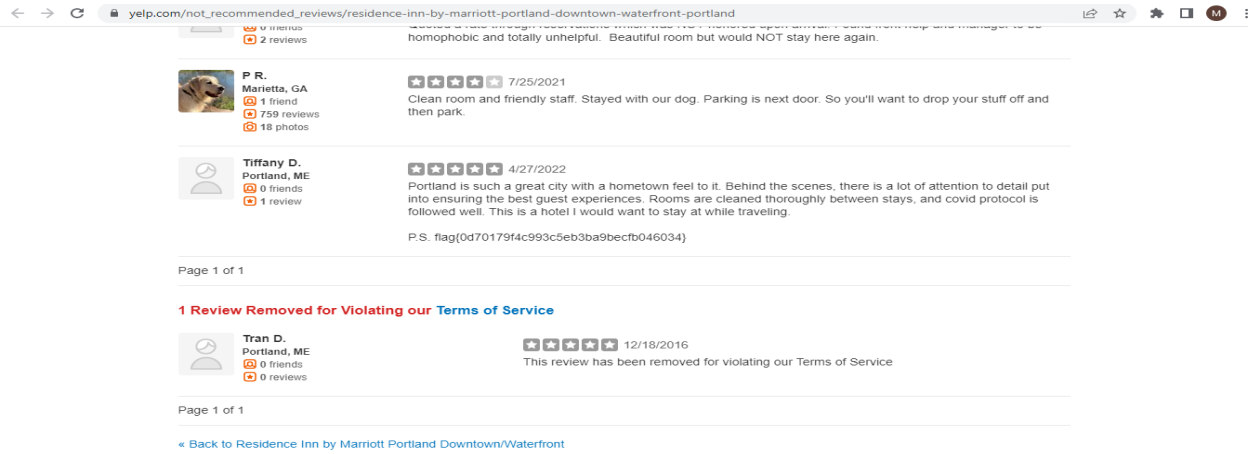


Hotel Name: Residence Inn by Marriott Portland Downtown/Waterfront.

Indoor Pool

Similar Lightening work etc.

Finally we get Tiffany review about hotel.

