

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 what's the picture is?

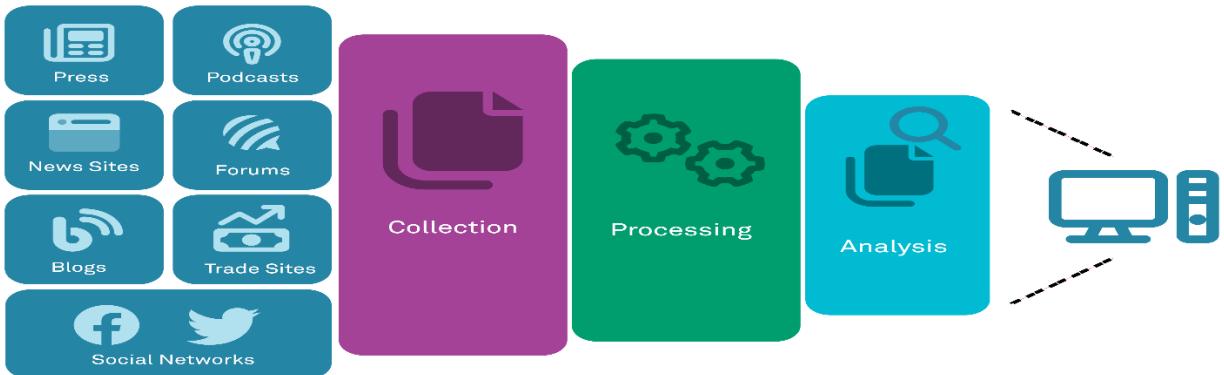
You got all of those data points together.

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 CISO's 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

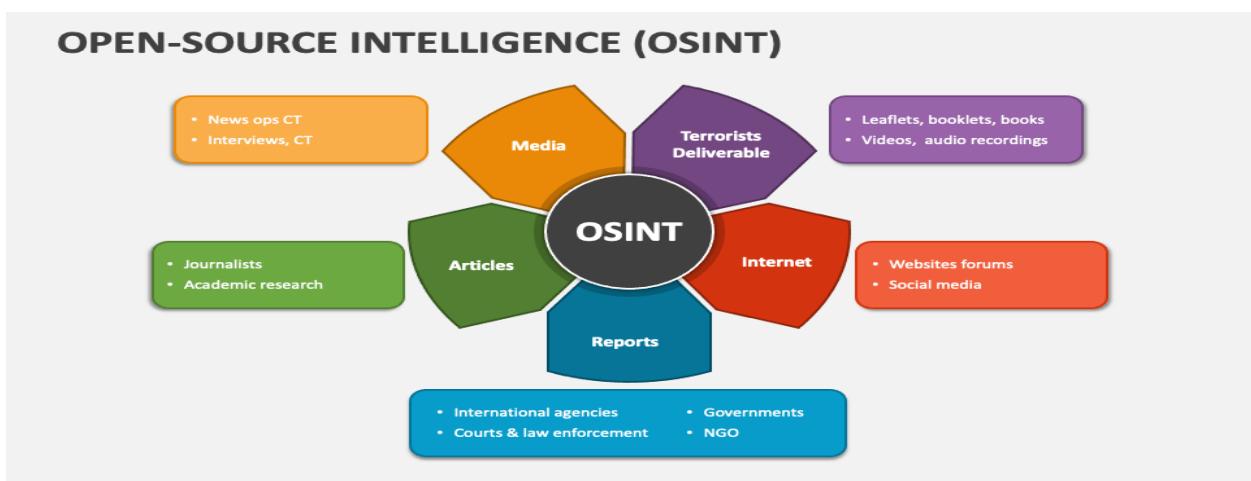
This type of collection requires more expertise. It directs traffic to a target server to obtain information about the server. Scanner traffic must be similar to normal Internet traffic to avoid detection.

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).

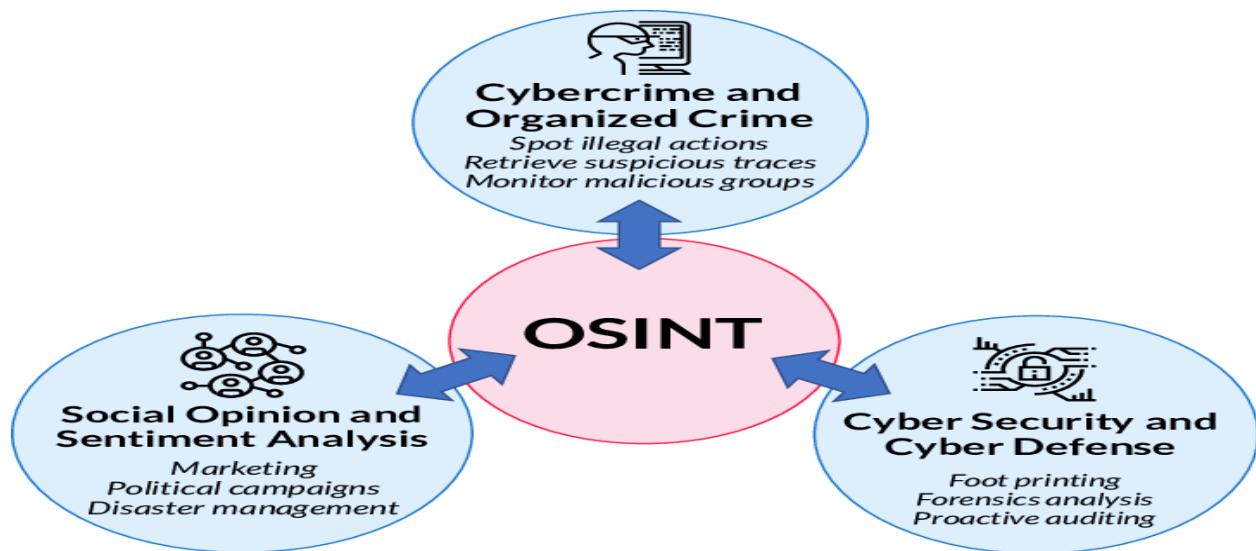
Social engineering attacks on targets are also considered a form of active intelligence gathering.



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.

