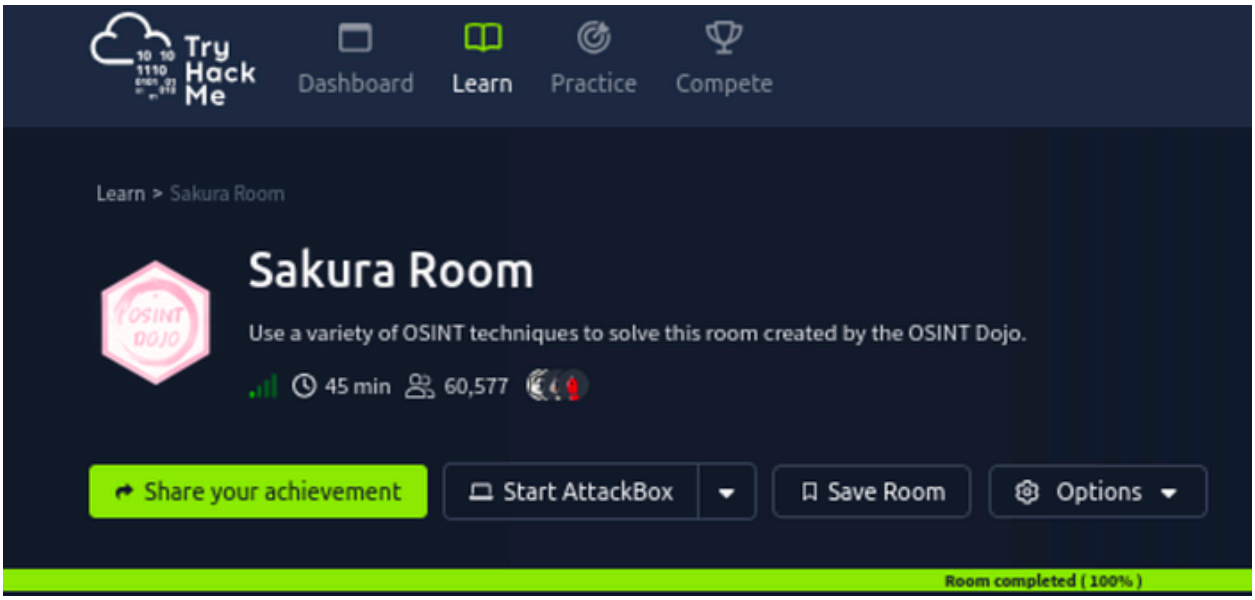
SAKURA ROOM -TRY HACK ME- ROOM

5kullk3r

7 min read

.

Oct 18, 2025



Hello everyone! This is a slightly different room compared to the others.

This is a beginner-friendly OSINT room from the TryHackMe platform titled “Sakura Room”

This room is classified as easy and is a OSINT ctf-type challenge. I hope this write-up helps guide you through the process!

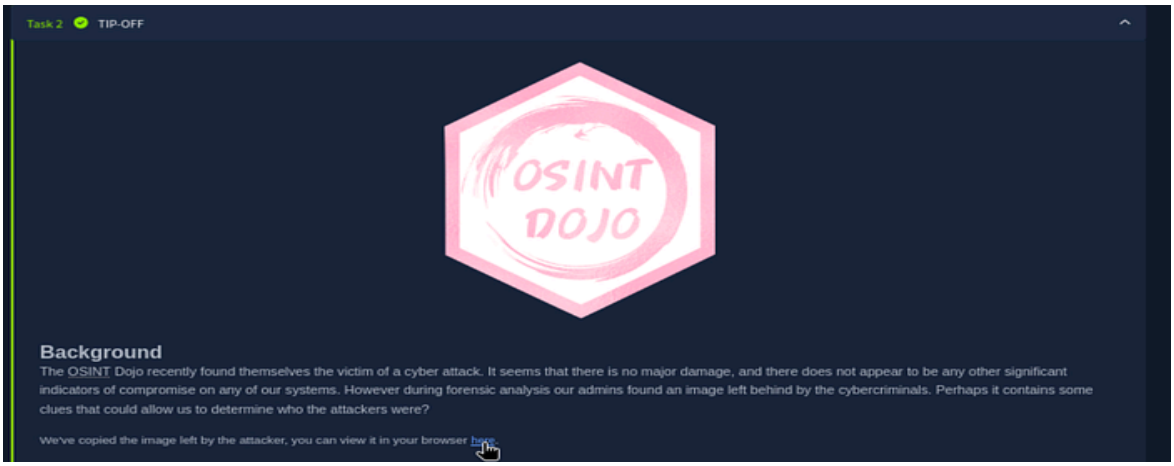
My goal is to help you understand each step and provide clear explanations so that anyone, whether a beginner or experienced, can follow along and understand the reasoning behind each action. I hope this write-up makes the process smoother and easier to grasp.

Enough talk — let's dive right in, and I hope you enjoy the journey! :)

Hecker supremacy xD

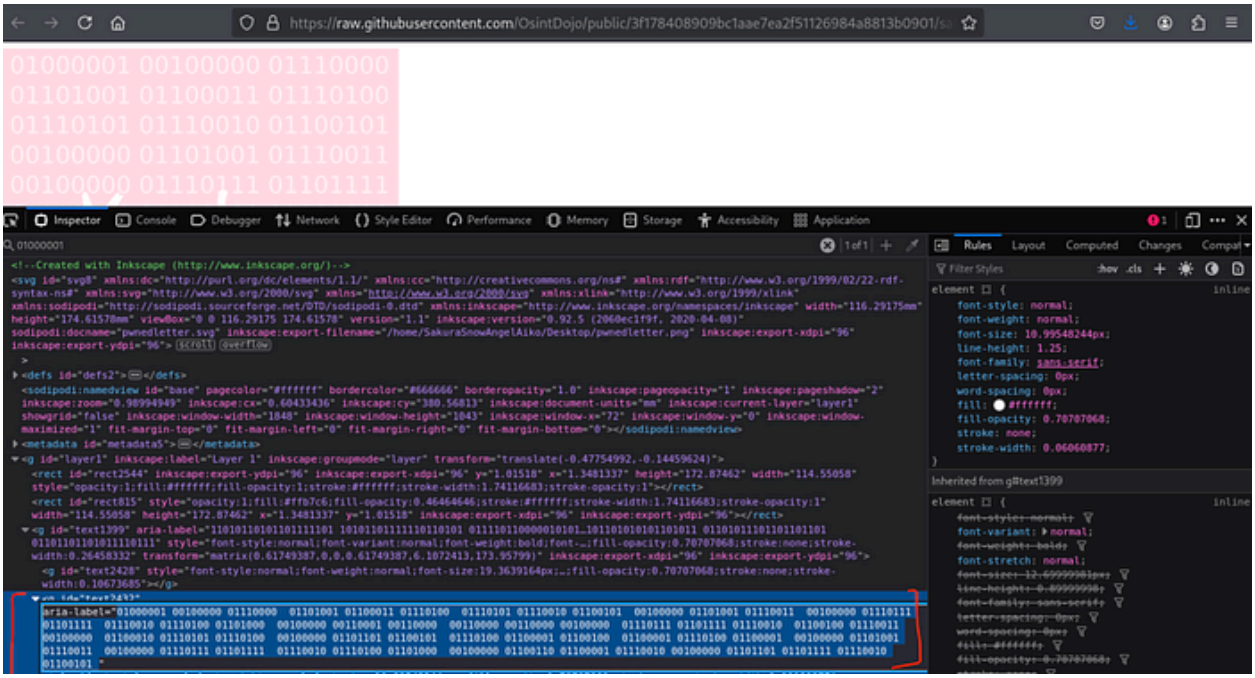
Task 1 —

Task 2 — Image inspection & metadata

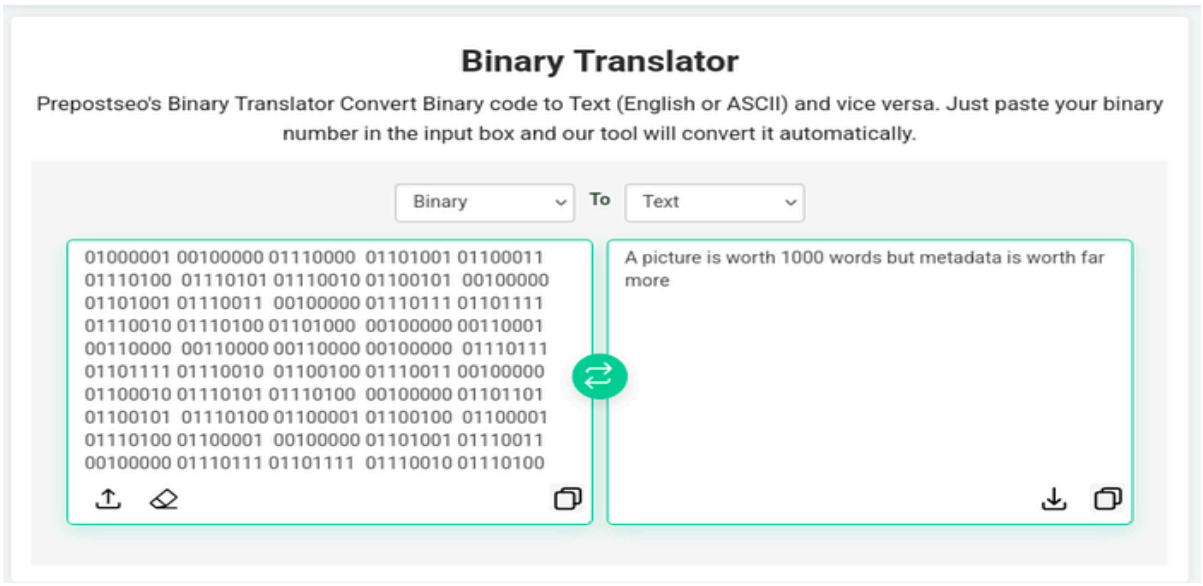


I start by clicking on the image and inspecting it

Since I see the binary blobs in the background I feel it has something to do with decoding binary to text.



