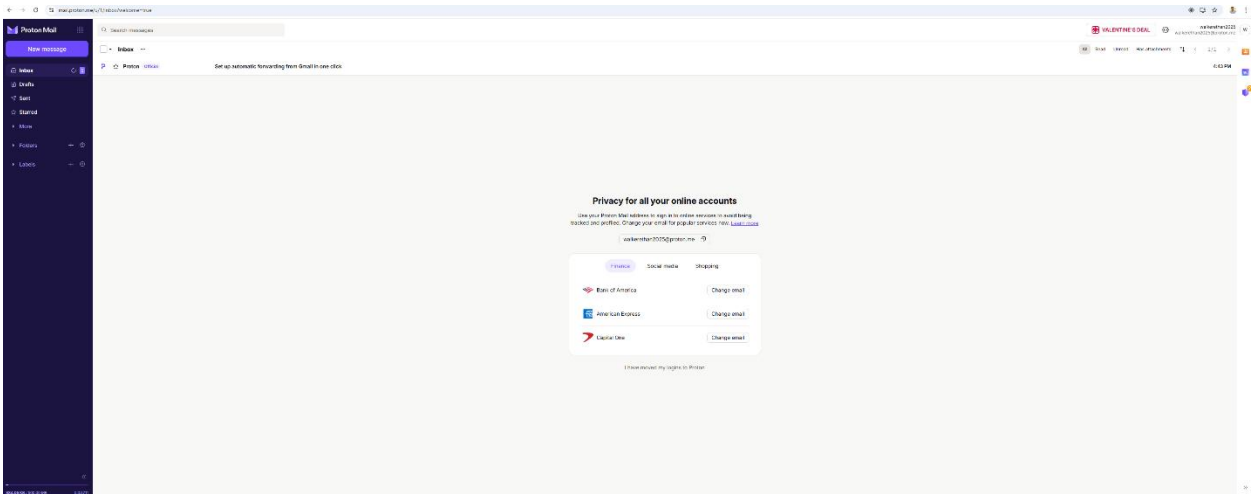
OSINT Sock Puppet Account Investigation Report

Creation of Sock Puppet Account

Sock Puppet Account Creation To conduct OSINT research, I created a sock puppet account following the techniques outlined in r/OSINT. The goal was to fabricate an online persona and use various OSINT tools to determine the extent of discoverable personal information.

- **Email Account**: Created a ProtonMail account for anonymity.
- **Fake Identity**: Used a randomly generated identity from Fake Name Generator.

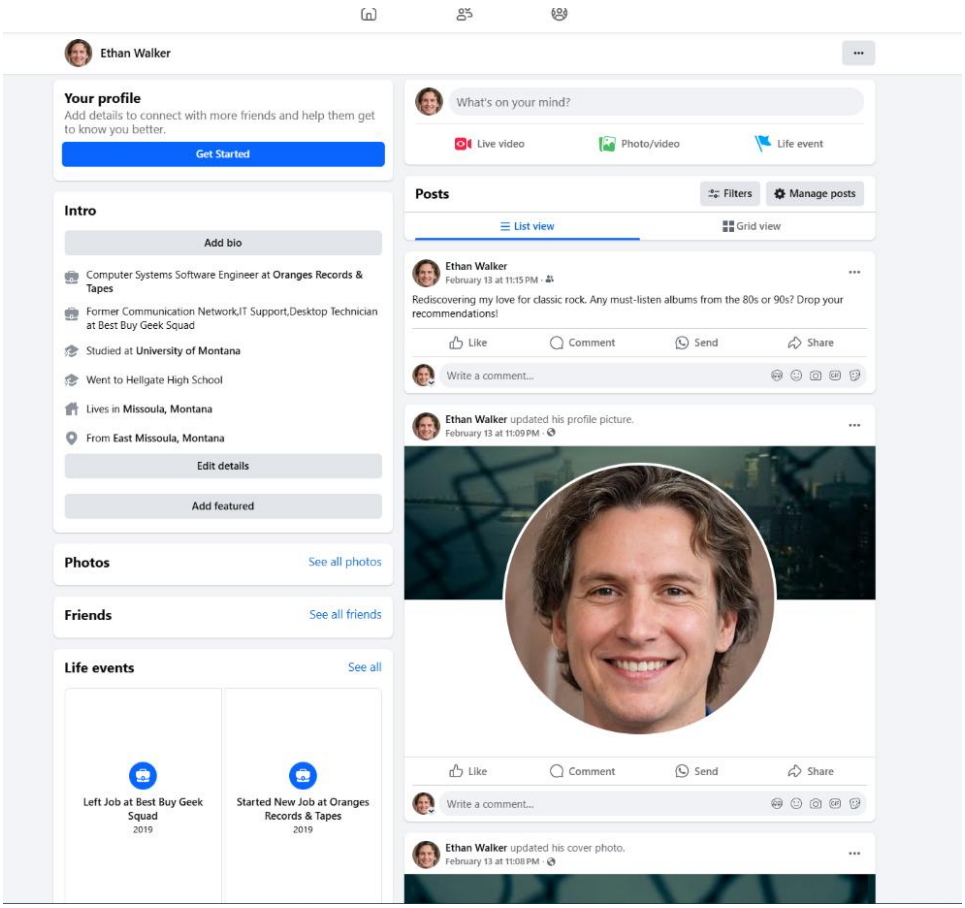
  Name: Ethan Walker
- **Profile Picture**: Selected from ThisPersonDoesNotExist.com to ensure uniqueness.
- **Temporary Phone Number**: Used 6463979486 for verification.
- **Social Media Account**: Created a Facebook account under the name "Michael Roberts" with additional fabricated details.



ProtonMail account

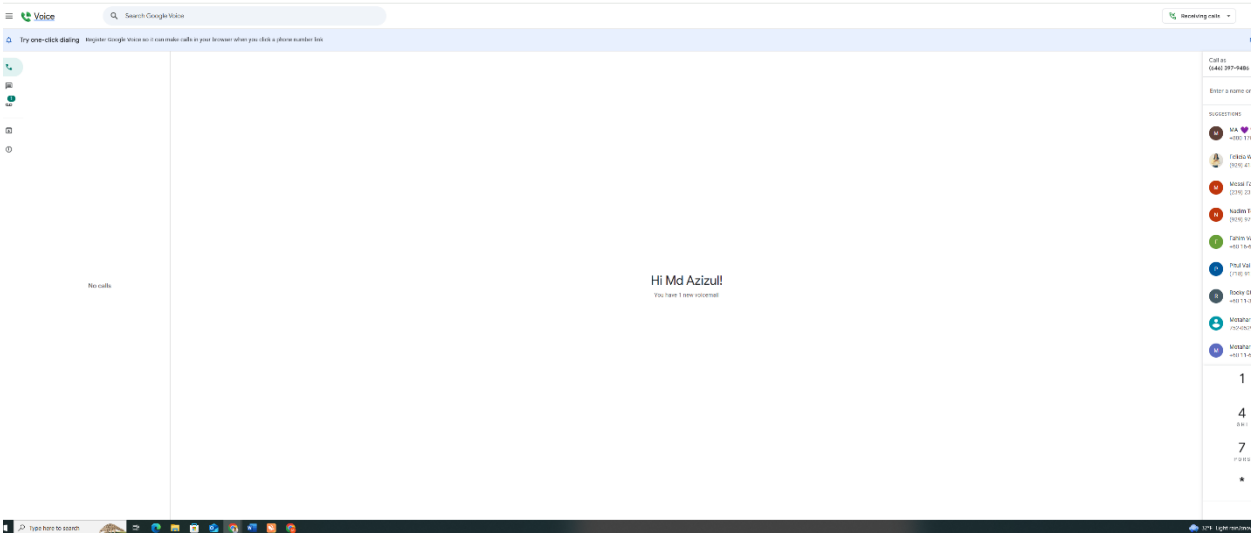
Data Points Used for Research

The OSINT research utilized various data points to analyze the sock puppet account's digital footprint. The fake identity was created using the name Ethan Walker from Fake Name Generator, with an AI-generated profile picture from **ThisPersonDoesNotExist.com** to ensure anonymity. The Facebook profile included realistic employment details, listing Oranges Records & Tapes as the current workplace and Best Buy Geek Squad as a former employer, along with an educational history at University of Montana and Hellgate High School. The location was set to Missoula, Montana, with a hometown of East Missoula, Montana, further strengthening the persona's credibility.



Facebook

A **ProtonMail** account was registered, using a temporary phone number **(6463979486)** for verification. OSINT techniques such as reverse image searches, username and email lookups, social media footprint analysis, and metadata extraction were applied to evaluate how much



Google Voice

information could be traced back to the fake persona. This research demonstrated the effectiveness of OSINT in gathering publicly available data while highlighting the importance of digital privacy.