The screenshot shows the Whois.com website interface. At the top, there's a navigation bar with links for DOMAINS, WEBSITE, CLOUD, HOSTING, SERVERS, EMAIL, SECURITY, WHOIS, SUPPORT, LOGIN, and a shopping cart icon. A search bar at the top right contains the text "WHOIS". Below the navigation is a search bar with the placeholder "Enter Domain or IP". The main content area displays the domain "keebersecuritygroup.com" with the status "Updated 3 days ago". Under "Domain Information", details include: Domain: keebersecuritygroup.com, Registrar: Name.com, Inc., Registered On: 2022-04-15, Expires On: 2023-04-15, Updated On: 2022-04-15, Status: clientTransferProhibited, and Name Servers: ns1cwy.name.com, ns2dfg.name.com, ns3cfp.name.com, ns4ksy.name.com. To the right of this section, a sidebar titled "Interested in similar domains?" lists several variations of the domain name with "Buy Now" buttons: keebersecuritygrp.com, keebersecuritypartners.com, keebersecuritygroupllc.com, drkeebersecuritygroup.com, keebersecuritygroup.net, and keebersecuritymarketing.com.

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.

The screenshot shows the Keeber Security Group website's team page. It features a grid of six employee profiles, each with a circular profile picture, the employee's name, their title, and their email address. The employees listed are: Jeff Stokes (CEO), Maria Haney (CFO), Mark Delcon (SENIOR SECURITY ENGINEER), Rachel Pollard (SECURITY ENGINEER), Rooney McConnell (HUMAN RESOURCES), and Stefan Atkison (SOCIAL MEDIA MANAGER). Each profile also includes a small link to their GitHub account.

| Employee | Title | Email |
|------------------|--------------------------|------------------------------|
| Jeff Stokes | CEO | keeber-jeff@protonmail.com |
| Maria Haney | CFO | keeber-maria@protonmail.com |
| Mark Delcon | 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 |

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.

The screenshot shows the GitHub repository page for 'keebersecuritygroup/security-evaluation-workflow'. The README.md file contains the following content:

```

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!


```

The repository has no releases, packages, or contributors listed.

[© 2023 GitHub, Inc.](#) [Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact GitHub](#) [Pricing](#) [API](#) [Training](#) [Blog](#) [About](#)

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:

The screenshot shows the Wayback Machine interface with the URL web.archive.org/web/20220901000000*/https://keebersecuritygroup.com/team. The timeline shows 7 saved snapshots between April 19, 2022, and November 4, 2022. The calendar view highlights April 19, 2022, with a callout showing the single snapshot taken at 21:22:59.

| JAN | FEB | MAR | APR |
|----------------------|----------------------|----------------------|--|
| 1 | 1 2 3 4 5 6 7 8 | 1 2 3 4 5 | 1 2 3 4 5 |
| 2 3 4 5 6 7 8 | 6 7 8 9 10 11 12 | 6 7 8 9 10 11 12 | 3 4 5 6 7 8 9 |
| 9 10 11 12 13 14 15 | 13 14 15 16 17 18 19 | 13 14 15 16 17 18 19 | 10 11 12 13 14 15 16 |
| 16 17 18 19 20 21 22 | 20 21 22 23 24 25 26 | 20 21 22 23 24 25 26 | 17 18 19 20 21 22 23 |
| 23 24 25 26 27 28 29 | 27 28 | 27 28 29 30 31 | 24 25 |
| 30 31 | | | APRIL 19, 2022 1 snapshot 21:22:59 |

| MAY | JUN | JUL |
|----------------------|----------------------|----------------------|
| 1 2 3 4 5 6 7 | 1 2 3 4 | 1 2 |
| 8 9 10 11 12 13 14 | 5 6 7 8 9 10 11 | 3 4 5 6 7 8 9 |
| 15 16 17 18 19 20 21 | 12 13 14 15 16 17 18 | 10 11 12 13 14 15 16 |
| 22 23 24 25 26 27 28 | 19 20 21 22 23 24 25 | 17 18 19 20 21 22 23 |
| 29 30 31 | 26 27 28 29 30 | 24 25 26 27 28 29 30 |
| | | 21 22 23 24 25 26 27 |
| | | 28 29 30 31 |
| | | 31 |

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

The screenshot shows the Wayback Machine interface with the URL <https://keebersecuritygroup.com/team/>. The capture date is April 19, 2022. The page displays five team members:

- Mark Deleon**, SENIOR SECURITY ENGINEER, keebersecuritygroup@protonmail.com
- Rachel Pollard**, SECURITY ENGINEER, keebersecuritygroup@protonmail.com
- Rooney McConnell**, HUMAN RESOURCES, keebersecuritygroup@protonmail.com
- Tiffany Douglas**, JUNIOR SECURITY ENGINEER, keebersecuritygroup@protonmail.com, flag{cddb59d78a6d50905340a62852e315c9}
- Stefan Atkison**

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.

The screenshot shows a GitHub commit page for the repository [keebersecuritygroup / security-evaluation-workflow](#). The commit hash is `3115bda63937831d2b43d52bbebe6b352ccedc30`. The commit message is "Removed secret from repository". It was made by **keeber-rachel** on April 21, 2022, and is verified. The commit has 1 parent (`e92e126`) and 1 commit (`3115bda`). The commit details show a single file change: `asana_secret.txt`. The commit message in the diff is "1/1202152286661684:f136d320deeffe730f6c71e91b2e4f7b1". Below the commit, there are 6 comments, with one from **Octomany** on April 29, 2022, containing the text "Oops...!".

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.

The screenshot shows two parts of the GitHub interface. The top part is a list of commits from a repository, and the bottom part is a detailed view of a specific commit.

Commit History:

- Updated code_reviews.txt (keeber-tiffany, Apr 21, 2022)
- Keep up the great work KSG! (torvalds, Apr 21, 2022)
- started code_reviews.txt (keeber-tiffany, Apr 21, 2022)
- Removed secret from repository (keeber-rachel, Apr 21, 2022) - Verified
- Fixed .gitignore (keeber-rachel, Apr 21, 2022) - Verified
- added .gitignore (keeber-tiffany, Apr 21, 2022)
- added code_reviews.txt (keeber-tiffany, Apr 21, 2022)
- fixed grammatical nuance (keeber-rachel, Apr 21, 2022) - Verified
- Create information_protection.txt (keeber-rachel, Apr 21, 2022) - Verified

Repository View:

Code tab selected.

Commit Details:

- added .gitignore (keeber-tiffany, Apr 21, 2022)
- Showing 2 changed files with 2 additions and 0 deletions.
- File Changes:
 - .gitignore: 1 addition, 0 deletions. Content: `asana_secret.txt`
 - asana_secret.txt: 1 addition, 0 deletions. Content: `Hi pls give flag`
- Comments: HirAvanCnIK on Apr 30, 2022: Hi pls give flag (3 replies)

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

Portfolio Project Report-01

google.com/search?q=asana&sxsrf=APwXEdet-0n6hXw96-HNHedfNBfmoQVYJA%3A1679986767746&ei=T5AiZOCZLaGN9u8Psdef-Ak&oq=Asana&gs_icp=Cgxn...