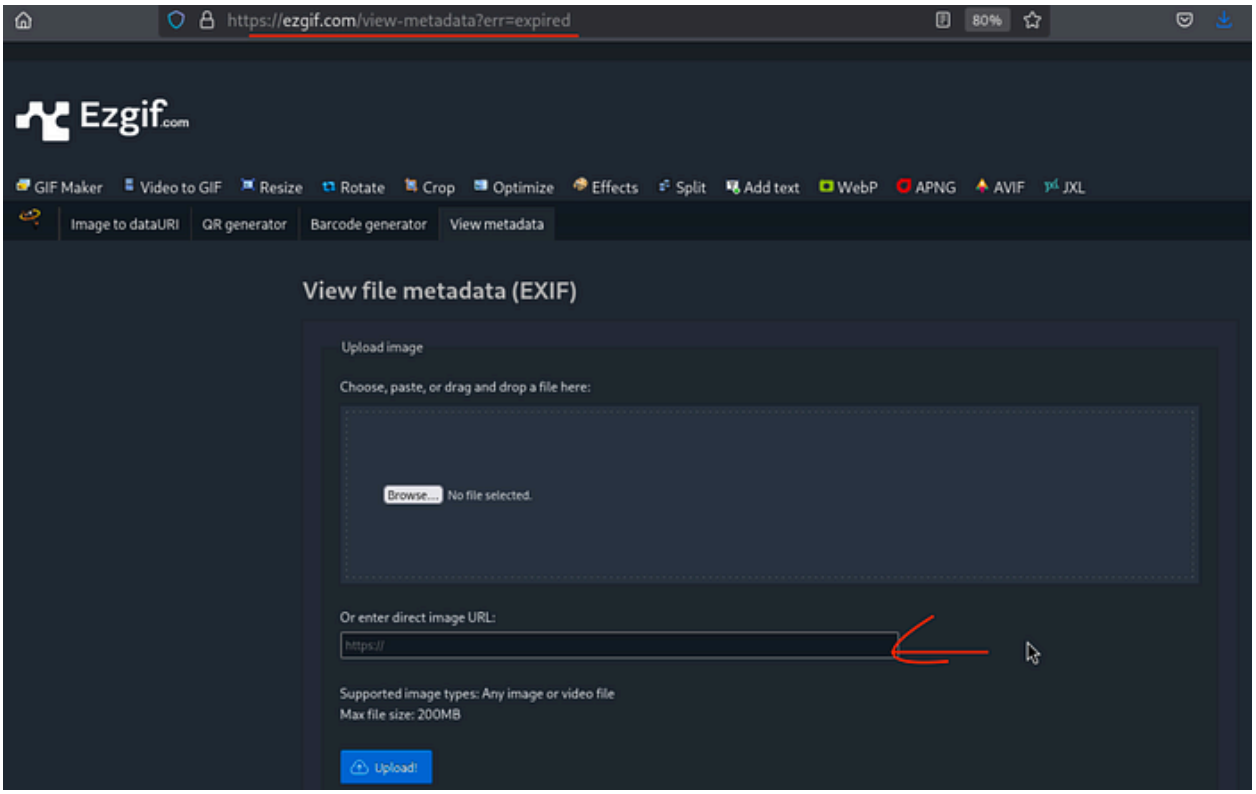
So through inspecting the page I find the Binary and copy paste it in a



Binary -> Text converter and I get hit with a message to check the metadata

The minute I see the word metadata, exif tools spawns in my mind

I head to the online tool



View file metadata (EXIF data) online

Easily view EXIF metadata of images and videos online. Upload files up to 200MB to access camera settings, date…

and paste the URL directly and that shows me the file path containing

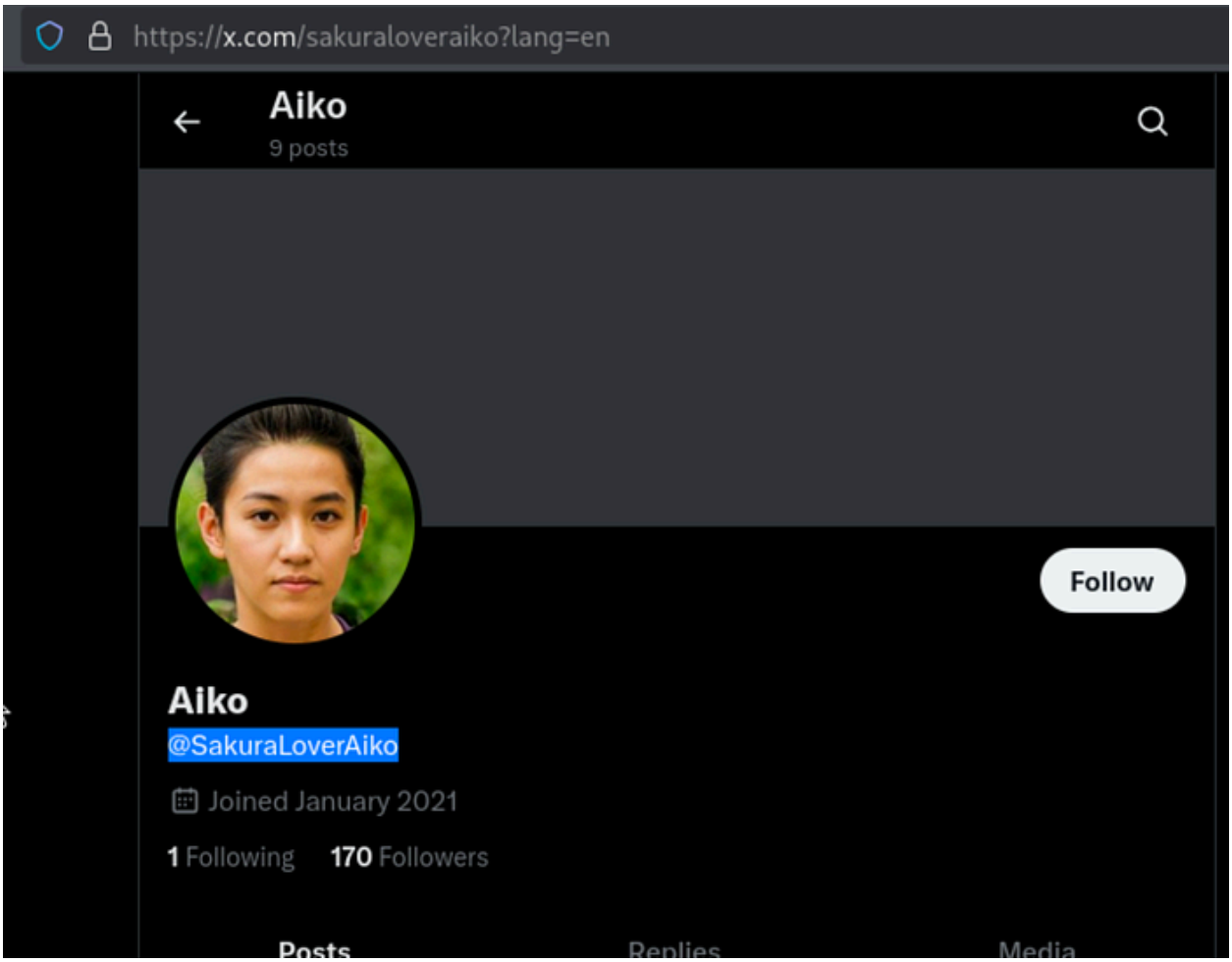
ExifTool output:

ExifTool Version Number	13.17
File Name	file.svg
Directory	.
File Size	850 kB
File Modification Date/Time	2025:09:27 06:19:06+02:00
File Access Date/Time	2025:09:27 06:19:06+02:00
File Inode Change Date/Time	2025:09:27 06:19:06+02:00
File Permissions	-rw-r--r--
File Type	SVG
File Type Extension	svg
MIME Type	image/svg+xml
Xmlns	http://www.w3.org/2000/svg
Image Width	116.29175mm
Image Height	174.61578mm
View Box	0 0 116.29175 174.61578
SVG Version	1.1
ID	svg8
Version	0.92.5 (2060ec1f9f, 2020-04-08)
Docname	pwnedletter.svg
Export-filename	/home/SakuraSnowAngelAiko/Desktop/pwnedletter.png
Export-xdpi	96
Export-ydpi	96
Metadata ID	metadata5
Work Format	image/svg+xml
Work Type	http://purl.org/dc/dcmitype/StillImage
Work Title	

`SakuraSnowAngelAiko/`

Task 3 — Find social profile, get real name, PGP to extract email

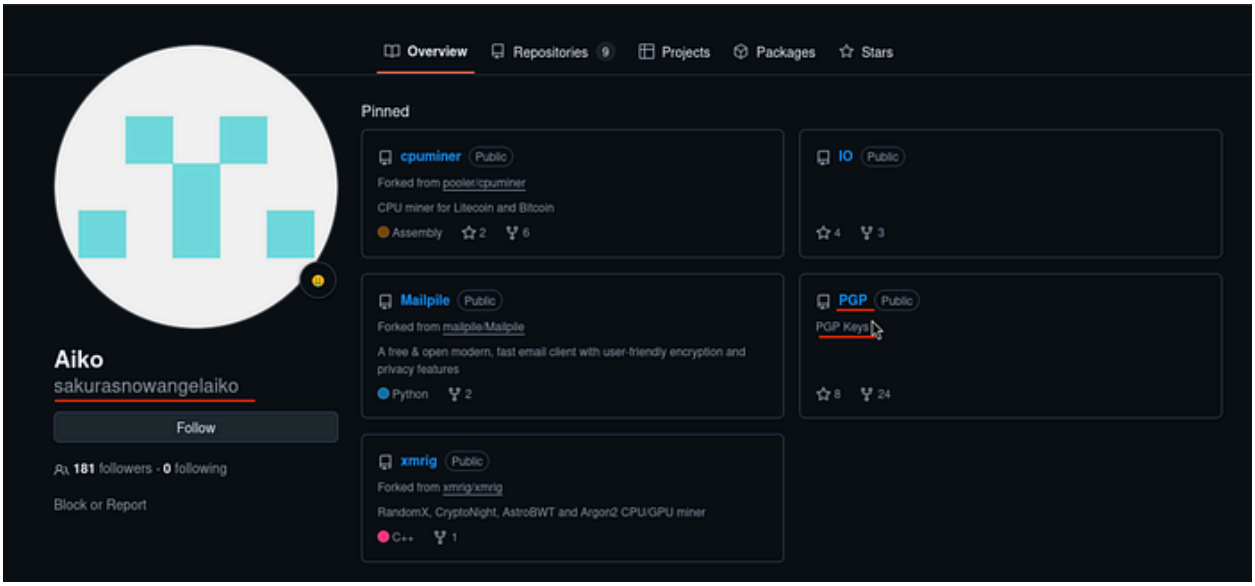
I go online to the browser and just search up: SakuraSnowAngelAiko and I see the x page(a.k.a Twitter) & Github link



Clicking on the x page and scrolling through I see the introduction post and from there I find the name is :

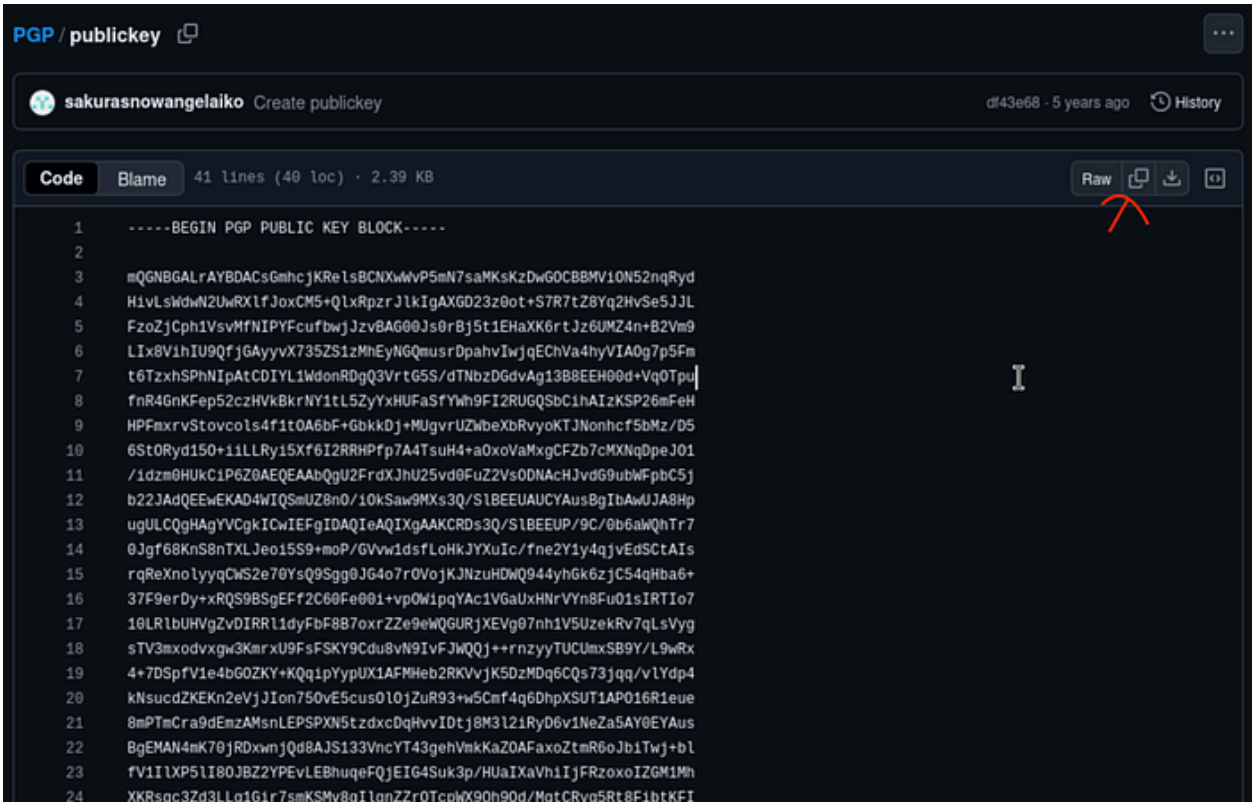
Aiko Abe

Now thinking about the e-mail, I remember seeing the pgp folder.

