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".

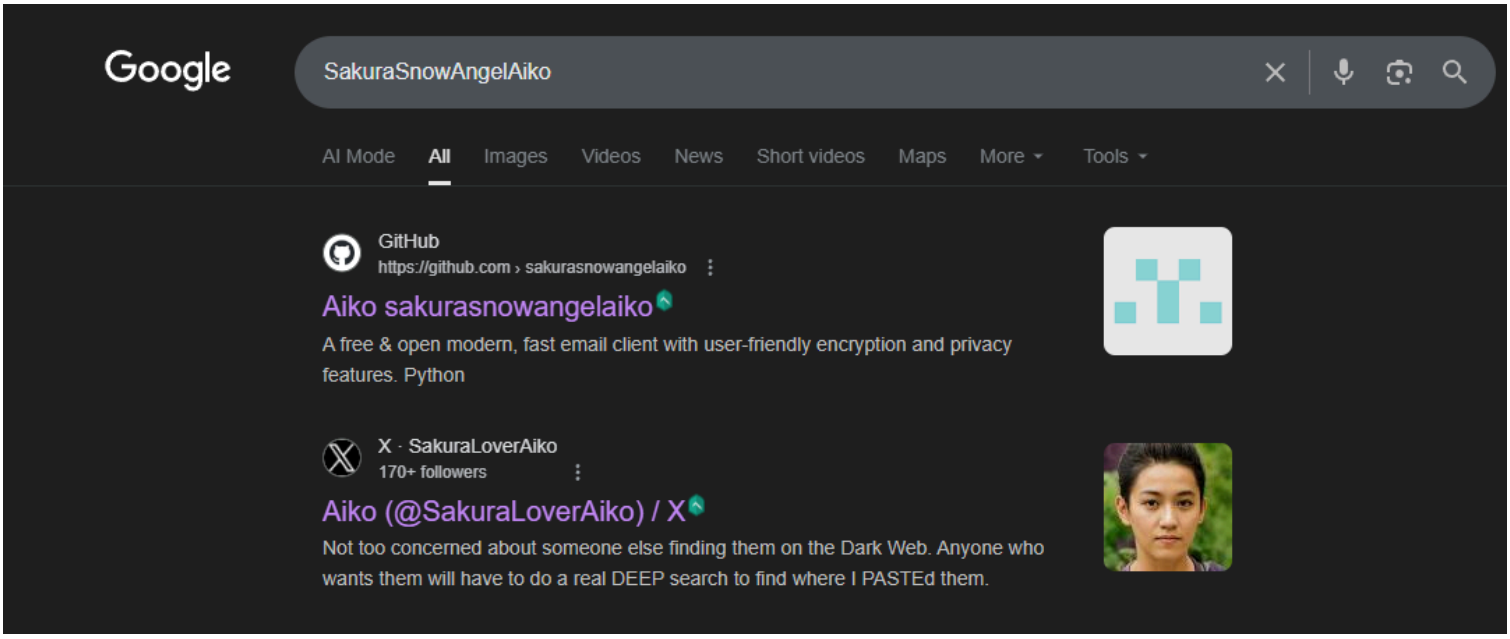
I also tried to turn it to a png using "SVGViewer", then tried to get any metadata out of the .svg & .png using "Metadata2Go", also nothing.

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

```
|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/2000/svg"|
|xmlns:xlink="http://www.w3.org/1999/xlink"|
|xmlns:sodipodi="http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd"|
|xmlns:inkscape="http://www.inkscape.org/namespaces/inkscape"|
|width="116.29175mm"|
|height="174.61578mm"|
|viewBox="0 0 116.29175 174.61578"|
|version="1.1"|
|id="svg8"|
|inkscape:version="0.92.5 (2060ec1f9f, 2020-04-08)"|
|sodipodi:docname="pwnedletter.svg"|
|inkscape:export-filename="/home/SakuraSnowAngelAiko/Desktop/pwnedletter.png"|
|inkscape:export-xdpi="96"|
|inkscape:export-ydpi="96">>|
```

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



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.

