

# Task 1 - 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.

## Approach

So I tried fetching the image as a png but i coulding, as the only possible extention to get is svg "Which doesn't help".

I also tried to turn it to a png using "SVGViewer", then tried to get any metadata out of the .svg & .png using "Metadata2Go", also nothing.

Translating the binaries on the image:

**a picture is worth a 1000 words but metadata worth a million**

So, after some digging I found the metadata hidden in the page source code

```
1 | xmlns:dc="http://purl.org/dc/elements/1.1/" |
2 | xmlns:cc="http://creativecommons.org/ns#" |
3 | xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" |
4 | xmlns:svg="http://www.w3.org/2000/svg" |
5 | xmlns="http://www.w3.org/2000/svg" |
6 | xmlns:xlink="http://www.w3.org/1999/xlink" |
7 | xmlns:sodipodi="http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd" |
8 | xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape" |
9 | width="116.29175mm" |
10 | height="174.61578mm" |
11 | viewBox="0 0 116.29175 174.61578" |
12 | version="1.1" |
13 | id="svg8" |
14 | inkscape:version="0.92.5 (2060ec1f9f, 2020-04-08)" |
15 | sodipodi:docname="pwnedletter.svg" |
16 | inkscape:export-filename="/home/SakuraSnowAngelAiko/Desktop/pwnedletter.png" |
17 | inkscape:export-xdpi="96" |
18 | inkscape:export-ydpi="96">>>|
```

Noticing the user's name in the filename, after searching it I found

The screenshot shows a Google search results page for the query "SakuraSnowAngelAiko". The top result is a GitHub profile for "Aiko sakurasnowangelaiko" with a link to https://github.com/sakurasnowangelaiko. Below it is an X (Twitter) account for "Aiko (@SakuraLoverAiko) / X" with a bio stating "Not too concerned about someone else finding them on the Dark Web. Anyone who wants them will have to do a real DEEP search to find where I PASTEd them." A small profile picture of a woman is also visible.

I tried submitting Github's username {**sakurasnowangelaiko**} as the first flag, and it was correct

## Task 2 - 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 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!

## Approach

After 60 min of deep Github investigation, I found a lead, finally.

I will leave it to Task 3.