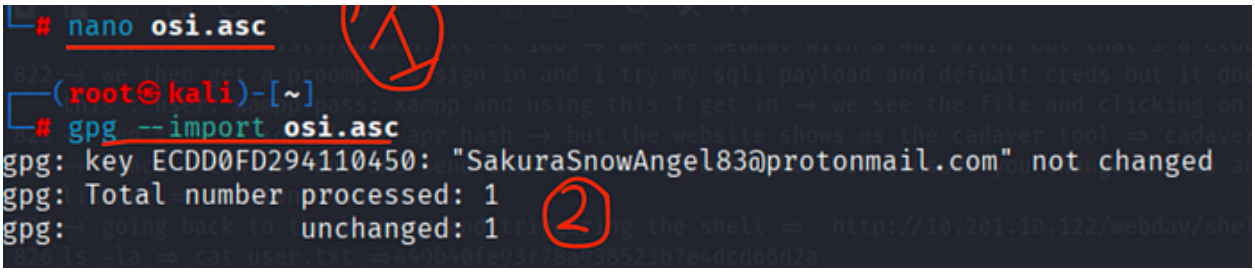


That lead the way to obtain the e-mail

I copied the pgp content from the public key file and head to the terminal



Next I create an .asc file :



nano osi.asc

Then I paste the pgp content here and save it

Then using this command :

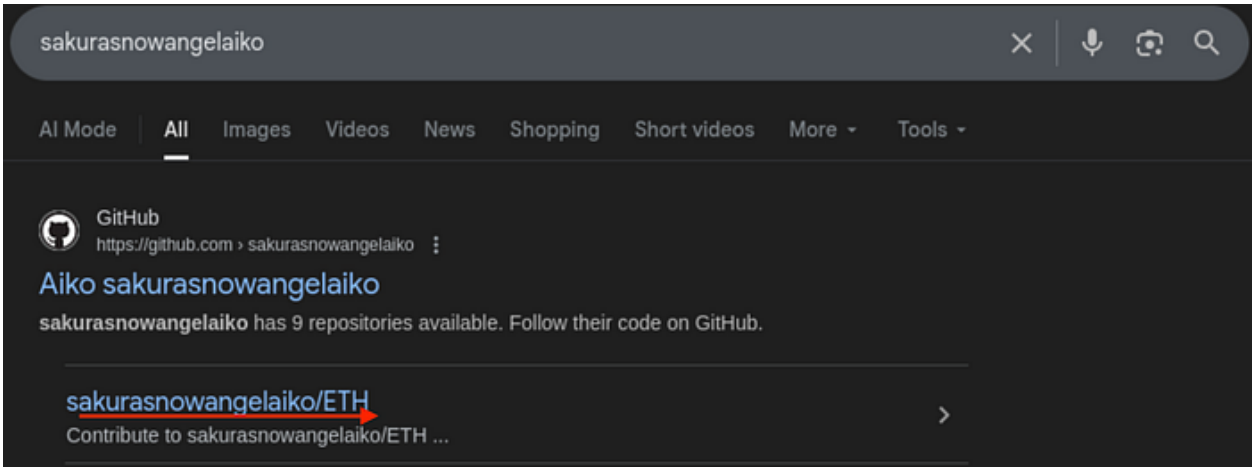
gpg — import osi.asc

This shows me the e-mail:

SakuraSnowAngel83@protonmail.com

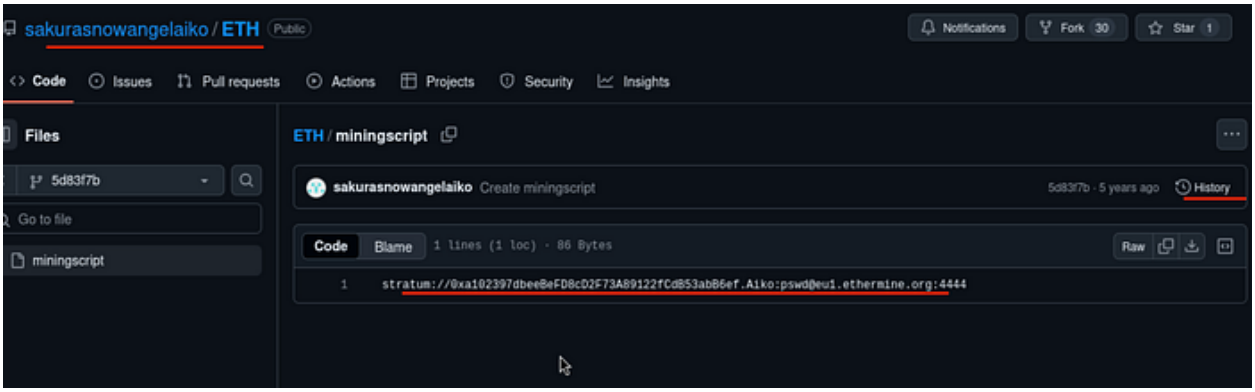
Task 4 — Ethereum address & blockchain tracing

I remember seeing a repo during the initial search which was called ETH



So I head to it and scour throught it, I end up seeing a crypto blockchain id

but it feels incorrect even when I searched it up.

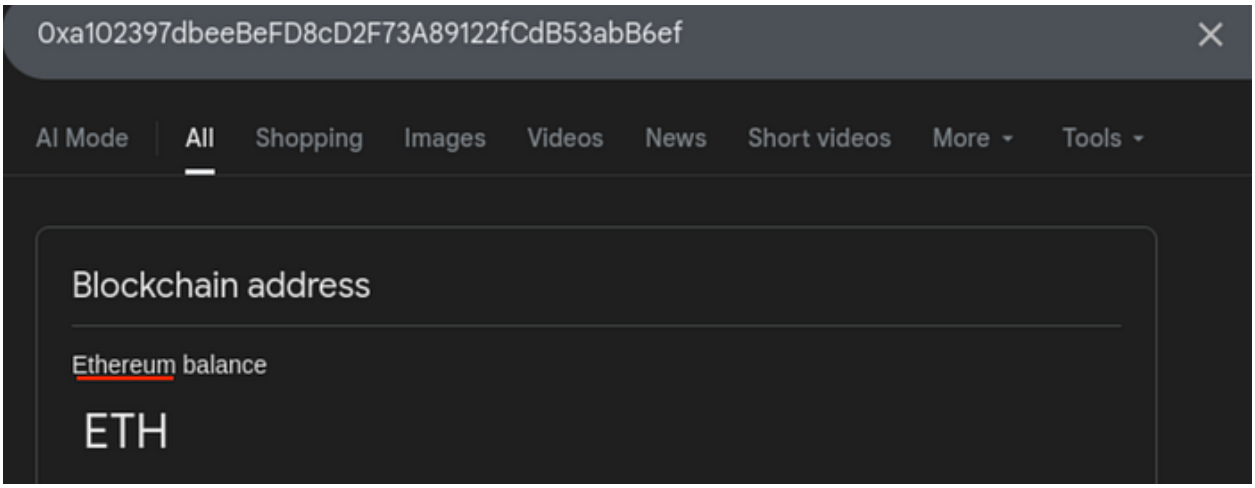


Then seeing the history tab I see the previous update and this leads me to crypto address, this leads me to 2nd subpart answer:

0xa102397dbeeBeFD8cD2F73A89122fCdB53abB

6ef

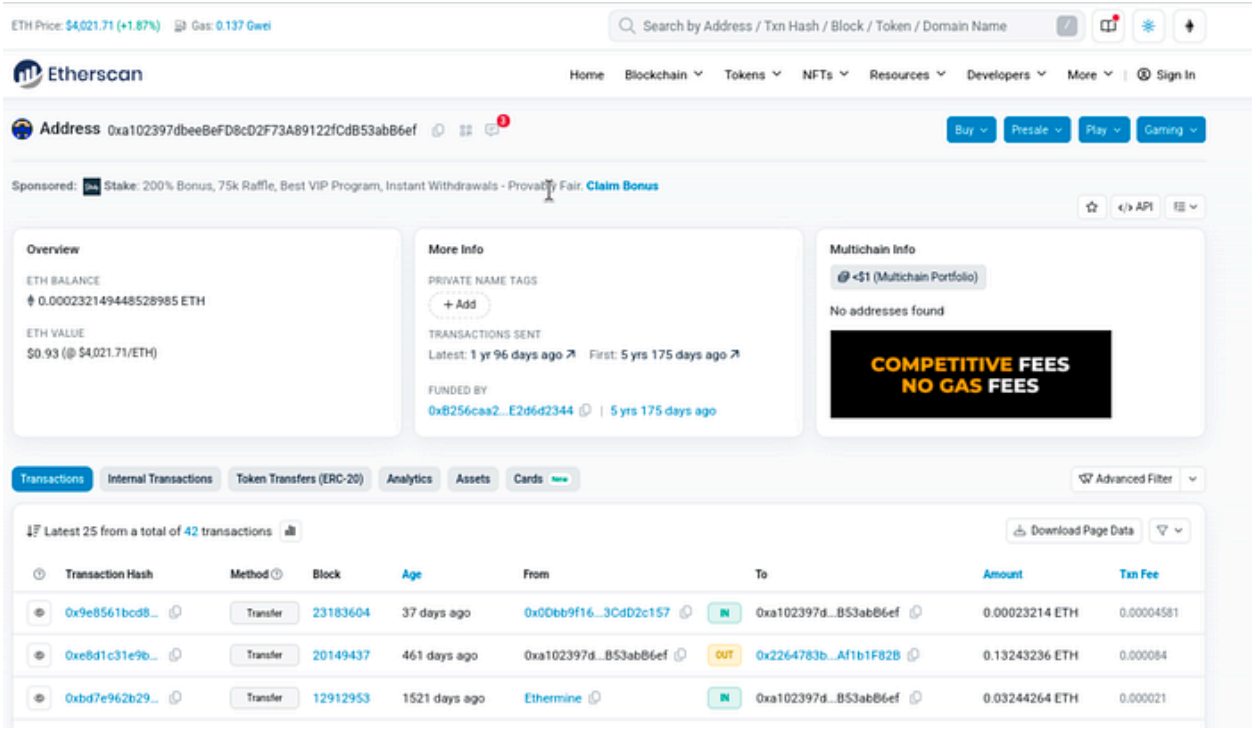
Now, through personal knowledge I know ETH stands for