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 [Trello](#) [Slack](#) [Jira](#) [ClickUp](#) [View 10+ more](#)

Feedback

People also ask :

asana.com/developers

Why Asana? Features Resources Enterprise Pricing Contact Sales Log In Get Started

LEARN CONNECT

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

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 discount program, and apply.

FEATURED READS

REPORT
Drive employee impact: New tools to empower resilient leadership
Read More

REPORT
The Anatomy of Work
The Anatomy of Work: Global Index 2023
Read More

Welcome back! How can we help you get started with Asana?

Download video from this page

asana.com/developers

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 →](#)

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.

The Asana API is a RESTful interface, providing programmatic access to much of the data in the system. It provides predictable URLs for accessing resources, and uses built-in HTTP features to receive commands and return responses. This makes it easy to communicate from a wide variety of environments: apps, command-line utilities, gadgets, and even the browser URL bar itself.

The API accepts JSON or form-encoded content in requests and returns JSON content in all of its responses, including errors. Only UTF-8 character encoding is supported for both requests and responses.

How documentation is structured

Documentation on this site is divided into two major sections:

- Guides:** Contextual information, guides, and tutorials regarding API usage
- API reference:** A comprehensive reference for objects, schemas, and endpoints available in the API

You may navigate between both sections at any time using the navigation bar above.

```
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:

```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

:C:\Users\3tee>curl https://app.asana.com/api/1.0/users/me -H "Authorization: Bearer 1/1202152286661684:f136d320deefe730f6c71a91b2e4f7b1"
"data": {"gid": "1202152286661684", "email": "keebersecuritygroup@protonmail.com", "name": "flag{49305a2a9dc503cb2bfdeef8a7ac04}", "photo": null, "resource_type": "user", "workspaces": [{"gid": "1202152372710256", "name": "IT", "resource_type": "workspace"}, {"gid": "1146735861536945", "name": "My Company", "resource_type": "workspace"}, {"gid": "120220209837958", "name": "Marketing", "resource_type": "workspace"}, {"gid": "1202201989074836", "name": "Informatique", "resource_type": "workspace"}, {"gid": "1202203933473664", "name": "Engineering", "resource_type": "workspace"}, {"gid": "1202205585474112", "name": "Design", "resource_type": "workspace"}, {"gid": "1202206423101119", "name": "IT", "resource_type": "workspace"}, {"gid": "1202166412558403", "name": "richdn.com", "resource_type": "workspace"}, {"gid": "1202206546743807", "name": "IT", "resource_type": "workspace"}]}
```

