

# **PORTFOLIO PROJECT-01**

**Project Title:**

**OPEN SOURCE INTELLIGENCE OSINT**

Presented by:

Muhammad Ansar Raza

Instructor Name:

Shahzaib Ali Khan

# **OUTLINE OF PROJECT-PRESENTATION**

- My Introduction
- Introduction of Open Source Intelligence OSINT
- History of OSINT
- Details regarding the Task/Portfolio Project-OSINT
- Conclusion
- Q&A

# **INTRODUCTION**

- Graduation: UET Lahore
- Mechanical Engineer
- Experience: 10 Years
- Government Officer
- Manager Mechanical
- Executive Engineer
- Husband
- Very Keen Interest in Cyber Security

# WHAT IS OPEN SOURCE INTELLIGENCE?

## OSINT

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.

The concept of OSINT basically works like this:

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

It is like a puzzle you don't know what the picture is?

You got all of those data points together

Assemble them

Analyze them

Now you can see the picture

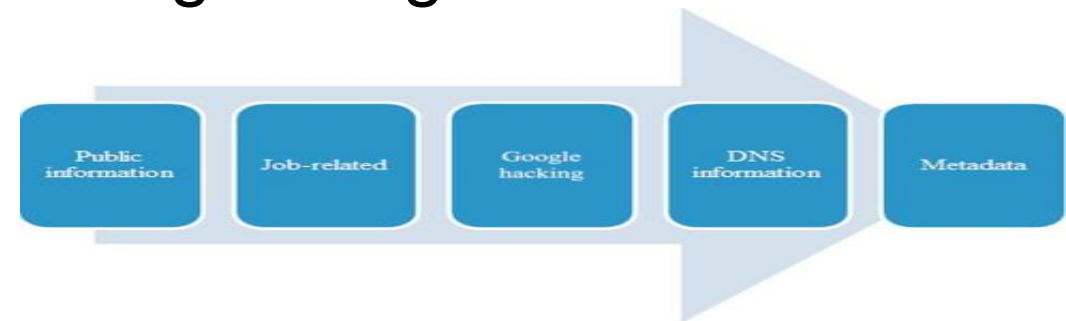


# HISTORY OF OSINT

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.

Cold war espionage focused on obtaining information via human sources or electronic signals.

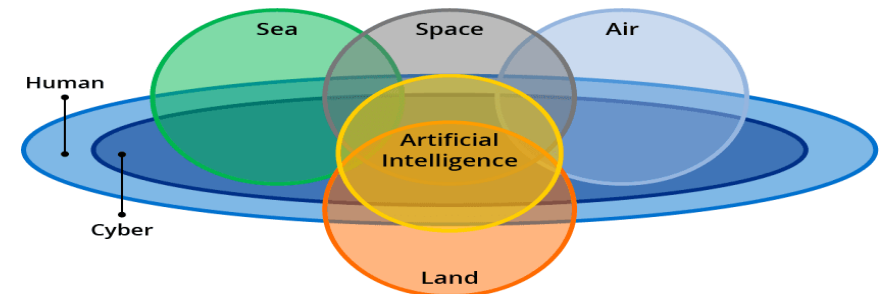
OSINT additional method of gathering intelligence.



# ARTIFICIAL INTELLIGENCE: THE FUTURE OF OSINT?

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.



# DETAILS REGARDING PORTFOLIO PROJECT TASK

## 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?

keebersecuritygroup.com

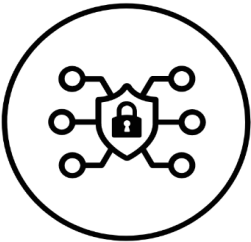
Keeber Security Group

Team About Contact

Keeber Security Group is a startup focused on helping small businesses with their security needs. Regardless of what your online business may be, cybersecurity is important to a company's success, and should be taken into account at all stages of the corporate lifecycle.