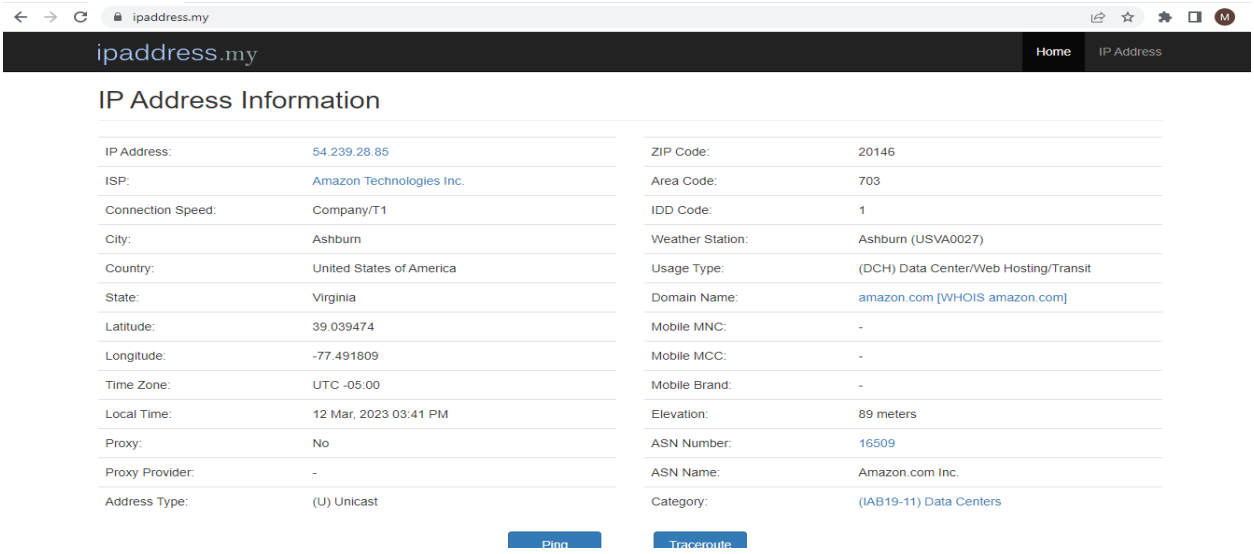


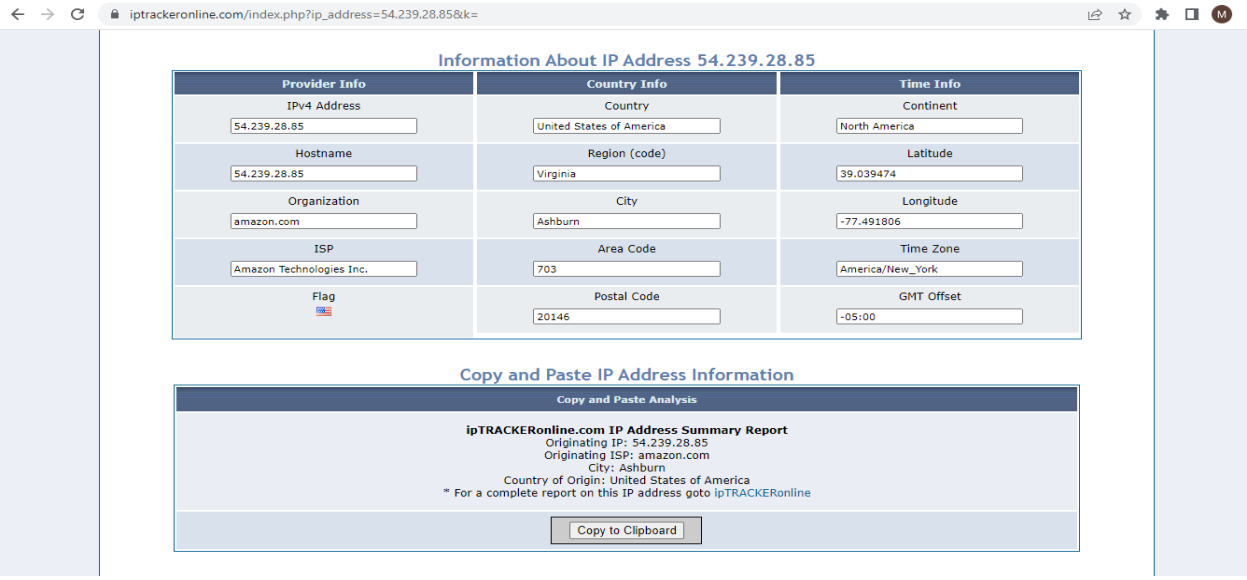
TASK 06: Which company does this IP belong 54.239.28.85?

Answer:

Searching website: ipaddress.my, iptrackeronline.com

IP address belongs to Amazon Technologies Inc.





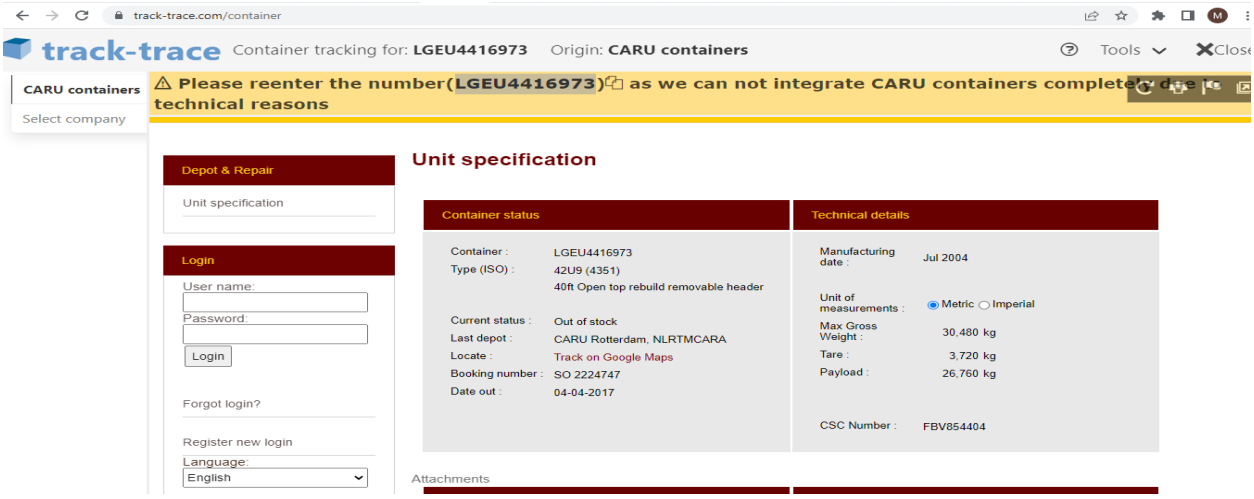
TASK 07: What is the manufacturing date of this container? (Month and year only) https://miro.medium.com/max/1400/1*WvTcWkiYxu6xZig9oZu4rw.webp