```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

:C:\Users\3tee>curl https://app.asana.com/api/1.0/users/me -H "Authorization: Bearer 1/1202152286661684:f136d320deefe730f6c71a91b2e4f7b1"
"data": {"gid": "1202152286661684", "email": "keebersecuritygroup@protonmail.com", "name": "flag{49305a2a9dc503cb2bfdeef8a7ac04}", "photo": null, "resource_type": "user", "workspaces": [{"gid": "1202152372710256", "name": "IT", "resource_type": "workspace"}, {"gid": "1146735861536945", "name": "My Company", "resource_type": "workspace"}, {"gid": "120220209837958", "name": "Marketing", "resource_type": "workspace"}, {"gid": "1202201989074836", "name": "Informatique", "resource_type": "workspace"}, {"gid": "1202203933473664", "name": "Engineering", "resource_type": "workspace"}, {"gid": "1202205585474112", "name": "Design", "resource_type": "workspace"}, {"gid": "1202206423101119", "name": "IT", "resource_type": "workspace"}, {"gid": "1202166412558403", "name": "richdn.com", "resource_type": "workspace"}, {"gid": "1202206546743807", "name": "IT", "resource_type": "workspace"}]}
```

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:

The screenshot shows a GitHub page for the repository 'keebersecuritygroup / password-manager'. The file 'ksg_passwd_db.kdbx' is displayed. The file was added by 'keeber-tiffany' via upload. It has a size of 2 KB and was last committed on April 27, 2022. There is one contributor listed. The file can be viewed raw or downloaded.

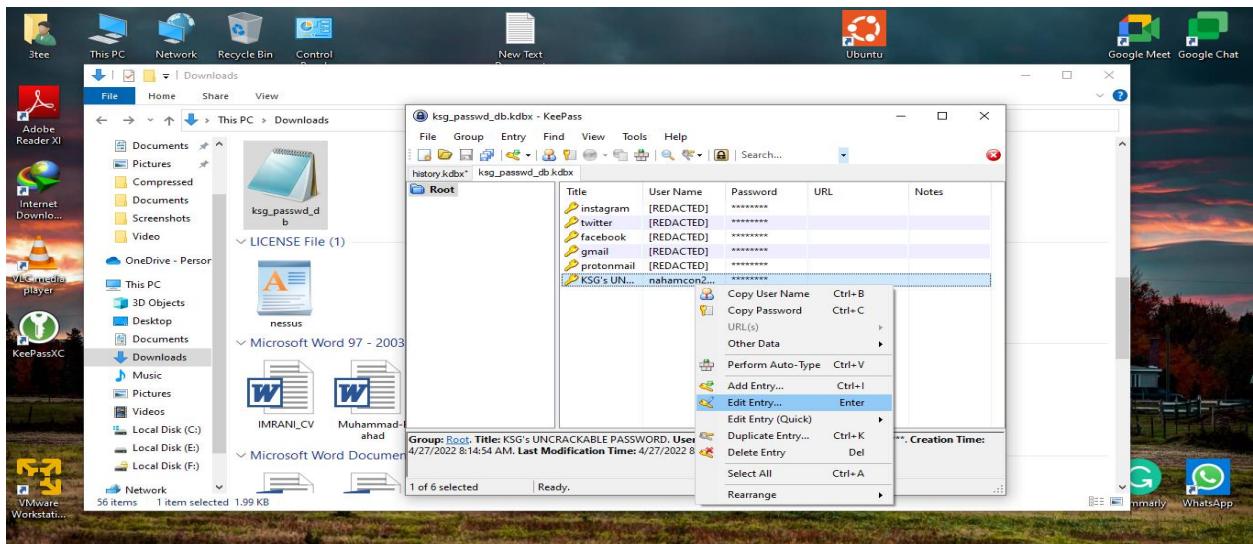
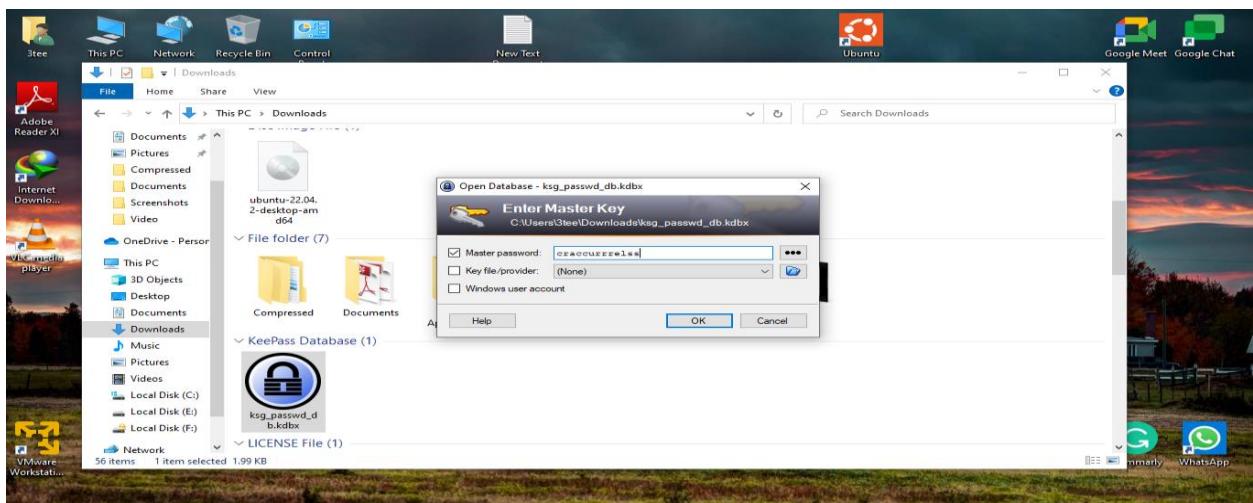
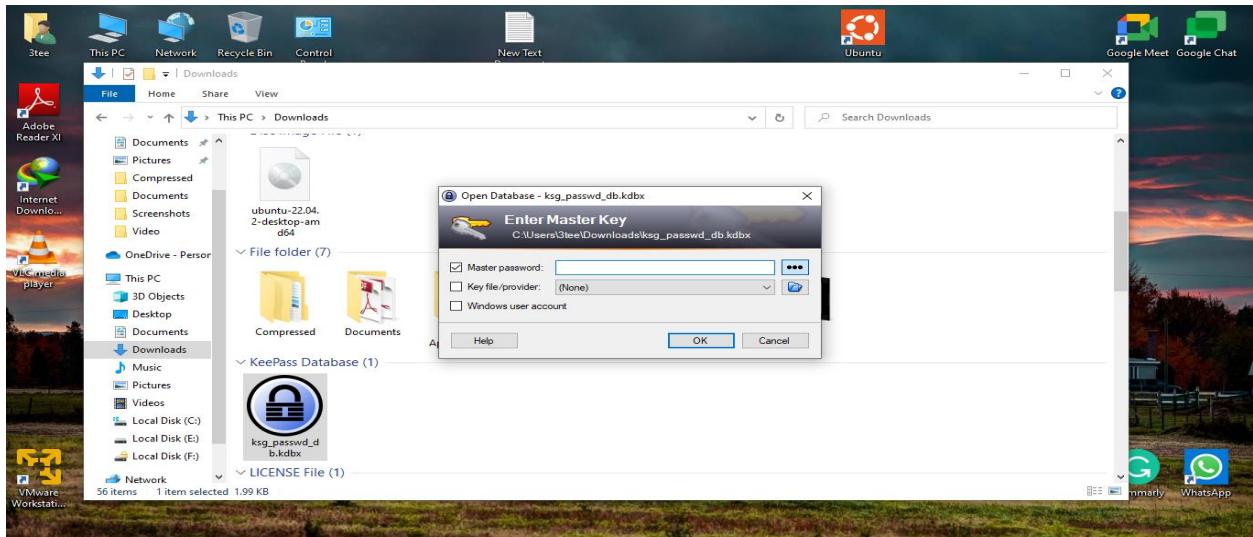
What is a .kdbx file? How to crack such a .kdbx file?

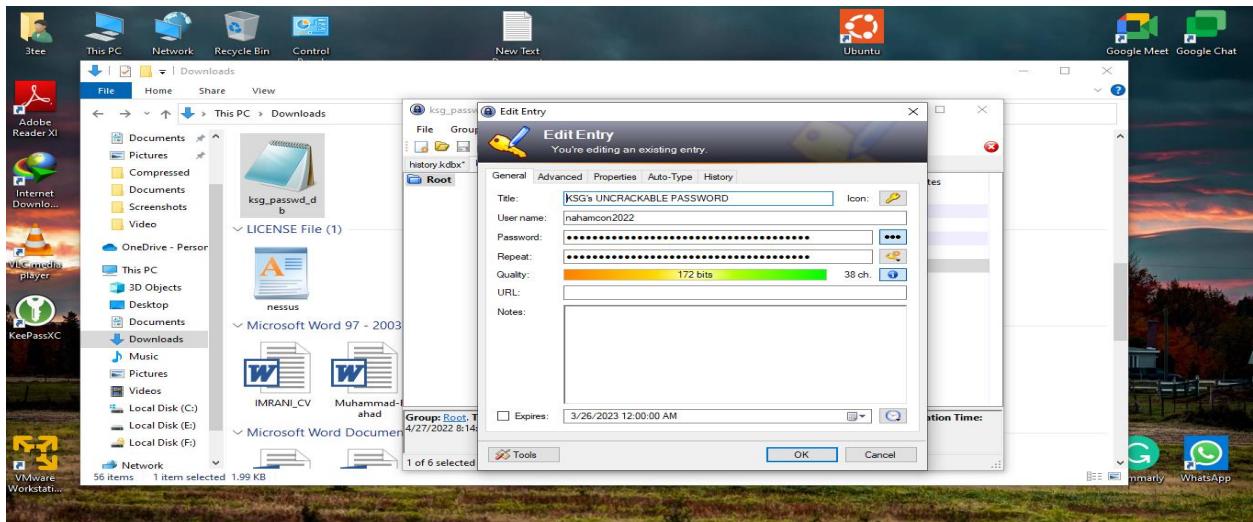
The screenshot shows a Google search result for 'how to open .kdbx file'. The top result is a snippet from 'File Magic' explaining how to open .kdbx files using KeePass Password Database. Below the snippet is a link to 'KDBX Files: What It Is and How to Open It'. The search bar shows the query 'how to open .kdbx file'.

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

The screenshot shows a Windows File Explorer window. In the center, a KeePass setup window titled 'Setup - KeePass Password Safe 2.53.1' is displayed, showing the progress of the installation. The progress bar is at 100%, indicating the process is complete. The background shows a folder structure with various application icons like Zoom, Grammarly, and VirtualBox.

Portfolio Project Report-01





A screenshot of a Google Classroom assignment page. The assignment title is 'Cyber Security Cohort 6'. The assignment details a series of tasks related to a company ex-employee's mistakes. Task 10 asks for the name of a place where a plane landed, with a link to a Miro board. Below the assignment, a KeePassXC 'Edit Entry' window is overlaid, showing the same password as the one in the assignment. The desktop background is the same as the top screenshot.

Flag is: 9a59bc85ebf02d5694d4b517143efba6

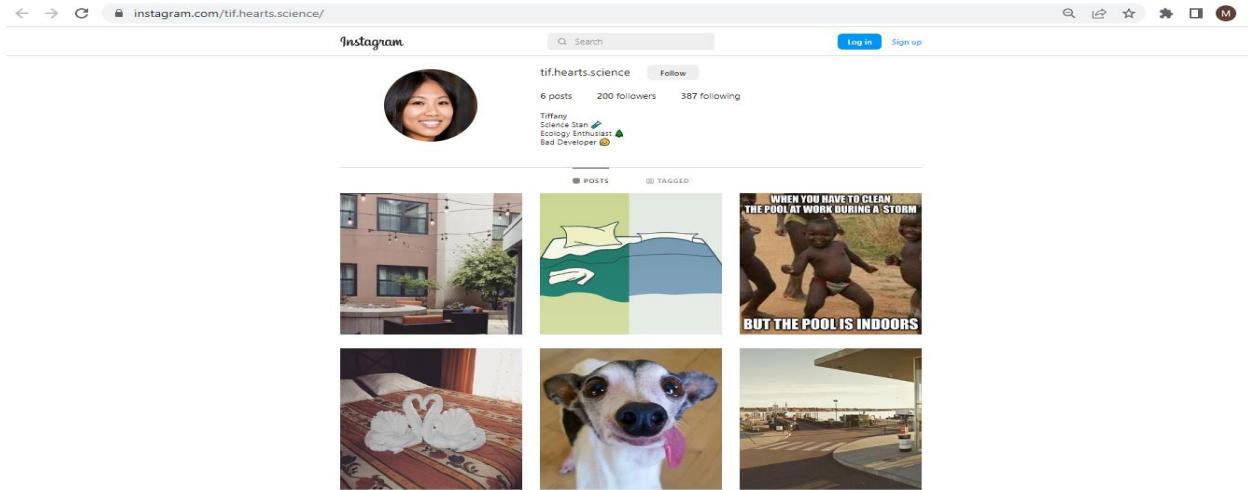