Data Points Used for OSINT Investigation

To analyze my own digital footprint, I used the following personal data points:

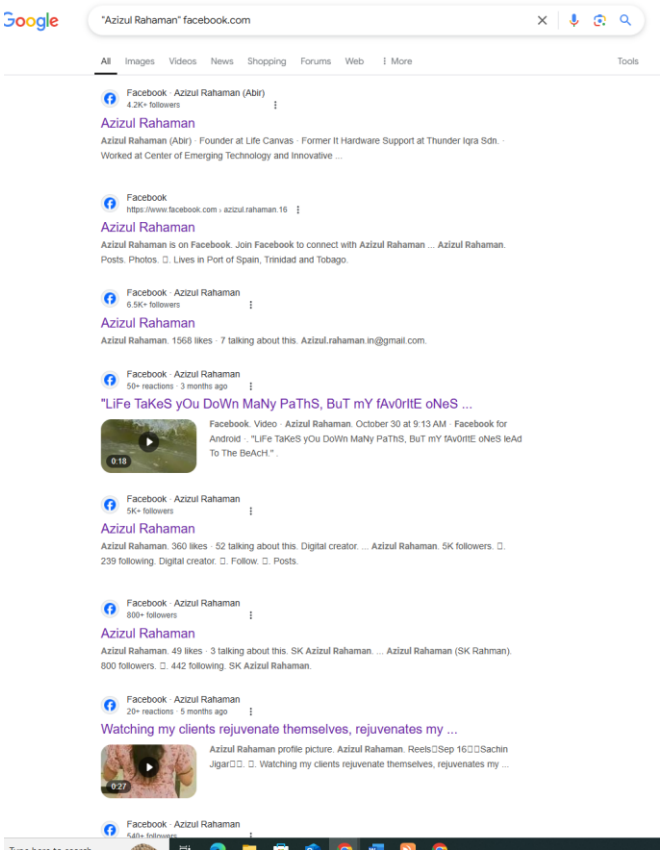
- **Name:** Azizul Rahaman (Real)
- **Alias Used for OSINT:** Ethan Walker
- **University:** Touro University, New York
- **Employers:** Previous job roles at Internship in Web Development, IT Support, and Assistant IT Executive.
- **Profile and Additional Pictures:** Selected pictures to blend in with the fabricated identity.

Findings & Privacy Risks

Google Dorking (Information Discovered)

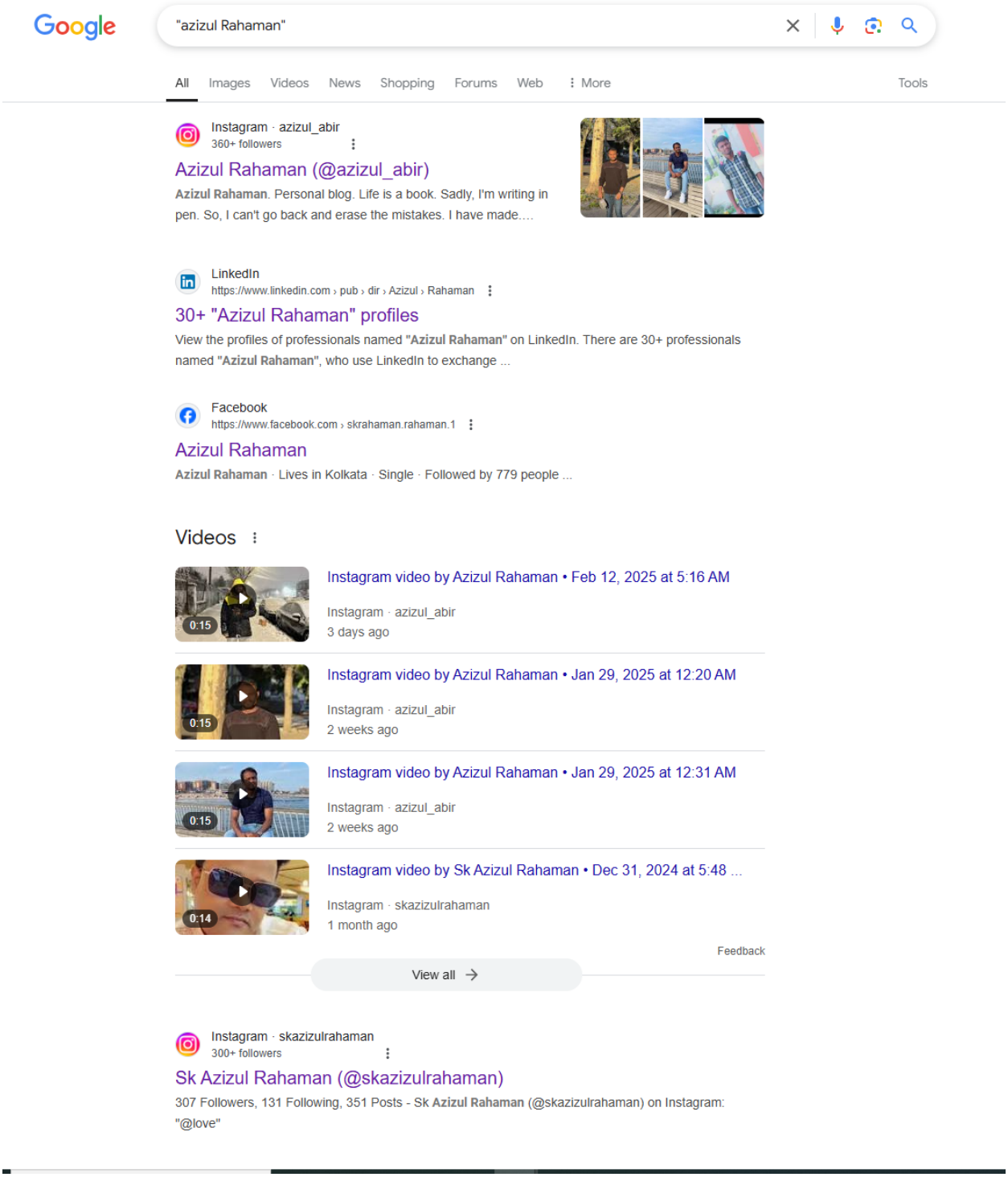
Facebook

My Facebook profile, **Azizul Rahaman (Abir)**, is publicly indexed on Google. This means anyone can access my basic information, follower count, and previous work experience without logging in.



Instagram

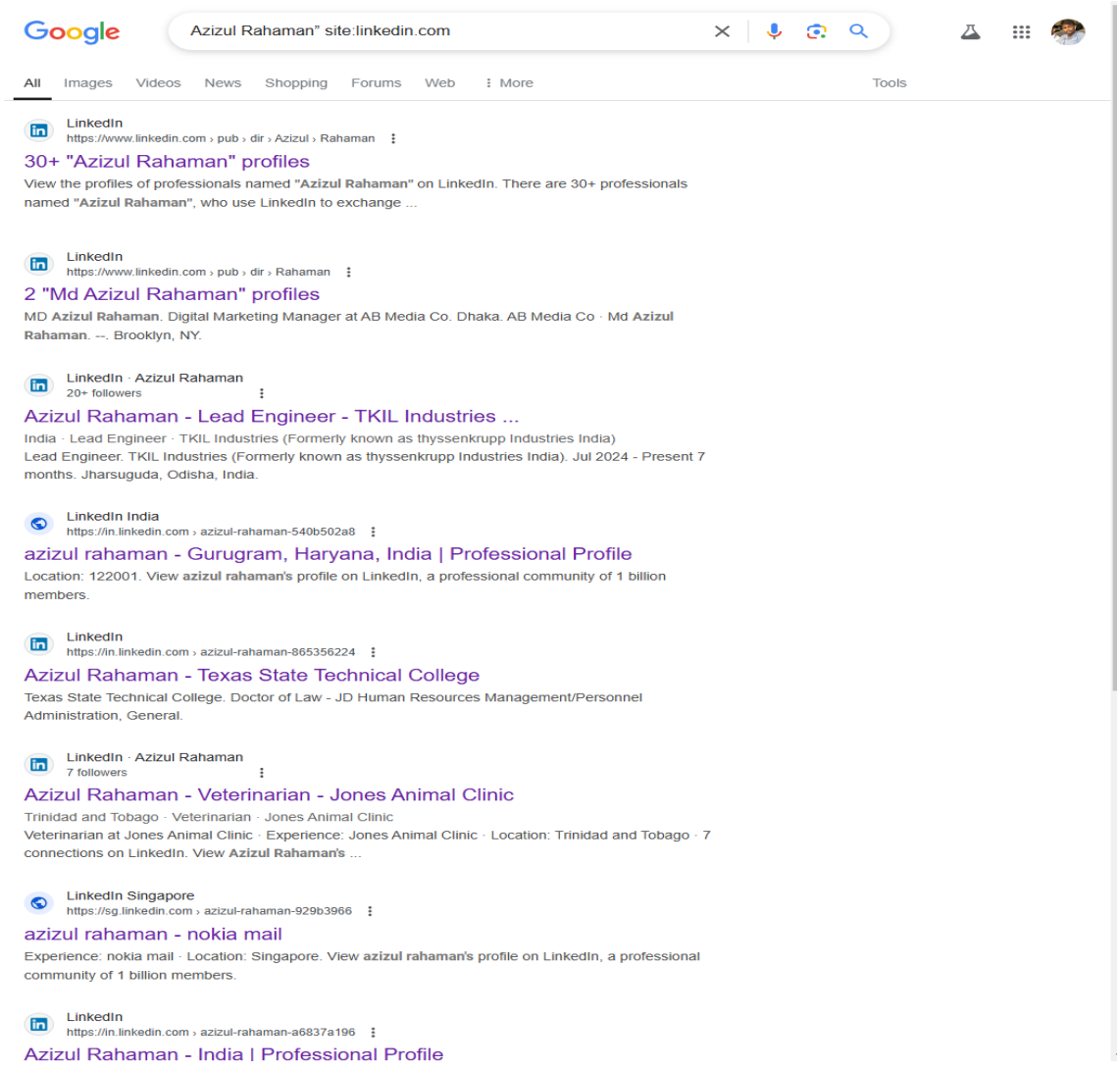
Instagram profile **(@azizul_abir)** appears at the top of the search results, displaying not only my profile but also multiple videos I have uploaded. This means that my Instagram activity, including posts and videos, is indexed by Google, making it easy for anyone searching my name to view your content without needing to visit my profile directly. Additionally, another Instagram profile, **@skazizulrahaman**, was found, which either belongs to me or to someone with a similar name.