Phone: 207-555-4786  
Email: keebersecuritygroup@protonmail.com

CONTACT



**KEEBER SECURITY GROUP**

whois.com/whois/keebersecuritygroup.com

Whois Identity for everyone

Enter Domain or IP WHOIS

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

keebersecuritygroup.com Updated 3 days ago

Interested in similar domains?

<b>Domain Information</b>	keebersecuritygrp.com Buy Now
Domain: keebersecuritygroup.com	keebersecuritypartners.com Buy Now
Registrar: Name.com, Inc.	keebersecuritygroupllc.com Buy Now
Registered On: 2022-04-15	drkeebersecuritygroup.com Buy Now
Expires On: 2023-04-15	keebersecuritygroup.net Buy Now
Updated On: 2022-04-15	keebersecuritymarketin.com Buy Now
Status: clientTransferProhibited	
Name Servers: ns1cwy.name.com ns2dfg.name.com ns3clp.name.com ns4ksy.name.com	
<b>Registrant Contact</b>	

## 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?

The image displays two browser windows side-by-side. The left window shows the Keeber Security Group team page, listing six team members: Jeff Stokes (CEO), Maria Haney (CFO), Mark Deleon (Senior Security Engineer), Rachel Pollard (Security Engineer), Rooney McConnell (Human Resources), and Stefan Atkison (Social Media Manager). The right window shows a GitHub repository for 'security-evaluation-workflow' with a README.md file. Below these, a Wayback Machine archive is shown for the team page, with a calendar view highlighting April 19, 2022, at 21:22:59. The calendar shows the month of April 2022, with the 19th highlighted in yellow.

**Team Members:**

- Jeff Stokes (CEO): keeber-jeff@protonmail.com
- Maria Haney (CFO): keeber-maria@protonmail.com
- Mark Deleon (Senior Security Engineer): keeber-mark@protonmail.com
- Rachel Pollard (Security Engineer): keeber-rachel@protonmail.com
- Rooney McConnell (Human Resources): keeber-rooney@protonmail.com
- Stefan Atkison (Social Media Manager): keeber-stefan@protonmail.com

**GitHub Repository: security-evaluation-workflow**

**README.md:**

Keeber Security Group: Security Evaluation Workflow

This repository is intended to serve as a reference for Keeber Security Group employees, and others looking to evaluate the security of their own company.

Our company focuses on three primary tasks:

- Penetration Testing
- Information Protection
- Code Reviews

In this repository, there are guides for each of our areas of focus. The material is high-level, and primarily introductory.

Do not hesitate to reach out with any feedback on the content of this repository!

**Contributors:**

- keeber-rachel Rachel Pollard
- keeber-tiffany Tiffany Douglas
- keeber-mark Mark Deleon
- keeber-jeff Jeff Stokes

**Wayback Machine Archive:**

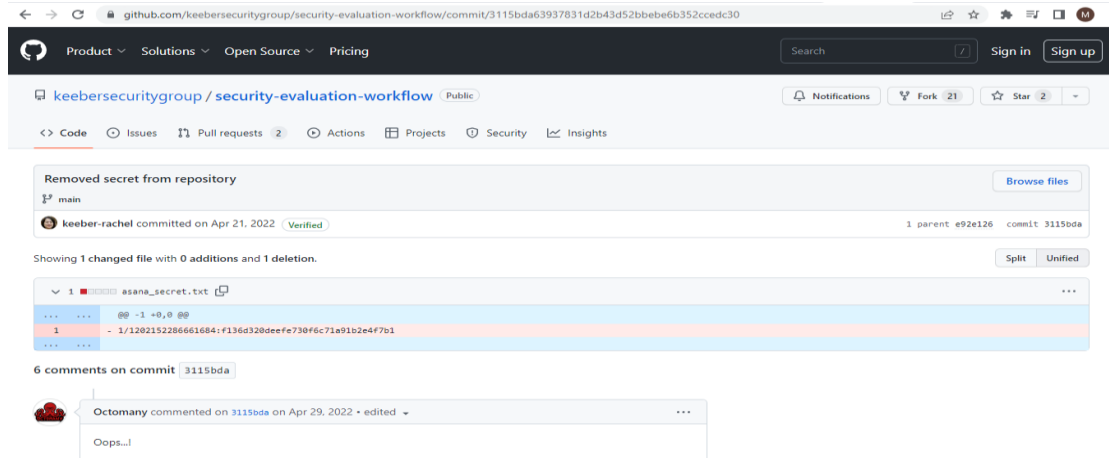
Saved 7 times between April 19, 2022 and November 4, 2022.