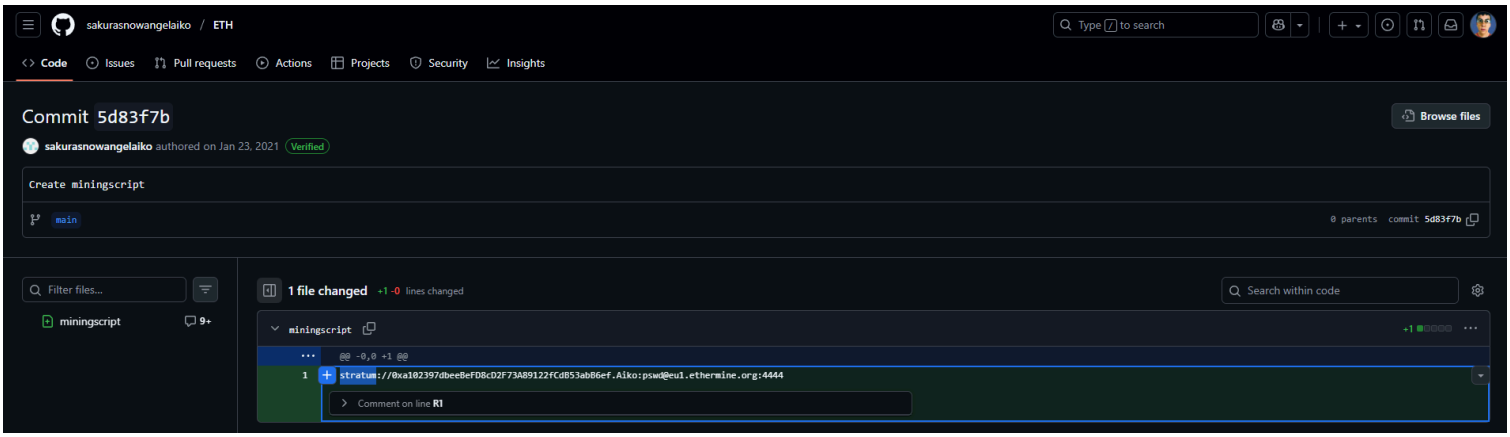
Instructions

> 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 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

