

# SAKURA ROOM -TRY HACK ME- ROOM



5kullk3r

7 min read

Oct 18, 2025

The screenshot shows the TryHackMe interface. At the top, there's a navigation bar with a cloud icon, the text "Try Hack Me", and three main categories: Dashboard, Learn, and Practice. Below this, a sub-navigation bar shows "Learn > Sakura Room". The main content area features a pink hexagonal badge with "OSINT DOJO" text. The title "Sakura Room" is prominently displayed. A descriptive text below it reads: "Use a variety of OSINT techniques to solve this room created by the OSINT Dojo." To the left of the badge is a small green progress bar icon. To the right are icons for time (45 min), users (60,577), and a red notification count (9). Below these are four buttons: "Share your achievement", "Start AttackBox", "Save Room", and "Options". At the bottom of the screen, a green footer bar indicates "Room completed (100%)".

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 1  INTRODUCTION



Welcome to the OSINT Dojo's Sakura Room!

### Background

This room is designed to test a wide variety of different OSINT techniques. With a bit of research, most beginner OSINT practitioners should be able to complete these challenges. This room will take you through a sample OSINT investigation in which you will be asked to identify a number of identifiers and other pieces of information in order to help catch a cybercriminal. Each section will include some pretext to help guide you in the right direction, as well as one or more questions that need to be answered in order to continue on with the investigation. Although all of the flags are staged, this room was created using working knowledge from having led and assisted in OSINT investigations both in the public and private sector.

NOTE: All answers can be obtained via passive OSINT techniques, DO NOT attempt any active techniques such as reaching out to account owners, password resets, etc to solve these challenges.

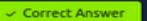
If you have any other questions, comments, or suggestions, please reach out to us at @OSINTDojo on Twitter.

### Instructions

Ready to get started? Type in "Let's Go!" in the answer box below to continue.

Answer the questions below

Are you ready to begin?

## Task 2 — Image inspection & metadata

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](#).

I start by clicking on the image and inspecting it

01000001 00100000 01110000  
01101001 01100011 01110100  
01110101 01110010 01100101  
00100000 01101001 01110011  
00100000 01110111 01101111  
01100000 01110100 01101000  
00100000 00110001 00110000  
00110000 00110000 00100000  
01110111 01101111 01110010  
01100100 01110000 01100000  
01100010 01110101 01110100  
00100000 01101101 01100101  
01110100 01101100 01100100  
00100000 01110111 01101111  
01110010 01101000 01101000  
00100000 00110000 01100001  
01110010 00110000 01101101  
01101111 01101010 01100101

You've  
**Been**  
**Pwned!**



---

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

The screenshot shows a browser window with the URL <https://raw.githubusercontent.com/OsintDojo/public/3f178408909bc1aae7ea2f51126984a8813b0901/s0>. The page displays a large block of binary code:

```
01000001 00100000 01110000  
01101001 01100011 01110100  
01110101 01110010 01100101  
00100000 01101001 01110011  
00100000 01110111 01101111
```

Below the binary code, the browser's developer tools are open, specifically the Elements tab. A red box highlights the binary code in the main content area. Another red box highlights a portion of the CSS styles for the text element containing the binary code.

```
<!-- Created with Inkscape (http://www.inkscape.org/) -->  
<svg id="svg8" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://creativecommons.org/ns#" xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/1999/xhtml" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:sodipodi="http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd" xmlns:inkscape="http://inkscape.org/namespaces/inkscape" width="116.29175mm" height="174.61578mm" viewBox="0 0 116.29175 174.61578" version="1.1" inkscape:version="0.92.5 (206dec19f, 2020-04-08)" sodipodi:docname="pwnedletter.svg" inkscape:export-filename="/home/SakuraSnowAngelAiko/Desktop/pwnedletter.png" inkscape:export-xdpi="96" inkscape:export-ydpi="96"></svg>
```

```
element #text {  
    font-style: normal;  
    font-weight: normal;  
    font-size: 10.99548244px;  
    line-height: 1.25;  
    font-family: sans-serif;  
    letter-spacing: 0px;  
    word-spacing: 0px;  
    fill: #000000;  
    fill-opacity: 1;  
    stroke: none;  
    stroke-width: 0.06060877;  
}  
Inherited from #text1399  
element #text {  
    font-style: normal;   
    font-variant: normal;   
    font-weight: bold;   
    font-stretch: normal;   
    font-size: 12.69999931px;   
    line-height: 1.2;   
    font-family: sans-serif;   
    letter-spacing: 0px;   
    word-spacing: 0px;   
    fill: #000000;   
    fill-opacity: 0.70707062; 
```

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

The screenshot shows a web-based binary translator tool titled "Binary Translator". The tool has two input fields: "Binary" and "To". The "Binary" field contains the previously copied binary code:

```
01000001 00100000 01110000 01101001 01100011  
01101001 01110101 01110010 01100101 00100000  
01101001 01110011 00100000 01110111 01101111  
01110010 01110100 01101000 00100000 00110001  
00110000 00110000 00110000 00100000 01110111  
01101111 01110010 01100100 00100000 01101101  
01100010 01110101 01110100 00100000 01101101  
01100101 01110100 01100001 01101001 01110011  
01110100 01100001 00100000 01101001 01110011  
00100000 01110111 01101111 01110010 01110100
```

The "To" field is set to "Text". The output text is:

