Lab11: Setup OSINT VM + Basic OSINT practice

Grade Weight: 6%

Background:

OSINT Lecture notes

Scenario Overview:

You are a forensic analyst working for a cybersecurity company. Your task is to investigate an individual known only by their online alias, "CyberHunter." This individual has been linked to several online activities of interest, and your goal is to gather as much information as possible using OSINT (Open-Source Intelligence) techniques. Follow the steps below to set up your lab environment and conduct the investigation.

Objectives:

OSINT Lab setup + Basic OSINT Investigation

Download and setup the following VM for OSINT Investigations –

https://www.tracelabs.org/initiatives/osint-vm

Follow this video if you need assistance in setting up the VM.

https://www.youtube.com/watch?v=jjK0nvmOeUA&embeds_widget_referrer=https%3A%2F%2Fwww.tracelabs.org%2F&embeds_referring_euri=https%3A%2F%2Fcdn.embedly.com%2F&embeds_referring_origin=https%3A%2F%2Fcdn.embedly.com&source_ve_path=MjM4NTE&feature=emb_title

Conducting the Investigation

Task 1: Identify Possible Real Name

Social Media Profiles:

- **Search Platforms:** Look for "CyberHunter" on Twitter, LinkedIn, Facebook, and Instagram. Examine profile descriptions, posts, comments, and connections for real name clues.

Forums and Communities:

- **Technical Forums:** Explore hacker forums, Reddit, GitHub, and Stack Overflow. Check profiles and postings for any personal details.

People Search Engines:

- **Use Tools:** Enter "CyberHunter" into Pipl, Spokeo, or BeenVerified to see if any useful information is returned.

Task 2: Find Associated Email Addresses

theHarvester:

- **Run Tool:**

```
sh
Copy code
theharvester -d cyberhunter -l 500 -b all
```

Pastebin and Similar Sites:

- **Search Dumps:** Look for the alias on Pastebin using keywords like "CyberHunter" and "email."

Domain Registration Records:

- **WHOIS Lookup:** Search for domain registrations linked to "CyberHunter" and check for associated email addresses.

Task 3: Locate Social Media Profiles

Username Search Tools:

- **Namechk, KnowEm:** Search for "CyberHunter" across multiple social media platforms.

OSINT Framework:

- **Explore Tools:** Use the OSINT Framework website to find additional resources for locating social media profiles.

Task 4: Uncover Employment History or Affiliations

LinkedIn:

- **Professional Network:** Search for "CyberHunter" on LinkedIn. Look at job titles, companies, and connections. Check if the username is part of their profile URL.

GitHub:

- **Repositories:** Search for repositories and contributions by "CyberHunter." Look for real names and affiliations in profiles.

Public Records:

- **Database Search:** Use public record databases like Intelius or TruthFinder to find professional affiliations or employment records.

Additional Investigation Tips

Google Dorks:

- **Advanced Search:**

```
"CyberHunter" site:linkedin.com
"CyberHunter" email
"CyberHunter" site:github.com
```

Reverse Image Search:

- **Image Verification:** Use Google Images or TinEye to perform a reverse image search on any profile pictures associated with "CyberHunter."

Check Metadata:

- **Hidden Information:** Download public documents or images shared by "CyberHunter" and examine the metadata for hidden details such as the author's name or location.

Practice Scenario

Imagine you are tasked with finding comprehensive information on "CyberHunter." Document your findings and the steps you took to gather this information. Your final report should include:

1. Possible real name.
2. Associated email addresses.

3. Social media profiles.
4. Employment history or affiliations.

By following these steps and using the provided tips, you will enhance your OSINT skills and complete the investigation successfully. Good luck!

Reminders

- Submit your report name: CYT215-Lab11-Student Name & ID
- Submit via the BB relevant link ONLY. NO submission via email please. Be sure to submit the final version file ONLY.
- NOTE – THIS IS AN INDVIDUAL REPORT AND MUST BE IN YOUR OWN WORDS. ALL THOUGH COLLABORATION IS ENCOURAGED, YOUR REPORT SHOULD BE YOUR OWN. Feel free to reference google when answering the above questions.

Please follow and abide by the Seneca Academic Integrity policy –

Academic Integrity at Seneca

What is Academic Integrity?

The International Center for Academic Integrity defines academic integrity as a commitment, even in the face of adversity, to six Fundamental Values of Academic Integrity: honesty, trust, fairness, respect, responsibility, and courage. From these values flow principles of behavior that enable academic communities to translate ideals into action.

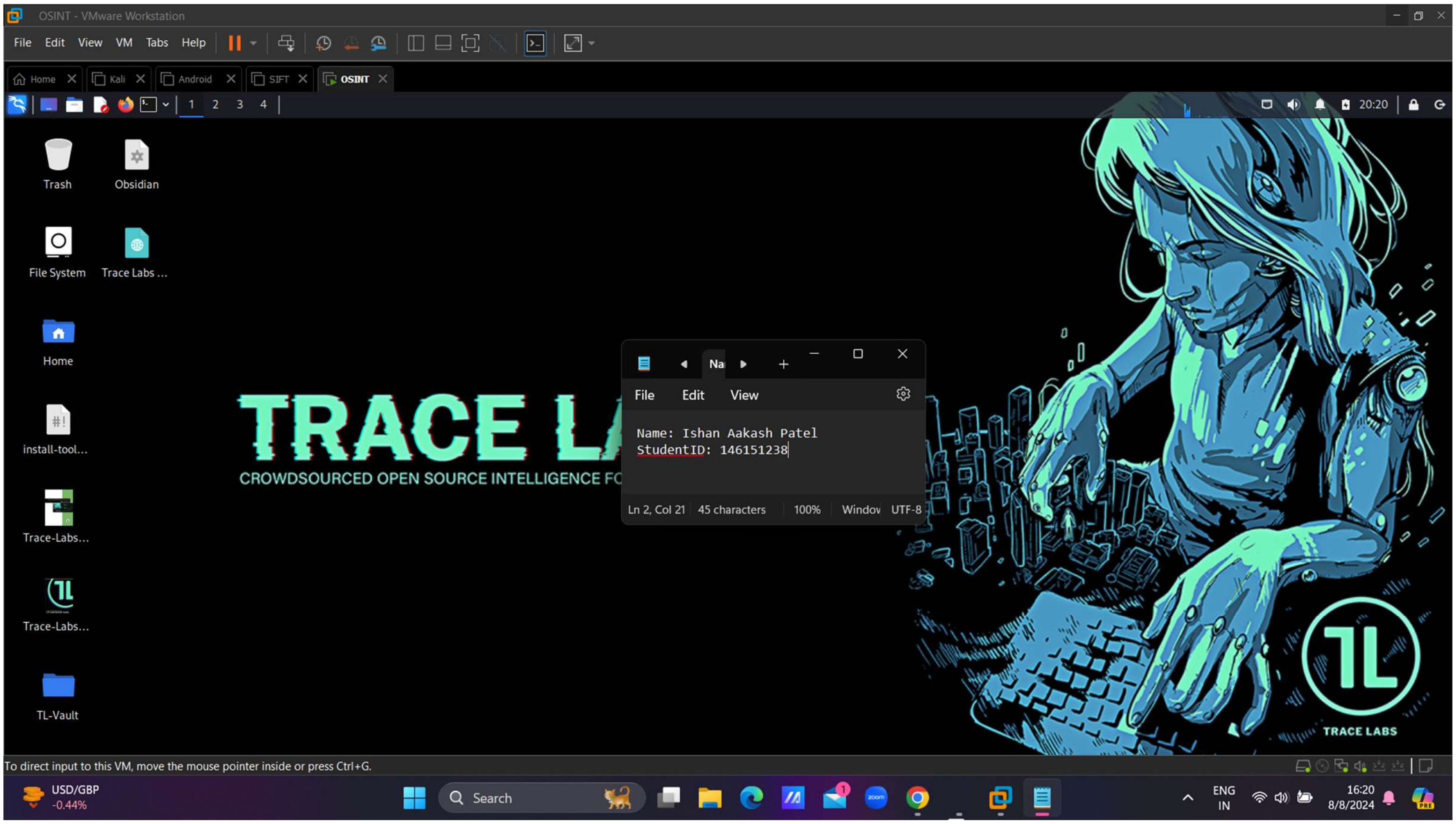
Why does Academic Integrity Matter?

When each member of the Seneca Community embraces and incorporates these values into our teaching, learning and working environments, then we are able to maintain the college's reputation as a leading educational institution and to graduate high quality students who are poised to succeed in their careers and contribute meaningfully to society.