Answer:

Firstly, convert above image in jpg format.

Google: Container number LGEU 441697-3

I find manufacturing date of the container is July 2004.



TASK 08: In which country this image is most likely taken?

https://miro.medium.com/max/1400/1*g7LFPFUO_cjSskMjLPTsCA.webp

Answer:

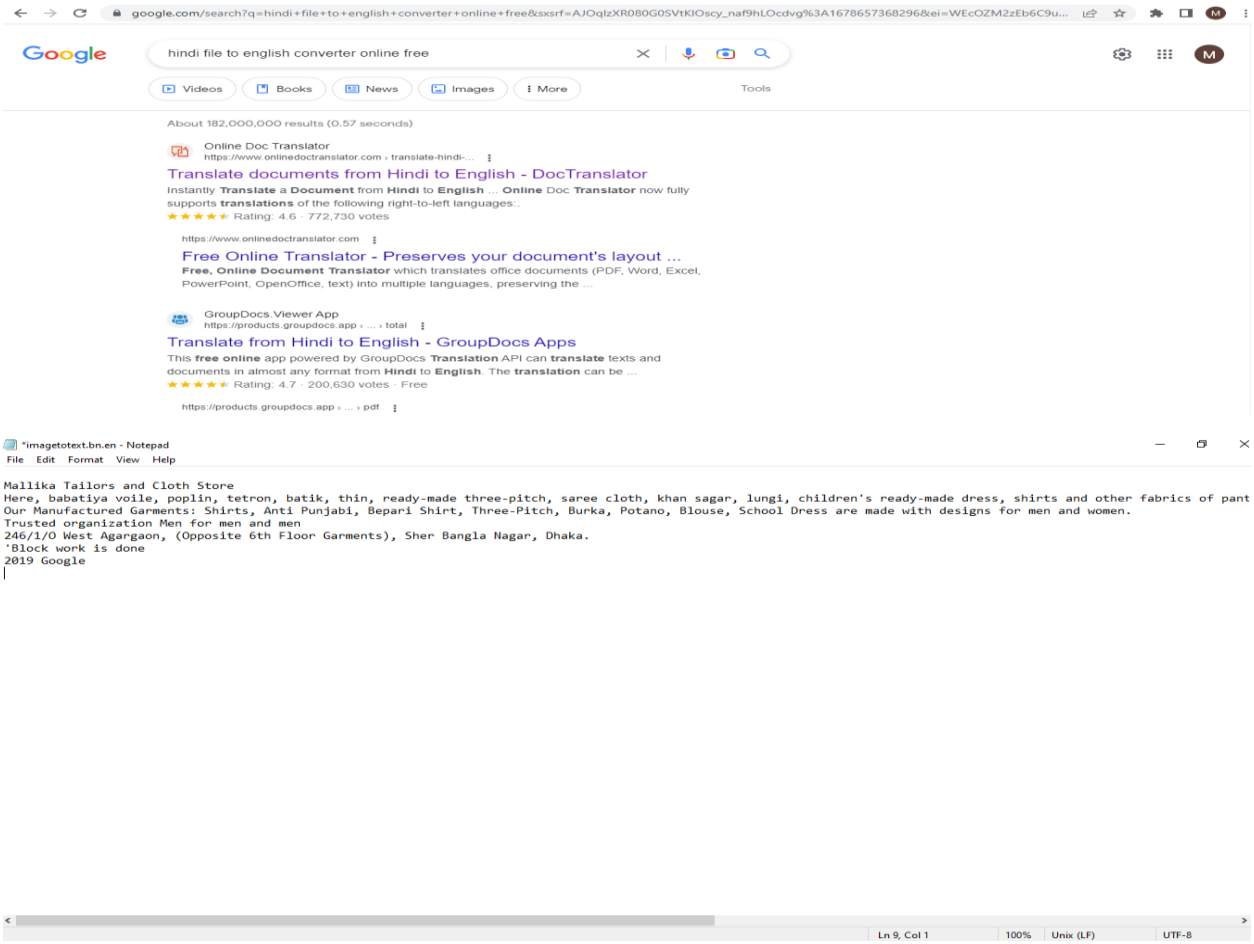
Firstly, convert above image in jpg format.