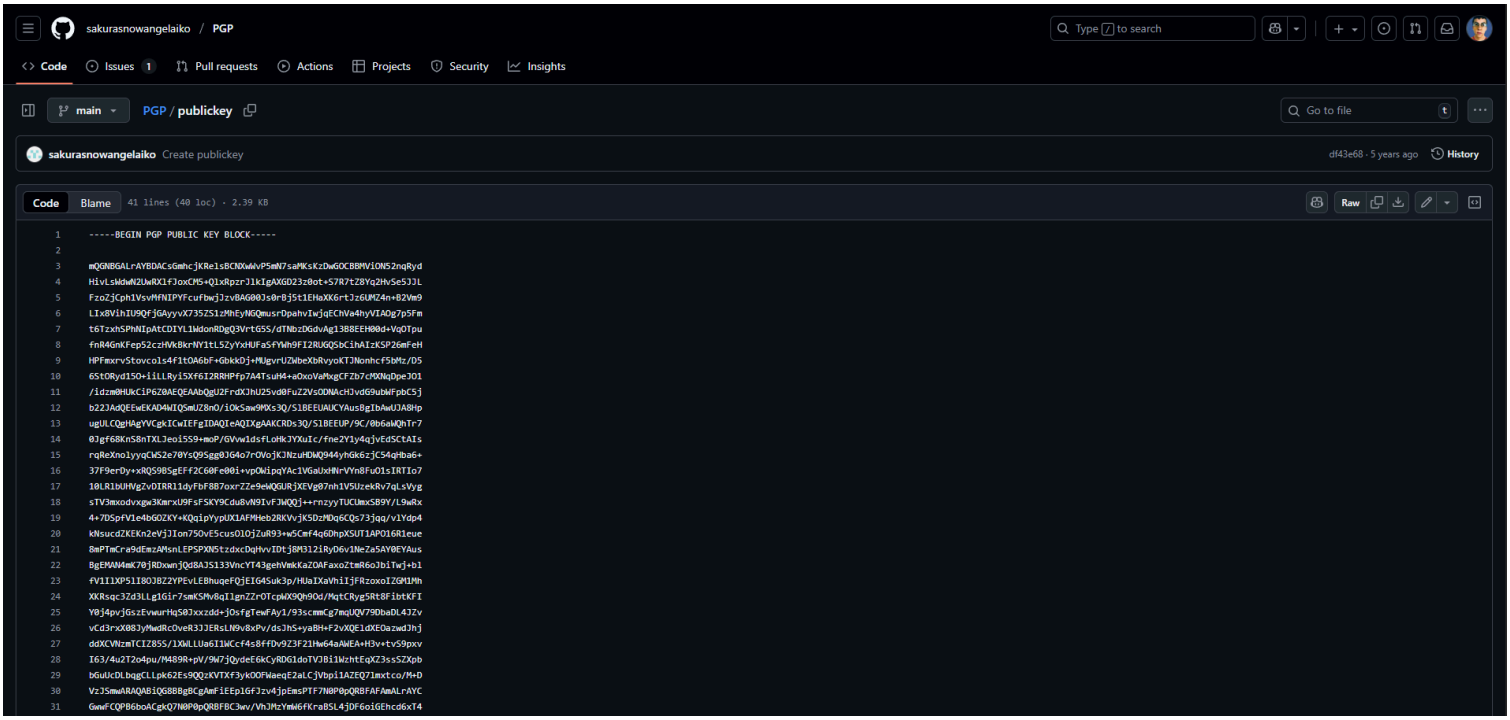
> in Task 2 to expand the OSINT investigation onto other platforms in order to gather additional identifying information on the attacker. Be wary of any false positives!

Approach

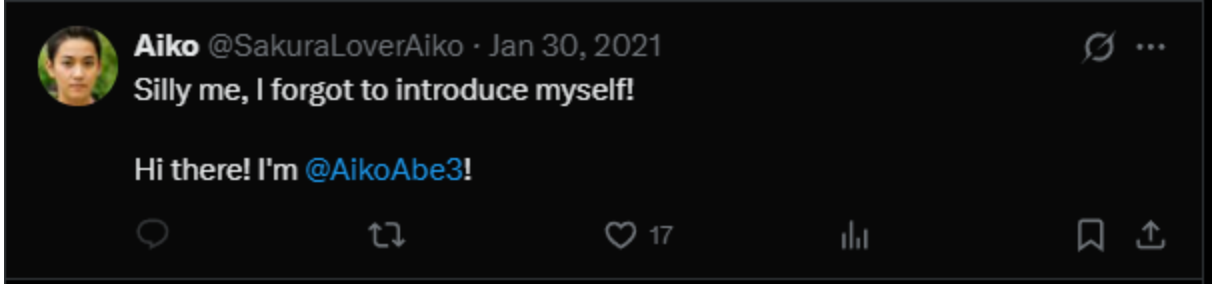
After 60 min of deep Github investigation, I found a lead, finally.
I will leave it to Task 3.