Commit 5d83f7b  
sakurasnowangelaiko authored on Jan 23, 2021 Verified

Create miningscript

main

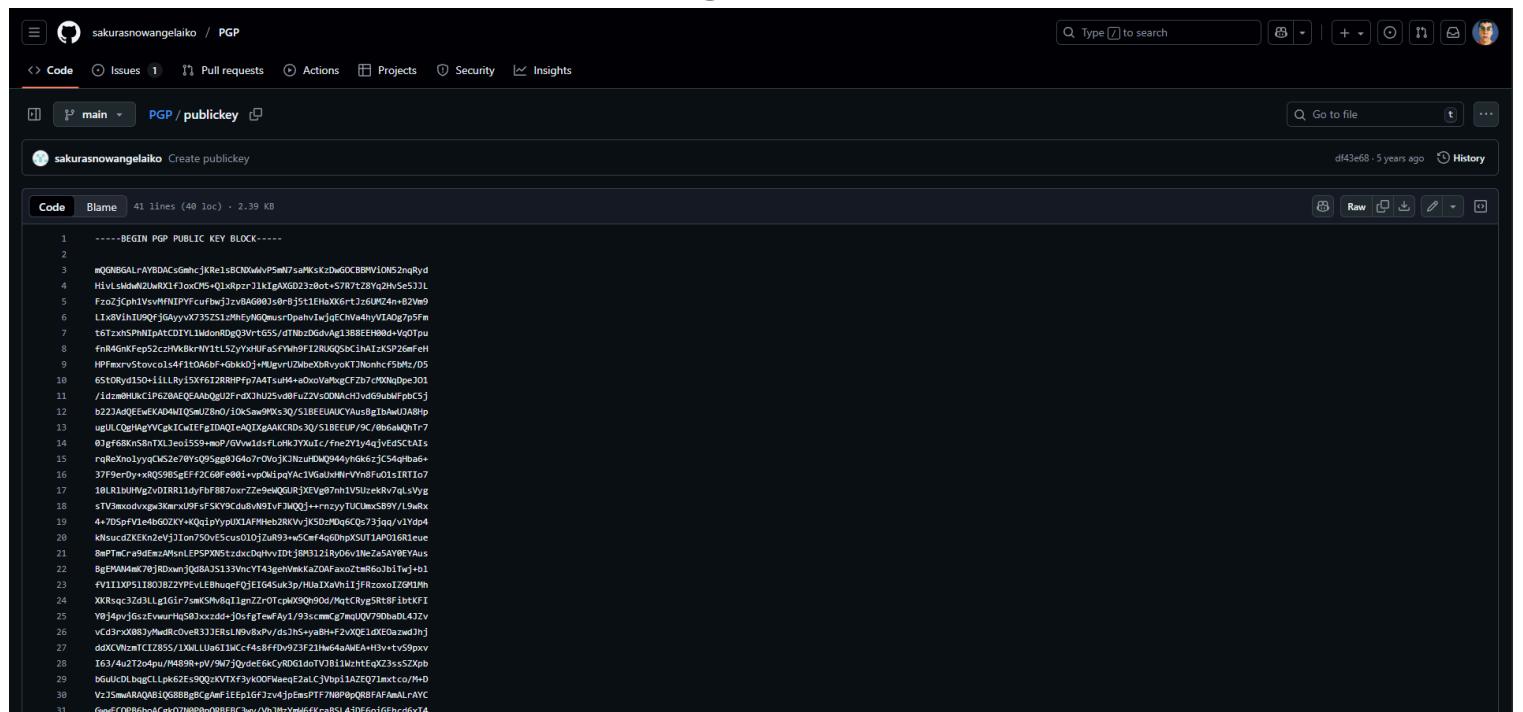
1 file changed +1 -0 lines changed

miningscript

stratum://0xa102397dbee8efD8cD2F73A89122fcdb853ab86ef. Aiko:psw@eu1.ethermine.org:4444

After some extra search, I found a PGP key which can lead me to the email, but I couldn't find a way to extract the email out of but by using [1] kleopatra.

So the email flag is **{SakuraSnowAngel83@protonmail.com}**.