Academic Integrity - Student Resources

-----------------------------------**Report goes Below** --

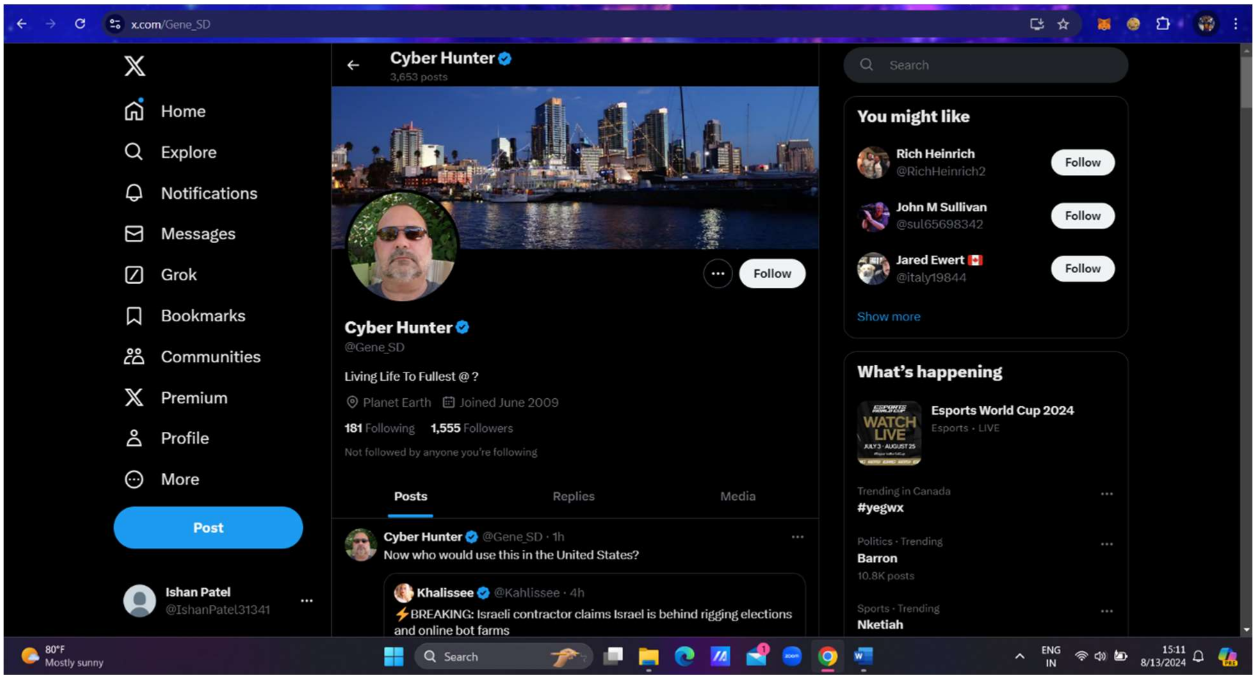
Installed OSINT VM



```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Task 1 : Identify Possible Real Name

1) X (Twitter)



Cyber Hunter
3,653 posts

Follow

Cyber Hunter
@Gene_SD

Living Life To Fullest @ ?

Planet Earth Joined June 2009

181 Following 1,555 Followers

Not followed by anyone you're following

Posts Replies Media

Cyber Hunter @Gene_SD · 1h
Now who would use this in the United States?

Khalissee @Kahlissee · 4h
⚡BREAKING: Israeli contractor claims Israel is behind rigging elections and online bot farms

You might like

Rich Heinrich @RichHeinrich2 Follow

John M Sullivan @sul65698342 Follow

Jared Ewert @italy19844 Follow

Show more

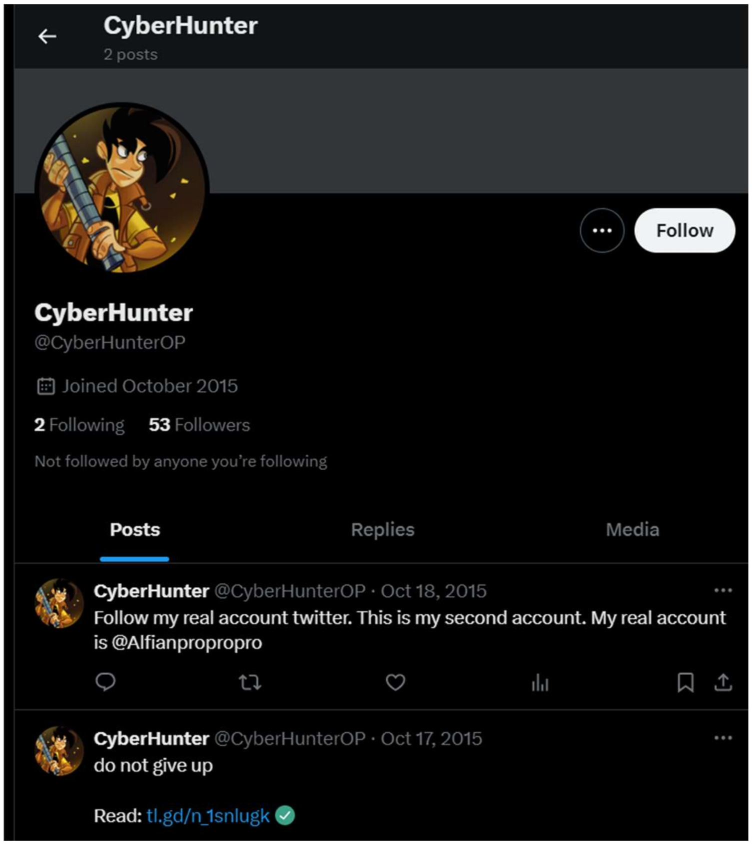
What's happening

Esports World Cup 2024
Esports · LIVE

Trending in Canada
#yegwx

Politics · Trending
Barron
10.8K posts

Sports · Trending
Nketiah



CyberHunter
2 posts

Follow

CyberHunter
@CyberHunterOP

Joined October 2015

2 Following 53 Followers

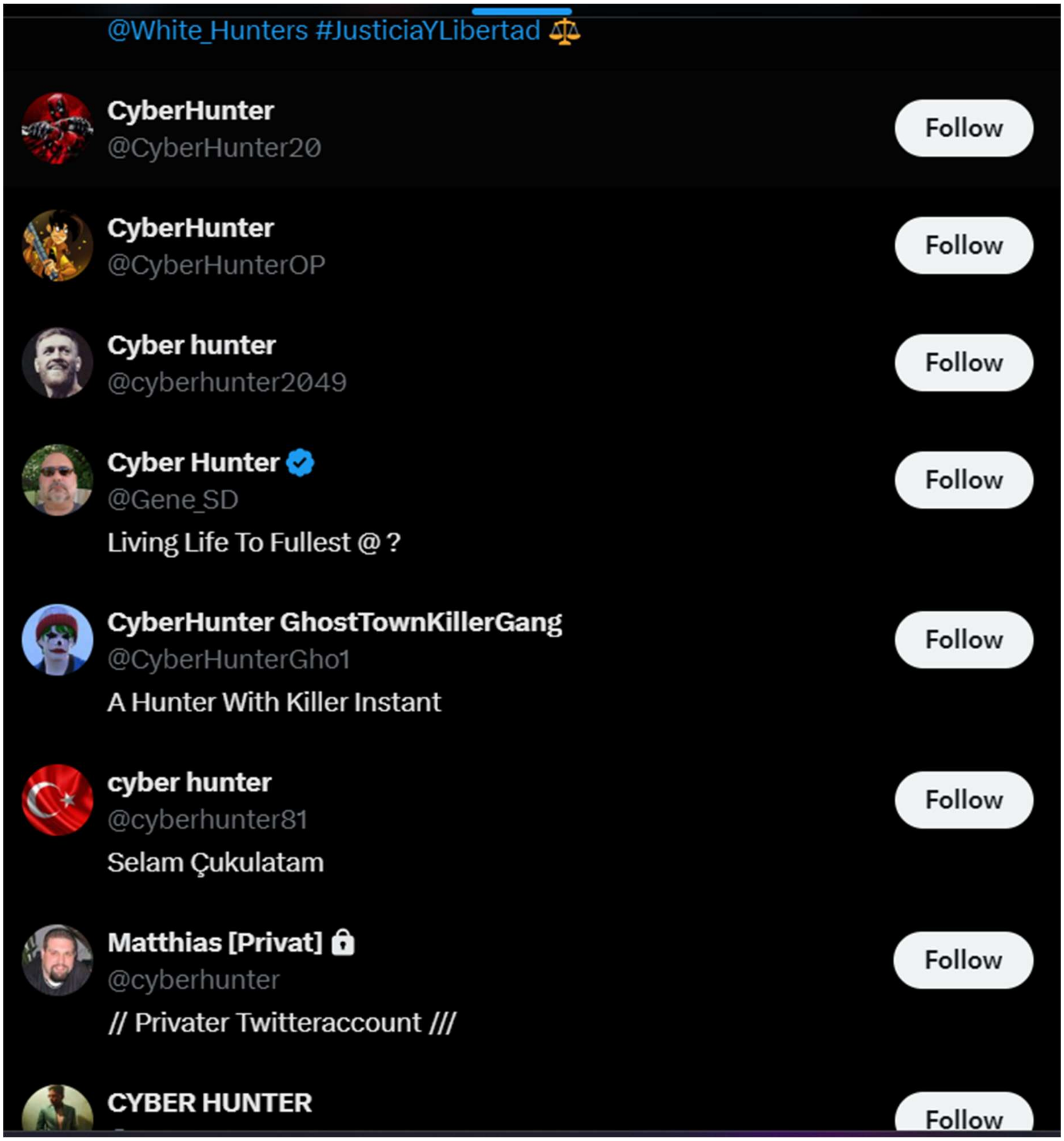
Not followed by anyone you're following

Posts Replies Media

CyberHunter @CyberHunterOP · Oct 18, 2015
Follow my real account twitter. This is my second account. My real account is @Alfianpropropro

CyberHunter @CyberHunterOP · Oct 17, 2015
do not give up

Read: tl.gd/n_1snlugk



@White_Hunters #JusticiaYLibertad ⚖️

CyberHunter
@CyberHunter20

CyberHunter
@CyberHunterOP

Cyber hunter