TASK 05: After all of the damage the ex-employees mistakes caused to the company, the Keeber Security Group is suing them for negligence! In order to file a proper lawsuit, we need to know where they are so someone can go and serve them. Can you find the ex-employee's new workplace? Her Instagram profile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

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

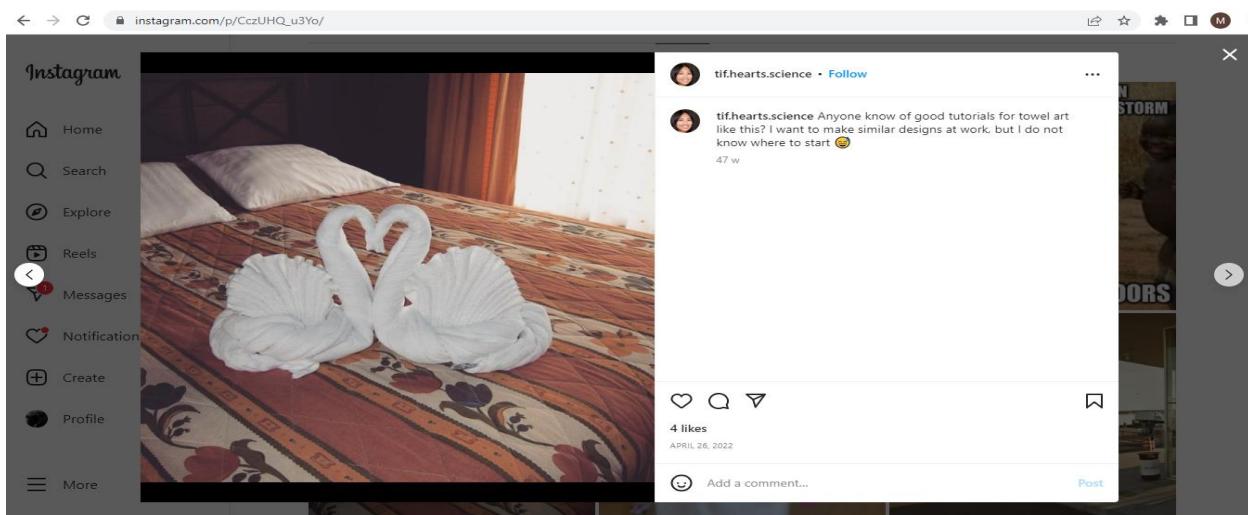
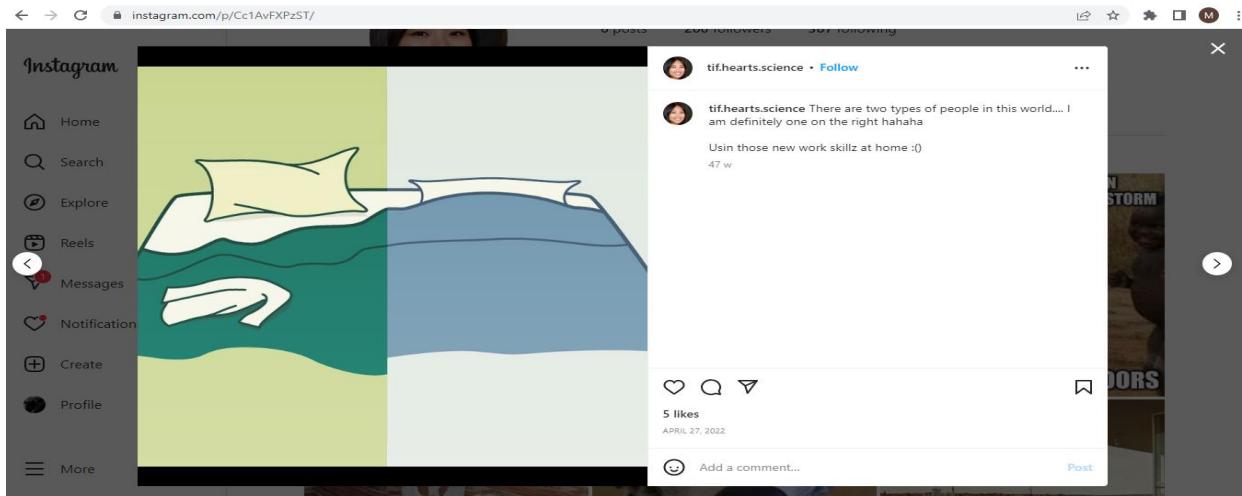
What is the name of her new work which is in the Maine area?

Answer:

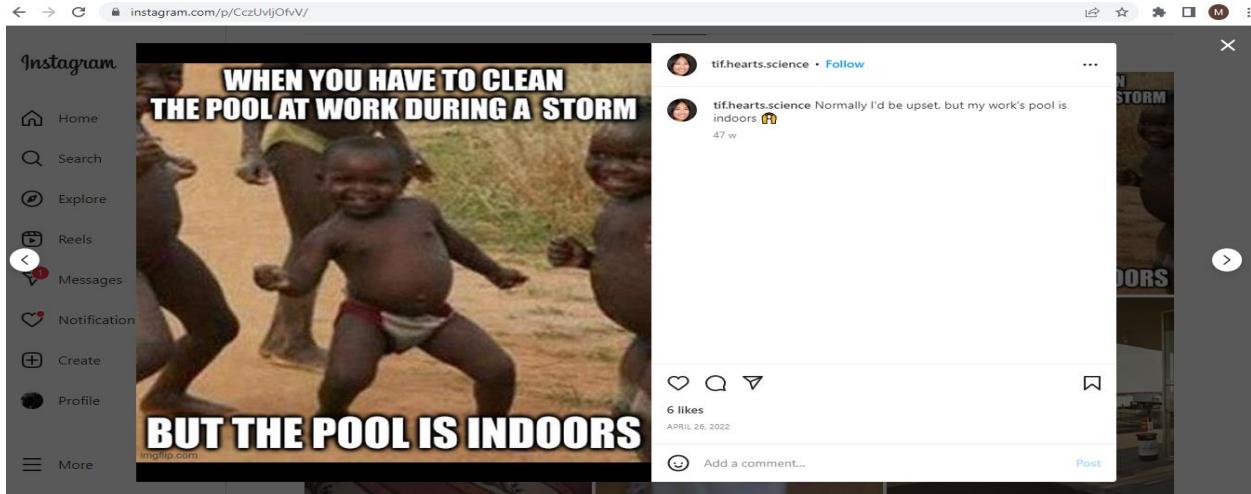
Tiffany Instagram account only contains 6 posts with some useful information.



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.

| | |
|--------------------------------------|--|
| Country Before statehood | United States Part of Massachusetts (District of Maine) |
| Admitted to the Union | March 15, 1820 (23rd) |
| Capital | Augusta |
| Largest city | Portland |
| Largest county or equivalent | Cumberland |
| Largest metro and urban areas | Portland |
| Government | |
| • Governor | Janet Mills (D) |
| • Senate President | Troy Jackson (D) ^[nb 1] |
| Legislature | Maine Legislature |
| • Upper house | Senate |
| • Lower house | House of Representatives |
| Judiciary | Maine Supreme Judicial Court |
| U.S. senators | Susan Collins (R) Angus King (I) |
| U.S. House delegation | 1. Chellie Pingree (D) 2. Jared Golden (D) (list) |
| Area | |
| • Total | 35,385 sq mi (91,646 km ²) |
| • Land | 30,862 sq mi (80,005 km ²) |
| • Water | 4,523 sq mi (11,724 km ²) |

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

The screenshot shows the Yelp search interface for Portland, ME. The search term is "Hotels and Resorts". The results page displays three hotel entries:

- 23. Blind Tiger - Portland**: Bed & Breakfast, West End. Status: Closed until Midnight. Review: "I can't wait to check out more of Lark Hotels properties." [more](#)
- 24. Residence Inn by Marriott Portland Downtown/Waterfront**: Hotels, \$\$, East Bayside. Status: Closed until Midnight. Review: "The fact that a luxury hotel would even provide a room like this is ridiculous." [more](#)
- 25. Chestnut Hill Bed & Breakfast**: Hotels, \$\$. Status: Open.

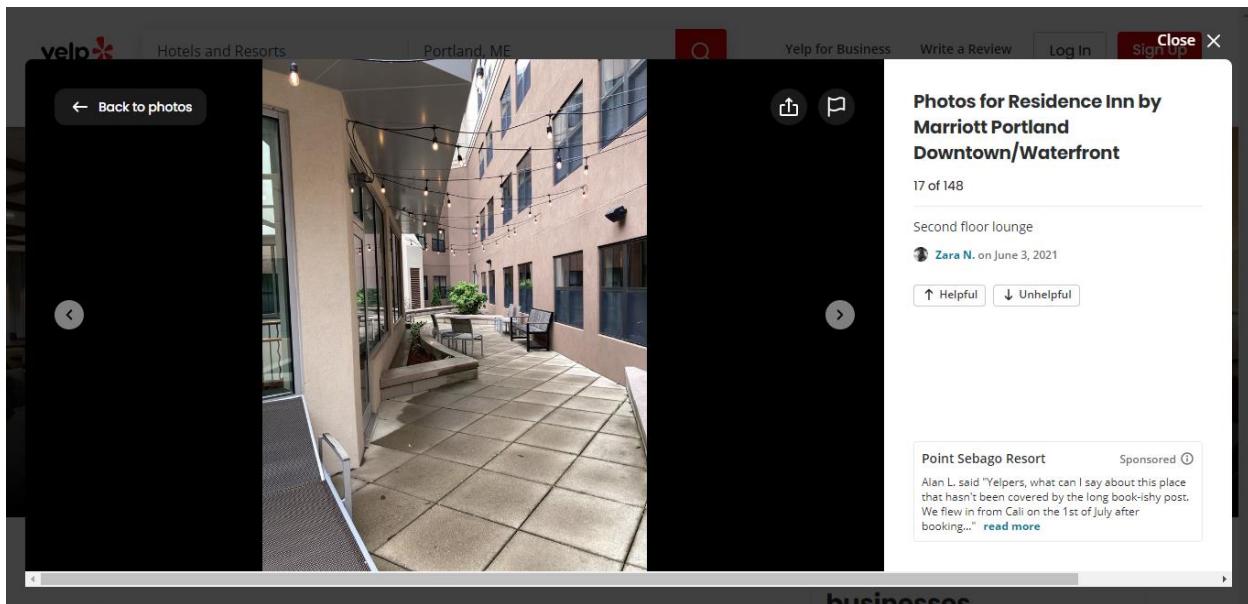
On the right, there is a map of the Portland area with numbered pins indicating various locations. A callout box on the map says: "Expand the map to get a better look at the businesses near you."

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

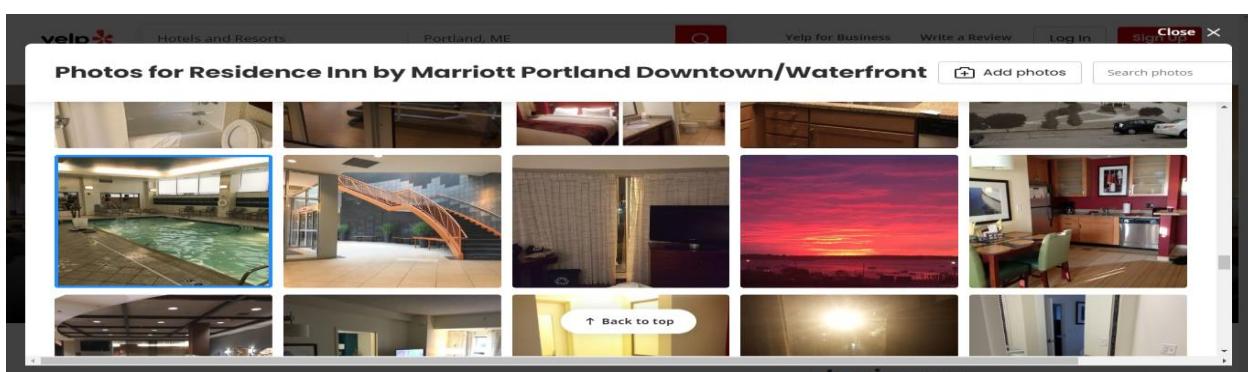
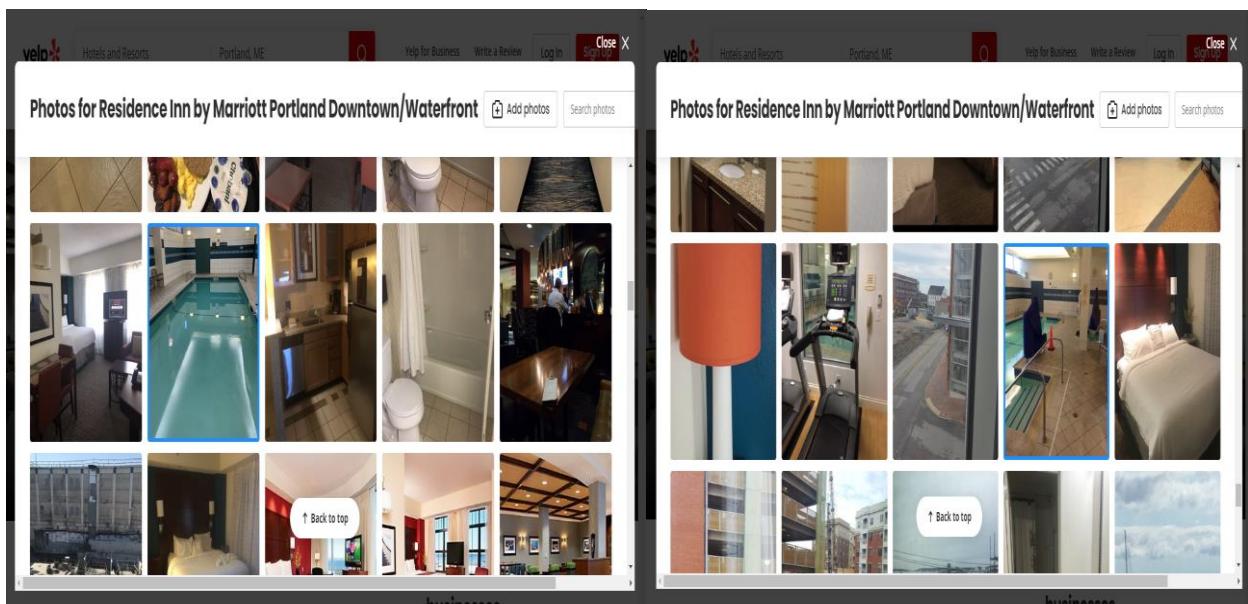
The image shows a side-by-side comparison between an Instagram post and a Yelp photo of the same hotel's outdoor lounge area.

Instagram Post (Left): A screenshot of an Instagram profile. The post shows a courtyard with a circular fire pit, string lights, and lounge chairs. The caption reads: "I'm glad I got to join the team this time of year. I set up all the lights in the courtyard, and it looks beautiful!" It has 10 likes and was posted on April 27, 2022. The caption ends with "47m".