Calendar view showing April 19, 2022, at 21:22:59.

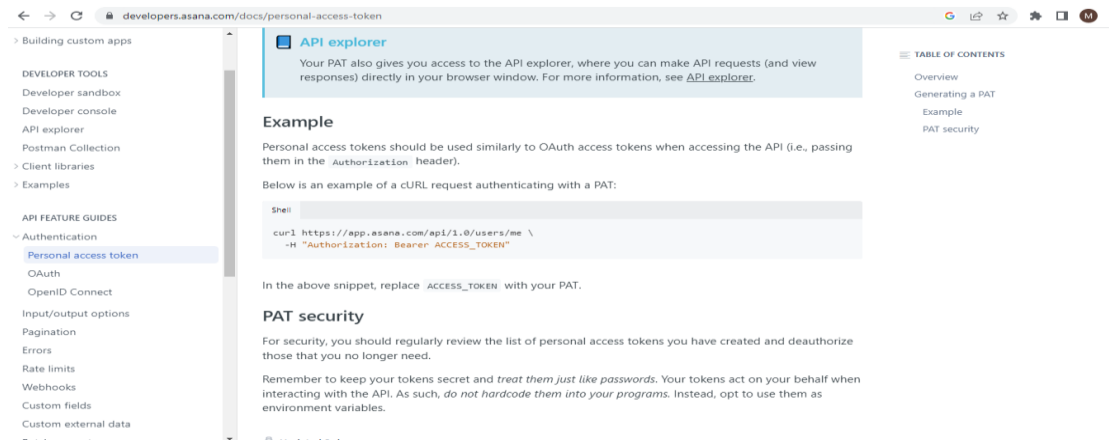


## TASK 03:

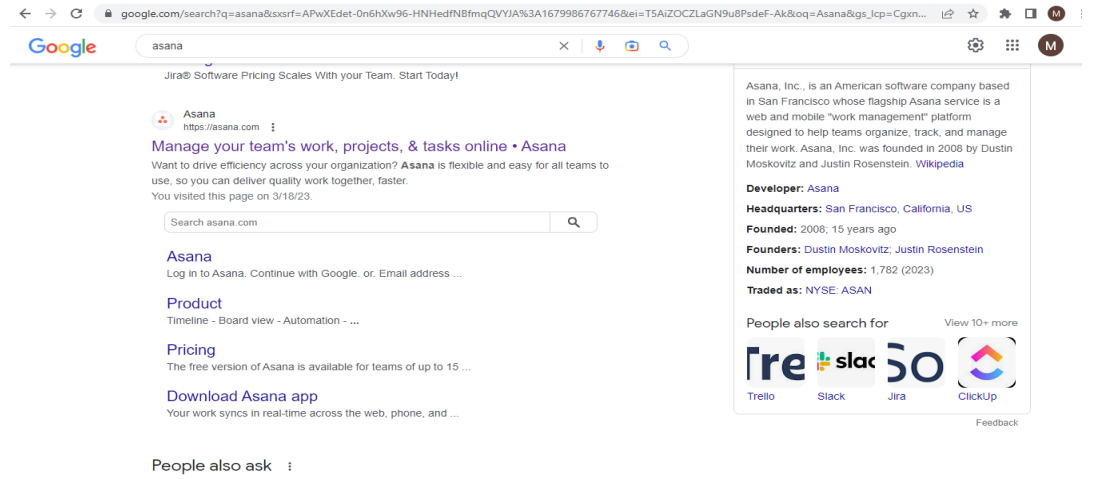
The ex-employee you found was fired for committing a secret to public GitHub repositories. Find the committed secret, and use that to find confidential company information. Also, find more information regarding the secret file?