Ethereum

it helps me with the initial answer

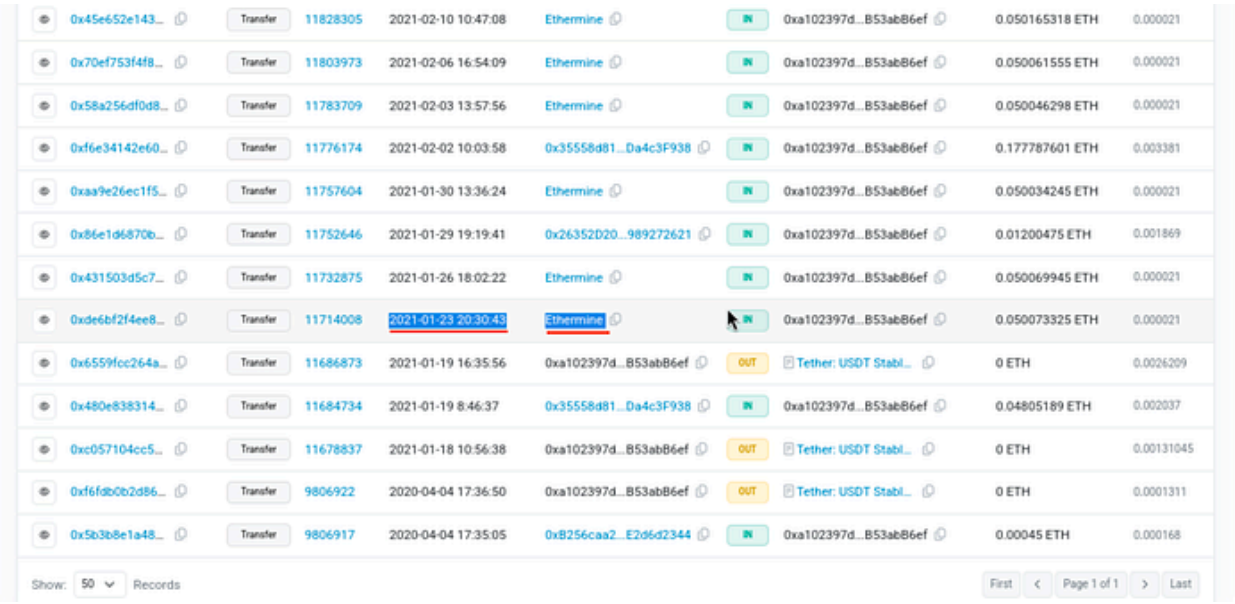
Next searchin up the crypto address online I get to see the activity in this website:



https://etherscan.io/txs?a=0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef

I head straight to the transactions bar and sort it.

Then scrolling down to 2021 and the specifics mentioned I find the mining pool which is:

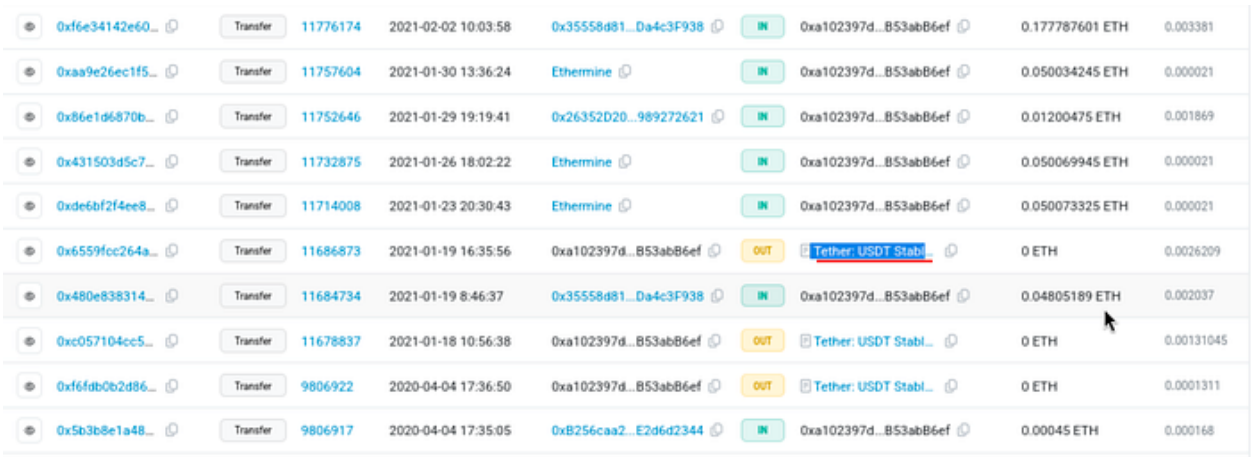


0x45e652e143...	Transfer	11828305	2021-02-10 10:47:08	Ethermine	IN	0xa102397d...B53abB6ef	0.050165318 ETH	0.000021
0x70ef753f4f8...	Transfer	11803973	2021-02-06 16:54:09	Ethermine	IN	0xa102397d...B53abB6ef	0.050061555 ETH	0.000021
0x58a256df0d8...	Transfer	11783709	2021-02-03 13:57:56	Ethermine	IN	0xa102397d...B53abB6ef	0.050046298 ETH	0.000021
0xf6e34142e60...	Transfer	11776174	2021-02-02 10:03:58	0x35558d81...Da4c3F938	IN	0xa102397d...B53abB6ef	0.177787601 ETH	0.003381
0xaa9e26ec1f5...	Transfer	11757604	2021-01-30 13:36:24	Ethermine	IN	0xa102397d...B53abB6ef	0.050034245 ETH	0.000021
0x86e1d6870b...	Transfer	11752646	2021-01-29 19:19:41	0x26352D20...989272621	IN	0xa102397d...B53abB6ef	0.01200475 ETH	0.001869
0x431503d5c7...	Transfer	11732875	2021-01-26 18:02:22	Ethermine	IN	0xa102397d...B53abB6ef	0.050069945 ETH	0.000021
0xde6bf2f4ee8...	Transfer	11714008	2021-01-23 20:30:43	Ethermine	IN	0xa102397d...B53abB6ef	0.050073325 ETH	0.000021
0x6559fcc264a...	Transfer	11686873	2021-01-19 16:35:56	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.0026209
0x480e838314...	Transfer	11684734	2021-01-19 8:46:37	0x35558d81...Da4c3F938	IN	0xa102397d...B53abB6ef	0.04805189 ETH	0.002037
0xc057104cc5...	Transfer	11678837	2021-01-18 10:56:38	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.00131045
0xf6fdb0b2d86...	Transfer	9806922	2020-04-04 17:36:50	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.0001311
0x5b3b8e1a48...	Transfer	9806917	2020-04-04 17:35:05	0xB256caa2...E2d6d2344	IN	0xa102397d...B53abB6ef	0.00045 ETH	0.000168

Show: 50 Records — First < Page 1 of 1 > Last

Ethermine

Through scrolling I see other type of crypto converted to :



0xf6e34142e60...	Transfer	11776174	2021-02-02 10:03:58	0x35558d81...Da4c3F938	IN	0xa102397d...B53abB6ef	0.177787601 ETH	0.003381
0xaa9e26ec1f5...	Transfer	11757604	2021-01-30 13:36:24	Ethermine	IN	0xa102397d...B53abB6ef	0.050034245 ETH	0.000021
0x86e1d6870b...	Transfer	11752646	2021-01-29 19:19:41	0x26352D20...989272621	IN	0xa102397d...B53abB6ef	0.01200475 ETH	0.001869
0x431503d5c7...	Transfer	11732875	2021-01-26 18:02:22	Ethermine	IN	0xa102397d...B53abB6ef	0.050069945 ETH	0.000021
0xde6bf2f4ee8...	Transfer	11714008	2021-01-23 20:30:43	Ethermine	IN	0xa102397d...B53abB6ef	0.050073325 ETH	0.000021
0x6559fcc264a...	Transfer	11686873	2021-01-19 16:35:56	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.0026209
0x480e838314...	Transfer	11684734	2021-01-19 8:46:37	0x35558d81...Da4c3F938	IN	0xa102397d...B53abB6ef	0.04805189 ETH	0.002037
0xc057104cc5...	Transfer	11678837	2021-01-18 10:56:38	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.00131045
0xf6fdb0b2d86...	Transfer	9806922	2020-04-04 17:36:50	0xa102397d...B53abB6ef	OUT	Tether: USDT Stabl...	0 ETH	0.0001311
0x5b3b8e1a48...	Transfer	9806917	2020-04-04 17:35:05	0xB256caa2...E2d6d2344	IN	0xa102397d...B53abB6ef	0.00045 ETH	0.000168

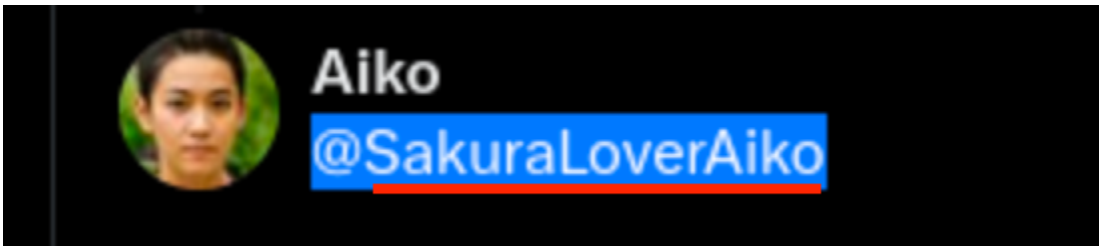
Tether USD

and this answers the 4th part of the question.

Task 5 — Twitter findings, Wi-Fi & BSSID

Now here to find the answers to the questions, I head back to the x page.

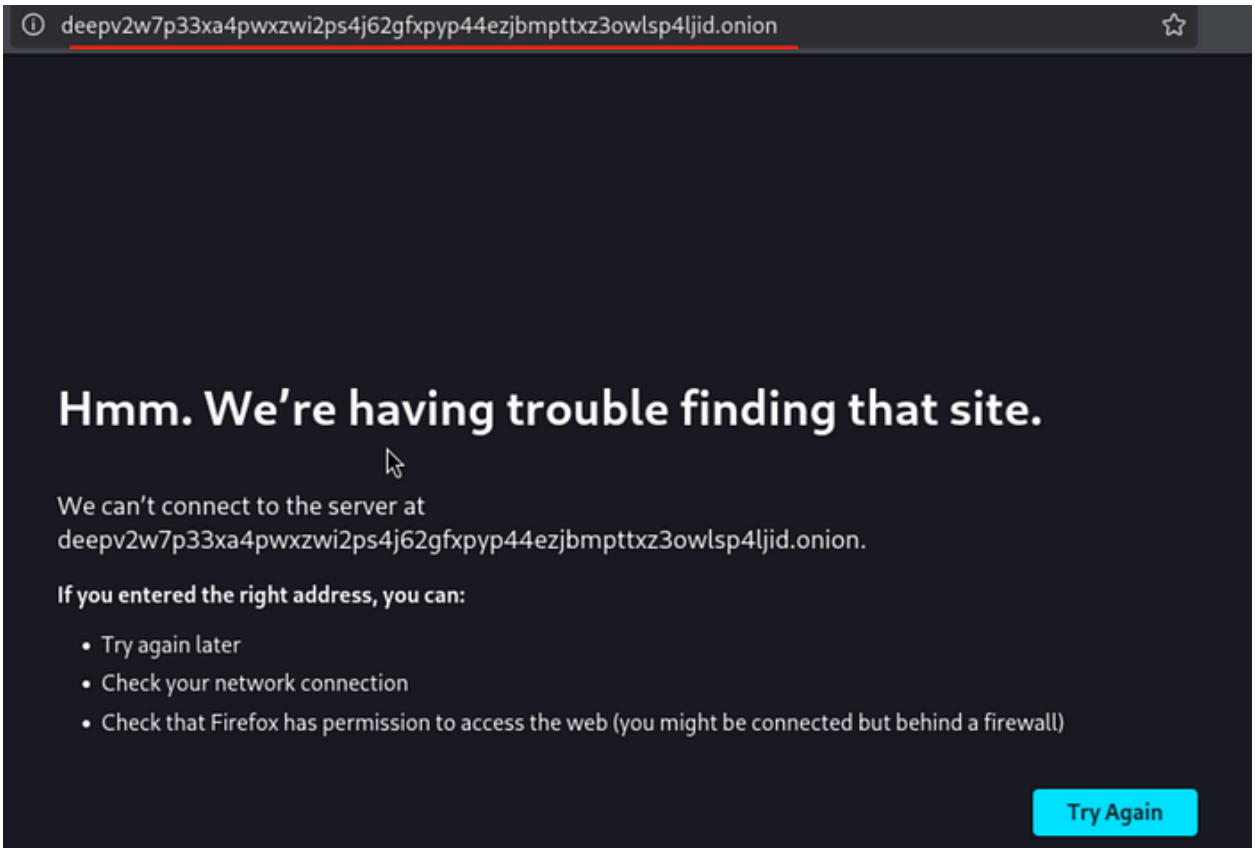
Since I already know both the x handles answering the username is very easy:



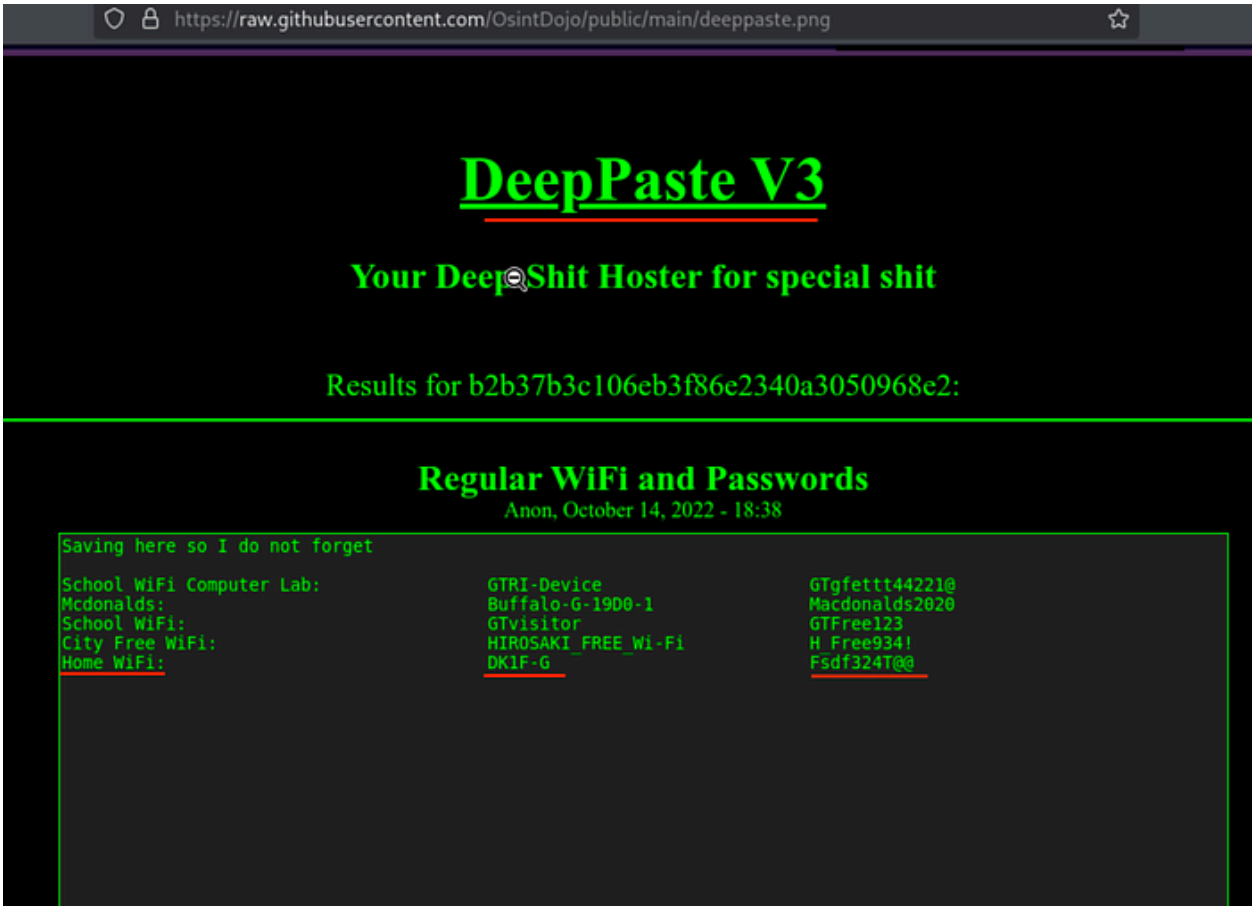
current handle: @SakuraLoverAiko

Now to find the BSSID, I remember seeing on the x page a screenshot with the clue of the wifi details.

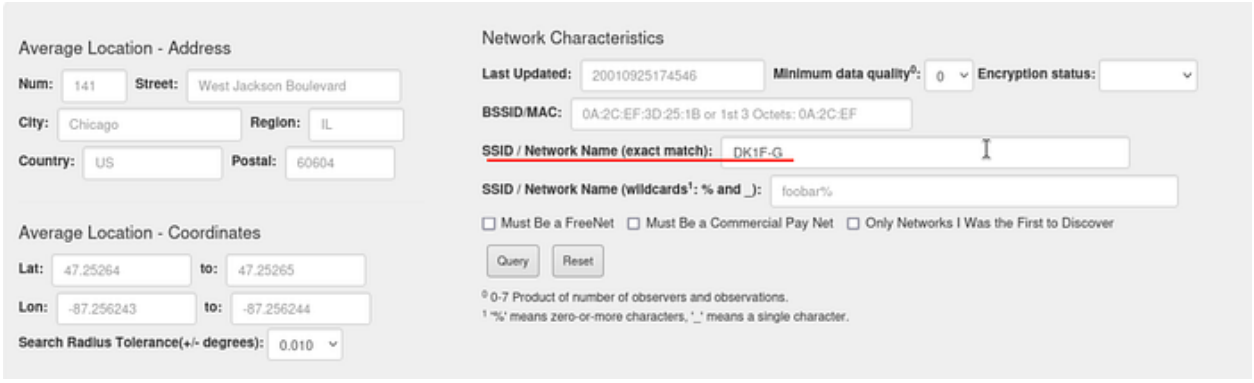
Heading to that post it hints something about deep searching and using a darknet tool(deeppaste)



But as I couldn't find an operating version of tool, by using the hint we see the image in deeppaste v3 and see the home wifi DK1F-G and password Fsdf324T@@



Now to get through this we use the famed tool: WiGLE



I create the account and use the advanced search feature and past the SSID value: DK1F-G and query it and that leads me to the BSSID:

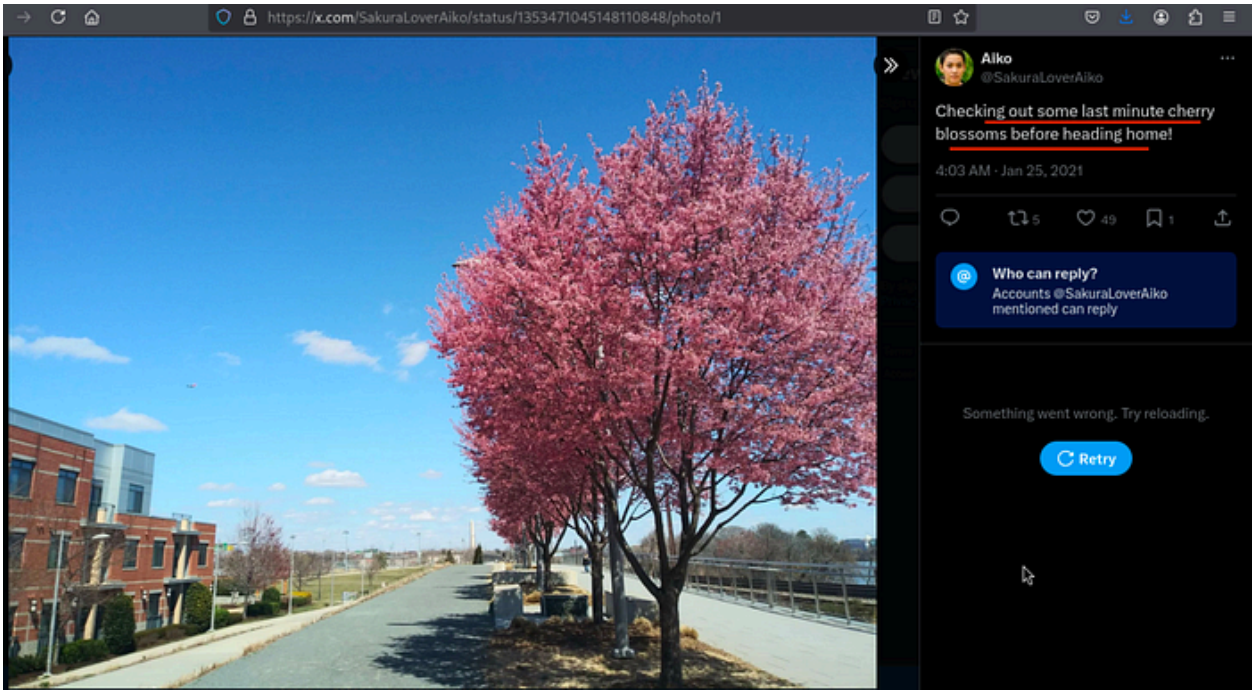

Computed Network Properties

Network ID	84:AF:EC:34:FC:F8
Network Name	
Type	infra
Encryption	WPA
Channel	11
Beacon Interval	
SSID	DK1F-G
Est. Latitude	40.60551453
Est. Longitude	140.4606781
First Seen	2019-04-24T18:54:29.000Z
Most Recently Seen	2019-05-02T12:21:09.000Z
comment	Appended by southrain on 2021-04-12 02:57:14: hey i am not the flag Appended by se6m6g on 2022-02-12 09:16:01: happy hacking :) Appended by test2345678907654323456 7 on 2022-07-06 02:04:04: THM{R4B1T_H0L3}