LinkedIn

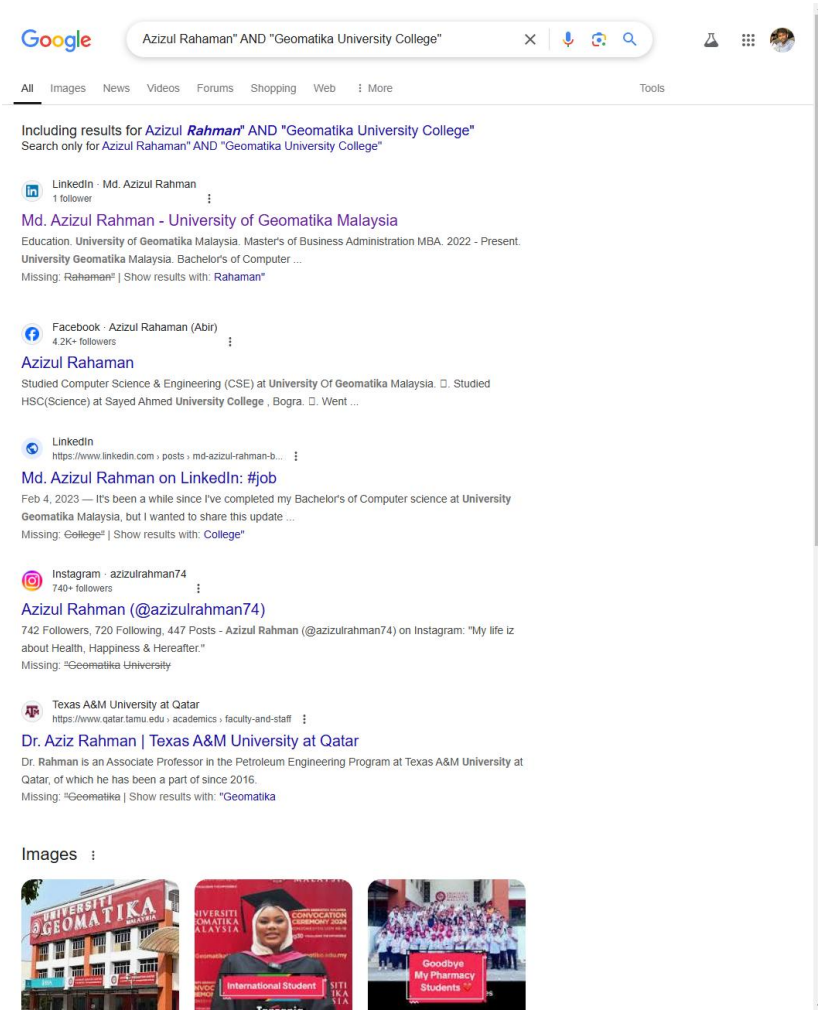
During my OSINT investigation, I attempted to locate my LinkedIn profile using Google Dorking techniques, specifically the query **"Azizul Rahaman" site:linkedin.com**. However, my profile did not

appear in the search results. This could be due to several factors, such as LinkedIn privacy settings restricting public visibility, my profile being relatively new and not yet indexed by Google, or Google's indexing delay. To address this, I can adjust my LinkedIn privacy settings to make my profile public, manually request indexing through Google Search Console, and use alternative search queries, including variations of my name and associated keywords like my university or field of study. This exercise highlights the importance of understanding online visibility and how OSINT techniques can be used to assess digital footprints.



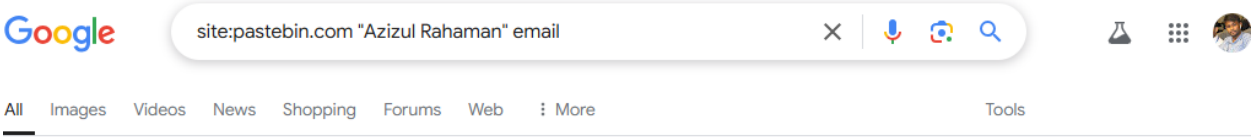
University Search

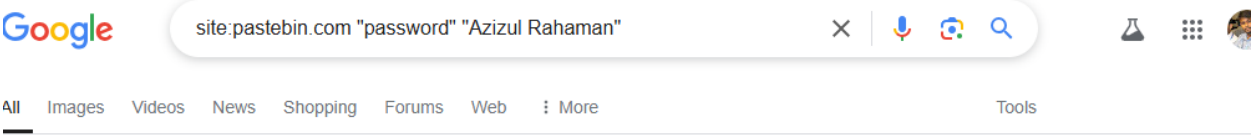
When searching for my name along with my previous university, **"Azizul Rahaman" AND "Geomatika University College,"** I was able to find multiple social media profiles, including Facebook, Instagram, and LinkedIn. This indicates that my educational background is a significant factor in my digital footprint, making it easier to trace my online presence. Interestingly, while my LinkedIn profile did not appear in a direct name search, it was visible when associated with my university, highlighting how different search queries yield different results. This exercise demonstrates the effectiveness of OSINT techniques in uncovering personal information through publicly available data. To enhance privacy, I could adjust my social media settings to limit public access to my profiles and review my LinkedIn visibility options.

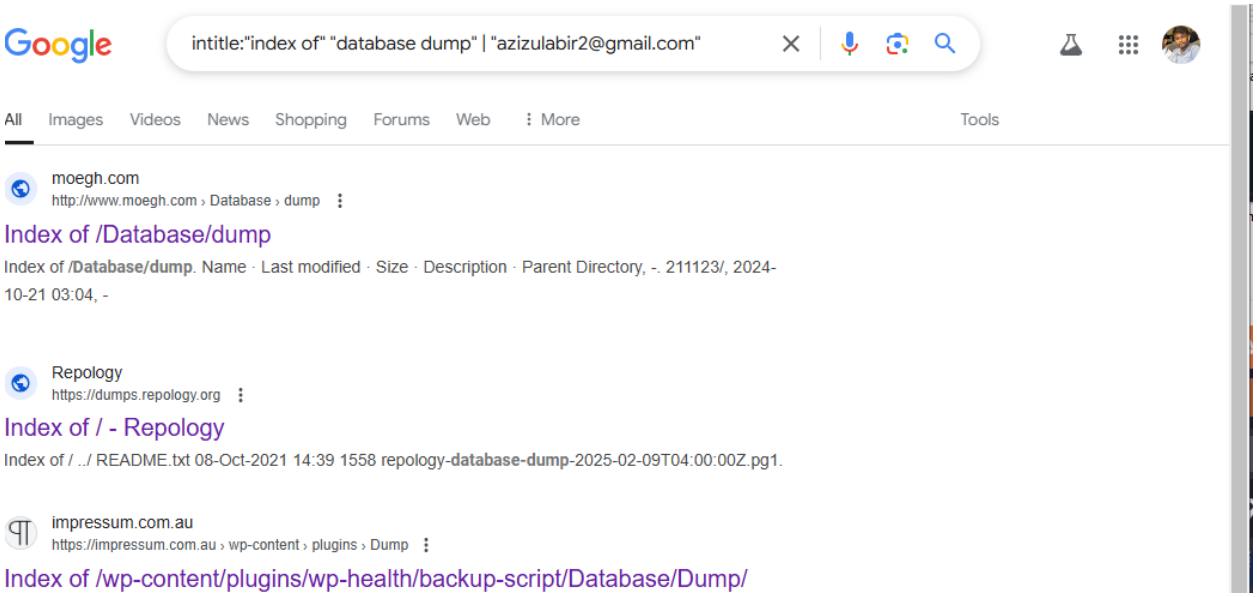


E-mail & Password

I used different search queries to check for leaked information. The searches on Pastebin for **"Azizul Rahaman" email and "password" "Azizul Rahaman"** returned no results, indicating that my email and credentials are not publicly listed on Pastebin. This is a positive sign, as Pastebin is often used for sharing leaked data. However, when searching for "index of" "database dump" | "email list", I found multiple publicly available email databases from various sources. While my specific email was not listed, this highlights how easily personal information can be exposed online. These results reinforce the importance of regularly monitoring data exposure, using strong passwords, and enabling two-factor authentication (2FA) to mitigate potential risks.