@cyberhunter2049

Cyber Hunter
@Gene_SD
Living Life To Fullest @ ?

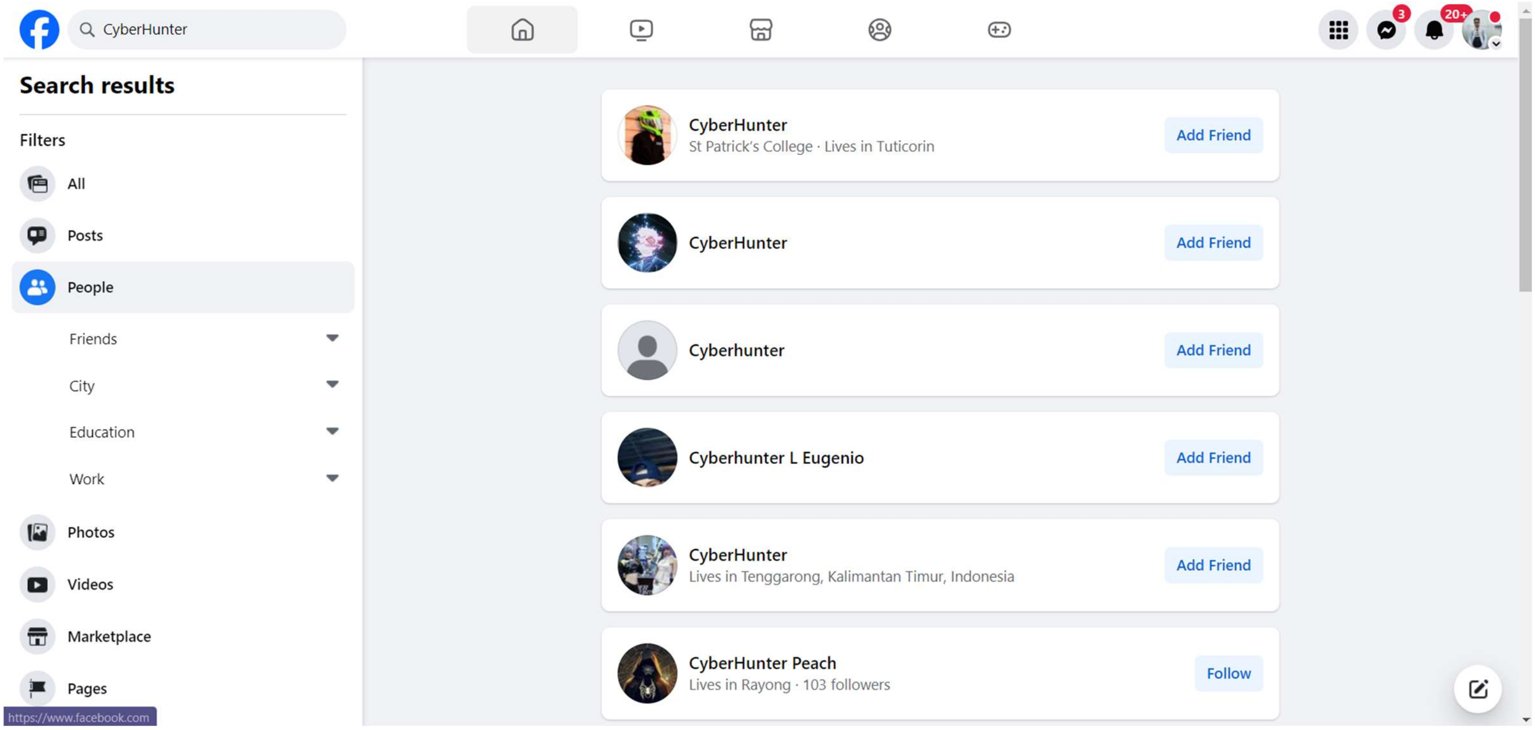
CyberHunter GhostTownKillerGang
@CyberHunterGho1
A Hunter With Killer Instant

cyber hunter
@cyberhunter81
Selam Çukulatam

Matthias [Privat] 🔒
@cyberhunter
// Privater Twitteraccount ///

CYBER HUNTER

2) Facebook



CyberHunter

Search results

Filters

All

Posts

People

Friends

City

Education

Work

Photos

Videos

Marketplace

Pages

https://www.facebook.com

CyberHunter
St Patrick's College · Lives in Tuticorin
Add Friend

CyberHunter
Add Friend

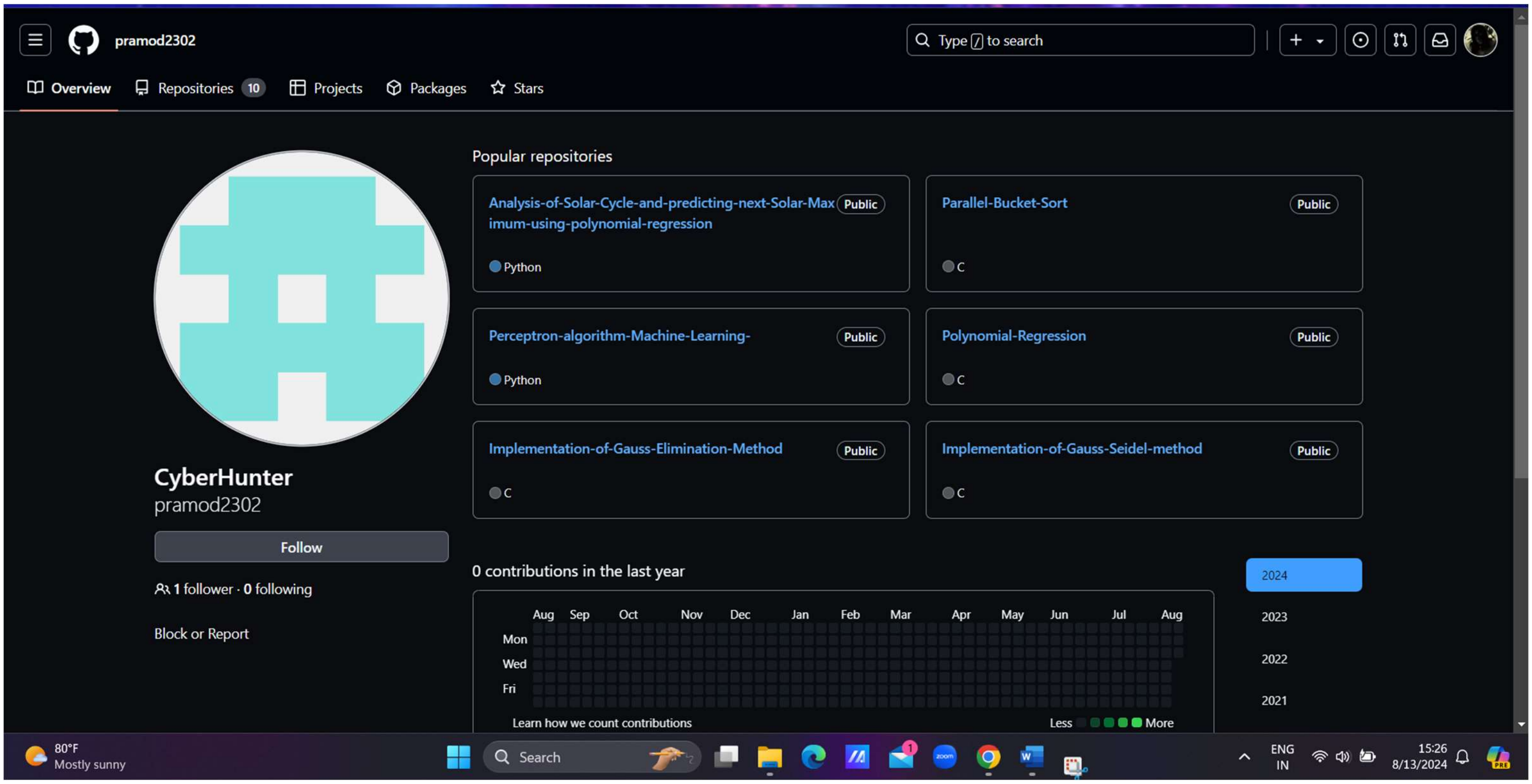
Cyberhunter
Add Friend

Cyberhunter L Eugenio
Add Friend

CyberHunter
Lives in Tenggarong, Kalimantan Timur, Indonesia
Add Friend

CyberHunter Peach
Lives in Rayong · 103 followers
Follow

3) Github



pramod2302

Type / to search

Overview · Repositories 10 · Projects · Packages · Stars

CyberHunter
pramod2302

Follow

1 follower · 0 following

Block or Report

Popular repositories

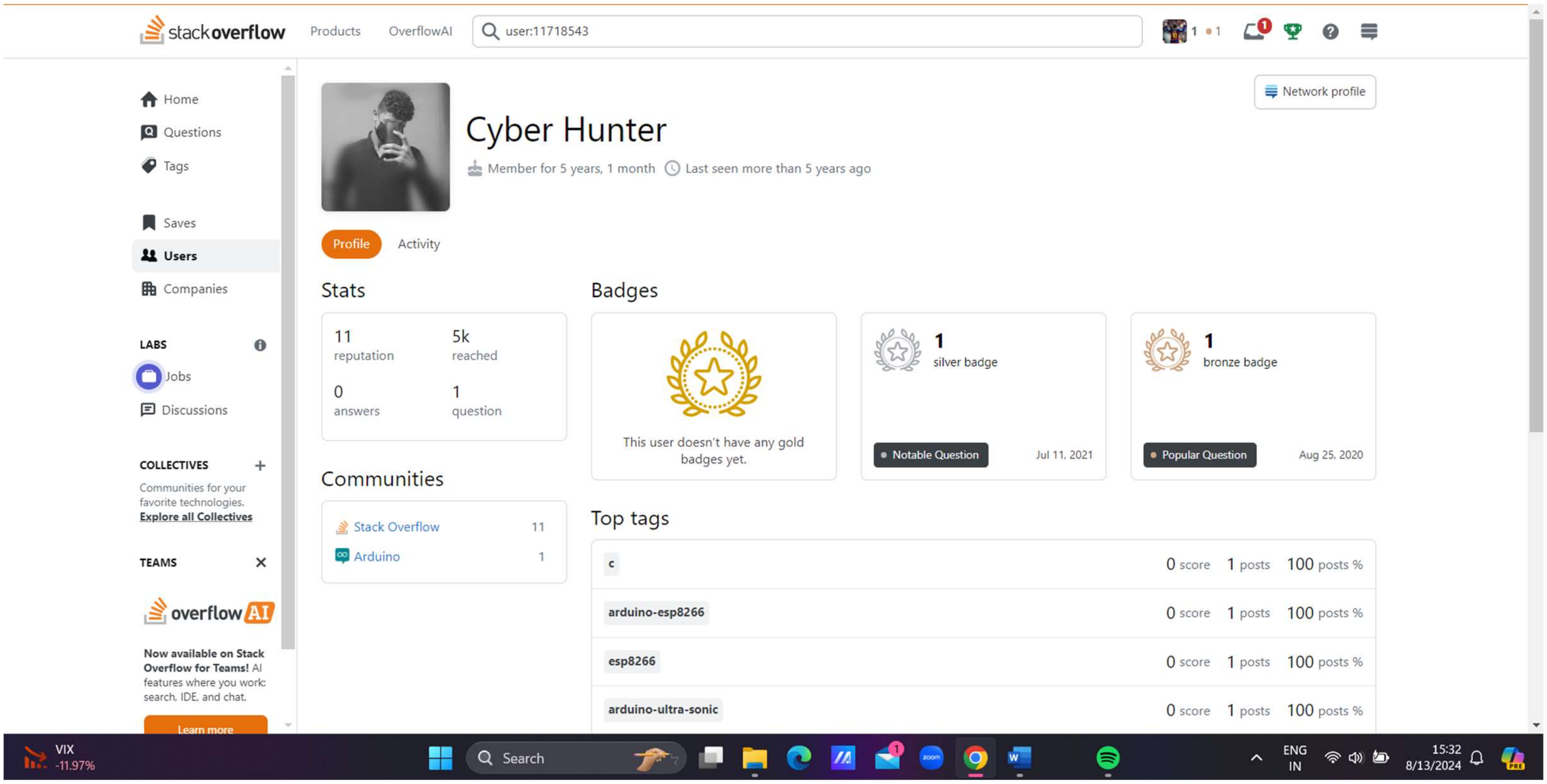
Analysis-of-Solar-Cycle-and-predicting-next-Solar-Maximum-using-polynomial-regression (Public) Python	Parallel-Bucket-Sort (Public) C
Perceptron-algorithm-Machine-Learning- (Public) Python	Polynomial-Regression (Public) C
Implementation-of-Gauss-Elimination-Method (Public) C	Implementation-of-Gauss-Seidel-method (Public) C

0 contributions in the last year

Learn how we count contributions

2024
2023
2022
2021

4) StackOverflow



Cyber Hunter

Member for 5 years, 1 month · Last seen more than 5 years ago

Stats