Yelp Photo (Right): A screenshot of a Yelp photo gallery. The photo shows a similar outdoor lounge area with a circular fire pit, string lights, and lounge chairs. The caption reads: "Photos for Residence Inn by Marriott Portland Downtown/Waterfront". Below the photo, it says "Second floor lounge". The photo was taken by "Zara N. on June 3, 2021".



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.

P.R.
Marietta, GA
1 friend
759 reviews
18 photos

Tiffany D.
Portland, ME
0 friends
1 review

homophobic and totally unhelpful. Beautiful room but would NOT stay here again.

★★★★★ 7/25/2021
Clean room and friendly staff. Stayed with our dog. Parking is next door. So you'll want to drop your stuff off and then park.

★★★★★ 4/27/2022
Portland is such a great city with a hometown feel to it. Behind the scenes, there is a lot of attention to detail put into ensuring the best guest experiences. Rooms are cleaned thoroughly between stays, and covid protocol is followed well. This is a hotel I would want to stay at while traveling.

P.S. flag(0d701794c993c5eb3ba9becfb046034)

1 Review Removed for Violating our Terms of Service

Tran D.
Portland, ME
0 friends
0 reviews

★★★★★ 12/18/2016
This review has been removed for violating our Terms of Service

Page 1 of 1

« Back to Residence Inn by Marriott Portland Downtown/Waterfront

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.

| | | | |
|-------------------|--------------------------|------------------|---------------------------------------|
| 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: | (IA819-11) Data Centers |

Ping Traceroute

The screenshot shows a web page from iptrackeronline.com. At the top, the URL is iptrackeronline.com/index.php?ip_address=54.239.28.85&k=. Below the header, there are two main sections: "Information About IP Address 54.239.28.85" and "Copy and Paste IP Address Information".

Information About IP Address 54.239.28.85

| Provider Info | Country Info | Time Info |
|---------------------------------|-------------------------------------|-------------------------------|
| IPv4 Address 54.239.28.85 | Country United States of America | Continent North America |
| Hostname 54.239.28.85 | Region (code) Virginia | Latitude 39.039474 |
| Organization amazon.com | City Ashburn | Longitude -77.491806 |
| ISP Amazon Technologies Inc. | Area Code 703 | Time Zone America/New_York |
| Flag USA | Postal Code 20146 | GMT Offset -05:00 |

Copy and Paste IP Address Information

Copy and Paste Analysis

ipTRACKERonline.com IP Address Summary Report
Originating IP: 54.239.28.85
Originating ISP: amazon.com
City: Ashburn
Country of Origin: United States of America
* For a complete report on this IP address goto ipTRACKERonline

[Copy to Clipboard](#)

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.

track-trace.com/container

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

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

Select company

Depot & Repair

Unit specification

Login

User name:

Password:

Login

[Forgot login?](#)

[Register new login](#)

Language:

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 |
| Current status : | Out of stock | Max Gross Weight : | 30,480 kg |