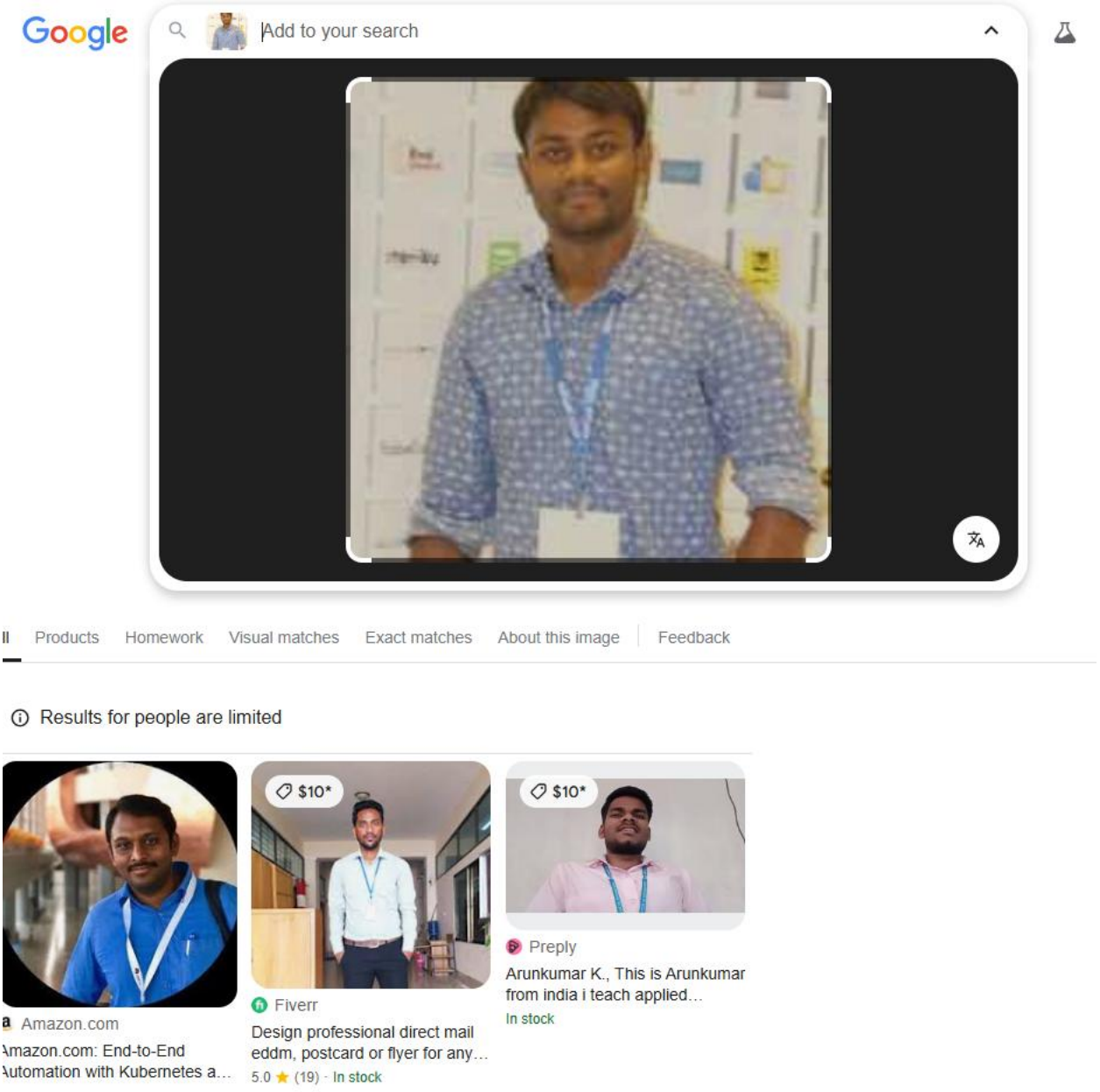






Google Reverse Image

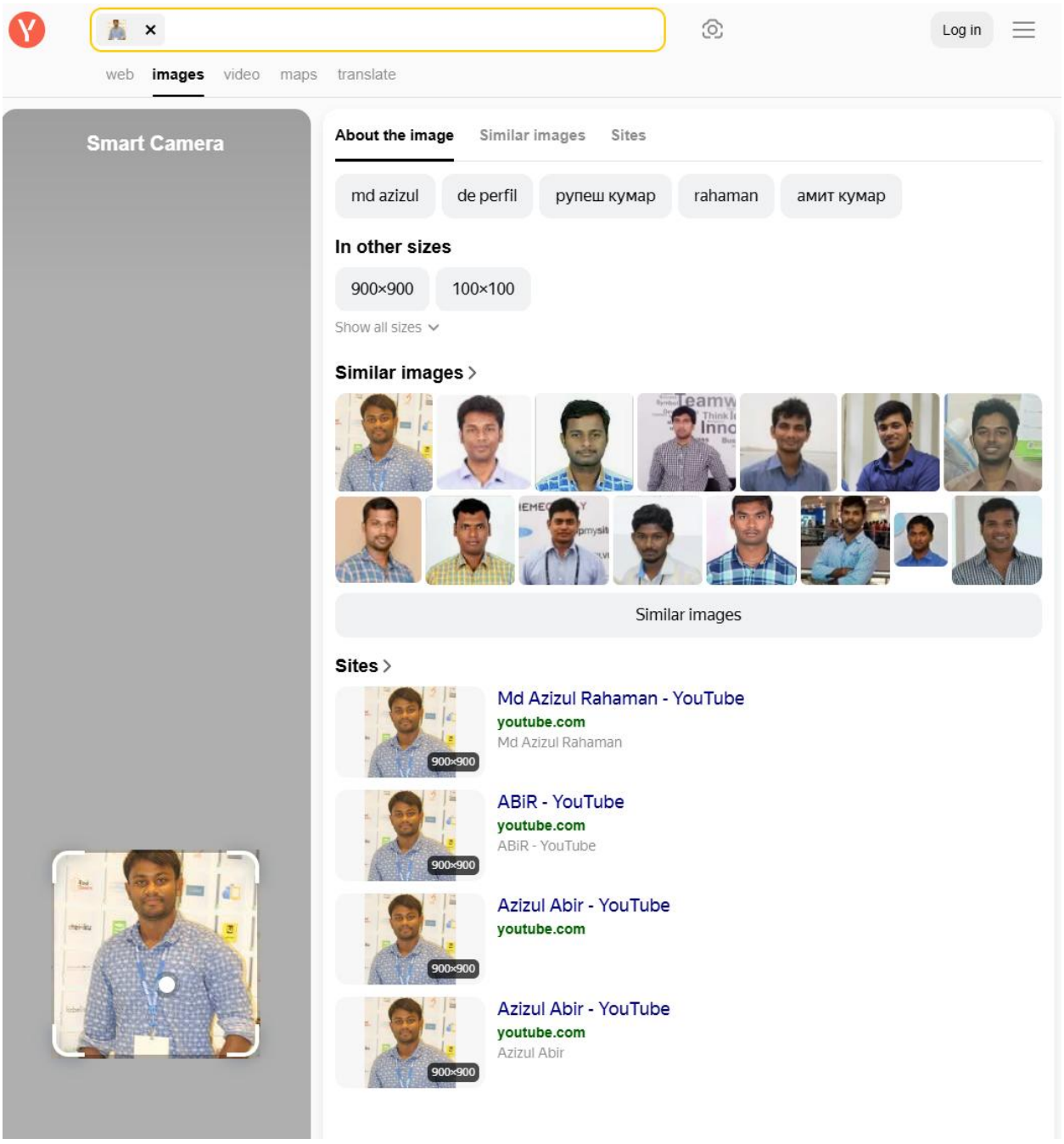
Google Reverse Image Search on my photo, I found that there were no exact matches, and the results for people were limited. This suggests that my image is not widely available or indexed in public databases, meaning my digital footprint in terms of images is relatively low. The search returned unrelated images of individuals with similar appearances, indicating that my photo is not directly linked to any major online profiles or websites. This is a positive outcome for privacy, as it implies that my personal photos are not easily traceable. To further test image exposure, I could use alternative reverse image search tools like **TinEye**, which are known for better facial recognition capabilities. If I want to maintain this level of privacy, I should be mindful of where I upload personal images and adjust privacy settings on social media platforms accordingly.



Yandex Reverse Image Search

I discovered that my image was linked to multiple YouTube accounts under different variations of my name, such as "Md Azizul Rahaman" and "Azizul Abir." Unlike Google, which did not return any exact matches, Yandex identified similar-looking individuals and found direct links to publicly available content featuring my image. This suggests that my digital footprint is more traceable on certain platforms, particularly YouTube. The presence of my image on public sites raises potential privacy concerns, as it indicates that

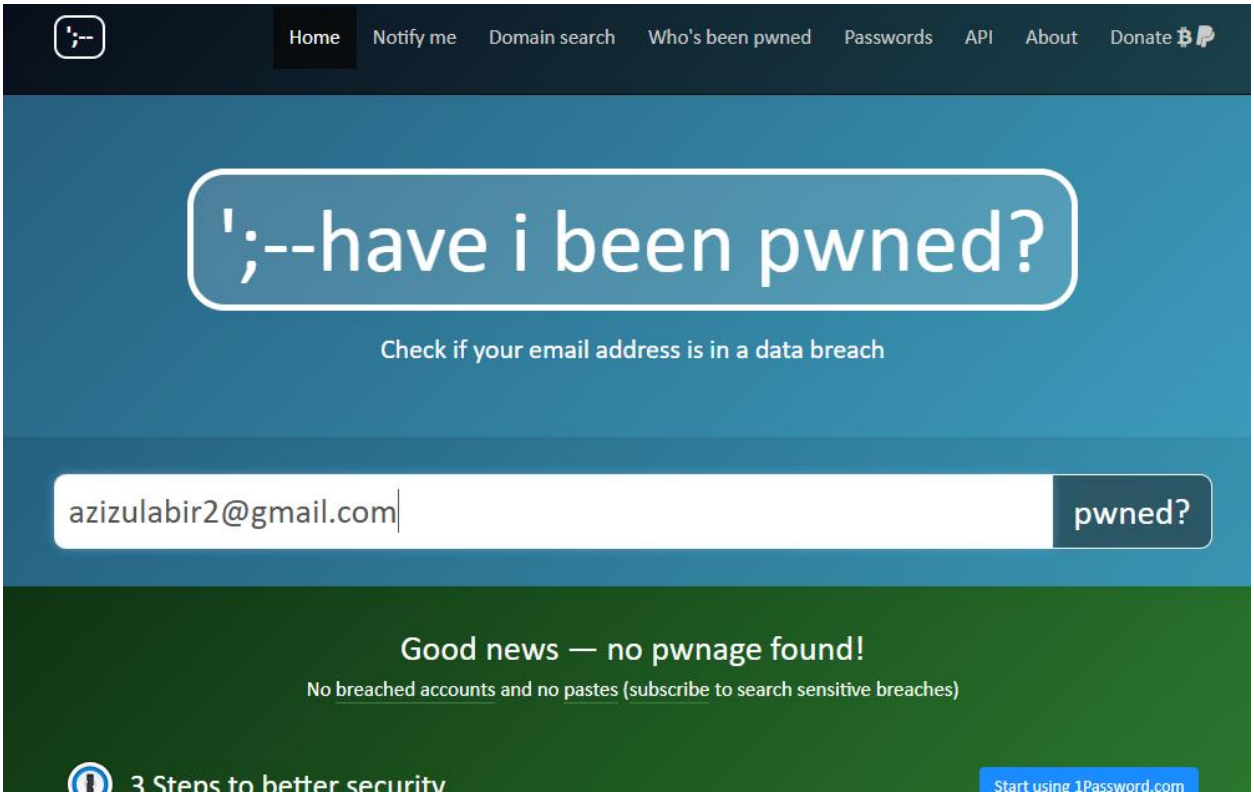
my photo is accessible through search engines. To mitigate this, I could review my YouTube privacy settings and restrict or remove any publicly available images associated with my account. This experiment highlights how different search engines use varying algorithms for image recognition, making it essential to conduct OSINT investigations across multiple platforms for a comprehensive assessment of online exposure.