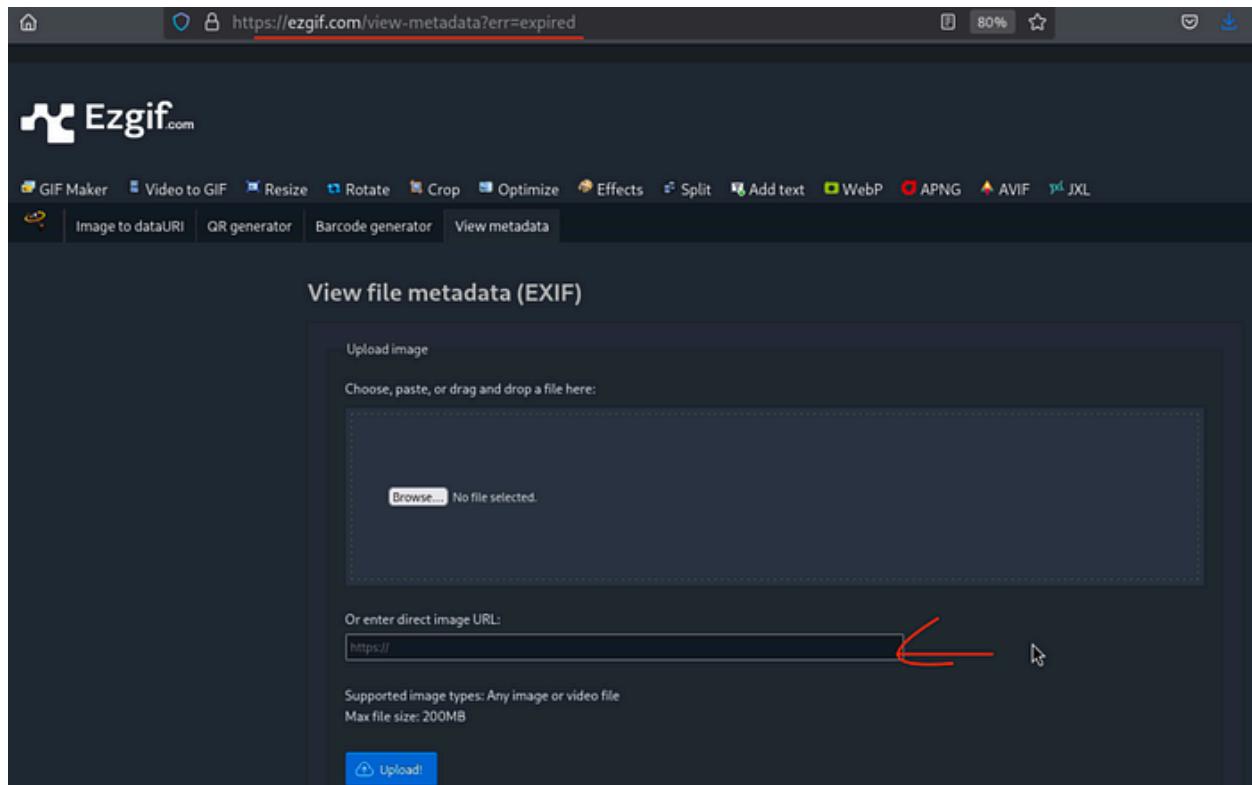
A picture is worth 1000 words but metadata is worth far more

Below the text output are download and copy icons.

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...

ezgif.com

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
Xmllns	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

A screenshot of a Twitter profile for a user named Aiko. The profile picture is a circular photo of a woman with dark hair. The bio information includes the handle **@SakuraLoverAiko**, the joining date **Joined January 2021**, and the follower count **170 Followers**. Below the bio, there are three navigation tabs: **Posts**, **Replies**, and **Media**. On the right side of the profile card, there is a **Follow** button.

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.

Aiko  
sakurasnowangelaiko

Follow  
181 followers · 0 following  
Block or Report

Pinned

- cpuminer** Public  
Forked from pooler/cpuminer  
CPU miner for Litecoin and Bitcoin  
Assembly ⭐ 2 ⚡ 6
- IO** Public  
⭐ 4 ⚡ 3
- Mailpile** Public  
Forked from mailpile/Mailpile  
A free & open modern, fast email client with user-friendly encryption and privacy features  
Python ⭐ 2 ⚡ 2
- xmrig** Public  
Forked from xmrig/xmrig  
RandomX, CryptoNight, AstroBlWT and Argon2 CPU/GPU miner  
C++ ⭐ 1 ⚡ 1