11 reputation	5k reached
0 answers	1 question

Communities

Stack Overflow	11
Arduino	1

Badges

This user doesn't have any gold badges yet.

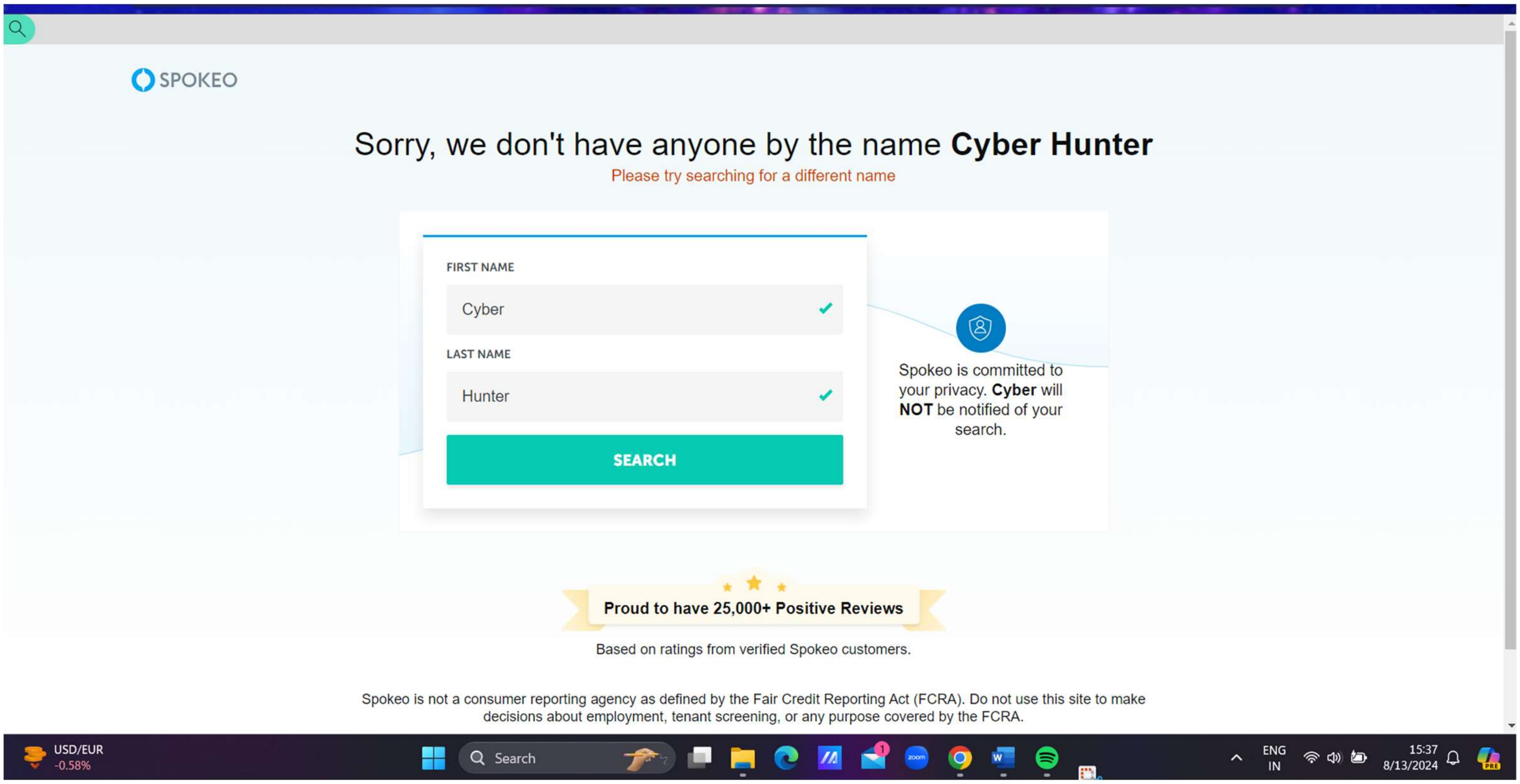
1 silver badge — Notable Question — Jul 11, 2021

1 bronze badge — Popular Question — Aug 25, 2020

Top tags

c	0 score	1 posts	100 posts %
arduino-esp8266	0 score	1 posts	100 posts %
esp8266	0 score	1 posts	100 posts %
arduino-ultra-sonic	0 score	1 posts	100 posts %

5) Spokeo



Sorry, we don't have anyone by the name **Cyber Hunter**

Please try searching for a different name

FIRST NAME: Cyber ✓

LAST NAME: Hunter ✓

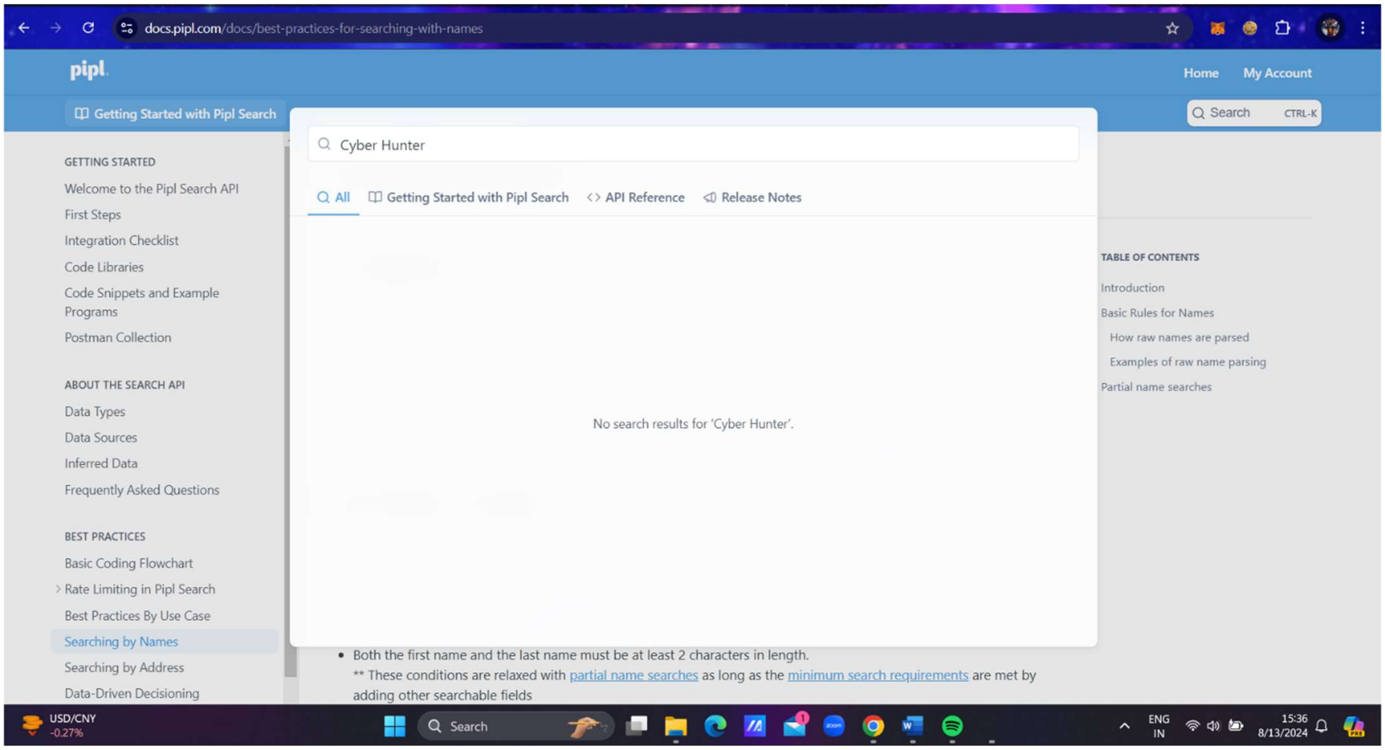
Spokeo is committed to your privacy. **Cyber** will **NOT** be notified of your search.

Proud to have 25,000+ Positive Reviews

Based on ratings from verified Spokeo customers.

Spokeo is not a consumer reporting agency as defined by the Fair Credit Reporting Act (FCRA). Do not use this site to make decisions about employment, tenant screening, or any purpose covered by the FCRA.

6) Pipl



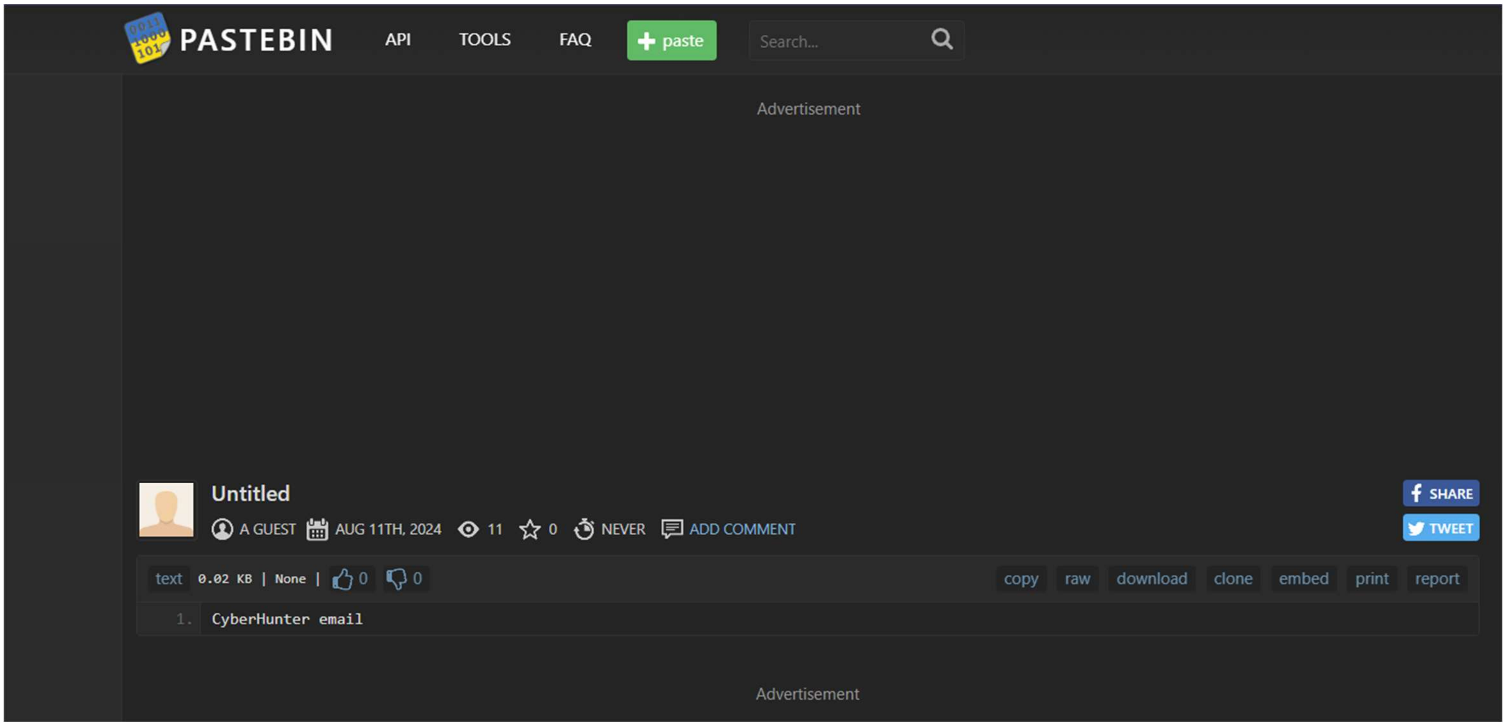
Cyber Hunter

No search results for 'Cyber Hunter'.

- Both the first name and the last name must be at least 2 characters in length.
  ** These conditions are relaxed with partial name searches as long as the minimum search requirements are met by adding other searchable fields

Task 2 : Find Associated Email Addresses

1) Pastebin



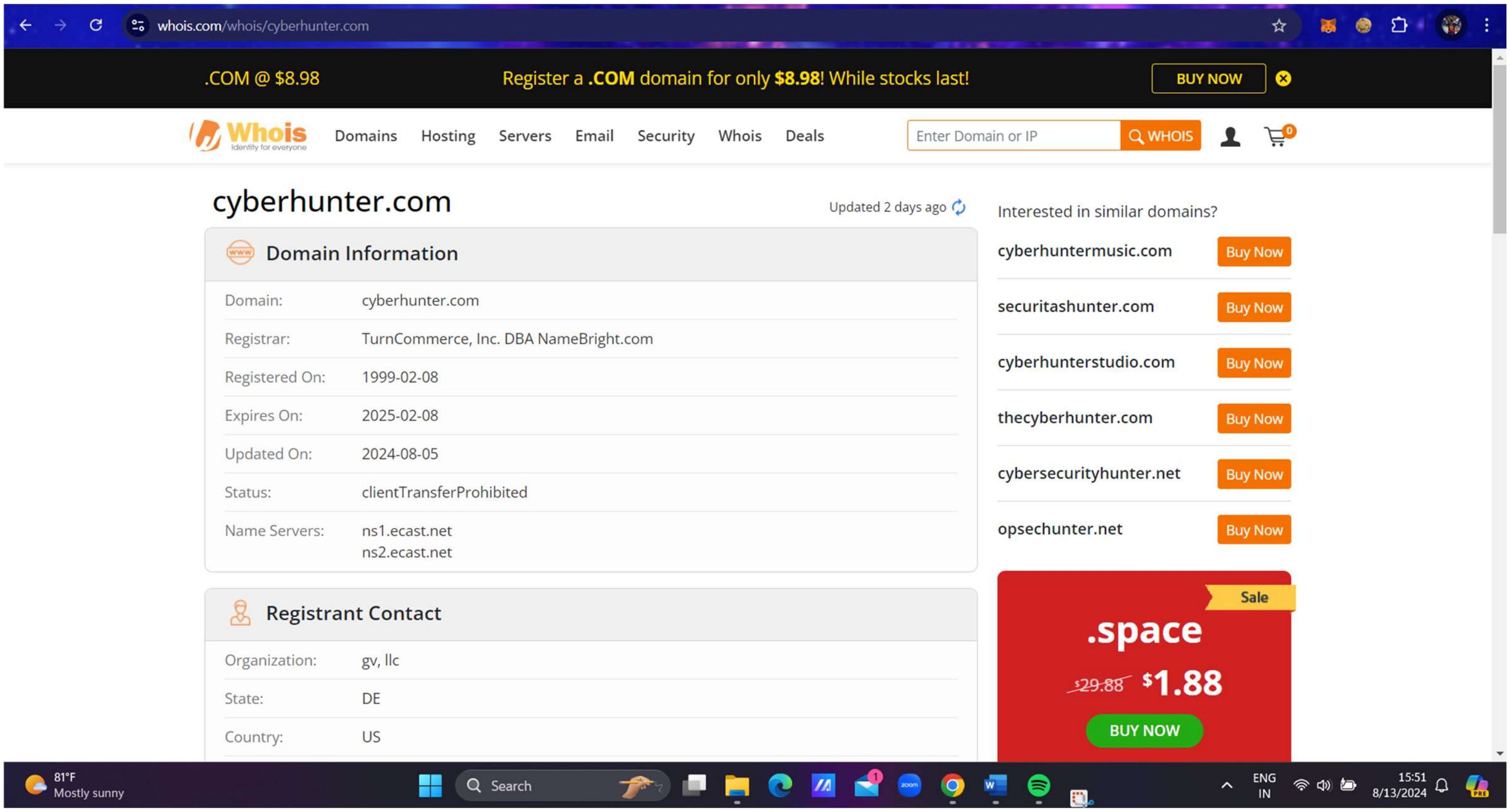
Untitled

A GUEST AUG 11TH, 2024 11 0 NEVER ADD COMMENT

text 0.02 KB | None | 0 0