Googling: Image to text converter

Download text file.

Google: Hindi file to English converter and upload downloaded file to get result.

Dhaka, Bangladesh.



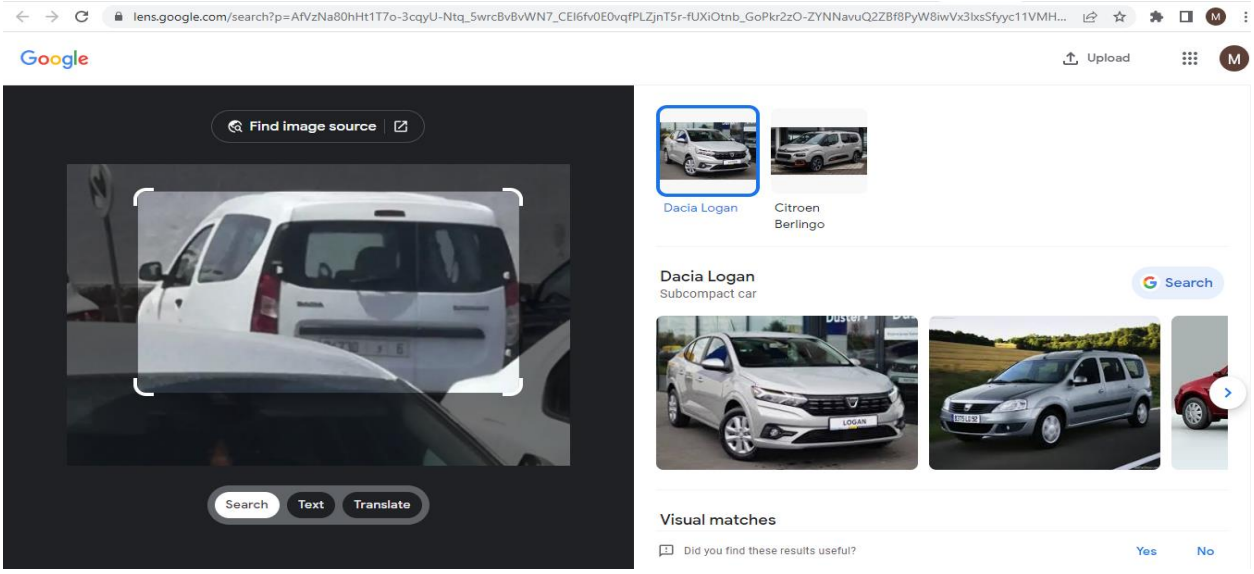
TASK 09: In which country is this vehicle registered?

https://miro.medium.com/max/1400/1*zY7esH5zLm_uffiwkWj9iQ.webp

Answer:

Firstly, convert above image in jpg format.

Using google lens to see the number plate of vehicle.



Just google similar number plate is registered in Morocco.