Data Breach Search

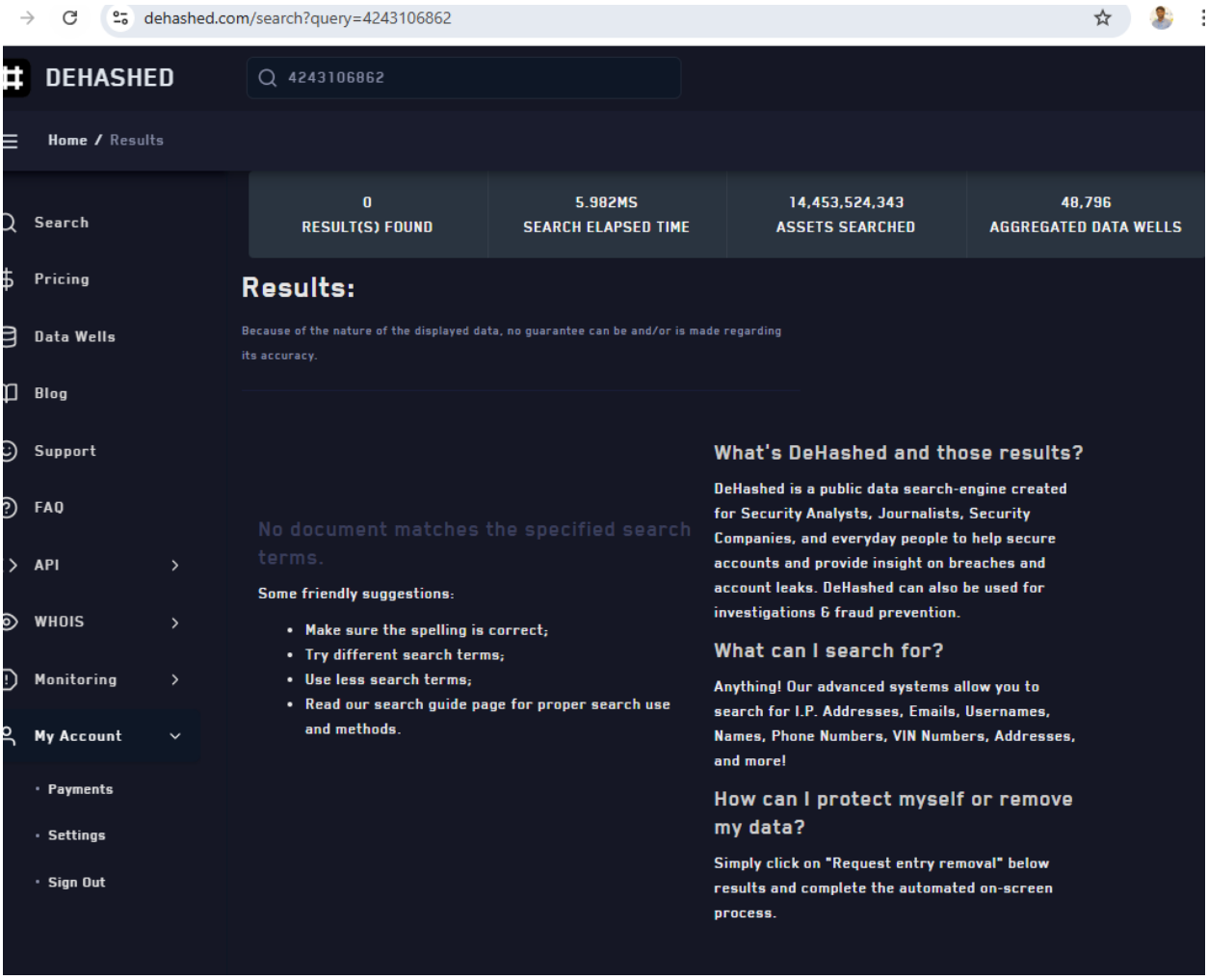
Have I Been Pwned Tool (OSINT Tool)

After performing a data breach search on Have I Been Pwned, I found that my email, has not been compromised in any known data breaches. The results indicate that my email has not been exposed in public databases or leaked in pastes, which is a positive sign for my online security. However, even though my email is currently safe, it is essential to follow best security practices to prevent future risks. Enabling two-factor authentication (2FA), using strong and unique passwords, and monitoring my email for any suspicious activity can help maintain a high level of security. Additionally, regularly checking for breaches is important, as new leaks can occur over time. This exercise highlights the importance of proactive cybersecurity measures in protecting personal data.

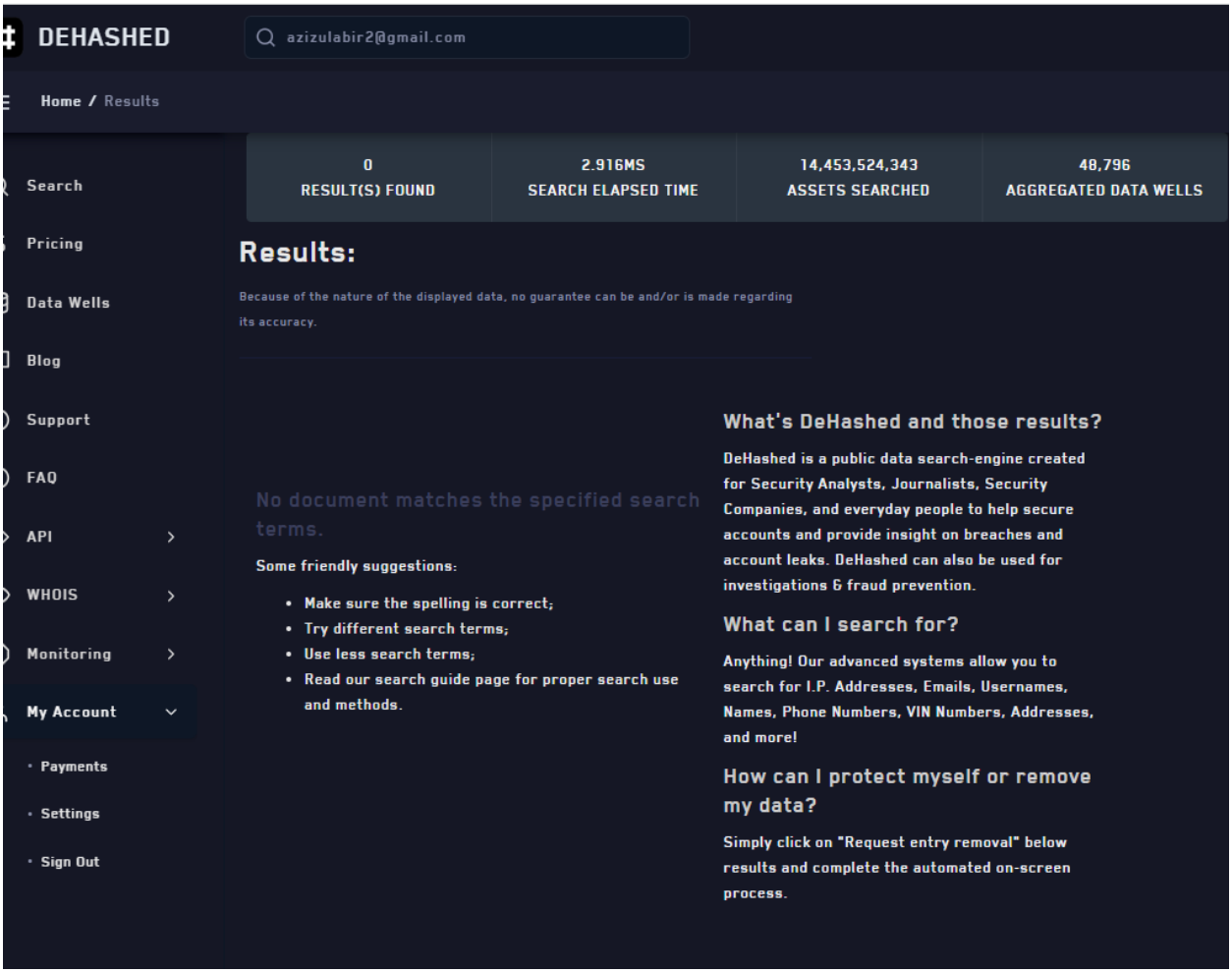


DeHashed (OSINT Tool)

After performing a search on DeHashed using the query **4243106862**, no results were found, indicating that the searched data does not appear in any known breached databases. This suggests that the provided information, whether a phone number, email, or another identifier, has not been exposed in public leaks or compromised datasets. While this is a positive result, it is essential to remain cautious and continue monitoring for potential breaches in the future. Security threats evolve over time, and new data breaches may occur, making regular checks important. Additionally, following best security practices, such as enabling two-factor authentication (2FA) and using unique, strong passwords, can further enhance protection against potential cyber risks.