```
CyberHunter email
```

2) Whois Lookup



cyberhunter.com

Updated 2 days ago

Domain Information

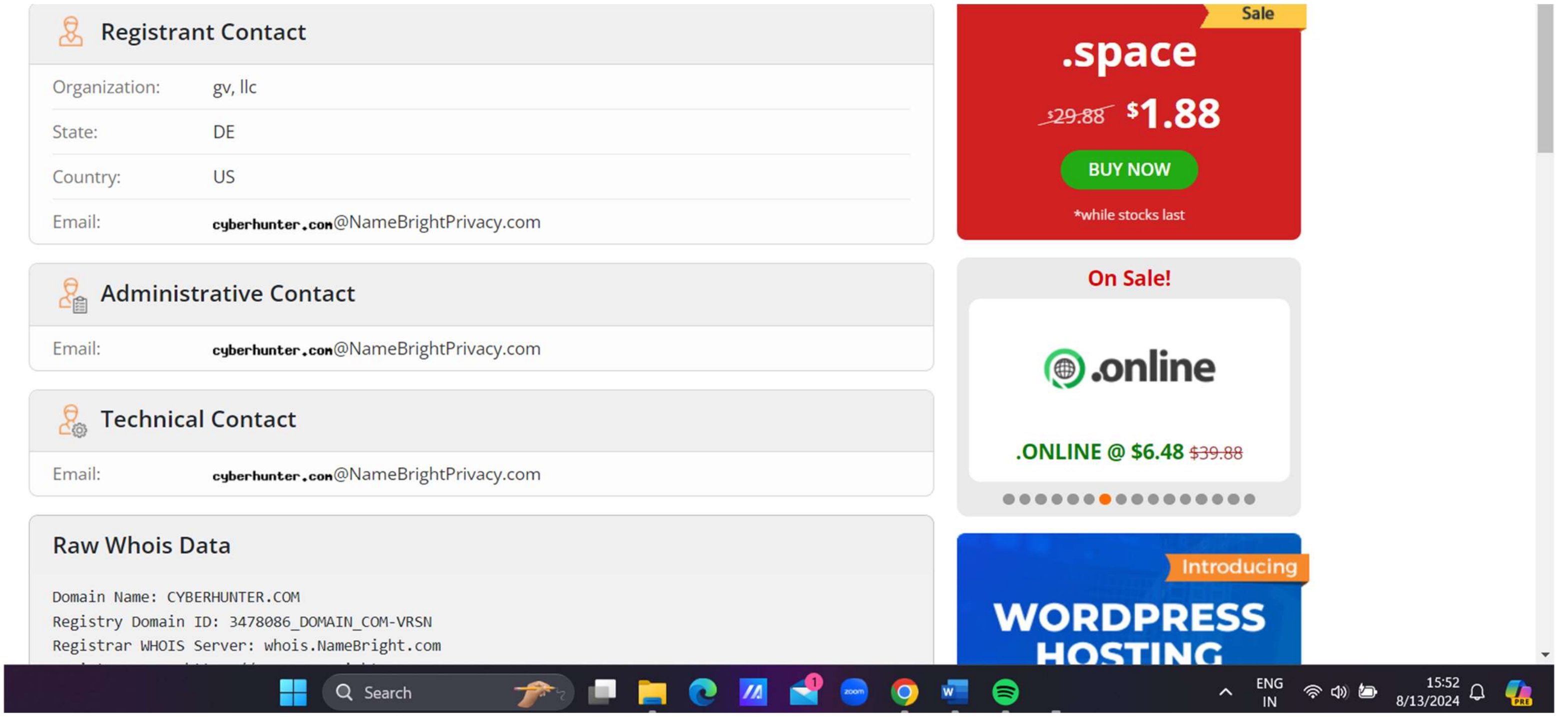
Domain:	cyberhunter.com
Registrar:	TurnCommerce, Inc. DBA NameBright.com
Registered On:	1999-02-08
Expires On:	2025-02-08
Updated On:	2024-08-05
Status:	clientTransferProhibited
Name Servers:	ns1.ecast.net ns2.ecast.net

Registrant Contact

Organization:	gv, llc
State:	DE
Country:	US

Interested in similar domains?

cyberhuntermusic.com	Buy Now
securitashunter.com	Buy Now
cyberhunterstudio.com	Buy Now
thecyberhunter.com	Buy Now
cybersecurityhunter.net	Buy Now
opsechunter.net	Buy Now



Registrant Contact

Organization:	gv, llc
State:	DE
Country:	US
Email:	cyberhunter.com@NameBrightPrivacy.com

Administrative Contact

Email:	cyberhunter.com@NameBrightPrivacy.com

Technical Contact

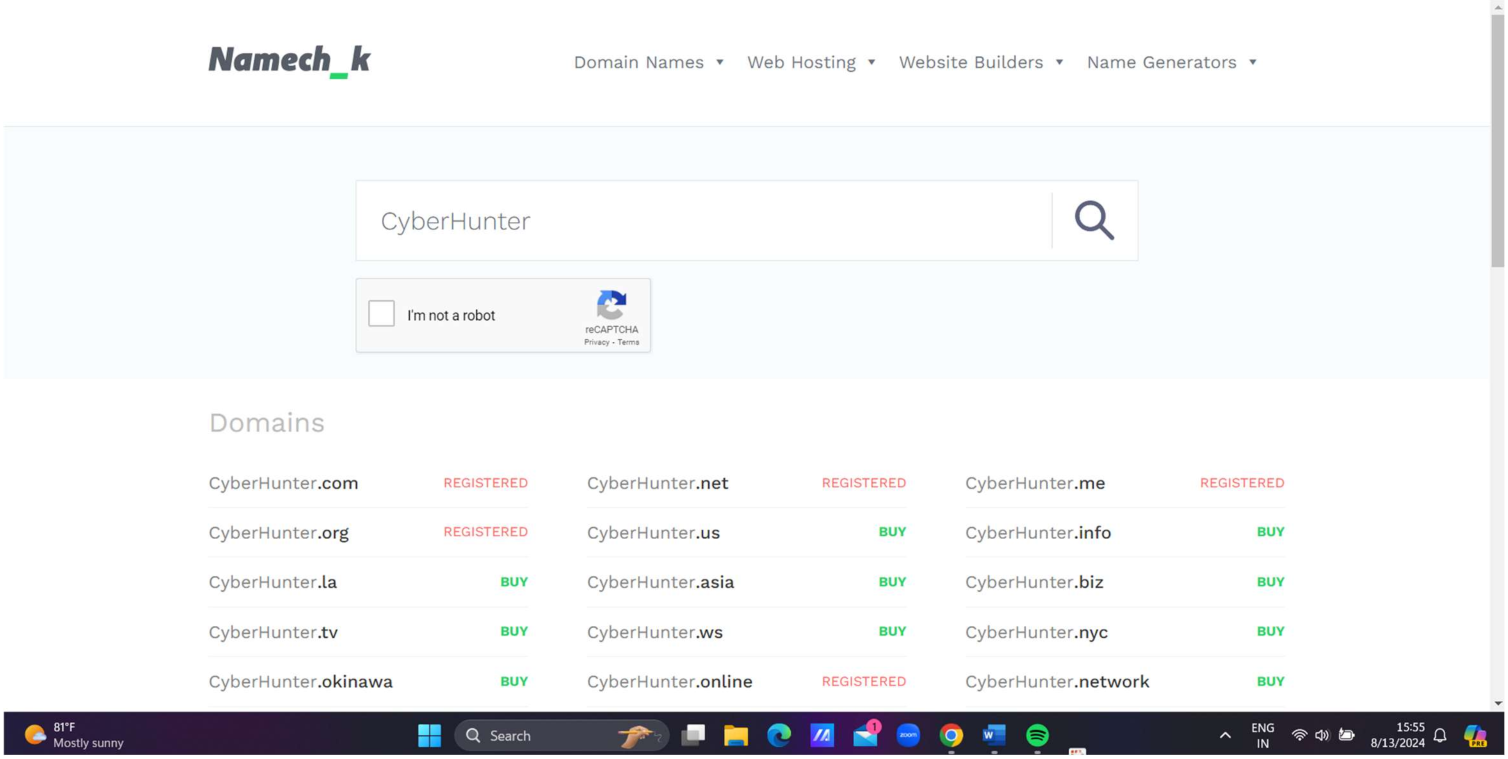
Email:	cyberhunter.com@NameBrightPrivacy.com

Raw Whois Data