Searching website: worldlicenseplates.com

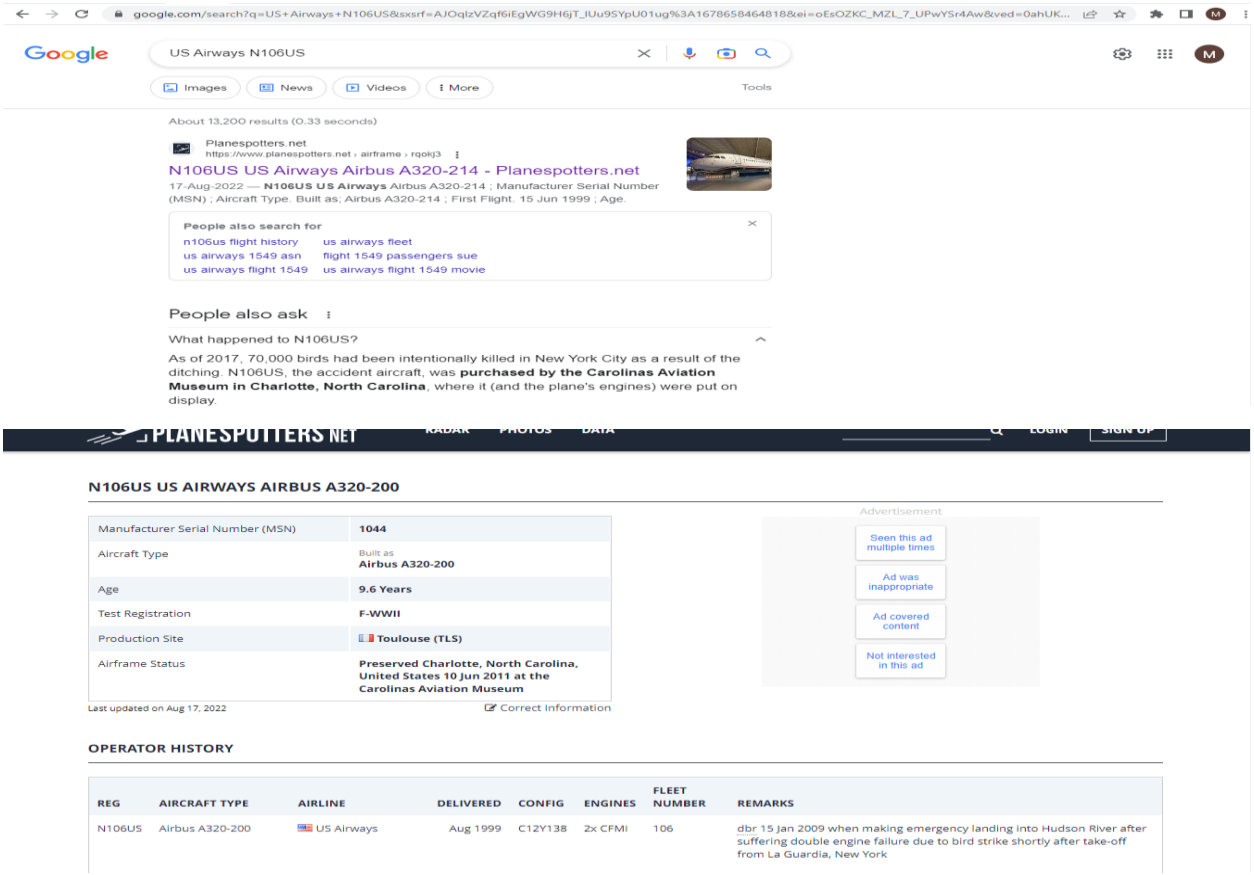
The vehicle is registered in Morocco.

TASK 10: Where did this plane land last as seen in the picture? Name of place? https://miro.medium.com/max/1400/1*VCzM4MDLSwpIQTuMz4noew.webp

Answer:

Firstly, convert above image in jpg format.

Google U.S Airways shuttle number-N106US.



The plane last seen at Hudson River.

Conclusion

OSINT tools that prioritize real time data allow security teams to get critical insights faster.

This gives organizations a much better chance of avoiding or mitigating threats from all angles.

Once investigative teams obtain data, they can follow the OSINT cycle to learn how to turn their data into useful intelligence, create OSINT reports, and share findings with the proper stakeholders.

- Wide array of information to collect.
- Easy to locate publicly available data.

As technology increases day by day the need of fast and specific information gathering arises, and it increases the need of OSINT.