sakurasnowangelaiko / PGP

Code Issues Pull requests Actions Projects Security Insights

main

PGP / publickey

sakurasnowangelaiko Create publickey

df43e68 · 5 years ago History

Code Blame 41 lines (40 loc) · 2.39 KB

```
-----BEGIN PGP PUBLIC KEY BLOCK-----  
1 mQGNBGLrAYBDACgSmhcJKE1sBCN0wMvP5mW7saIKskzDwGOCBBMVi0Ns2nqRyd  
2 H1vLslwhf2u0RX4LfxM+Q1kpxrzr1k1gAGD23z8ot+S7R7tz8y2hSe5J3L  
3 FzoJ3gh1VsYHNTIPYcfu1nwJzv846000+jb15t1EHxXG6rJz6UW4r+82Vw9  
4 L1xVh1tRQfjGdyyx7x35ZSLjMhEyQGusOpahIwjqfChNvdyIAQ7g5f9m  
5 t6TzxhSPN1pAtCD1L1mDnRQg3VrtG55+dThex2Gdvxlg1388EEH90d-Vq0TpU  
6 fnRAknKep5cczNk0xNyt1lSzYxxifox5ym9f128UGG5bc1h1zKS26efH  
7 HPFmxryStovc0l4f10a6F7Gbk0j1+HgjwUzbexRvokTJNohnf3Mh/05  
8 6St0Ryv10u+1LLRy15x6f12RIRfp74741suH4+eoovxwrgC7bzrXNgDp+301  
9 1dzm0hUkCLPj62AAEQAAbdgj2fxchuz5v0fUz2Vs0DNCh1vG9ubJpbc5j  
10 b223ad0EEwEKADNtQSjZ6n/1OK5m9Wx3Q/S1BEELAUJCYaus9gtbwJU8hp  
11 ugULCQgHqVWcpTCwTfFgT0dQ1eAQTxAKCRD3Q/S1BEUEP/9c/B664QkTr7  
12 81gf68Kn8nTxlTeo1559+np/GWvwlidsFluHkTzYuIc/rne271y4qjveSCSTATs  
13 rQRxno1lyyQMs2e8YQ95ggB364o/crMoK3Nu1DWQ944yh6zjC54qhb6+  
14 37FerDyxnG95gSEFF2C68r-e01+v0kipqYac1wGuxNrYmfd018RT107  
15 10LRtHWg2t1RRI1dyfb7B8/oxrzzew9wQ0URjXtVg7t1h1yS0ekRvql5Vg  
16 sTV1m0dvdxg3KmrJ05fSKY9Cu8uN91fJWQj++nzytUCuwsB9Y/Lwhx  
17 4+7D5PrfV1e4bG0GKXY+KQ1q1rypx1APMhe2RKwjk5d2W0q6QsJ3jgqvV1ydp4  
18 kNsudcZKEKn2eV1J1on50vEScus010jzur9+wsCef4c60hpSU1AP03RLeue  
19 8ePTmra9dEmZ4Ms1LEPSXPN5tzdxQghvxD1t189121Ry06v1Neza5AY0EYaus  
20 BgEWAhak70jRdwkmj068A1S1339mcY143geWkkxz0AfaxotmR63jbTw+j1  
21 F11LYX51180JB27PVeLRehnupefQf1G14Auksky/HlaXayh11fJfzxxoZG1Nh  
22 XKRsqc3zd3Llg7swSHv8e1lgnZ2rOtcpx9Q909od/wt1Cryg5Rt8f1btKFI  
23 YqJ4pvjgs2ewuwnHg50xxcds+0+jfgTewFa1.933mcG/mUQ/790b0d4J2zv  
24 v.cdrxx880jYhdcvle333ERsL1nv9xpdydJns+yabH+r2vXQE1dxEOzwJhj  
25 d0XWzrmfC12855/1XMLLub611McC4+s8F0v923F21h64AwEAHdV+v5pxv  
26 163/4uT204pu/14849R-pv-9MfjQdce6EcYr060d1TVB11mkhtgx3cs5zXpb  
27 bGukDl_bqgCLpK62EsQQxKVTx3y400FNaeq2aljVbp11AEZQ7inxco/M+D  
28 VzJ5muwRAQ810688BgCgAfIEEp1gf3zv4jpmsTF7NB0p0QRBFAlFamAL+VC  
29 GowfCQfB6ba0CgkQ7H0P0pQR8FB3ev/VhJHjpm6FKr=BSL4JdfgoiGEHcd6xT4
```

So, we need to search for the attacker's real name.

So after scrolling through Github & X profile for a while I found this other X profile on a tweet.



Aiko @SakuraLoverAiko · Jan 30, 2021  
Silly me, I forgot to introduce myself!

...

Hi there! I'm @AikoAbe3!



17



The screenshot shows the X (Twitter) mobile application interface. On the left, a sidebar menu includes Home, Explore, Notifications, Messages, Grok, Lists, Bookmarks, Communities, and a partially visible option. The main area displays the profile of a user named 'Ai' (@AiKOABE3). The profile picture is a close-up of a person with pink hair. Below the profile picture, the username 'Ai', handle '@AiKOABE3', and the bio 'Joined October 2022' are visible. The stats show '34 Following' and '31 Followers'. A note indicates 'Not followed by anyone you're following'. At the bottom of the profile card, there are tabs for 'Posts' (which is selected), 'Replies', and 'Media'.

So, the real name flag is {aiko abe}.

## Task 3 - UNVEIL

### 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.

## Approach

Going back to the crypto wallet I found earlier.

```
1 stratum://0xa102397dbeebefD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:4
```

So, the "What crypto wallet does the attacker own" flag is **{Ethereum}**, and the address flag is **{0xa102397dbeebefD8cD2F73A89122fCdB53abB6ef}**.