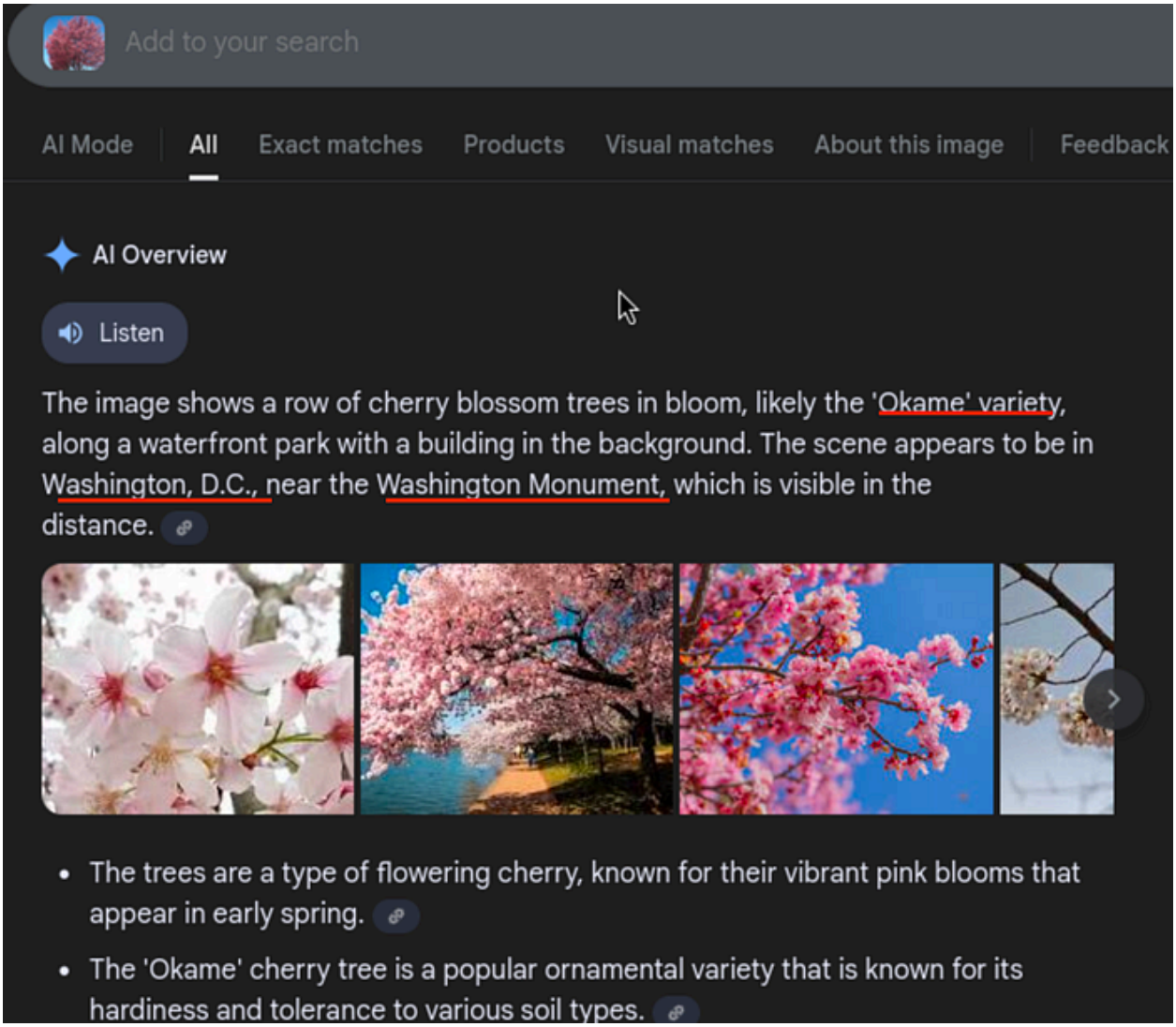
84:AF:EC:34:FC:F8

Task 6 — Visual geolocation (landmarks & blossoms)

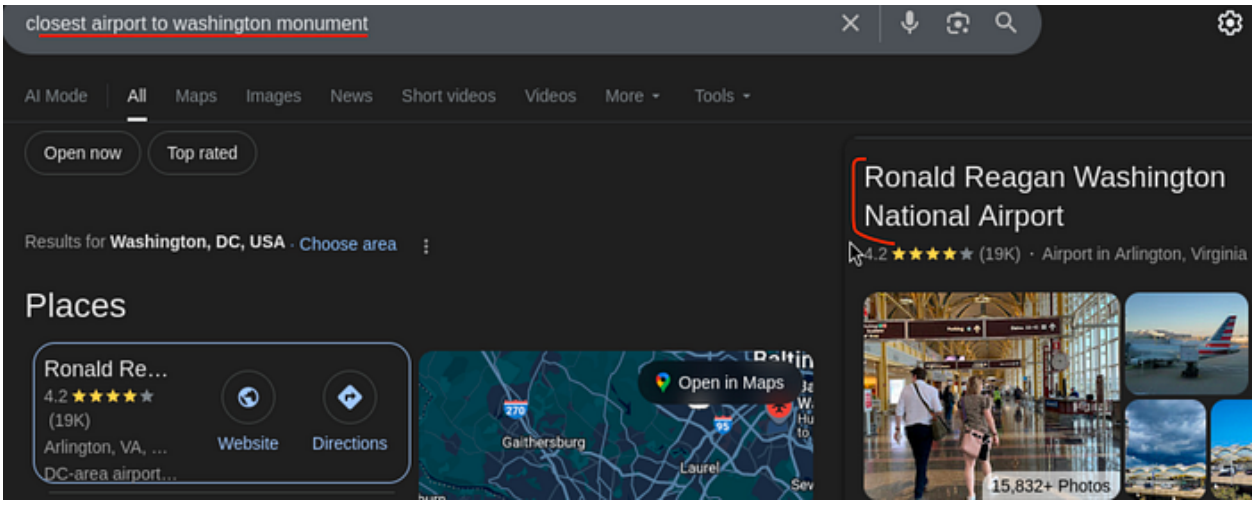
Now for the final set of tasks,



I head back to the x page and as per the question the image shows a beautiful scenery of cherry blossoms.



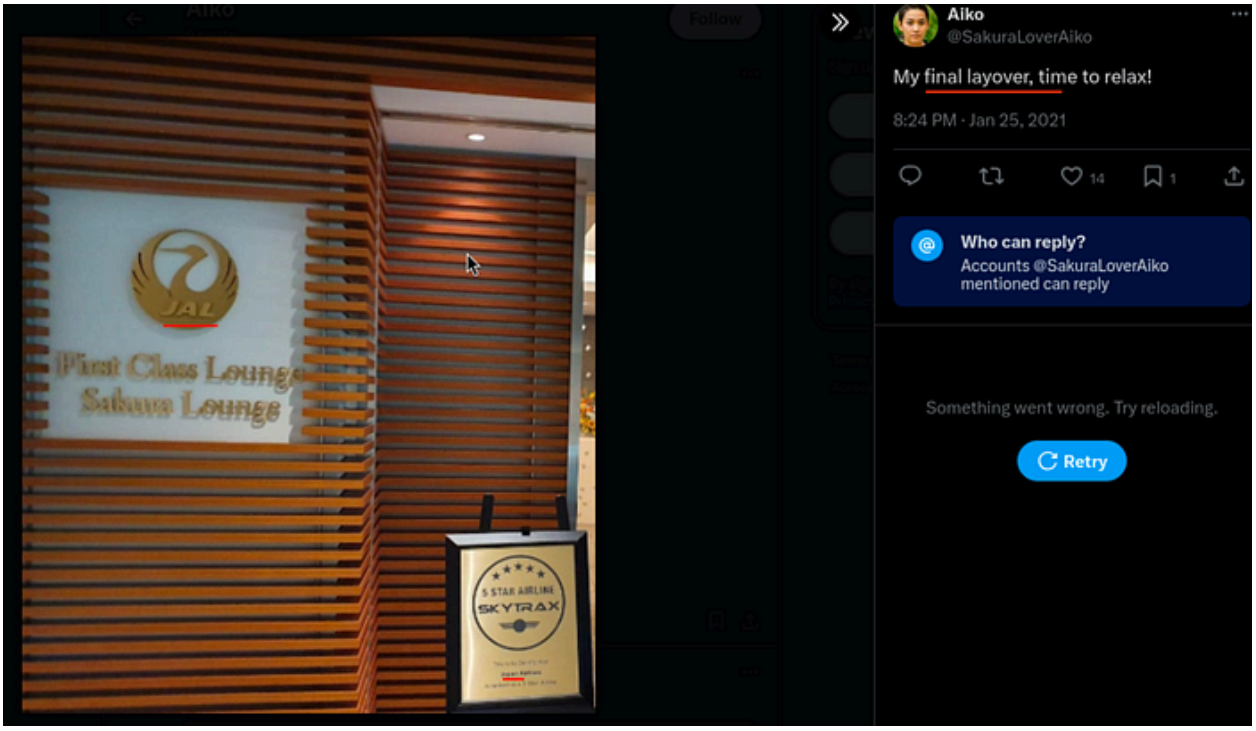
Now taking the image, I simply throw it to Google lens and it automatically showed me the clue about the Okame variety of blossom and the Washington monument in the background.



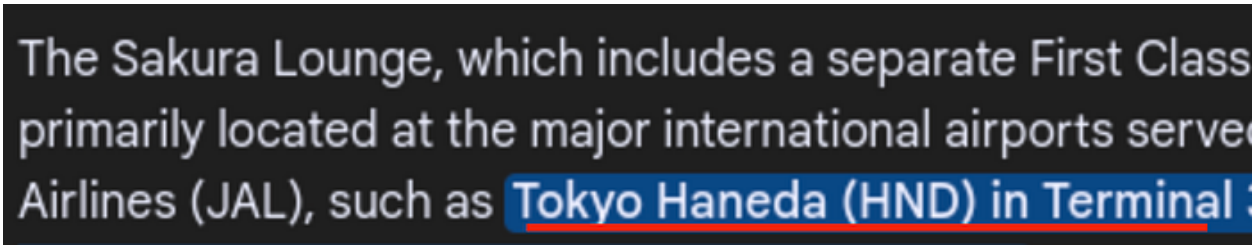
This was a major prompt and by searching the closest airport we see:

Ronald Reagan Airport {DCA}

Next, for the layover there is a post and the first thing that catches my eye is the logo and name below(JAL) which confirmed my suspicion that it was Japan Airlines.

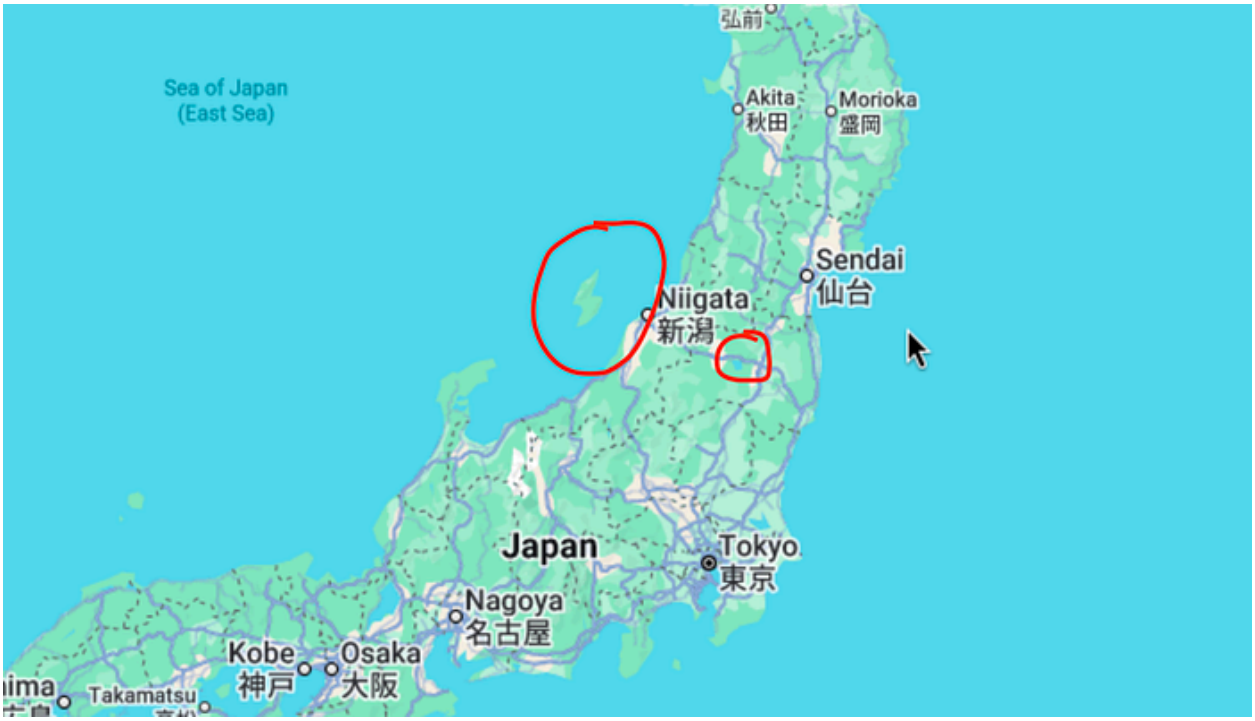


Now with a tiny search I confirmed that it was in the famous:



Haneda Airport {HND}

Next, with it already being in the Japanese region I take one good look at the map and head to Google Maps right away and look at Japan Zoomed out