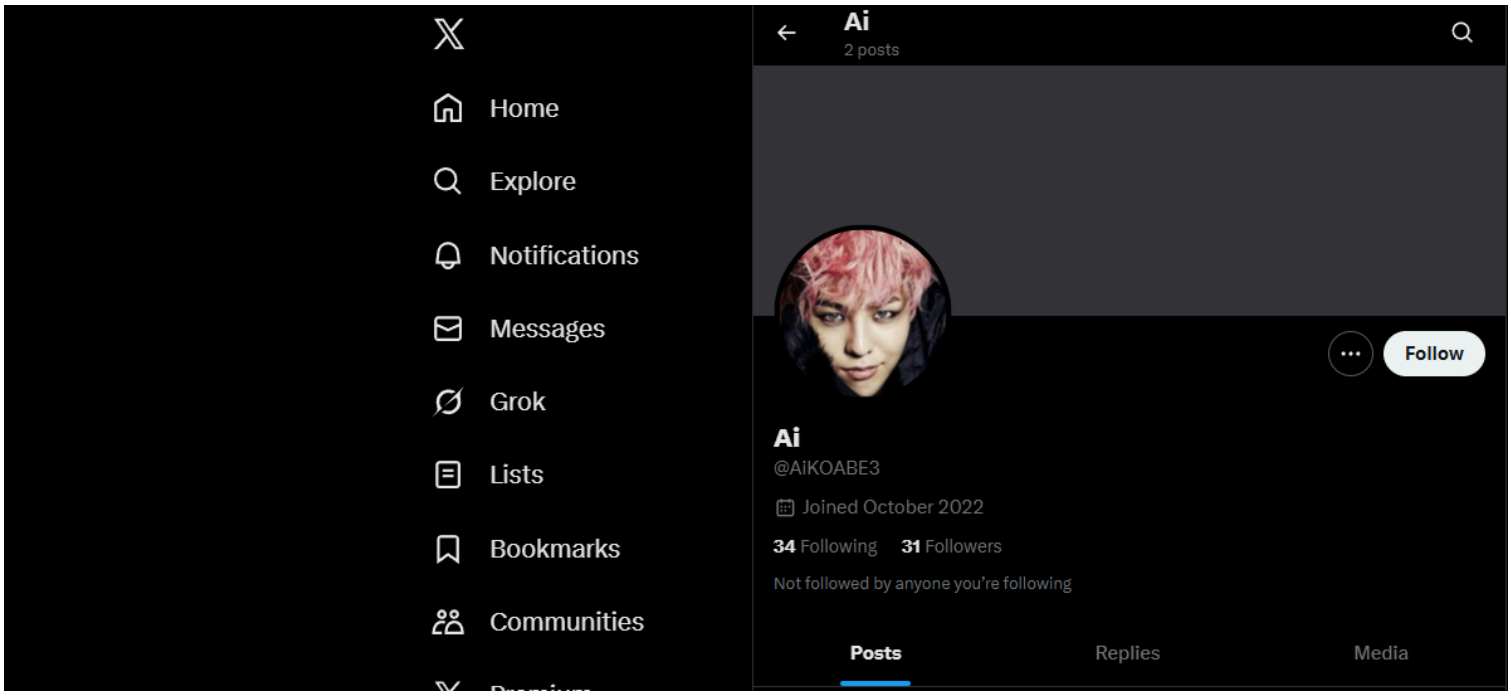


After some extra search, I found a PGP key which can lead me to the email, but I couldn't find a way to extract the email out of but by using [1]kleopatra.
So the email flag is {**SakuraSnowAngel83@protonmail.com**}.



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.





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.