I scanned the address on etherscan.

Etherscan

Address 0xa102397dbeebefD8cD2F73A89122fCdB53abB6ef

Sponsored: Betpanda: Anon crypto casino with instant wd's & 10% weekly cashback. [Play now](#).

Overview

ETH BALANCE  
0.000232149448528985 ETH

ETH VALUE  
\$0.90 (@ \$3,880.32/ETH)

More Info

PRIVATE NAME TAGS  
+ Add

TRANSACTIONS SENT  
Latest: 1 yr 116 days ago → First: 5 yrs 195 days ago →

FUNDED BY  
0xB256caa2...E2d6d2344 | 5 yrs 195 days ago

Multichain Info

<\$1 (Multichain Portfolio)

No addresses found

I found that at Jan 23, 2021 he received a payment from Ethermine, so the sender flag is **{Ethermine}**.

Transfer 11732875 1/24 days ago 2021-01-23 20:30:43

0xde6bf2f4ee8... Transfer 11714008 1727 days ago Ethermine IN 0xa102397dbeebefD8cD2F73A89122fCdB53abB6ef 0.050069945 ETH 0.000021

After scanning the address on another site, I found "What other cryptos did he use the wallet for" so the flag is **{Tether}**.

0xa10-bB6ef

Ethereum Address  
0xa102397dbeebefD8cD2F73A89122fCdB53abB6ef

Ethereum Balance  
0.000232149448528985 • \$0.90

Wallet Tokens

Summary

This address has transacted 42 times on the Ethereum blockchain. It has received a total of 4.304280744220200681 ETH \$16,678.79 and has sent a total of 4.298285139771671696 ETH \$16,655.55. The current value of this address is 0.000232149448528985 ETH \$0.90.

Total Received  
4.304280744220200681 ETH  
\$16,678.79

Total Sent  
4.298285139771671696 ETH  
\$16,655.55

Total Volume  
8.602565883991871 ETH  
\$33,334.34

Total Fees  
0.005763455 ETH  
\$22.33

Nonce  
6

Transactions  
42  
1 Internal Txs

Token Portfolio • 1 →

# Task 4 - 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](#).

The screenshot shows a Twitter direct message interface. At the top, the recipient's profile is shown: Aiko Abe (@AikoAbe3), Senior SDE, Former @Microsoft, Joined January 2021. The message itself consists of two messages from the same user:

Don't think I don't see what you're doing!

You won't catch me BTW. I'm already heading back home, byyyeeee!

The timestamp for the messages is 5:50 PM.

## 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.

## Approach

Back to X the handle flag is **{SakuraLoverAiko}**.

I also noticed this tweet, where he is talking about "APs" or Access Points.



Aiko @SakuraLoverAiko · Jan 24, 2021

∅ ...

No more forgetting my APs when I get new phones!

Results for 0a5c6e136a98a60b8a21643ce8c15a74:

## Regular WiFi and Passwords

Anon, January 24, 2021 - 1:44 am UTC

4

7

31

111

Bookmark Up



Aiko @SakuraLoverAiko · Jan 24, 2021

∅ ...

Not too concerned about someone else finding them on the Dark Web.

Anyone who wants them will have to do a real DEEP search to find where I PASTEd them.

1

7

19

111

Bookmark Up

after some reading and analyzing the above image, with the 2 words "DEEP" "PASTE" written in capitals, I found a website called Deep Paste V3.

# 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 GTgfettt44221@Macdonalds2020
School WiFi: GTvisitor GTFree123
City Free WiFi: HIROSAKI_FREE_Wi-Fi H_Free934!
Home WiFi: DK1F-G Fsd324T@@