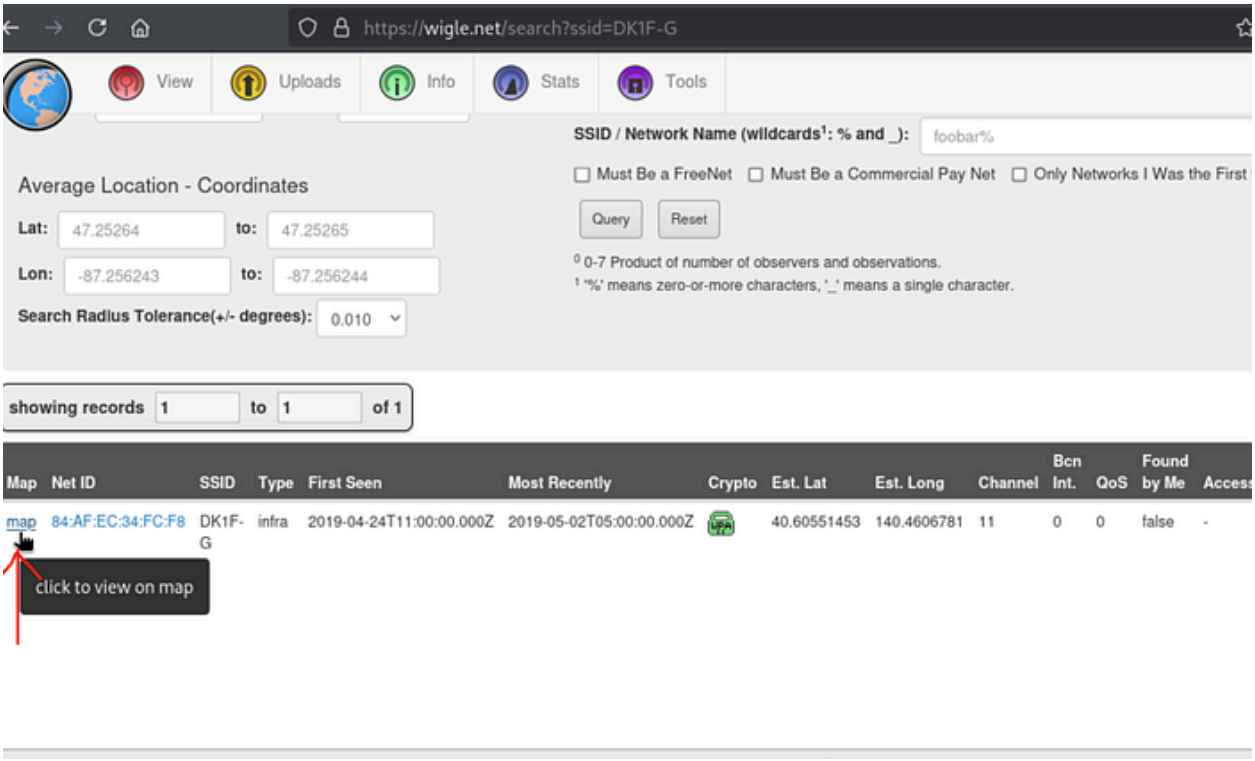


I see the unique island structure {I'm referring to Sado Island :)}

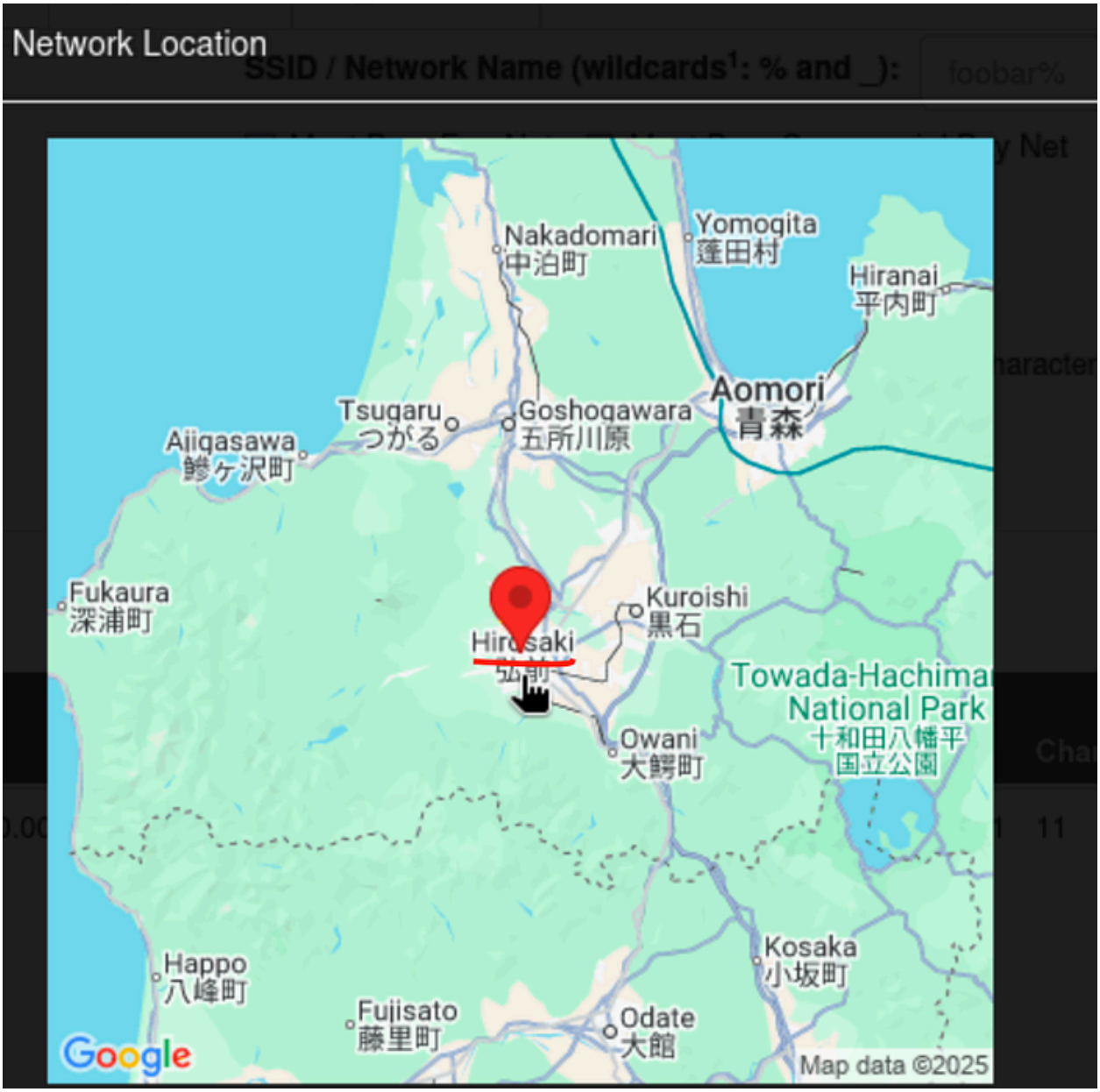
Quickly zooming in I see the lake and it's name is:

Lake Inawashiro

And, for the last part to find out which is his home region/city, I head straight back to WiGLE



And in the same page of the SSID where I found the BSSID I see the Map feature and clicking on it I see:



Hirosaki

These are the answers compiled :)

Task 2 TIP-OFF

Background

The OSINT Dojo recently found themselves the victim of a cyber attack. It seems that there is no major damage, and there does not appear to be any other significant indicators of compromise on any of our systems. However during forensic analysis our admins found an image left behind by the cybercriminals. Perhaps it contains some clues that could allow us to determine who the attackers were?

We've copied the image left by the attacker, you can view it in your browser here.

Instructions

Images can contain a treasure trove of information, both on the surface as well as embedded within the file itself. You might find information such as when a photo was created, what software was used, author and copyright information, as well as other metadata significant to an investigation. In order to answer the following question, you will need to thoroughly analyze the image found by the OSINT Dojo administrators in order to obtain basic information on the attacker.

Answer the questions below

What username does the attacker go by?

SakuraSnowAngelAiko

✓ Correct Answer

Task 3 RECONNAISSANCE

Background

It appears that our attacker made a fatal mistake in their operational security. They seem to have reused their username across other social media platforms as well. This should make it far easier for us to gather additional information on them by locating their other social media accounts.

Instructions

Most digital platforms have some sort of username field. Many people become attached to their usernames, and may therefore use it across a number of platforms, making it easy to find other accounts owned by the same person when the username is unique enough. This can be especially helpful on platforms such as on job hunting sites where a user is more likely to provide real information about themselves, such as their full name or location information.

A quick search on a reputable search engine can help find matching usernames on other platforms, and there are also a large number of specialty tools that exist for that very same purpose. Keep in mind, that sometimes a platform will not show up in either the search engine results or in the specialized username searches due to false negatives. In some cases you need to manually check the site yourself to be 100% positive if the account exists or not. In order to answer the following questions, use the attacker's username found in Task 2 to expand the OSINT investigation onto other platforms in order to gather additional identifying information on the attacker. Be wary of any false positives!