The screenshot shows a GitHub commit page for the repository `keebersecuritygroup / security-evaluation-workflow`. The commit message is "Removed secret from repository" and it was made by `keeber-rachel` on April 21, 2022. The commit shows a file `asana_secret.txt` that was removed. The file's content, which was a personal access token, is visible in the diff view: `1/1202152286661684:f136d320deef730f6c71a91b2e4f7b1`. There are 6 comments on this commit, with the most recent one from `Octomany` on April 29, 2022, saying "Oops...".



The screenshot shows the Asana API explorer documentation page. It explains how to use a Personal Access Token (PAT) to access the Asana API. The page includes an "Example" section showing a cURL request to `https://app.asana.com/api/1.0/users/me` with the `Authorization: Bearer ACCESS_TOKEN` header. It also includes a "PAT security" section advising users to keep their tokens secret and to regularly review and deauthorize them.



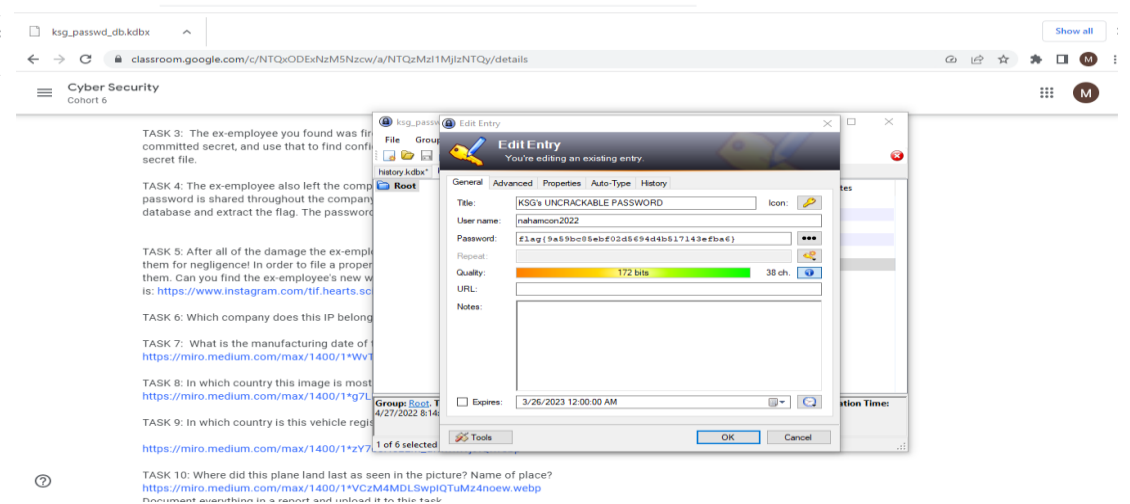
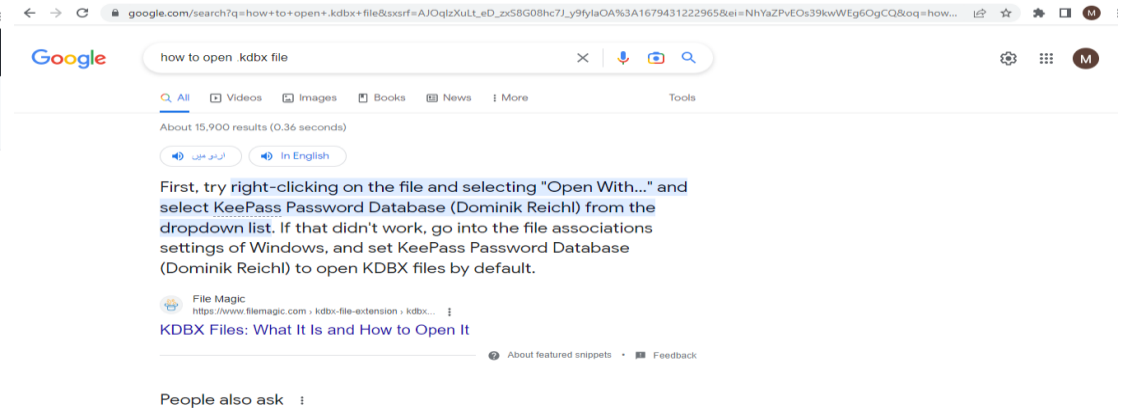
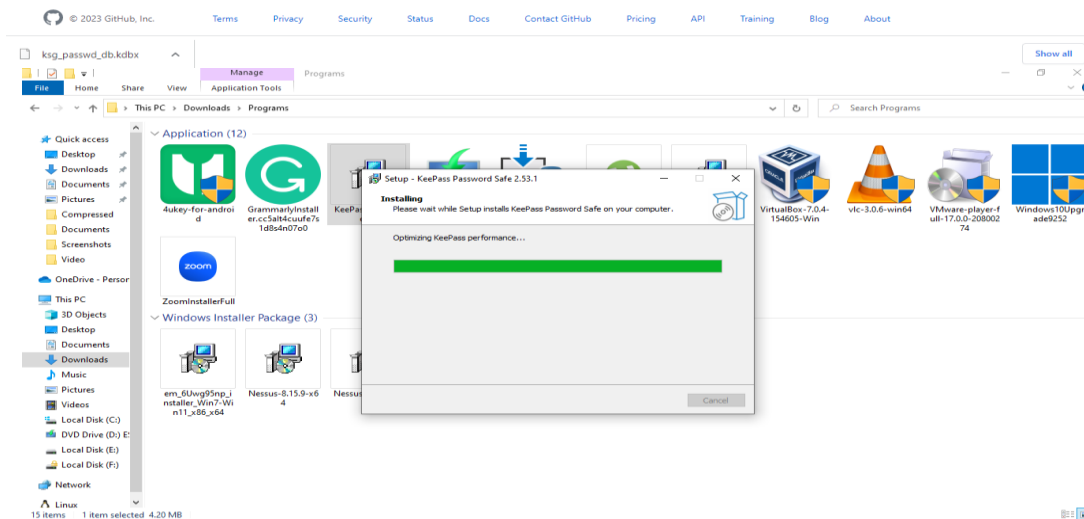
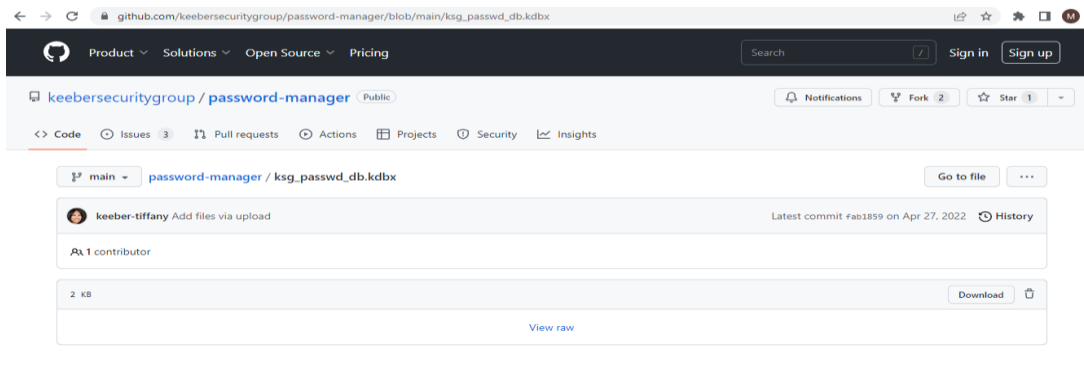
The screenshot shows the Asana company website. The page includes the Asana logo, a search bar, and a navigation menu. The main content area features a "Manage your team's work, projects, & tasks online" headline, a brief description of the company, and a "Log in to Asana" button. The right sidebar contains a "People also search for" section with links to Trello, Slack, Jira, and ClickUp, as well as a "People also ask" section.