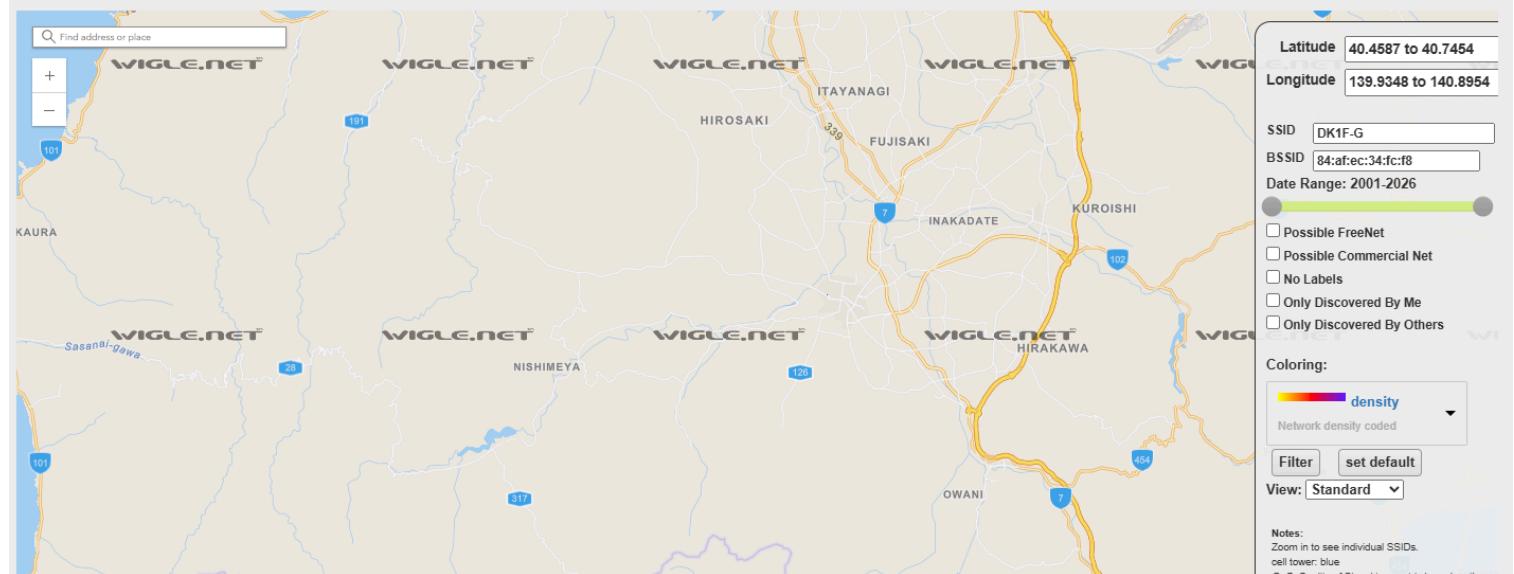
[REDACTED]
```

Views: 1 | Voting: 0 ↑ Up ↓ Down

Login to vote

Comments:

So, now we know what's his home town's name "Hirosaki" and his home WIFI SSID. I searched "DK1F-G" on wigle.net, and I found his BSSID.



So, the BSSID flag is {84:af:ec:34:fc:f8}.

# Task 5 - HOMEBOUND

## 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.

## Approach

Back to the image THM provided earlier, all we get from it that he was still out of Japan during January.

Aiko Abe @AikoAbe3

Senior SDE

Former @Microsoft

Joined January 2021

Don't think I don't see what you're doing!

You won't catch me BTW. I'm already heading back home, byyyyyeeeee!

5:50 PM

I scrolled through his tweets until Jan tweet, and that was the only lead.



Aiko @SakuraLoverAiko · Jan 25, 2021

∅ ...

Checking out some last minute cherry blossoms before heading home!



5

53



Bookmark Up

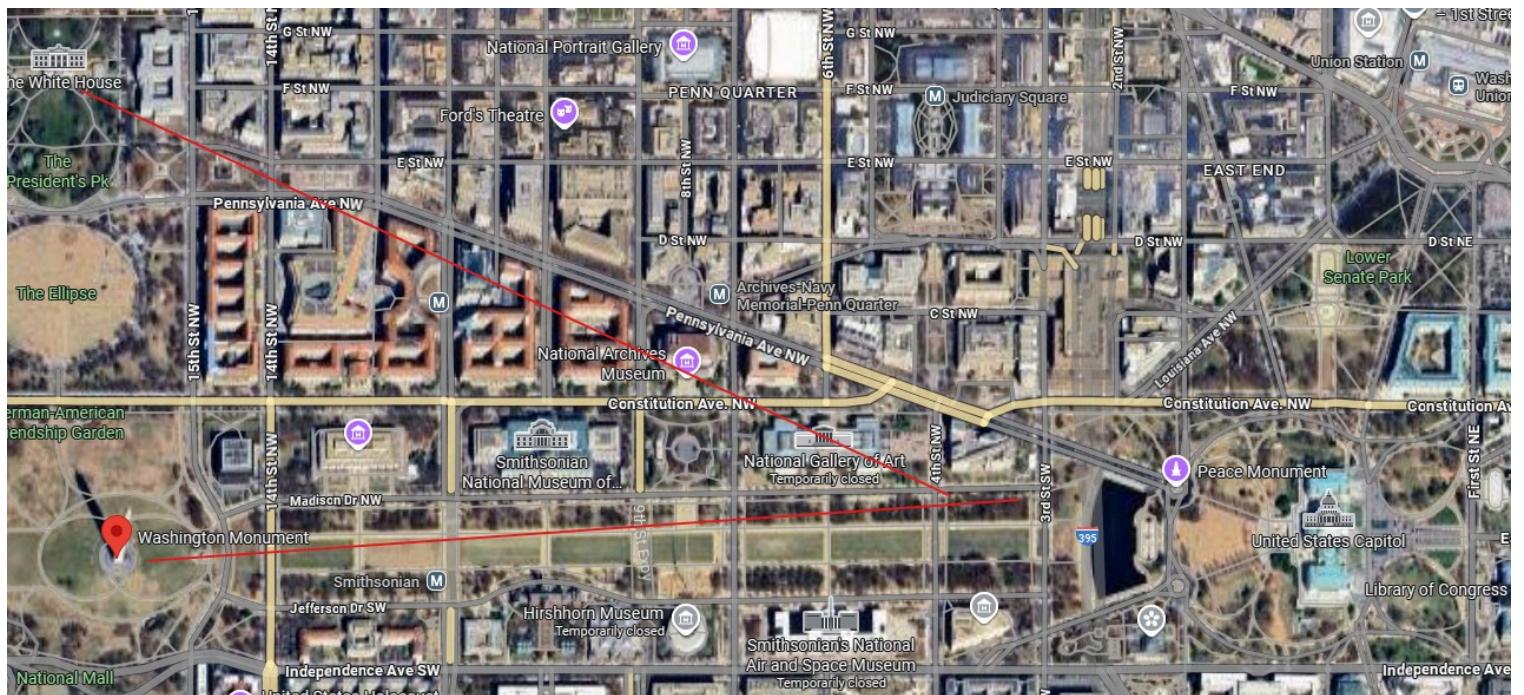
I noticed the Monument in the back, I couldn't think of any place but Washington DC.



I also noticed a white dome in the far away right side, which seemed like the white house.



I Google Maped the monument to make sure, it seemed too legit.



I tried drawing some crookie lines to simulate where were the photo taken from, so I tried searching for all the airports in the area, and the closest one was "Ronald Reagan Washington National Airport(DCA)"