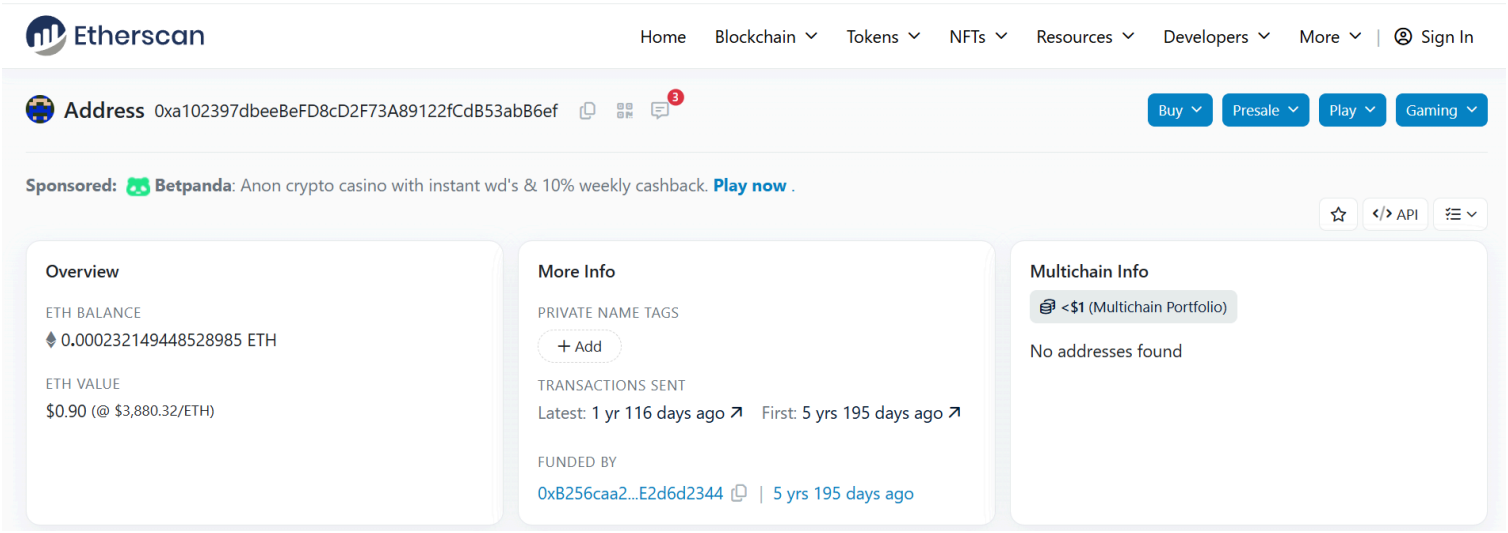
Approach

Going back to the crypto wallet I found earlier.

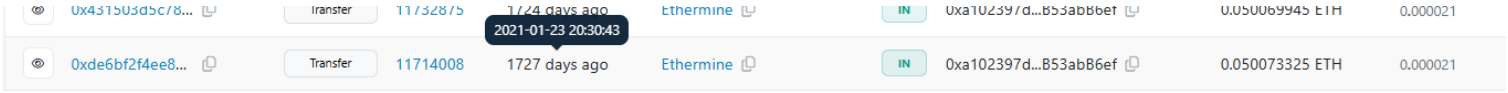
```
stratum://0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:
```

So, the "What crypto wallet does the attacker own" flag is {**Ethereum**}, and the address flag is {**0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef**}.