```
Domain Name: CYBERHUNTER.COM
Registry Domain ID: 3478086_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.NameBright.com
```

Task 3 : Locate Social Media Profiles

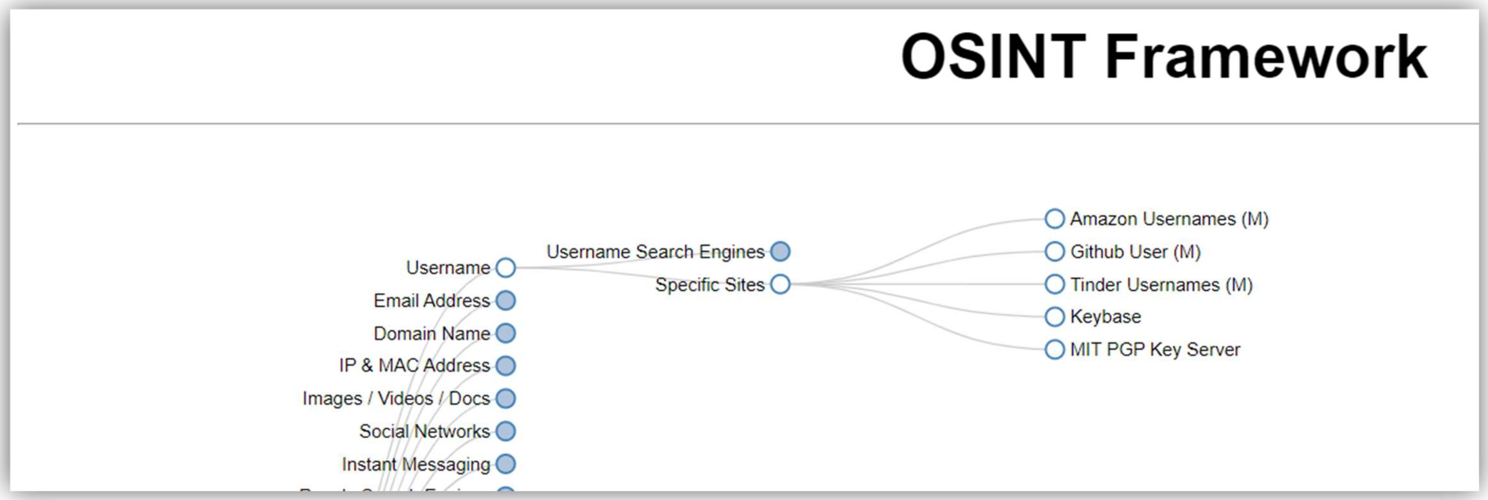
1) Nameche

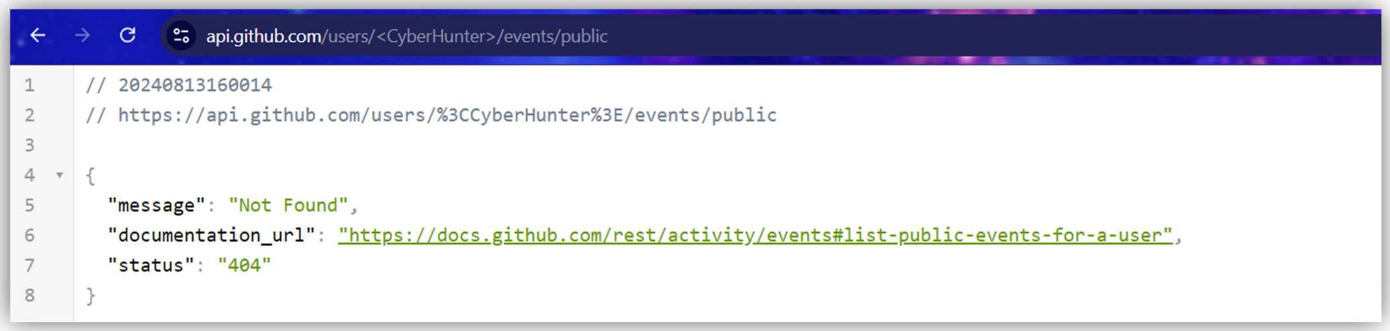


Domains

CyberHunter.com	REGISTERED	CyberHunter.net	REGISTERED	CyberHunter.me	REGISTERED
CyberHunter.org	REGISTERED	CyberHunter.us	BUY	CyberHunter.info	BUY
CyberHunter.la	BUY	CyberHunter.asia	BUY	CyberHunter.biz	BUY
CyberHunter.tv	BUY	CyberHunter.ws	BUY	CyberHunter.nyc	BUY
CyberHunter.okinawa	BUY	CyberHunter.online	REGISTERED	CyberHunter.network	BUY

2) OSINT Framework

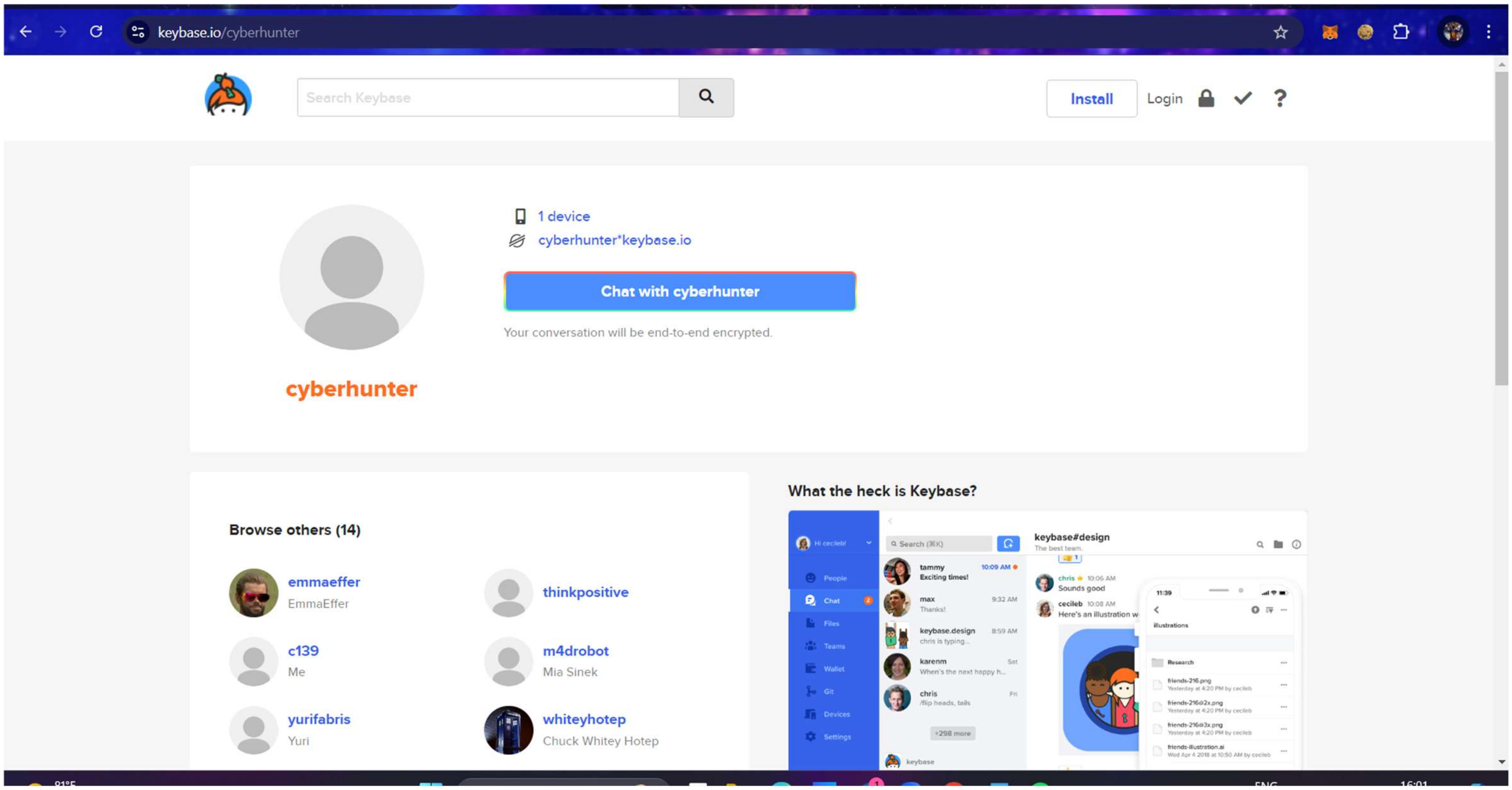




api.github.com/users/<CyberHunter>/events/public