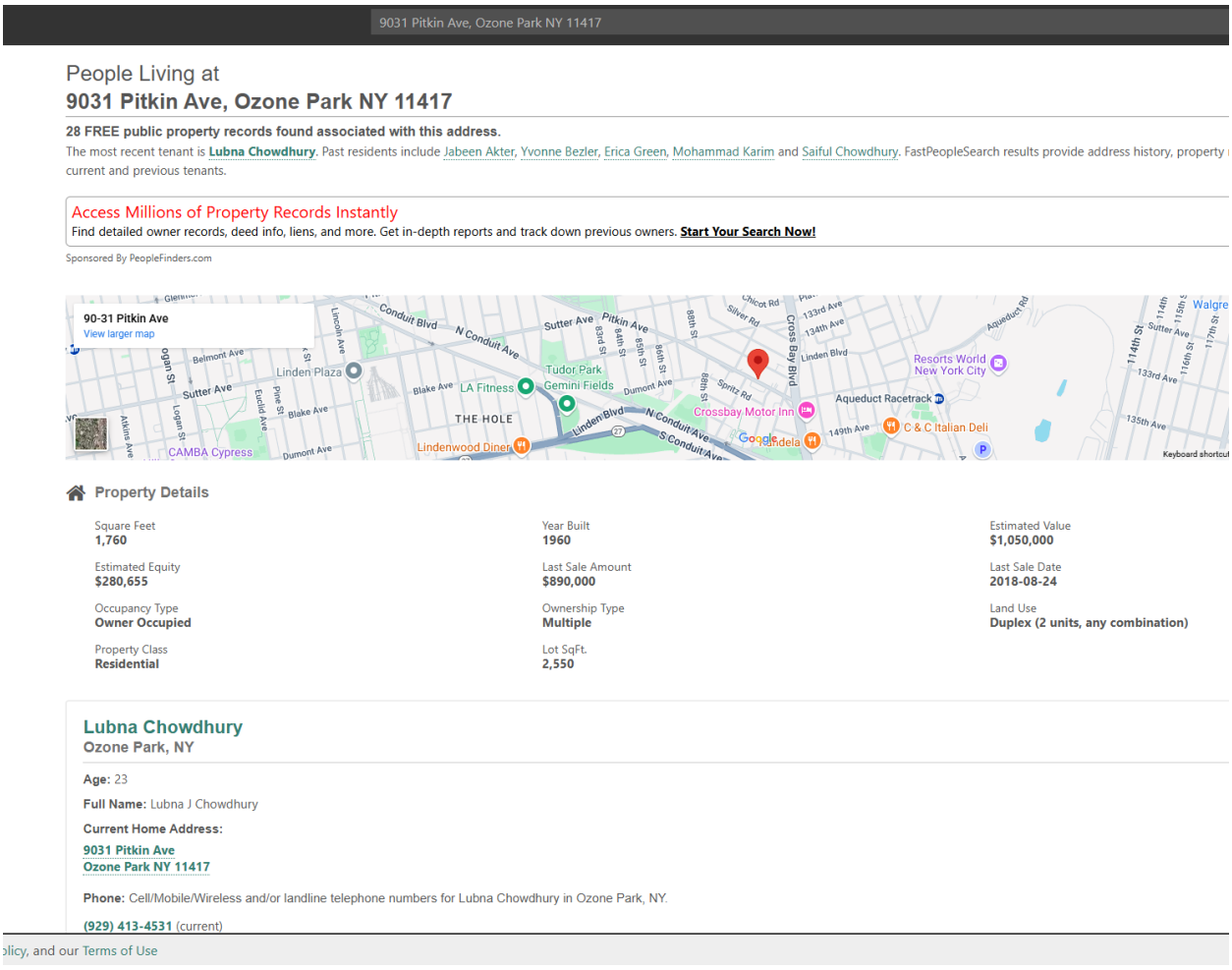
After performing a search for azizulabir2@gmail.com on DeHashed, no results were found, indicating that this email has not been exposed in any known data breaches or leaked databases. This is a positive outcome, suggesting that the email remains secure and has not been compromised in publicly available records. However, while no breaches were detected, it is still important to take precautionary measures, such as enabling two-factor authentication (2FA), using unique and strong passwords, and regularly monitoring for potential future leaks. Since data breaches occur frequently, continuous vigilance and periodic rechecking using platforms like DeHashed and Have I Been Pwned can help maintain a strong security posture.



People Search Engines

FastPeopleSearch (OSINT Tool)

I found that public records linked to various names and addresses were available. The search for **"Azizul Rahaman"** returned records of individuals in different locations, including Kalamazoo, MI, and Flagstaff, AZ, along with details such as current and past addresses, possible aliases, and associated phone numbers. Additionally, a search for a specific phone number, **424-310-6862**, did not return direct results but suggested checking other paid search services like Spokeo and BeenVerified. Another search for an address in **Ozone Park, NY**, provided property ownership details, resident names, and even phone numbers. This demonstrates how people search engines collect and publicly display addresses, property records, phone numbers, and potential relatives, making it easier to track individuals. These findings highlight the importance of privacy awareness and the need to regularly check and remove personal data from such databases to prevent unwanted exposure.



Top results found for phone:
424-310-6862

We could not find any results based on your search criteria:

Phone: 424-310-6862

Please review your search and try again.

Search Results for **424-310-6862**
Paid Results Sponsored by **BeenVerified.com**

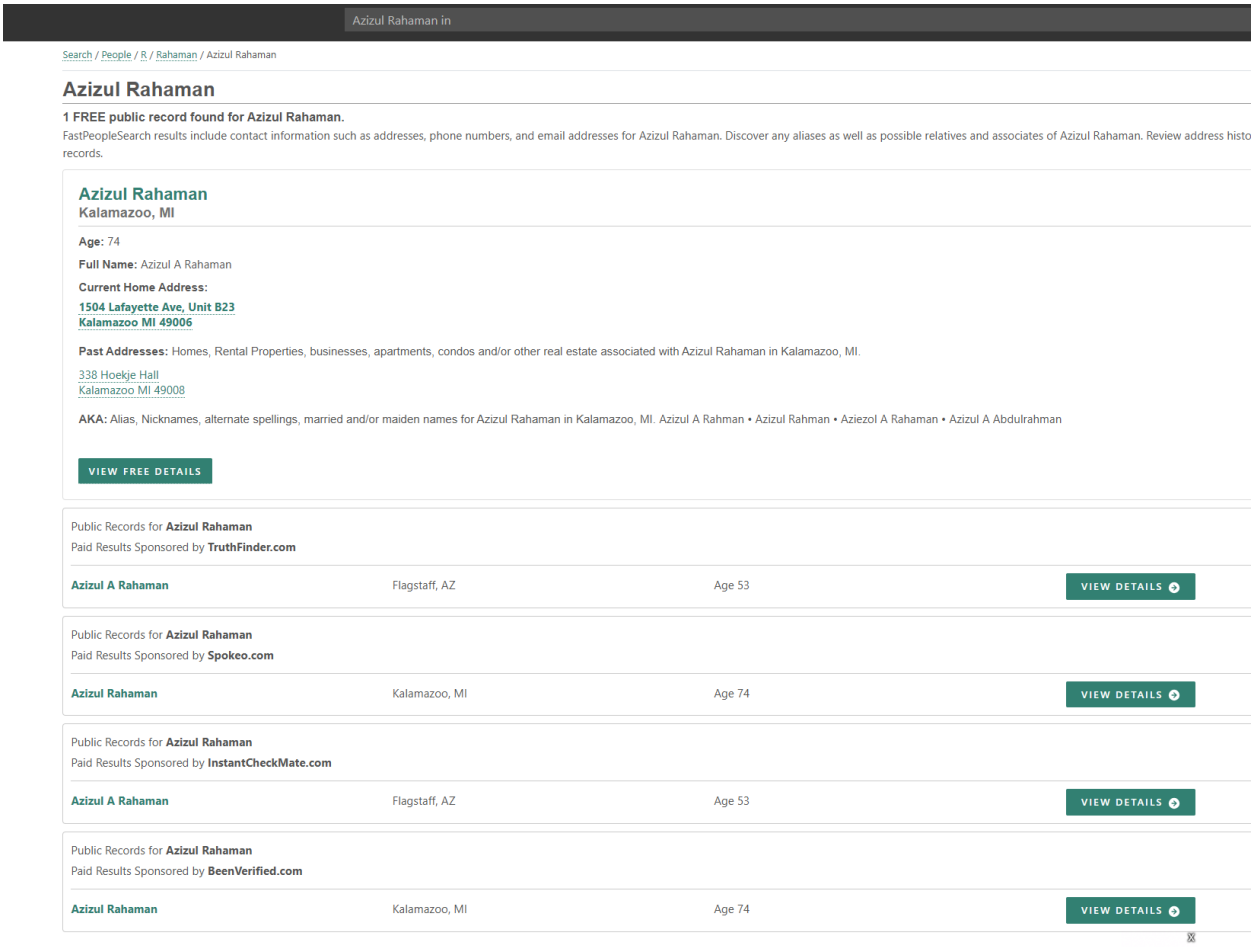
Search Full Name of the owner for 424-310-6862	PHONE SEARCH
Search Current Address of the owner for 424-310-6862	PHONE SEARCH
Search Email Address of the owner for 424-310-6862	PHONE SEARCH
Search Social Profiles of the owner for 424-310-6862	PHONE SEARCH