| Last depot : | CARU Rotterdam, NLRTMCARA | Tare : | 3,720 kg |
| Locate : | Track on Google Maps | Payload : | 26,760 kg |
| Booking number : | SO 2224747 | CSC Number : | FBV854404 |
| Date out : | 04-04-2017 | | |

Attachments

| | | |
|--|--------------------------------------|--|
| Payload: 27000 kgs CSC-number: NL-LR 70003-03/07 | | |
| Identification | Date of Manufacture | Expiring date |
| LGEU 441697-3 | 07/2004 | 04/2018 |
| Original Rotterdam | 1 st copy LR Rotterdam | 2 nd copy CONTAINERS WITNESSED <input type="checkbox"/> REVIEWED <input checked="" type="checkbox"/> D. van Spankeren 19 April 2017 D. VAN SPANKEREN RE 10204344 Rotterdam Surveyor to Lloyd's Register Nederland B.V. Lloyd's Register Verification Limited A subsidiary of Lloyd's Register Group Limited |
| | Issuing office and control number | Signature |
| | Is now | |

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

The screenshot shows the homepage of imagetotext.info. The main title is "Image To Text" and "Image to Text Converter". Below the title, there is a sub-instruction: "We present an online OCR (Optical Character Recognition) service to extract text from image. Upload photo to our image to text converter, click on submit and get your text file instantly." A large text area displays the extracted text from an uploaded image. To the right, there is a "Premium" offer box for \$11.99, which includes 50 images at once, 10,000 images monthly, image size up to 10 MB, no ads, and 3X faster processing. At the bottom, there are buttons for "Copy To Clipboard" and "Download Text File".

Download text file.

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

Dhaka, Bangladesh.

The screenshot shows a Google search results page for the query "hindi file to english converter online free". The top result is "Online Doc Translator" with a link to <https://www.onlinedoctranslator.com>. Below it is "Translate documents from Hindi to English - DocTranslator", which is described as instantly translating documents from Hindi to English. The next result is "Free Online Translator - Preserves your document's layout ...", which translates office documents like PDF, Word, Excel, PowerPoint, OpenOffice, etc., into multiple languages while preserving layout. The third result is "Translate from Hindi to English - GroupDocs Apps", which translates texts and documents in almost any format from Hindi to English. The bottom of the page shows a snippet of a document titled "Mallika Tailors and Cloth Store" with details about their products and services.

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.

A screenshot of the Google Lens interface. On the left, there is a dark overlay with a white rectangular frame containing a portion of the white hatchback image. Below this frame are three buttons: "Search", "Text", and "Translate". To the right of the image, there is a grid of search results. The first result shows two small images: one of a white hatchback labeled "Dacia Logan" and another of a white van labeled "Citroen Berlingo". Below this, there is a larger image of a white hatchback labeled "Dacia Logan Subcompact car". Further down, there are two more images of different cars labeled "Visual matches". At the bottom of the interface, there is a feedback section with a "Did you find these results useful?" checkbox, and "Yes" and "No" buttons.