```
// 20240813160014
// https://api.github.com/users/%3CCyberHunter%3E/events/public

{
  "message": "Not Found",
  "documentation_url": "https://docs.github.com/rest/activity/events#list-public-events-for-a-user",
  "status": "404"
}
```



keybase.io/cyberhunter

1 device

cyberhunter*keybase.io

Chat with cyberhunter

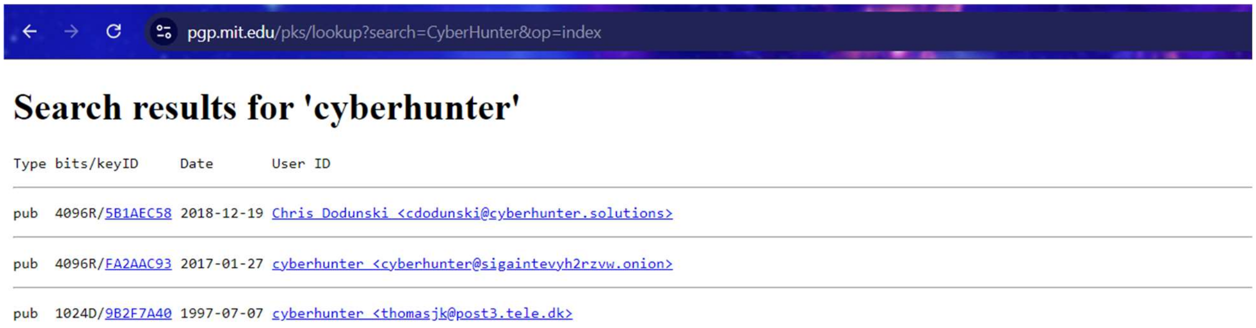
Your conversation will be end-to-end encrypted.

cyberhunter

Browse others (14)

emmaeffer EmmaEffer	thinkpositive
c139 Me	m4drobot Mia Sinek
yurifabris Yuri	whiteyhotep Chuck Whitey Hotep

What the heck is Keybase?

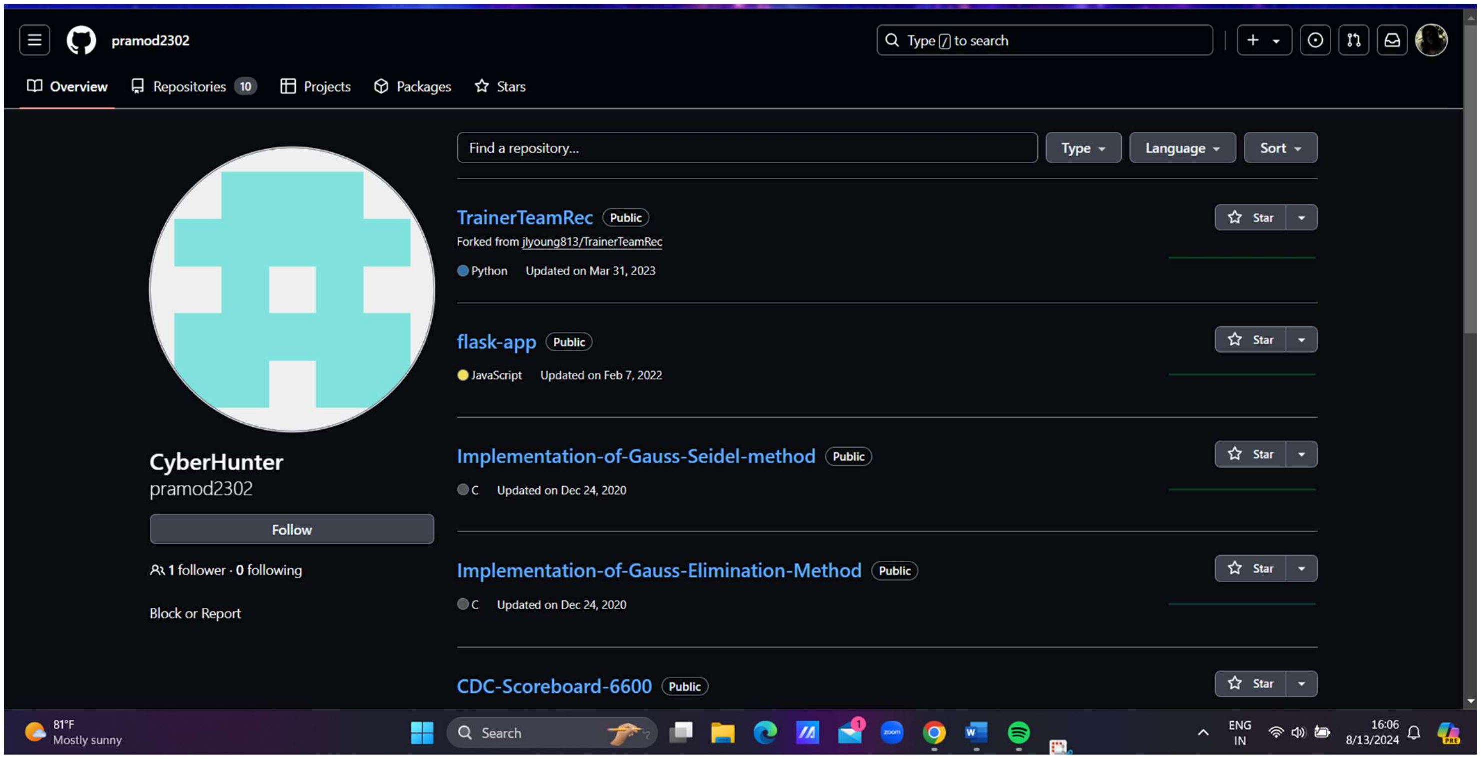


pgp.mit.edu/pks/lookup?search=CyberHunter&op=index

Search results for 'cyberhunter'