Search Results for **424-310-6862**
Paid Results Sponsored by **Spokeo.com**

Search Full Name of the owner for 424-310-6862	PHONE SEARCH
Search Current Address of the owner for 424-310-6862	PHONE SEARCH
Search Email Address of the owner for 424-310-6862	PHONE SEARCH
Search Social Profiles of the owner for 424-310-6862	PHONE SEARCH

Search Results for **424-310-6862**
Paid Results Sponsored by **TruthFinder.com**

Search Full Name of the owner for 424-310-6862	PHONE SEARCH
Search Current Address of the owner for 424-310-6862	PHONE SEARCH
Search Email Address of the owner for 424-310-6862	PHONE SEARCH
Search Social Profiles of the owner for 424-310-6862	PHONE SEARCH



Spokeo (OSINT Tool)

The results indicated that the phone number **(424) 310-6862** is linked to a wireless T-Mobile account and associated with a location in Hawthorne, CA. Additional details, such as the owner's full name, current address, family members, and address history, were marked as available but required a paid subscription to access. This demonstrates how Spokeo aggregates public records, telecom data, and online profiles to provide detailed personal information. Another search for Md Rahaman was in progress, highlighting Spokeo's ability to pull data from multiple sources, including real estate records, social media profiles, and background checks. These findings emphasize the importance of personal data privacy, as phone numbers and names can be linked to multiple pieces of sensitive information, making it crucial to monitor and secure online presence to prevent unwanted exposure.

SPOKEO

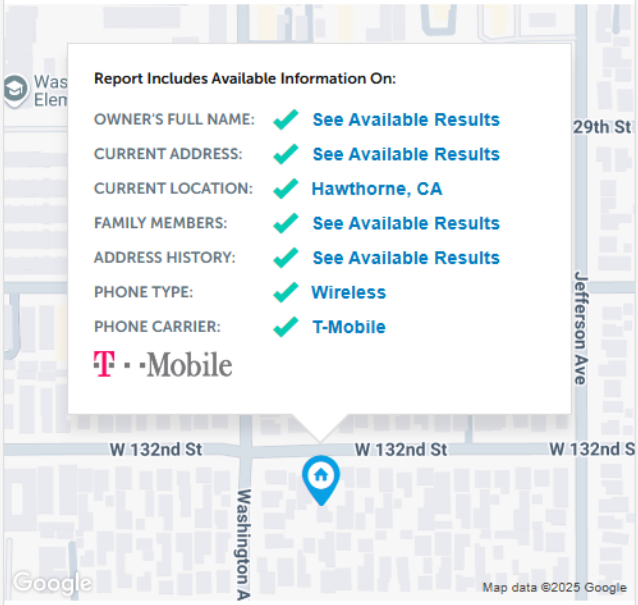
Get Instant Information on (424) 310-6862

Your Purchase is confidential. The Phone Owner of **(424) 310-6862** will **NOT** be notified of your purchase.

RESULTS ARE READY!

(424) 310-6862

Latest report as of 02/16/2025



CAUTION: Spokeo uses proprietary deep web technology to search over billions of phone records. The results may contain detailed information that might shock you, so please prepare yourself for the unexpected.

SPECIAL TRIAL OFFER

FULL PHONE REPORT

$0.95

SPECIAL PRICE

CONTINUE >

429 people have purchased this recently

Report with **FREE** Trial Membership gives you:

- **Full Access to Phone Search**
  Find people in the U.S. by phone to quickly see their full name home address, email address, and more.
- **Instant Access to Name, Email & Address Search**

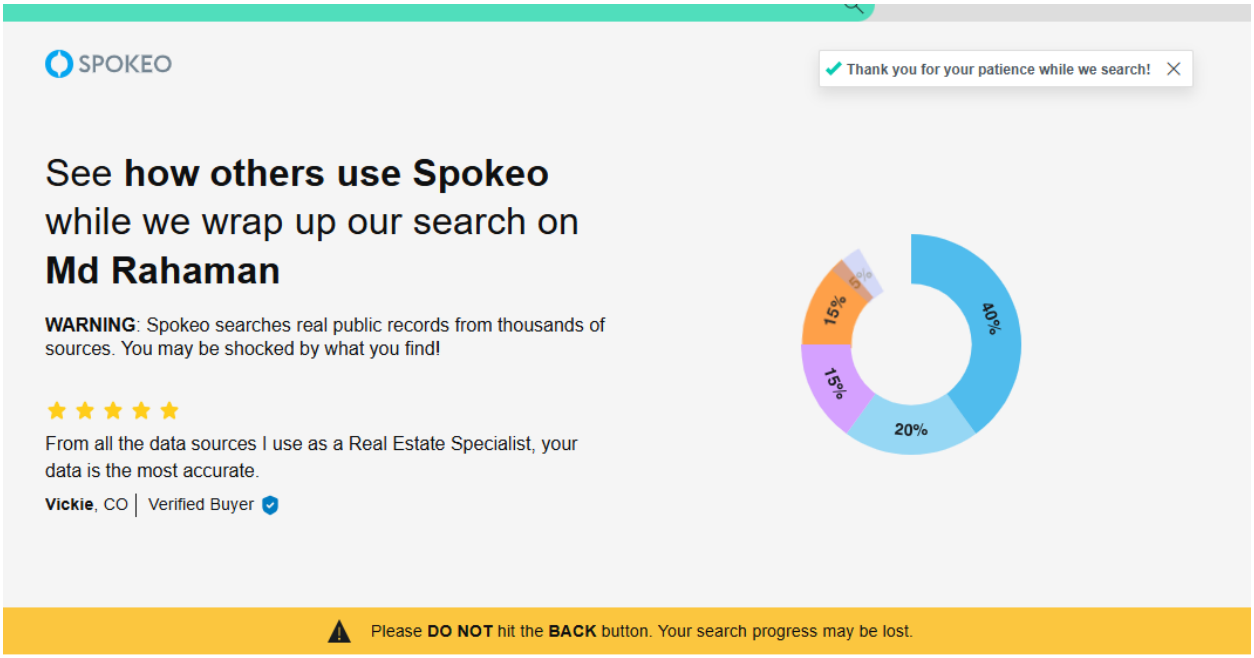
YOUR SATISFACTION IS IMPORTANT TO US

BEST VALUE

If you are dissatisfied with our product, please contact ou Customer Care team at 1 (888) 906-0850. We are available 7 days a week to assist you.

SPOKEO HAS BEEN FEATURED ON

CNN FOX NEWS CBS abc NBC NEWS WS



TruePeopleSearch (OSINT Tool)

I found that the platform returned a record for Azizul Rahaman, listing an individual in Flagstaff, AZ, who previously lived in Kalamazoo, MI. The record included age details and residential history, with additional paid search options through TruthFinder, Spokeo, and BeenVerified. When searching for the phone number **(424) 310-6862**, no direct records were found, but paid services were suggested for obtaining potential ownership details, addresses, and social profiles. Similarly, a search for the email **azizulabir2@gmail.com** yielded no results, indicating that the email is not publicly linked to any known records in this database. These findings reinforce how people search engines collect and display publicly accessible information, emphasizing the need for individuals to be cautious about their digital footprint and take steps to remove or secure sensitive personal data.

1 record found for Azizul Rahaman

Azizul A Rahaman

Age 74
Lives in Flagstaff, AZ
Used to live in Kalamazoo MI

View Details

Sponsored Links

Paid service sponsored by **TruthFinder.com**

Name	Age	Location	
Azizul A Rahaman	53	Flagstaff, AZ	View Details

Paid service sponsored by **BeenVerified.com**

Name	Age	Location	
Azizul Rahaman	53	Flagstaff, AZ	Search Details

Paid service sponsored by **Spokeo.com**

Name	Age	Location	
Azizul A Rahaman	74	Flagstaff, AZ	Search Details

Paid service sponsored by **PeopleLooker.com**

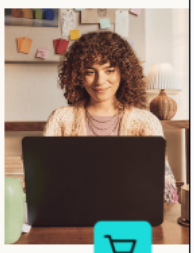
Name	Age	Location	
Azizul A Rahaman	74	Flagstaff, AZ	Search Details

Name Search | **Phone Search** | Address Search | Email Search

TruePeopleSearch (424) 310-6862

GoDa

Forget something?



We could not find any records for that search criteria.

Sponsored Links

Paid service sponsored by **BeenVerified.com**

Search owner of **(424) 310-6862** — Search Details

Search current address of **(424) 310-6862** — Search Details

Search email address of **(424) 310-6862** — Search Details

Paid service sponsored by **Spokeo.com**

Search owner of **(424) 310-6862** — Search Details

Search current address of **(424) 310-6862** — Search Details

Search email address of **(424) 310-6862** — Search Details

Paid service sponsored by **Intelius.com**

Search owner of **(424) 310-6862** — View Details

Search current address of **(424) 310-6862** — View Details

Search email address of **(424) 310-6862** — View Details

Paid service sponsored by **PeopleLooker.com**

tinuing to use this website, you agree to accept our use of cookies. Learn More / Privacy

Name Search | Phone Search | Address Search | **Email Search**

Search azizulabir2@gmail.com

We could not find any records for that search criteria.

Zero is waiting for you!