The screenshot shows a terminal window with a cURL command and its output. The command is `curl https://app.asana.com/api/1.0/users/me -H "Authorization: Bearer 1/1202152286661684:f136d320deef730f6c71a91b2e4f7b1"`. The output is a JSON object containing user information, including the user's email, name, photo, and a list of workspaces. The workspaces listed include "Marketing", "Design", "IT", and "Informative".

## 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





## TASK 06:

Which company does this IP belong 54.239.28.85?

ipaddress.my

HomeIP Address

### IP Address Information

IP Address:	54.239.28.85	ZIP Code:	20146
ISP:	Amazon Technologies Inc.	Area Code:	703
Connection Speed:	Company/T1	IDD Code:	1
City:	Ashburn	Weather Station:	Ashburn (USVA0027)
Country:	United States of America	Usage Type:	(DCH) Data Center/Web Hosting/Transit
State:	Virginia	Domain Name:	amazon.com [WHOIS amazon.com]
Latitude:	39.039474	Mobile MNC:	-
Longitude:	-77.491809	Mobile MCC:	-
Time Zone:	UTC -05:00	Mobile Brand:	-
Local Time:	12 Mar, 2023 03:41 PM	Elevation:	89 meters
Proxy:	No	ASN Number:	16509
Proxy Provider:	-	ASN Name:	Amazon.com Inc.
Address Type:	(U) Unicast	Category:	(IAB19-11) Data Centers

Ping

Traceroute

## TASK 07:

What is the manufacturing date of this container? (Month and year only)

[https://miro.medium.com/max/1400/1\\*WvTcWkiYxu6xZig9oZu4rw.webp](https://miro.medium.com/max/1400/1*WvTcWkiYxu6xZig9oZu4rw.webp)



track-trace Container tracking for: LGEU4416973 Origin: CARU containers

⚠ Please reenter the number (LGEU4416973) as we can not integrate CARU containers completely due to technical reasons

CARU containers

Select company

Unit specification

Unit specification

Login

User name:

Password:

Login

Forgot login?

Register new login

Language: English

### Unit specification

Container status	Technical details
Container : LGEU4416973	Manufacturing date : Jul 2004
Type (ISO) : 42U9 (4351)	Unit of measurements : <input checked="" type="radio"/> Metric <input type="radio"/> Imperial
40ft Open top rebuild removable header	Max Gross Weight : 30,480 kg
Current status : Out of stock	Tare : 3,720 kg
Last depot : CARU Rotterdam, NLRTMCARA	Payload : 26,760 kg
Locate : <a href="#">Track on Google Maps</a>	CSC Number : FBV854404
Booking number : SO 2224747	
Date out : 04-04-2017	