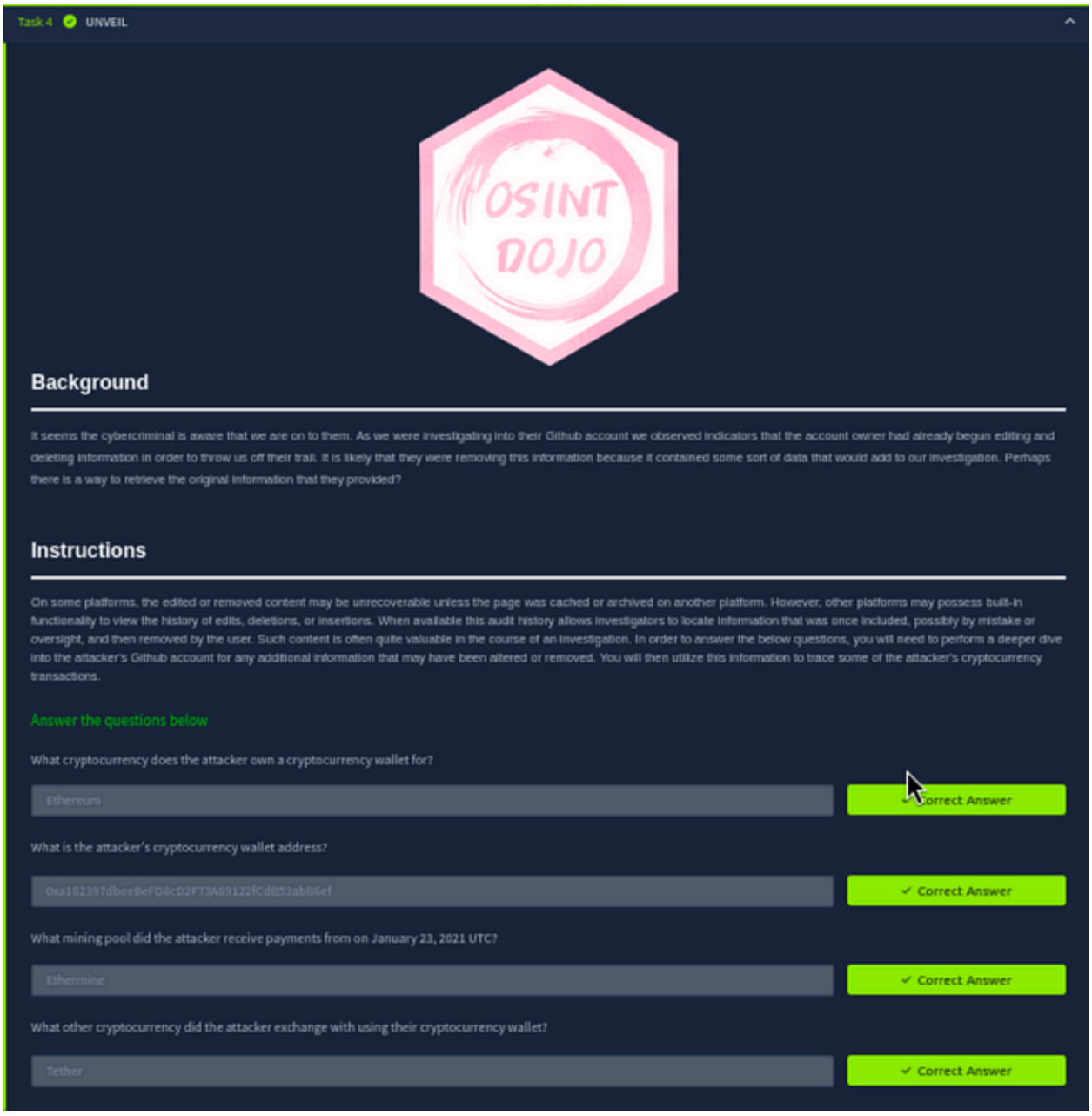
Answer the questions below

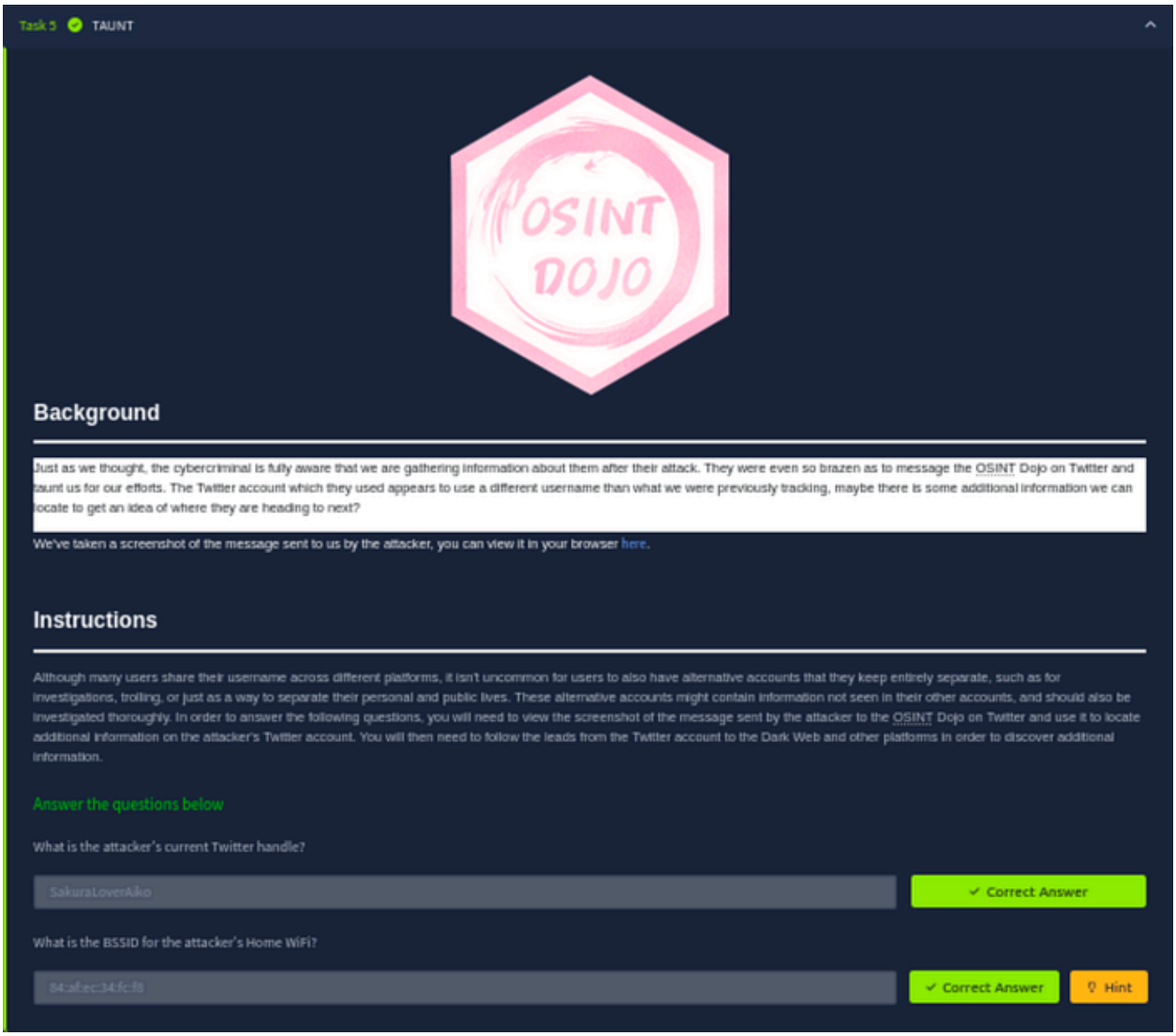
What is the full email address used by the attacker?

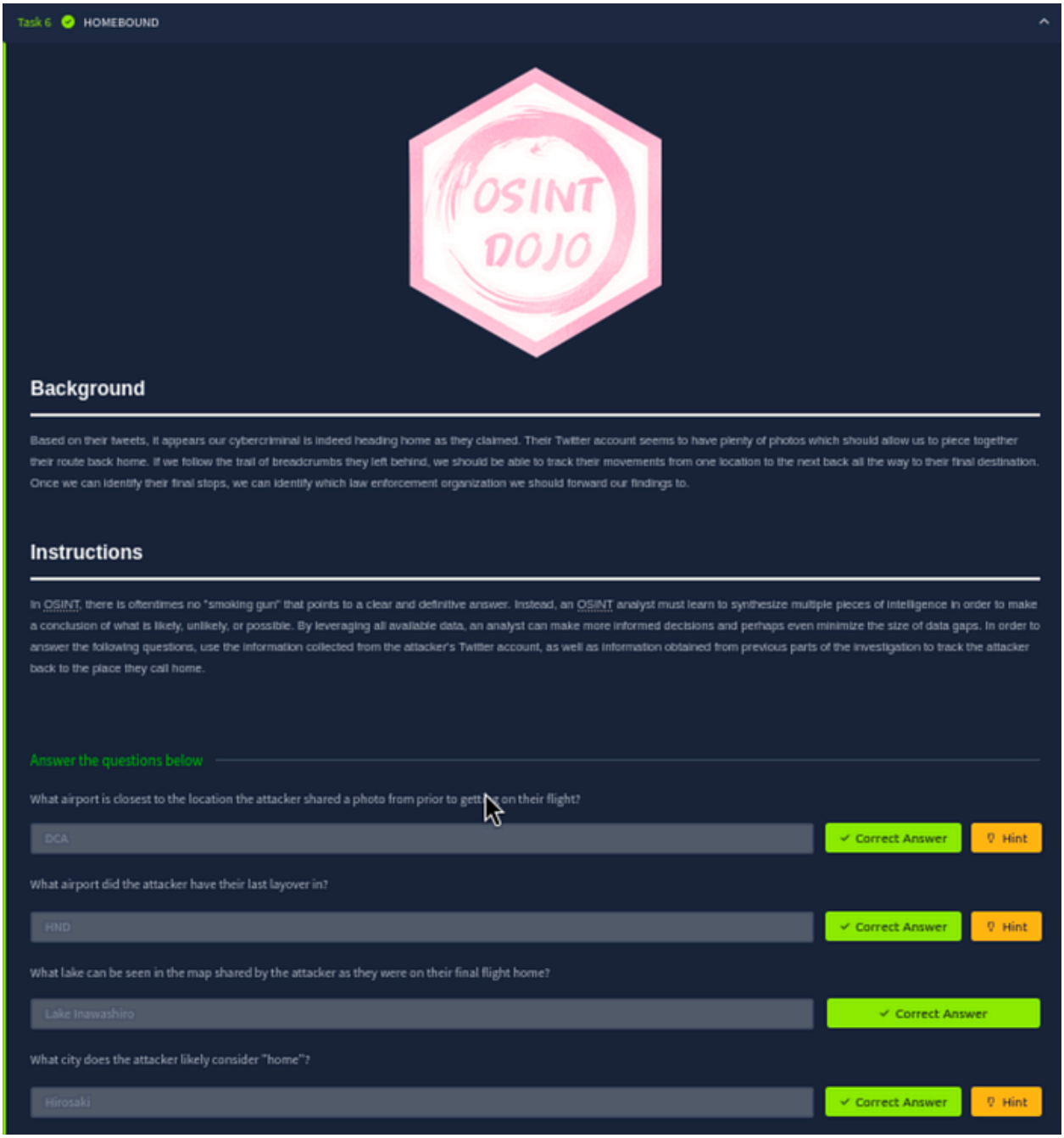
SakuraSnowAngel83@protonmail.com ✓ Correct Answer

What is the attacker's full real name?

Aiko Abe ✓ Correct Answer


Task 4 UNVEIL
OSINT DOJO
Background
It seems the cybercriminal is aware that we are on to them. As we were investigating into their Github account we observed indicators that the account owner had already begun editing and deleting information in order to throw us off their trail. It is likely that they were removing this information because it contained some sort of data that would add to our investigation. Perhaps there is a way to retrieve the original information that they provided?
Instructions
On some platforms, the edited or removed content may be unrecoverable unless the page was cached or archived on another platform. However, other platforms may possess built-in functionality to view the history of edits, deletions, or insertions. When available this audit history allows investigators to locate information that was once included, possibly by mistake or oversight, and then removed by the user. Such content is often quite valuable in the course of an investigation. In order to answer the below questions, you will need to perform a deeper dive into the attacker's Github account for any additional information that may have been altered or removed. You will then utilize this information to trace some of the attacker's cryptocurrency transactions.
Answer the questions below
What cryptocurrency does the attacker own a cryptocurrency wallet for?
Ethereum
Correct Answer
What is the attacker's cryptocurrency wallet address?
0xa102397dbeeBeFD8cD2F73A89122fCd853abB6ef
Correct Answer
What mining pool did the attacker receive payments from on January 23, 2021 UTC?
Ethermine
Correct Answer
What other cryptocurrency did the attacker exchange with using their cryptocurrency wallet?
Tether
Correct Answer


Task 5
TAUNT
OSINT
DOJO
Background
Just as we thought, the cybercriminal is fully aware that we are gathering information about them after their attack. They were even so brazen as to message the OSINT Dojo on Twitter and taunt us for our efforts. The Twitter account which they used appears to use a different username than what we were previously tracking, maybe there is some additional information we can locate to get an idea of where they are heading to next?
We've taken a screenshot of the message sent to us by the attacker, you can view it in your browser here.
Instructions
Although many users share their username across different platforms, it isn't uncommon for users to also have alternative accounts that they keep entirely separate, such as for investigations, trolling, or just as a way to separate their personal and public lives. These alternative accounts might contain information not seen in their other accounts, and should also be investigated thoroughly. In order to answer the following questions, you will need to view the screenshot of the message sent by the attacker to the OSINT Dojo on Twitter and use it to locate additional information on the attacker's Twitter account. You will then need to follow the leads from the Twitter account to the Dark Web and other platforms in order to discover additional information.
Answer the questions below
What is the attacker's current Twitter handle?
SakuraLoveAiko
Correct Answer
What is the BSSID for the attacker's Home WiFi?
84:af:ec:34:fc:f8
Correct Answer
Hint



CONCLUSION:

I hope this write-up walkthrough was helpful to you all!

Doing this room gave me 2 takeaways:

1. OSINT though complex is actually fun
2. Japan is so beautiful, I have to pay a visit and soak in some the beauty

Now that I've gotten through it, I hope it helps you and gets you through the room as well. I plan on putting out more like these in the future!

If you guys want me to cover any specific room or challenge, or if you have any queries, feel free to drop a comment.

Imma bounce for now, but I'll catch you all in the next writeup!