0% INTRO APR

18 BILLING CYCLES on purchases and balance transfers

Platinum Credit Card

WINDSTONE

LEARN MORE

NEED MORE DATA IN REAL-TIME?

endato

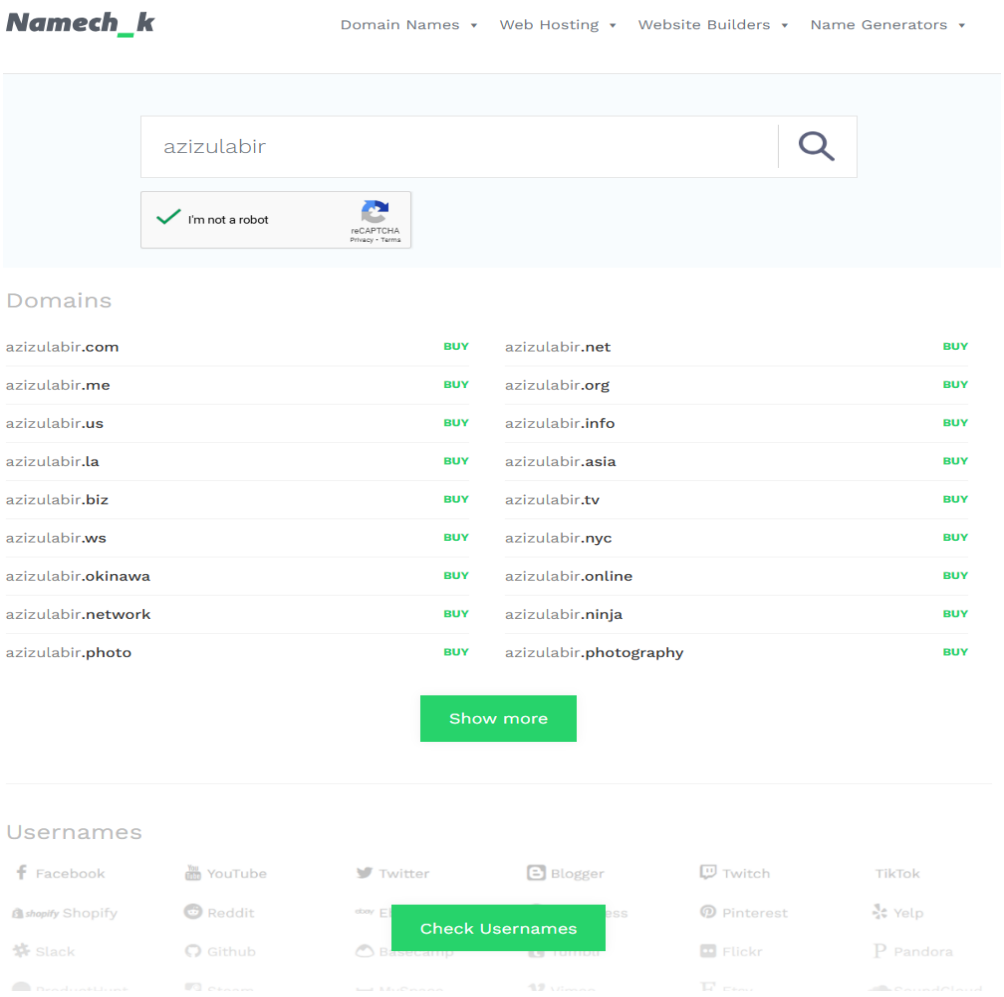
Get access to our partner **Endato's Fast Developer API** for Contact Enrichment, Sales and Marketing Intelligence.

Try Our API

Username Enumeration

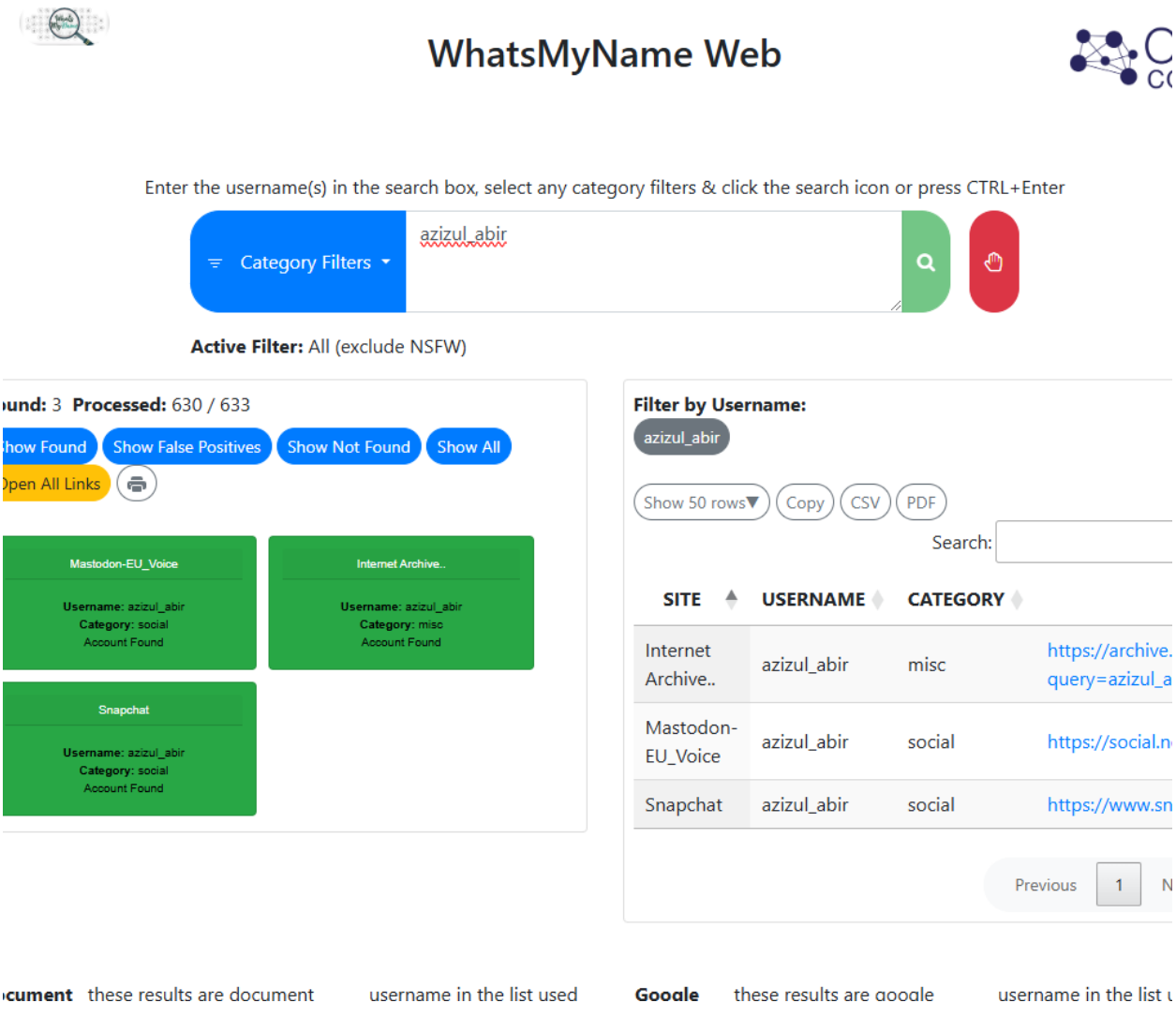
Namechk (OSINT Tool)

The Namechk search results indicate that the username azizulabir is available for domain registration, meaning that websites such as azizulabir.com, azizulabir.net, and azizulabir.org can still be purchased. This suggests that no one has yet claimed these domains, making it an opportunity to secure a personal website or brand. However, the username check for social media platforms has not been completed, meaning it is unclear whether azizulabir is already in use on platforms like Facebook, Twitter, Instagram, or GitHub. To find out, the next step is to click the Check Usernames button, which will scan various platforms for availability. If the username is available, it can be registered to prevent others from using it. If it is already taken, further investigation can determine whether it is linked to an existing account or used by someone else.



WhatsMyName Web (OSINT Tool)

The WhatsMyName search results show that the username azizul_abir has been found on three platforms: Mastodon-EU Voice, Internet Archive, and Snapchat. This indicates that accounts with this username exist on these sites, suggesting that either the user has created accounts there or someone else is using the same username. The results categorize the Mastodon and Snapchat accounts under social, while the Internet Archive listing falls under misc, meaning it may be associated with a repository or archival data. If this username belongs to you, it is essential to verify and manage these accounts to ensure security and privacy. If it does not belong to you, further investigation can help determine whether someone else is impersonating or using the username. This highlights the importance of monitoring online identities to prevent unauthorized use and enhance digital privacy.



Conclusion

This OSINT investigation revealed how much personal information can be uncovered using publicly available tools and techniques. My social media presence, particularly on platforms like Facebook and Instagram, is easily accessible, making it possible for outsiders to view my activities and personal details. Additionally, my educational background played a significant role in linking my identity across different platforms, even when my LinkedIn profile was not directly indexed. While my email and passwords were not found in known data breaches, continuous monitoring remains essential as new leaks can occur over time. Reverse image searches indicated that my photos are not widely indexed, but some traces were found on YouTube, highlighting potential risks of impersonation. Furthermore, people search engines contained past address records and other identifiable information, demonstrating how aggregators collect and display personal data. To mitigate these privacy risks, I should strengthen my social media privacy settings, regularly monitor my credentials for breaches, opt out of data aggregator sites, and enable two-factor authentication on all accounts. This exercise underscored the importance of maintaining a low digital footprint and being proactive in safeguarding personal information in the age of increasing online exposure.