**Ronald Reagan Washington National Airport**  
4.2 ★★★★☆ (19,535)  
Airport · 2401 Smith Blvd  
DC-area airport with subway service  
+1 703-417-8000  
"A fairly easy to navigate airport without excessively long walks."

**Dulles International Airport**  
4.1 ★★★★☆ (23,164)  
International airport · 1 Saarinen Cir  
Airport serving Washington, D.C. area  
+1 703-572-2700  
"The access to the airport is well designed and well marked."

**Washington National Airport**  
3.7 ★★★★☆ (21)  
Transportation service · 1  
"I like flying into and out of Reagan."

**College Park Airport**  
4.6 ★★★★★ (46)  
Domestic airport · 1909 Corporate Frank Scott Dr

**Directions**

**Overview**   **Reviews**   **About**

Directions Save Nearby Send to phone Share

This modern riverfront airport serving the DC area features direct subway service into the city.

2401 Smith Blvd, Arlington, VA 22202, United States  
flyreagan.com  
+1 703-417-8000

**Directions**

**Search this area**

The map shows the Washington, D.C. area with major landmarks like the White House, Smithsonian National Museum of Natural History, and Lincoln Memorial. It also shows Dulles International Airport (IAD) and Ronald Reagan Washington National Airport (DCA) marked with red dots. Other locations like the Wharf DC, The Yards, and Anacostia are also visible.