Just google similar number plate is registered in Morocco.

Searching website: worldlicenseplates.com

Not secure | worldlicenseplates.com

Home Index What's New? A B C D E F G H I J K L M N O P Q R S T U V W Y Z

 MOROCCO

Home > Africa > Morocco

Private/Passenger
More Moroccan Plates
United States Forces
Country Information
Credits

Private/Passenger


1956 Series, 71 = Agadir


1956 Series, 39 = Casablanca


1983, 4 = Marrakesh

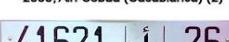

2000, 11 = Al Fida (Casablanca)


2000, 1 = Rabat


2000, 6 = Casablanca


2000, Al-Sebaa (Casablanca) (2)


2000, 11 = Al Fida (Casablanca)


2000, 26 = Marrakesh (2)


2000, 33 = Agadir (2)


2000, 26 = Marrakesh (2)


2000, 1 = Rabat (2)

worldlicenseplates.com September 2018

Not secure | worldlicenseplates.com

Home Index What's New? A B C D E F G H I J K L M N O P Q R S T U V W Y Z


1956 - 1975, Diplomatic Corps (1)

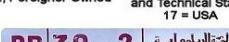

1956 - 1975, Consular Corps (1)


1975 - 1978, Diplomatic Corps, 29 = Italy


1972, Foreigner Owned


1978 - 1990, Admin. and Technical Staff, 17 = USA


1978 - 1990, Administrative and Technical Staff, 42 = Netherlands


1992 Series, Diplomatic Corps, 2 = Germany


Army


Navy


Diplomatic Corps, 8 = Bulgaria


International Organization (OI)

Show all

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.

Google US Airways N106US

About 13,200 results (0.33 seconds)

Planespotters.net https://www.planespotters.net/airframe/n106us

N106US US Airways Airbus A320-214 - Planespotters.net
 17-Aug-2022 — N106US US Airways Airbus A320-214 ; Manufacturer Serial Number (MSN) ; Aircraft Type. Built as; Airbus A320-214 ; First Flight. 15 Jun 1999 ; Age.

People also search for
 n106us flight history us airways fleet
 us airways 1549 asn flight 1549 passengers sue
 us airways flight 1549 us airways flight 1549 movie

People also ask :
 What happened to N106US?
 As of 2017, 70,000 birds had been intentionally killed in New York City as a result of the ditching. N106US, the accident aircraft, was purchased by the **Carolina Aviation Museum** in Charlotte, North Carolina, where it (and the plane's engines) were put on display.

PLANESPOTTERS.NET

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-WVII |
| Production Site | France Toulouse (TLS) |
| Airframe Status | Preserved Charlotte, North Carolina, United States 10 Jun 2011 at the Carolina Aviation Museum |

Last updated on Aug 17, 2022 Correct Information

OPERATOR HISTORY

| REG | AIRCRAFT TYPE | AIRLINE | DELIVERED | CONFIG | ENGINES | FLEET NUMBER | REMARKS |
|--------|-----------------|------------|-----------|---------|---------|--------------|---|
| N106US | Airbus A320-200 | US Airways | Aug 1999 | C12Y13B | 2x CFMI | 106 | dbr 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 |

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.