That lead the way to obtain the e-mail

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

PGP / publickey

sakurasnowangelaiko Create publickey d#43e68 - 5 years ago History

**Code** **Blame** 41 lines (40 loc) · 2.39 KB

```

1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3 mQGNBGAjRABDAsGmhcjKRelsBCNxwWp5mN7saMKsKzDw6OCBBMVi0N52nqRyd
4 HivLsWdwN2UwRXlfJoxCM5+QlxRpzrJ1kIgAXGD23z0t+S7R7tZ8Yq2HvSe5JJL
5 FzoZjCph1VsvMFNIPYFcufbwjJzv8AG00JsoRbj5t1EHaxXK6rtJz6UMZ4n+B2Vm9
6 Lix8VihIU90fj6Ayyvx735ZS1zMhEyNG0msurDpahvIwjqeChVa4hyVIA0g7p5Fm
7 t6TzxhSPhiPAtCDIYL1WdonRDq3VrtG55/dTNbzDgdvAg13B8EHH0d+vq0Tpj
8 fn4GnKFep52czHVkBkrNY1tL5ZyYxHuFaSfYwh9FI2RUGQScCihAIzKSP26mFeH
9 HPFmxrvStovcols4f1t0A6bF-GbkkDj+MuqvrUZwbeXbRvyoKTJNonhcf5bMz/05
10 6St0Ryd150+i1LRy15XF6I2RRHPfp7A4Tsuh4+a0xoVaXgCFzb7cMXNlqOpeJ01
11 /idzm@HUKC1p6Z0AEQEAAbQg2FrDXJhU25vd0FuZ2Vs0DNAchJvdG9ubWFpbC5j
12 b22JAdQEEwEKAD4WIQSmlZ8n0/10KSaw9MXs3Q/S1BEEUAUCYAusBgIbAwUJA8Hp
13 ugULCQgHAgYVCgkICwIEFgIDAQTeAQIXgAAKCRDs3Q/S1BEEUP/9C/0b6aWQhTr7
14 0Jgf68KnS8nTXLJeo15S9+m0P/GVvw1dsfLoHKJYXuIc/fnc2Y1y4qjvEdSctAis
15 rqReXnolyyqCwS2e70ysQ9Sgg0JG4o7r0VojkJNzuHDWQ944yhGk6zjC54qHba6+
16 379erDy+xRQS9BSgEFf2C60Fe001+vp0WpqYAc1VGauXHNrVYn8Fu01sIRTIo7
17 10LR1bUHVgZvDIRR11dyFbF887oxrZZe9eWQGURjXEvg97nh1V5UzekRv7qLsVyg
18 sTV3mxodvXgw3KmrXU9FsFSKY9Cdu8vN9IVFJWQQj++rnzyyTUCUmxB9Y/L9wRx
19 4+7DSpfV1e4bG0ZKY+KQq1pYypUX1AFMHeb2RKVvjK5DzDq6CQs73jqq/v1Ydp4
20 kNsucdZKEKn2eVjJIon750vE5cus0l0jZuR93+w5Cmf4q6DhpXSUT1AP016R1ue
21 8mPTmCra9dEmzAMsnLEPSPXN5tzdxcdqHvVIdtj8M312iRyD6v1Neza5AY0EYAus
22 BgEMAN4mK70jRDxwnjQd8AJS133VncYT43gehVmkaZOAFaxoZtmR6oJb1Twj+b1
23 fV1IIXP51I80JBZ2YPEvLEBhuqeFQjEIG4Su3p/HuAIxAvh1IjFRzoxoIZGM1Mh
24 XKRsnc3Zd3LLa1G1r7smKSMvBaIlqnZ7rOTcnWx90h90d/MotCRvnsRt8EhtKEI

```

Next I create an .asc file :

```

└─# nano osi.asc
[root@kali]# gpg --import osi.asc
gpg: key ECDD0FD294110450: "SakuraSnowAngel83@protonmail.com" not changed
gpg: Total number processed: 1
gpg:          unchanged: 1

```

**nano osi.asc**

Then I paste the pgp content here and save it

Then using this command :

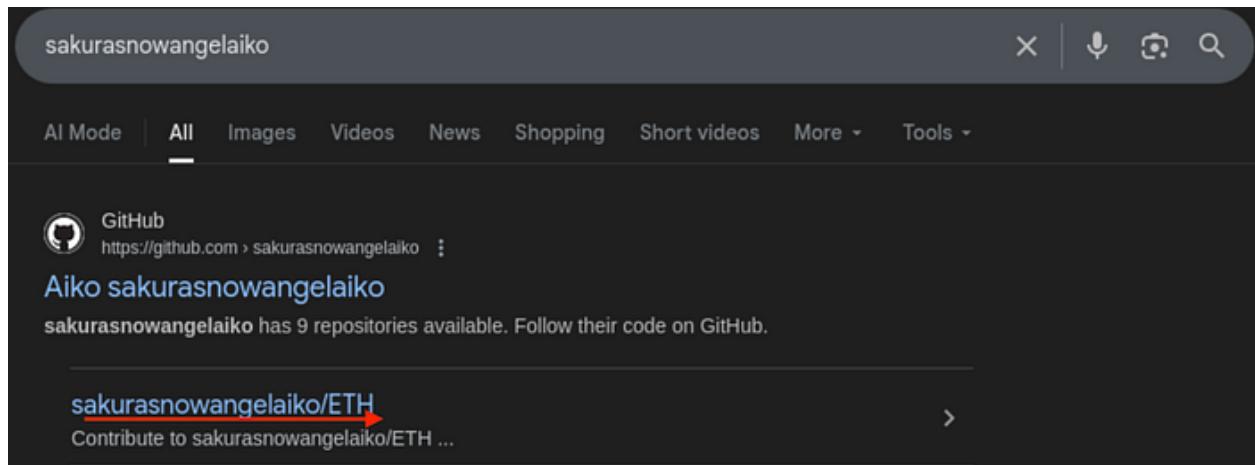
***gpg – import osi.asc***

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.

The screenshot shows a GitHub repository page for 'sakurasnowangelaiko / ETH'. The 'Code' tab is selected, displaying a single file named 'miningscript'. The code content is as follows:

```
stratum://0xa102397dbeebFD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:4444
```

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

The screenshot shows a GitHub commit history for the 'miningscript' file. The commit message is:

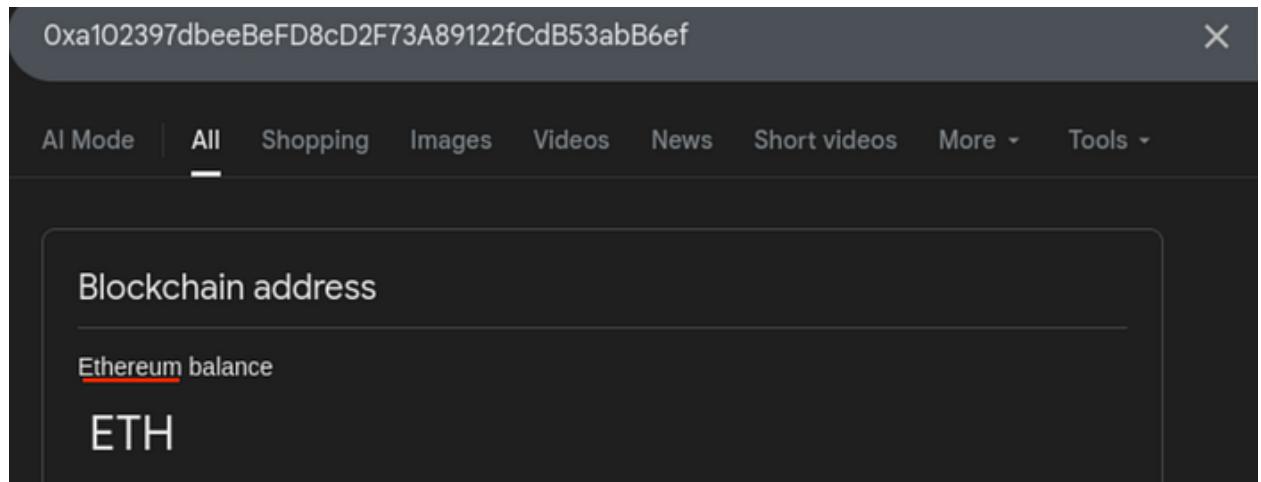
```
+ stratum://0xa102397dbeebFD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:4444
```

A comment from 'michael-brooks-365' on Mar 3, 2024, says 'hey :)'

0xa102397dbeebFD8cD2F73A89122fCdB53abB

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:

ETH Price: \$4,021.71 (+1.87%) Gas: 0.137 Gwei

Etherscan

Address 0xa102397dbeebefd8cd2f73a89122fcdb53abb6ef

Sponsored: Stake: 200% Bonus, 75k Raffle, Best VIP Program, Instant Withdrawals - Provably Fair. [Claim Bonus](#)

Buy Presale Play Gaming

Overview

ETH BALANCE: 0.000232149448528985 ETH

ETH VALUE: \$0.93 (@ \$4,021.71/ETH)

More Info

PRIVATE NAME TAGS + Add

TRANSACTIONS SENT: Latest: 1 yr 96 days ago First: 5 yrs 175 days ago

FUNDED BY: 0xb256caa2...E2d6d2344 | 5 yrs 175 days ago

Multichain Info

<\$1 (Multichain Portfolio)

No addresses found

COMPETITIVE FEES  
NO GAS FEES

Transactions Internal Transactions Token Transfers (ERC-20) Analytics Assets Cards Advanced Filter

Latest 25 from a total of 42 transactions

Transaction Hash	Method	Block	Age	From	To	Amount	Tax Fee
0x9e8561bcd8...	Transfer	23183604	37 days ago	0x0bb9f16...3CdD2c157	IN 0xa102397d...B53abb6ef	0.0002314 ETH	0.00004581
0xe8d1c31e9b...	Transfer	20149437	461 days ago	0xa102397d...B53abb6ef	OUT 0x2264783b...Af1bf82B	0.13243236 ETH	0.000084
0xbd7e962b29...	Transfer	12912953	1521 days ago	Ethermine	IN 0xa102397d...B53abb6ef	0.03244264 ETH	0.000021

<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:

<a href="#">0x45e652e143...</a>	<a href="#">Transfer</a>	<a href="#">11828305</a>	2021-02-10 10:47:08	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050165318 ETH	0.000021
<a href="#">0x70ef753f4f8...</a>	<a href="#">Transfer</a>	<a href="#">11803973</a>	2021-02-06 16:54:09	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050061555 ETH	0.000021
<a href="#">0x58a256df0d8...</a>	<a href="#">Transfer</a>	<a href="#">11783709</a>	2021-02-03 13:57:56	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050046298 ETH	0.000021
<a href="#">0xf6e34142e60...</a>	<a href="#">Transfer</a>	<a href="#">11776174</a>	2021-02-02 10:03:58	0x35558d81...Da4c3F938	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.177787601 ETH	0.003381
<a href="#">0xaa9e26ec1f5...</a>	<a href="#">Transfer</a>	<a href="#">11757604</a>	2021-01-30 13:36:24	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050034245 ETH	0.000021
<a href="#">0x86e1d6870b...</a>	<a href="#">Transfer</a>	<a href="#">11752646</a>	2021-01-29 19:19:41	0x26352D20...989272621	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.01200475 ETH	0.001869
<a href="#">0x431503d5c7...</a>	<a href="#">Transfer</a>	<a href="#">11732875</a>	2021-01-26 18:02:22	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050069945 ETH	0.000021
<a href="#">0xde6bf2f4ee8...</a>	<a href="#">Transfer</a>	<a href="#">11714008</a>	2021-01-23 20:30:43	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050073325 ETH	0.000021
<a href="#">0x6559fcc264a...</a>	<a href="#">Transfer</a>	<a href="#">11686873</a>	2021-01-19 16:35:56	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.0026209
<a href="#">0x480e838314...</a>	<a href="#">Transfer</a>	<a href="#">11684734</a>	2021-01-19 8:46:37	0x35558d81...Da4c3F938	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.04805189 ETH	0.002037
<a href="#">0xe057104cc5...</a>	<a href="#">Transfer</a>	<a href="#">11678837</a>	2021-01-18 10:56:38	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.00131045
<a href="#">0xf6fdb0b2d86...</a>	<a href="#">Transfer</a>	<a href="#">9806922</a>	2020-04-04 17:36:50	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.0001311
<a href="#">0xb3b8e1a48...</a>	<a href="#">Transfer</a>	<a href="#">9806917</a>	2020-04-04 17:35:05	0xB256caa2...E2d6d2344	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.00045 ETH	0.000168