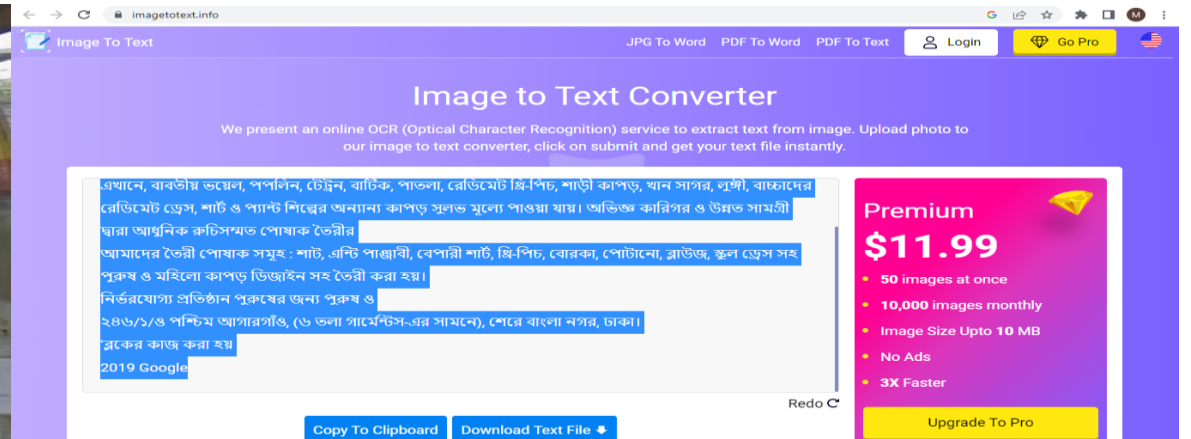
Attachments



## TASK 08:

In which country this image is most likely taken?

[https://miro.medium.com/max/1400/1\\*g7LFPFUO\\_cjSskMjLPTsCA.webp](https://miro.medium.com/max/1400/1*g7LFPFUO_cjSskMjLPTsCA.webp)



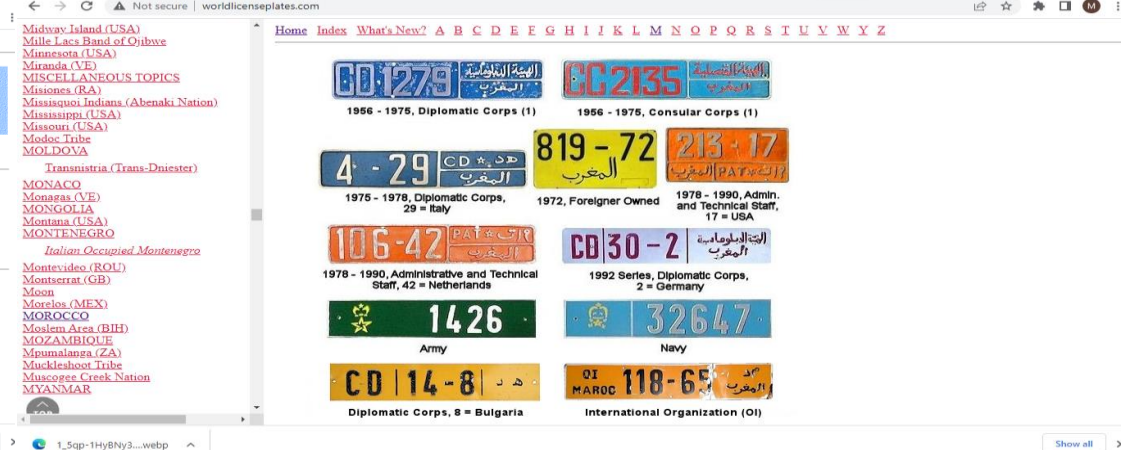
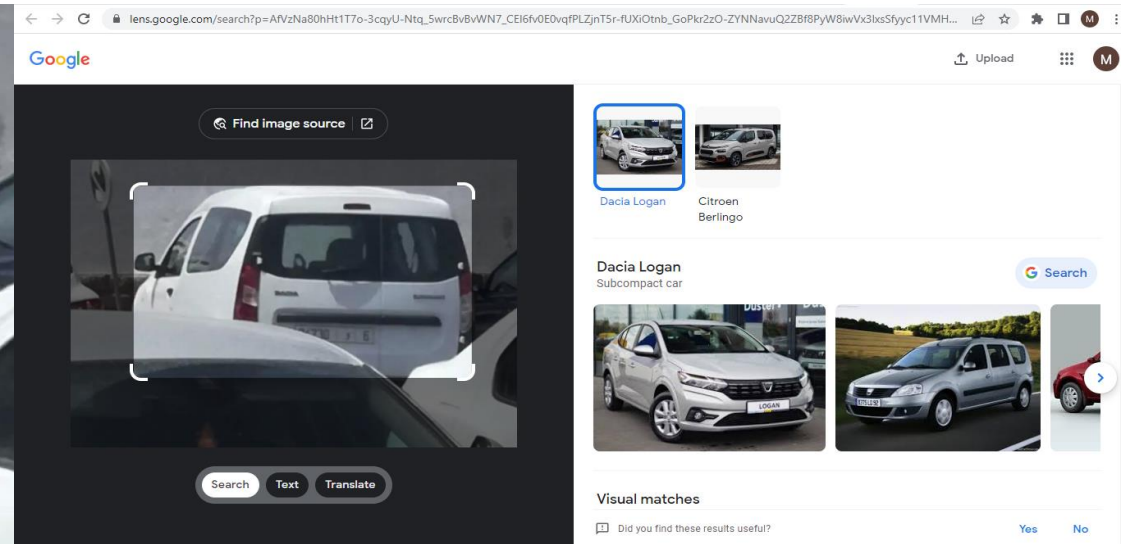
\*imagetotext.bn.en - Notepad  
File Edit Format View Help