```
Type bits/keyID     Date       User ID
pub  4096R/5B1AEC58 2018-12-19 Chris Dodunski <cdodunski@cyberhunter.solutions>
pub  4096R/FA2AAC93 2017-01-27 cyberhunter <cyberhunter@sigaintevyh2rzvw.onion>
pub  1024D/9B2F7A40 1997-07-07 cyberhunter <thomasjk@post3.tele.dk>
```

Task 4 : Uncover Employment History or Affiliations



CyberHunter
pramod2302

1 follower · 0 following

TrainerTeamRec Public
Forked from jlyoung813/TrainerTeamRec
Python Updated on Mar 31, 2023

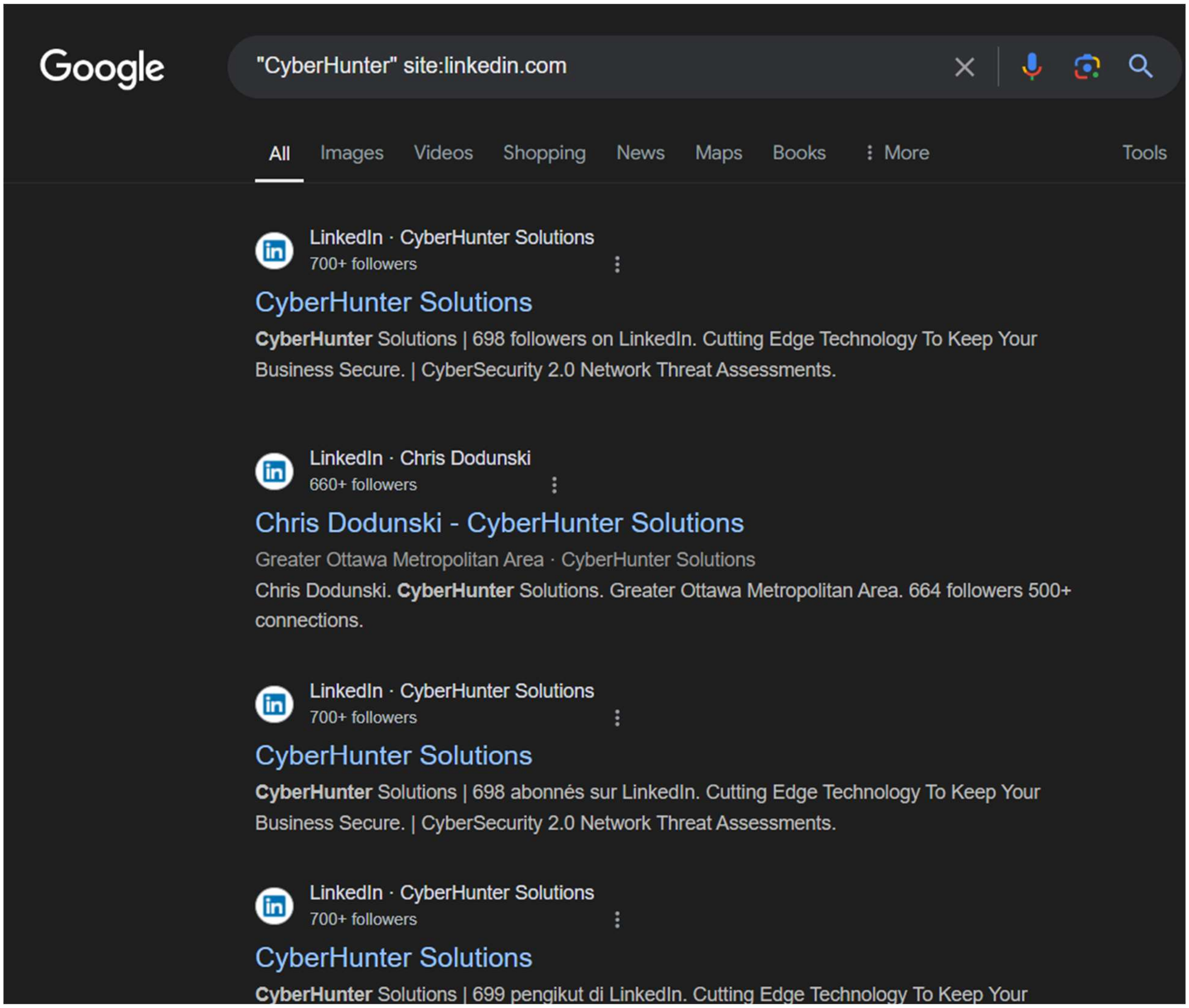
flask-app Public
JavaScript Updated on Feb 7, 2022

Implementation-of-Gauss-Seidel-method Public
C Updated on Dec 24, 2020

Implementation-of-Gauss-Elimination-Method Public
C Updated on Dec 24, 2020

CDC-Scoreboard-6600 Public

Google Dorks



"CyberHunter" site:linkedin.com

LinkedIn · CyberHunter Solutions
700+ followers

CyberHunter Solutions

CyberHunter Solutions | 698 followers on LinkedIn. Cutting Edge Technology To Keep Your Business Secure. | CyberSecurity 2.0 Network Threat Assessments.

LinkedIn · Chris Dodunski
660+ followers

Chris Dodunski - CyberHunter Solutions

Greater Ottawa Metropolitan Area · CyberHunter Solutions

Chris Dodunski. **CyberHunter** Solutions. Greater Ottawa Metropolitan Area. 664 followers 500+ connections.

LinkedIn · CyberHunter Solutions
700+ followers

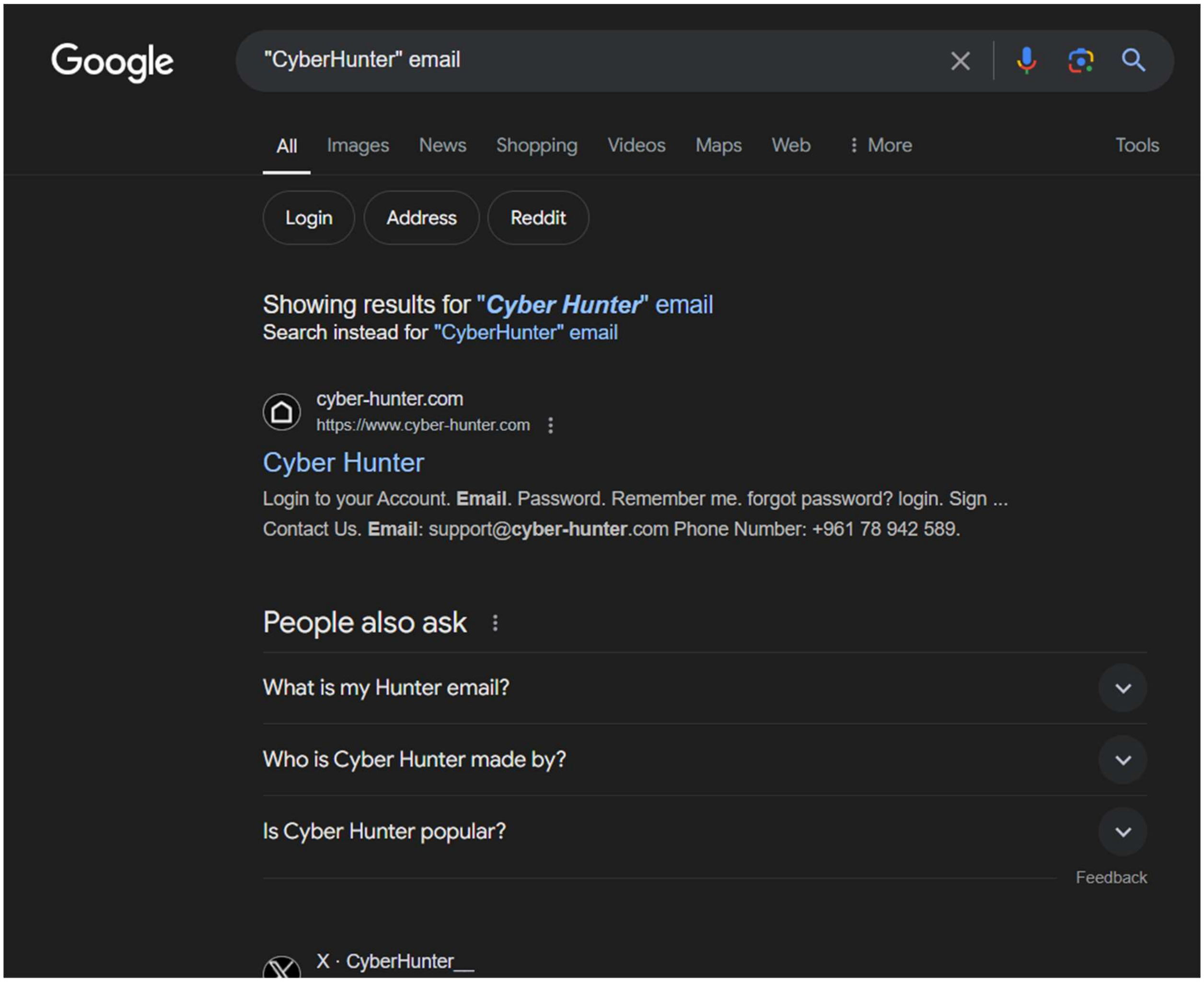
CyberHunter Solutions

CyberHunter Solutions | 698 abonnés sur LinkedIn. Cutting Edge Technology To Keep Your Business Secure. | CyberSecurity 2.0 Network Threat Assessments.

LinkedIn · CyberHunter Solutions
700+ followers

CyberHunter Solutions

CyberHunter Solutions | 699 pengikut di LinkedIn. Cutting Edge Technology To Keep Your



Showing results for "*Cyber Hunter*" email
Search instead for "CyberHunter" email

cyber-hunter.com
https://www.cyber-hunter.com

Cyber Hunter

Login to your Account. **Email**. Password. Remember me. forgot password? login. Sign ...
Contact Us. **Email**: support@**cyber-hunter**.com Phone Number: +961 78 942 589.

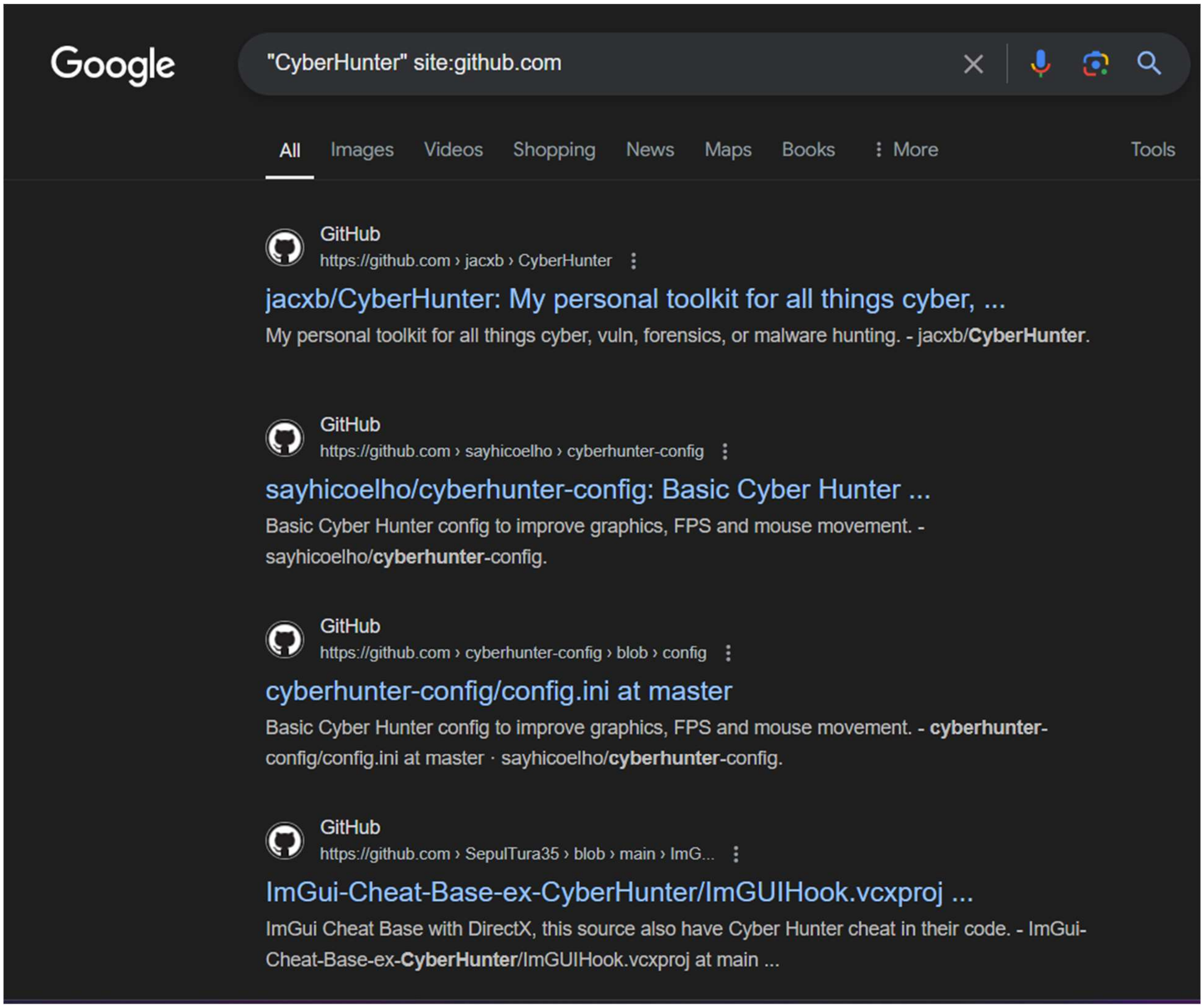
People also ask

What is my Hunter email?

Who is Cyber Hunter made by?

Is Cyber Hunter popular?

X · CyberHunter__



"CyberHunter" site:github.com

GitHub
https://github.com › jacxb › CyberHunter

jacxb/CyberHunter: My personal toolkit for all things cyber, ...

My personal toolkit for all things cyber, vuln, forensics, or malware hunting. - jacxb/**CyberHunter**.

GitHub
https://github.com › sayhicoelho › cyberhunter-config

sayhicoelho/cyberhunter-config: Basic Cyber Hunter ...

Basic Cyber Hunter config to improve graphics, FPS and mouse movement. - sayhicoelho/**cyberhunter**-config.

GitHub
https://github.com › cyberhunter-config › blob › config

cyberhunter-config/config.ini at master

Basic Cyber Hunter config to improve graphics, FPS and mouse movement. - **cyberhunter-**config/config.ini at master · sayhicoelho/**cyberhunter**-config.

GitHub
https://github.com › SepulTura35 › blob › main › ImG...

ImGui-Cheat-Base-ex-CyberHunter/ImGUIHook.vcxproj ...

ImGui Cheat Base with DirectX, this source also have Cyber Hunter cheat in their code. - ImGui-Cheat-Base-ex-**CyberHunter**/ImGUIHook.vcxproj at main ...

1) Possible real name:

- The screenshots don't reveal a definitive real name for CyberHunter.

2) Associated email addresses:

- No specific email addresses are shown in the screenshots.

3) Social media profiles:

- Twitter (X): A profile for @CyberHunter is shown, but don't have much detail about the content.

4) Employment history or affiliations:

- The screenshots don't reveal any clear employment history or affiliations for CyberHunter.

Learning Experience

In this lab, I learned how to set up and use an OSINT (Open-Source Intelligence) virtual machine to investigate an online persona. I practiced using various tools and techniques to search for information across different platforms like social media, forums, and public records. The lab taught me how to look for clues about someone's real identity, find their email addresses, and uncover their online presence. I also learned about using advanced search techniques like Google Dorks. While the screenshots didn't show much specific information about "CyberHunter," the exercise helped me understand the process of gathering and organizing online intelligence. This experience showed me how OSINT can be used in cybersecurity investigations, but also made me aware of the importance of privacy and responsible use of these tools.