Show: 50 

First &lt; Page 1 of 1 &gt; Last

## Ethermine

Through scrolling I see other type of crypto converted to :

<a href="#">0xf6e34142e60...</a>	<a href="#">Transfer</a>	<a href="#">11776174</a>	2021-02-02 10:03:58	0x35558d81...Da4c3F938	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.177787601 ETH	0.003381
<a href="#">0xaa9e26ec1f5...</a>	<a href="#">Transfer</a>	<a href="#">11757604</a>	2021-01-30 13:36:24	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050034245 ETH	0.000021
<a href="#">0x86e1d6870b...</a>	<a href="#">Transfer</a>	<a href="#">11752646</a>	2021-01-29 19:19:41	0x26352D20...989272621	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.01200475 ETH	0.001869
<a href="#">0x431503d5c7...</a>	<a href="#">Transfer</a>	<a href="#">11732875</a>	2021-01-26 18:02:22	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050069945 ETH	0.000021
<a href="#">0xde6bf2f4ee8...</a>	<a href="#">Transfer</a>	<a href="#">11714008</a>	2021-01-23 20:30:43	Ethermine	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.050073325 ETH	0.000021
<a href="#">0x6559fcc264a...</a>	<a href="#">Transfer</a>	<a href="#">11686873</a>	2021-01-19 16:35:56	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.0026209
<a href="#">0x480e838314...</a>	<a href="#">Transfer</a>	<a href="#">11684734</a>	2021-01-19 8:46:37	0x35558d81...Da4c3F938	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.04805189 ETH	0.002037
<a href="#">0xe057104cc5...</a>	<a href="#">Transfer</a>	<a href="#">11678837</a>	2021-01-18 10:56:38	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.00131045
<a href="#">0xf6fdb0b2d86...</a>	<a href="#">Transfer</a>	<a href="#">9806922</a>	2020-04-04 17:36:50	0xa102397d...B53abB6ef	<span style="background-color: #FFC107; color: black; padding: 2px;">OUT</span>	<span style="color: #FFC107;">Tether: USDT Stabil...</span>	0 ETH	0.0001311
<a href="#">0xb3b8e1a48...</a>	<a href="#">Transfer</a>	<a href="#">9806917</a>	2020-04-04 17:35:05	0xB256caa2...E2d6d2344	<span style="background-color: #4CAF50; color: white; padding: 2px;">IN</span>	<a href="#">0xa102397d...B53abB6ef</a>	0.00045 ETH	0.000168

## Tether USD

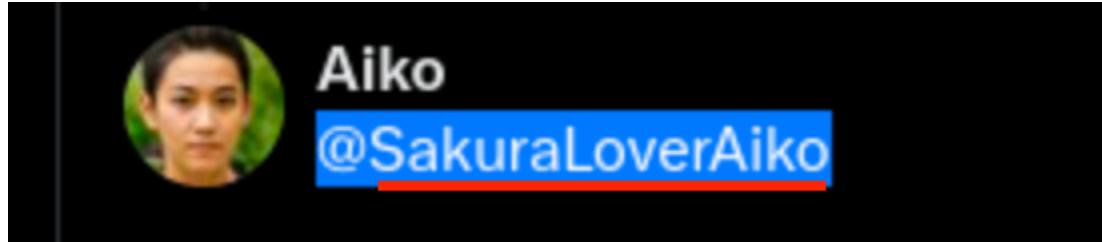
and this answers the 4th part of the question.

### **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

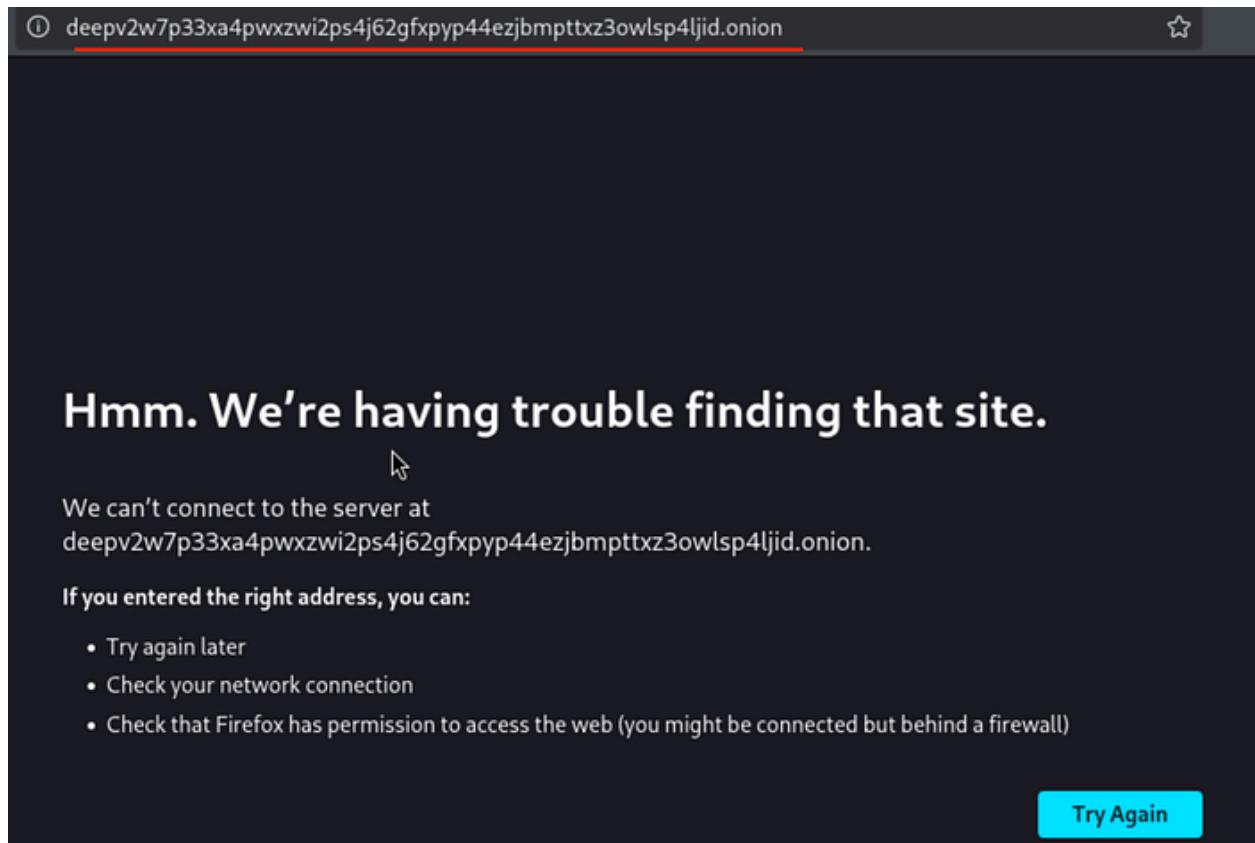
easy:



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@@

https://raw.githubusercontent.com/OsintDojo/public/main/deeppaste.png

# DeepPaste V3

Your Deep~~Shit~~ Hoster for special shit

Results for b2b37b3c106eb3f86e2340a3050968e2:

## Regular WiFi and Passwords

Anon, October 14, 2022 - 18:38

```
Saving here so I do not forget
School WiFi Computer Lab: GTRI-Device
Mcdonalds: Buffalo-G-19D0-1
School WiFi: GTvisitor
City Free WiFi: HIROSAKI_FREE_Wi-Fi
Home WiFi: DK1F-G
GTgfett44221@Macdonalds2020
GTFree123
H_Free934!
Fsdf324T@0
```

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

Average Location - Address

Num: 141 Street: West Jackson Boulevard

City: Chicago Region: IL

Country: US Postal: 60604

Average Location - Coordinates

Lat: 47.25264 to: 47.25265

Lon: -87.256243 to: -87.256244

Search Radius Tolerance(+/- degrees): 0.010

Network Characteristics

Last Updated: 20010925174546 Minimum data quality: 0 Encryption status:

BSSID/MAC: 0A:2C:EF:3D:25:1B or 1st 3 Octets: 0A:2C:EF

SSID / Network Name (exact match): DK1F-G

SSID / Network Name (wildcards<sup>2</sup>: % and \_) : foobar%

Must Be a FreeNet  Must Be a Commercial Pay Net  Only Networks I Was the First to Discover

Query  Reset

<sup>2</sup> 0.7 Product of number of observers and observations.  
% means zero-or-more characters, \_ means a single character.

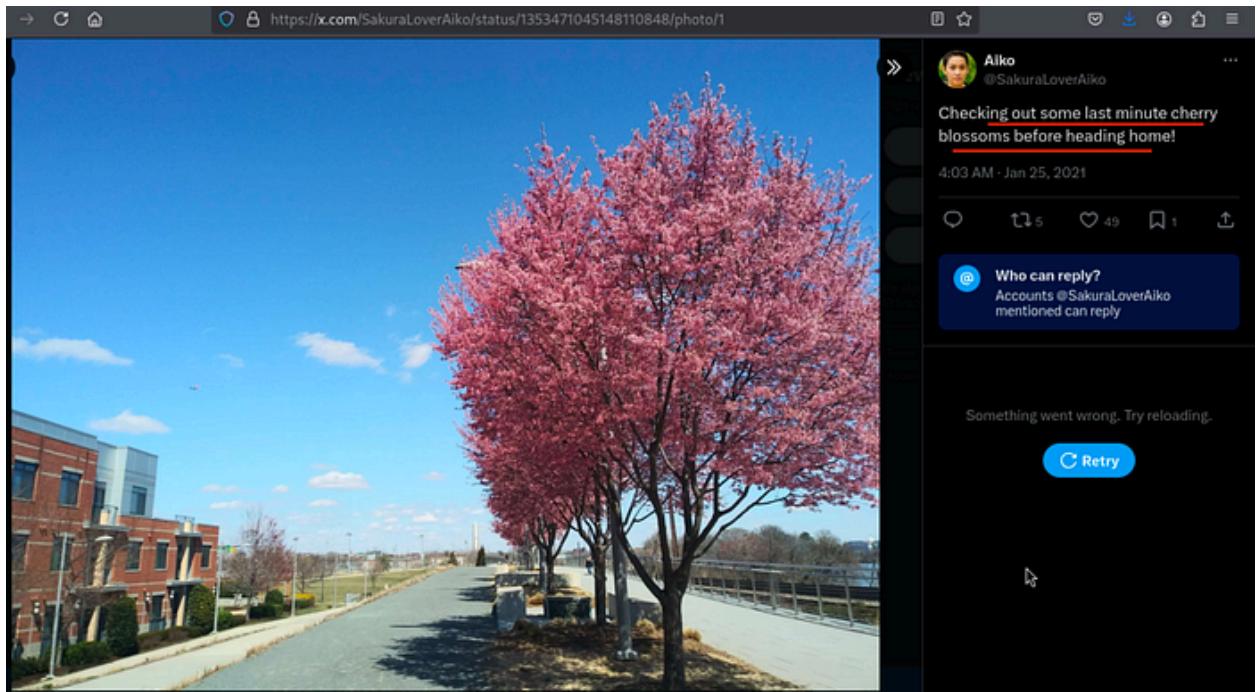
I create the account and use the advanced search feature and past the SSID value: DK1F-G and query it and that leads me to the BSSID:

Computed Network Properties	
Network ID	84:AF:EC:34:FC:F8
Network Name	
Type	infra
Encryption	WPA2
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 southtrain 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 test23456789076543234567 on 2022-07-06 02:04:04: THM(R4B1T_HOL3)

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.



Add to your search

AI Mode

All

Exact matches

Products

Visual matches

About this image

Feedback

### ❖ AI Overview

Listen



The image shows a row of cherry blossom trees in bloom, likely the 'Okame' variety, along a waterfront park with a building in the background. The scene appears to be in Washington, D.C., near the Washington Monument, which is visible in the distance. 



- The trees are a type of flowering cherry, known for their vibrant pink blooms that appear in early spring. 
- The 'Okame' cherry tree is a popular ornamental variety that is known for its hardiness and tolerance to various soil types. 

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.

closest airport to washington monument

AI Mode All Maps Images News Short videos Videos More Tools

Open now Top rated

Results for Washington, DC, USA - Choose area

Places

Ronald Re...  
4.2 ★★★★☆ (19K)  
Arlington, VA, ...  
DC-area airport...

Website Directions

Open in Maps

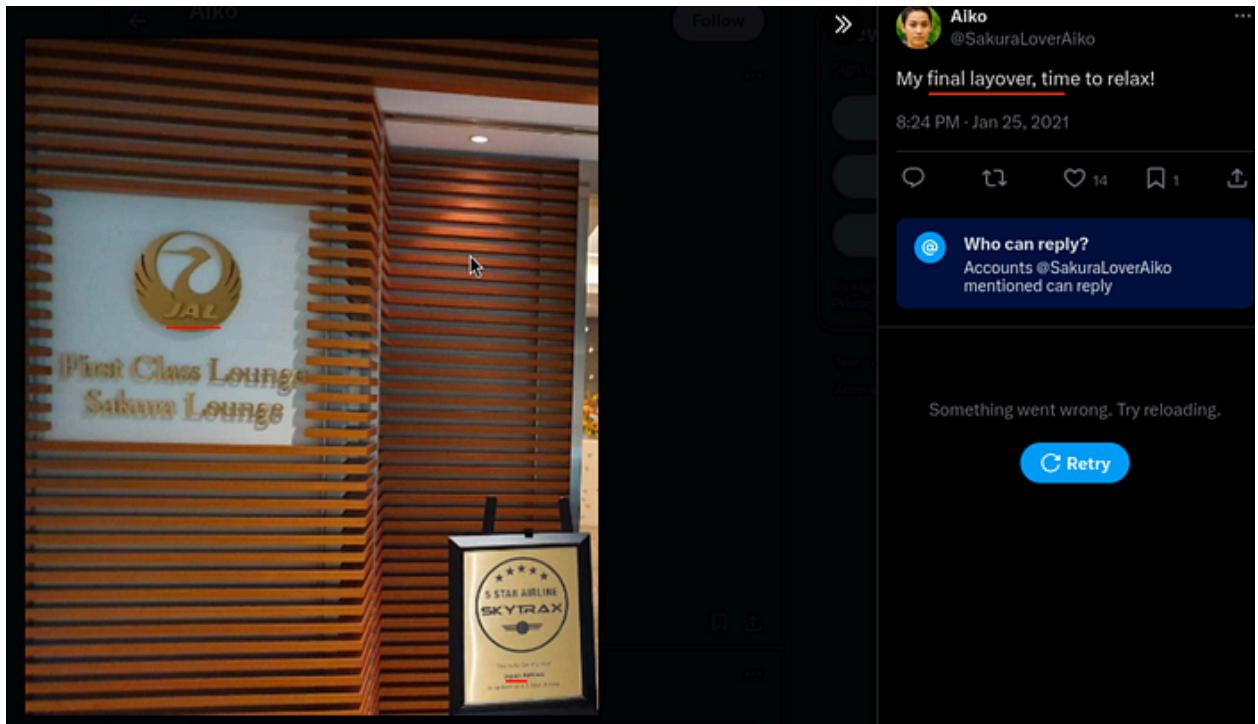
Ronald Reagan Washington National Airport  
4.2 ★★★★☆ (19K) · Airport in Arlington, Virginia

15,832+ Photos

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:

The Sakura Lounge, which includes a separate First Class primarily located at the major international airports served by Japan Airlines (JAL), such as [Tokyo Haneda \(HND\) in Terminal 2](#)