Mallika Tailors and Cloth Store  
Here, babatiya voile, poplin, tetron, batik, thin, ready-made three-pitch, saree cloth, khan sagar, lungi, children's ready-made dress, shirts and other fabrics of pant  
Our Manufactured Garments: Shirts, Anti Punjabi, Bepari Shirt, Three-Pitch, Burka, Potano, Blouse, School Dress are made with designs for men and women.  
Trusted organization Men for men and men  
246/1/O West Agargaon, (Opposite 6th Floor Garments), Sher Bangla Nagar, Dhaka.  
\*Block work is done  
2019 Google

## TASK 09:

In which country is this vehicle registered?

[https://miro.medium.com/max/1400/1\\*zY7esH5zLm\\_uffiWkWj9iQ.webp](https://miro.medium.com/max/1400/1*zY7esH5zLm_uffiWkWj9iQ.webp)



## TASK 10:

Where did this plane land last as seen in the picture? Name of place?

[https://miro.medium.com/max/1400/1\\*VCzM4MDLSwplQTuMz4noew.webp](https://miro.medium.com/max/1400/1*VCzM4MDLSwplQTuMz4noew.webp)



PLANESPOTTERS.NET

KADAKPHOTOSDATA

QLOGIN

SIGN UP

### N106US US AIRWAYS AIRBUS A320-200

Manufacturer Serial Number (MSN)	1044
Aircraft Type	Built as Airbus A320-200
Age	9.6 Years
Test Registration	F-WWII
Production Site	Toulouse (TLS)
Airframe Status	Preserved Charlotte, North Carolina, United States 10 Jun 2011 at the Carolinas Aviation Museum

Last updated on Aug 17, 2022

☒ Correct Information

Advertisement

Seen this ad  
multiple times

Ad was  
inappropriate

Ad covered  
content

Not interested  
in this ad

### OPERATOR HISTORY

REG	AIRCRAFT TYPE	AIRLINE	DELIVERED	CONFIG	ENGINES	FLEET NUMBER	REMARKS
N106US	Airbus A320-200	US Airways	Aug 1999	C12Y138	2x CFMI	106	db: 15 Jan 2009 when making emergency landing into Hudson River after suffering double engine failure due to bird strike shortly after take-off from La Guardia, New York



# **CONCLUSION**

we have identified the key ingredients and potential issues that are common in any information retrieval system.

Advances in technology can help to address these issues and move toward fully automated OSINT.

The greatest challenge is to correctly interpret the users intended search in the face of not organized search expressions and ambiguity.