So, the closest airport to the location the attacker shared a photo from prior to getting on their flight is **{DCA}**.

I also found his layover airport after looking for the location of Japan Airlines (JAL) First Class and Sakura Lounge.

Which was included at Narita(NRT) and Haneda(HND) airports.

I tried both as flags and {Haneda} worked out.



Aiko @SakuraLoverAiko · Jan 25, 2021

My final layover, time to relax!

🔗 ...



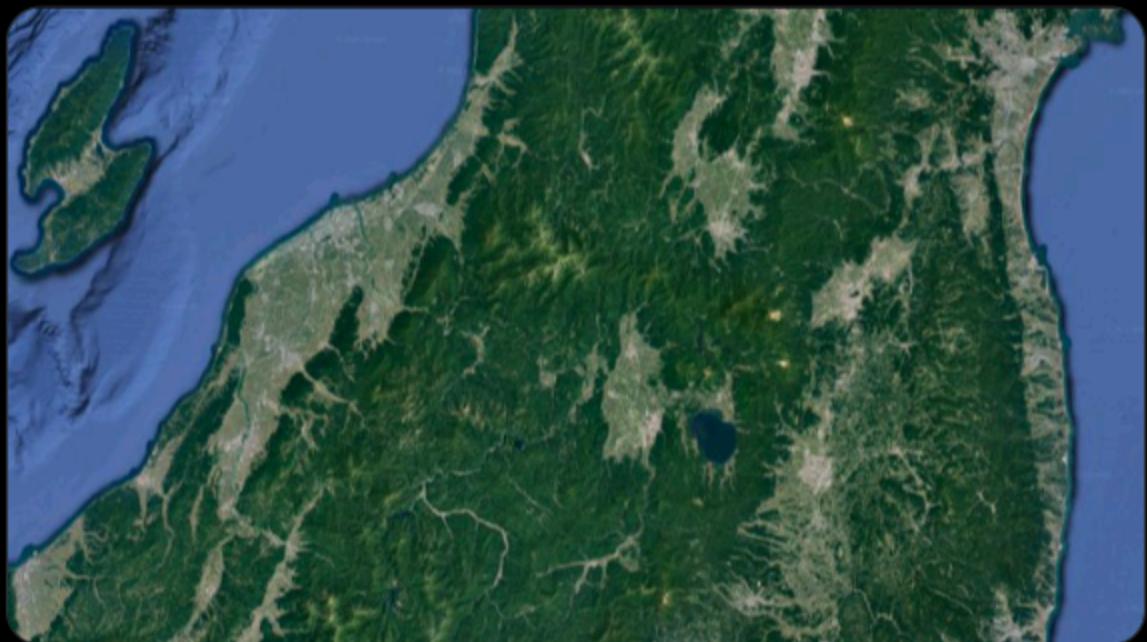
The name of the lake that can be seen in the map shared by the attacker as they were on their final flight home, is {Lake Inawashiro}.



Aiko @SakuraLoverAiko · Jan 25, 2021

∅ ...

Sooo close to home! Can't wait to finally be back! :)



For last, as we mentioned the attacker's home before in Task 4 is **{Hirosaki}**.

## Reference

---

---

1. Kleopatra is an open-source graphical tool for managing cryptographic keys and for encrypting and decrypting files and emails. It serves as a user-friendly front-end for encryption programs like [GnuPG](#) (GPG), handling the generation, management, and use of OpenPGP and X.509 certificates. Users can use it to create, import, and export keys, sign and verify data, and encrypt/decrypt content securely. ↵