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

Average Location - Coordinates

Lat: 47.25264 to 47.25265

Lon: -87.256243 to -87.256244

Search Radius Tolerance(+/- degrees): 0.010

Showing records 1 to 1 of 1

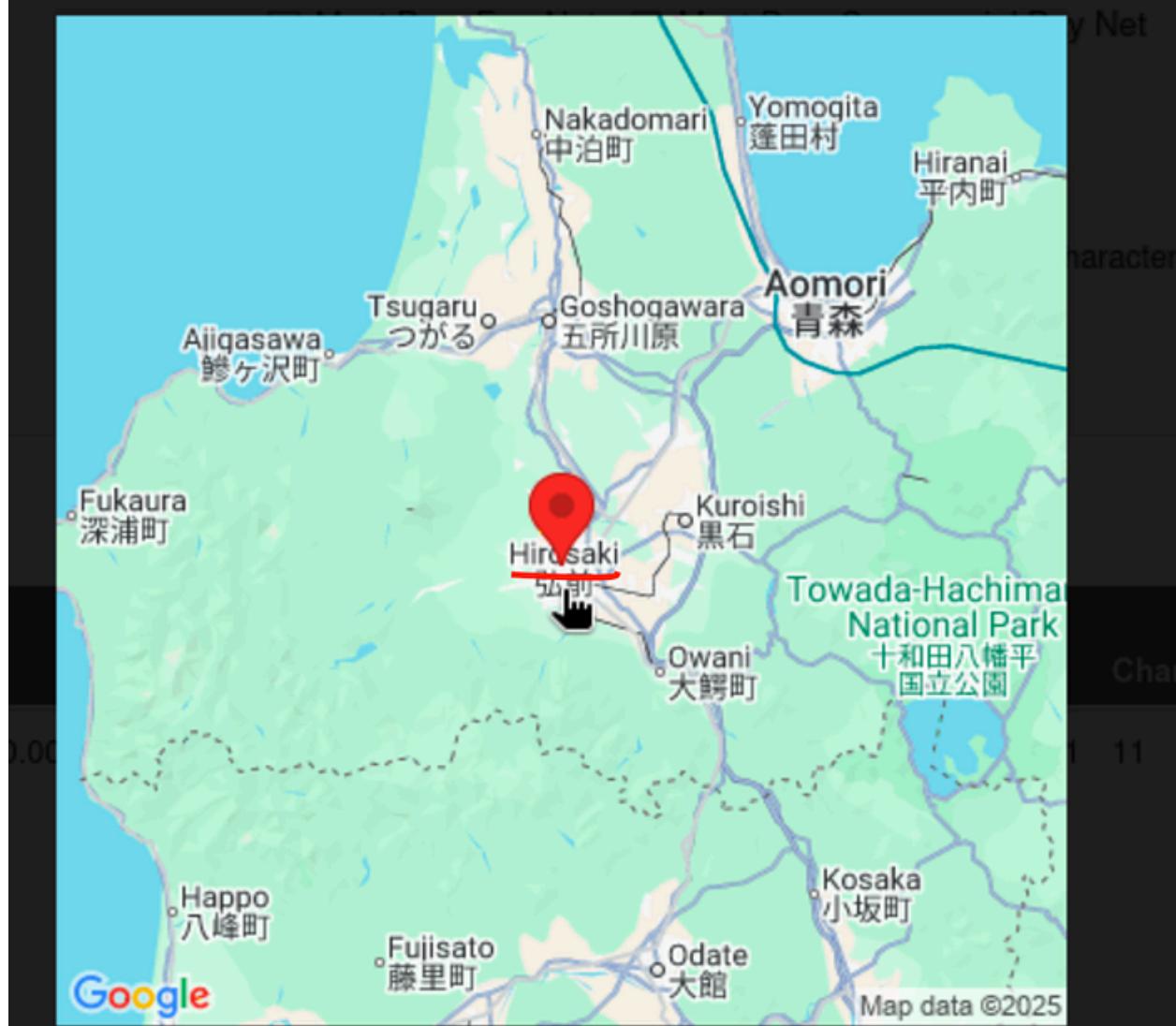
Map	Net ID	SSID	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS	Found by Me	Access
<a href="#">map</a>	84:AF:EC:34:FC:F8	DK1F-	infra	2019-04-24T11:00:00.000Z	2019-05-02T05:00:00.000Z		40.60551453	140.4606781	11	0	0	false	-

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

Network Location

SSID / Network Name (wildcards<sup>1</sup>: % and \_):

foobar%



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



## 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 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?

Aika Abe

✓ Correct Answer



## 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?

Etherium

Correct Answer

What is the attacker's cryptocurrency wallet address?

0xa12397dbecBcFD8cD2F73A89122fCd833bB6ef

✓ 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



## 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?

SakuraLovesAiko

Correct Answer

What is the BSSID for the attacker's Home WiFi?

84:a8:e3:34:fc:18

Correct Answer

0 Hint



## Background

Based on their tweets, it appears our cybercriminal is indeed heading home as they claimed. Their Twitter account seems to have plenty of photos which should allow us to piece together their route back home. If we follow the trail of breadcrumbs they left behind, we should be able to track their movements from one location to the next back all the way to their final destination. Once we can identify their final stops, we can identify which law enforcement organization we should forward our findings to.

## Instructions

In OSINT, there is oftentimes no "smoking gun" that points to a clear and definitive answer. Instead, an OSINT analyst must learn to synthesize multiple pieces of intelligence in order to make a conclusion of what is likely, unlikely, or possible. By leveraging all available data, an analyst can make more informed decisions and perhaps even minimize the size of data gaps. In order to answer the following questions, use the information collected from the attacker's Twitter account, as well as information obtained from previous parts of the investigation to track the attacker back to the place they call home.

### Answer the questions below

What airport is closest to the location the attacker shared a photo from prior to getting on their flight?

✓ Correct Answer

Hint

What airport did the attacker have their last layover in?

✓ Correct Answer

Hint

What lake can be seen in the map shared by the attacker as they were on their final flight home?

✓ Correct Answer

What city does the attacker likely consider "home"?

✓ 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!