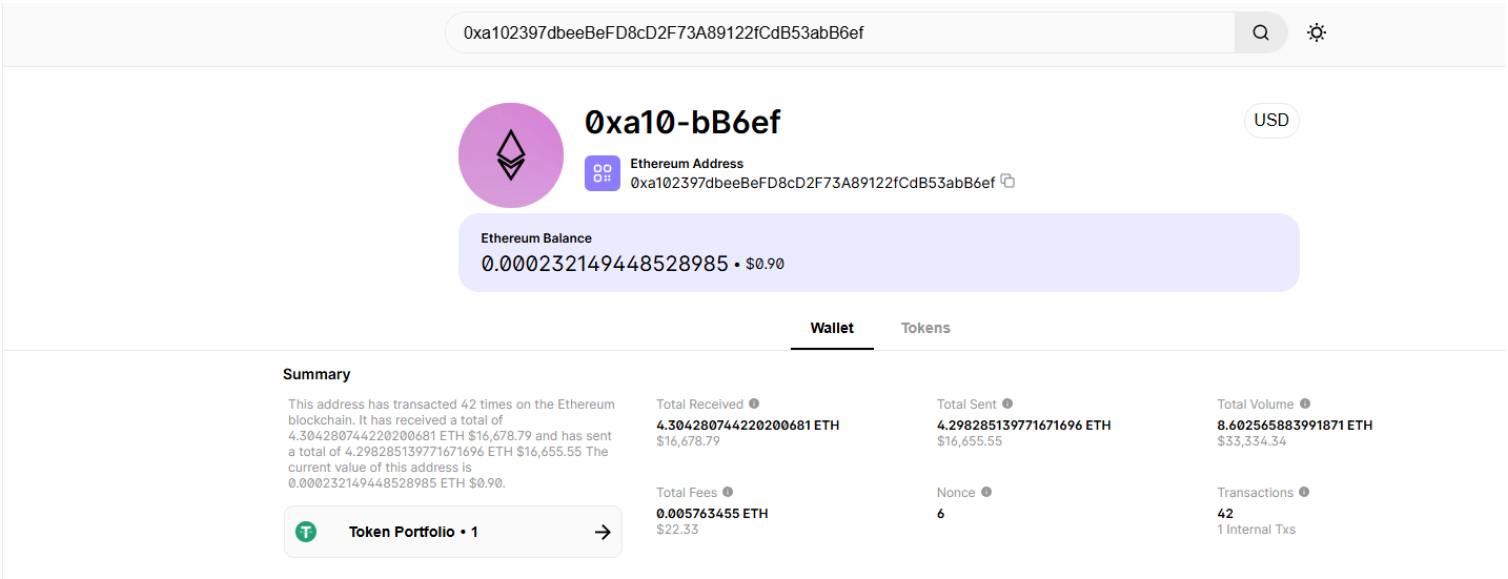
I scanned the address on etherscan.



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



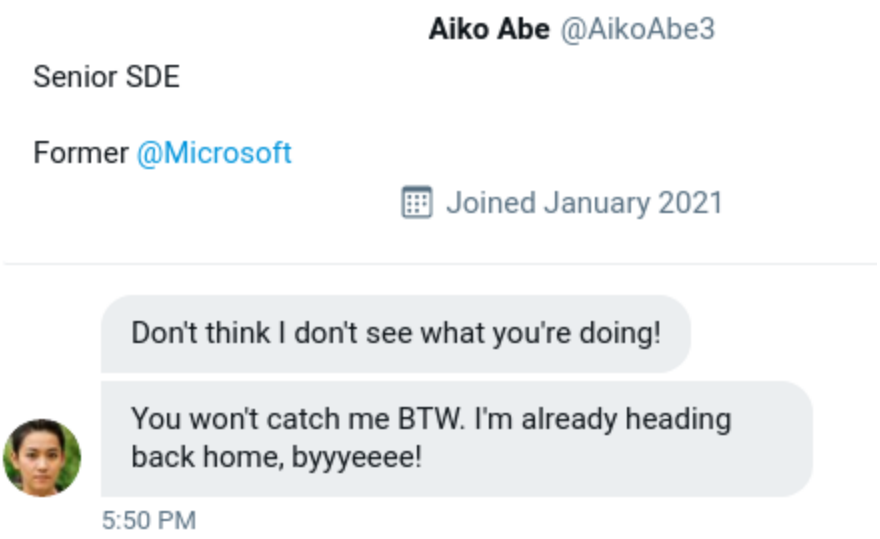
After scanning the address on another site, I found "What other cryptos did he use the wallet for" so the flag is {**Tether**}.



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 browserhere.



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.

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.

Not secure | deepv2w7p33xa4pwxzwi2ps4j62gfxpyp44ezjbmpttxz3owlsp4ljid.onion/show.php?md5=

DeepPaste V3

Your Deep-Shit Hoster for special shit

Results for b2b37b3c106eb3f86e2340a3050968e2:

Regular WiFi and Passwords

Anon, October 14, 2022 - 18:38

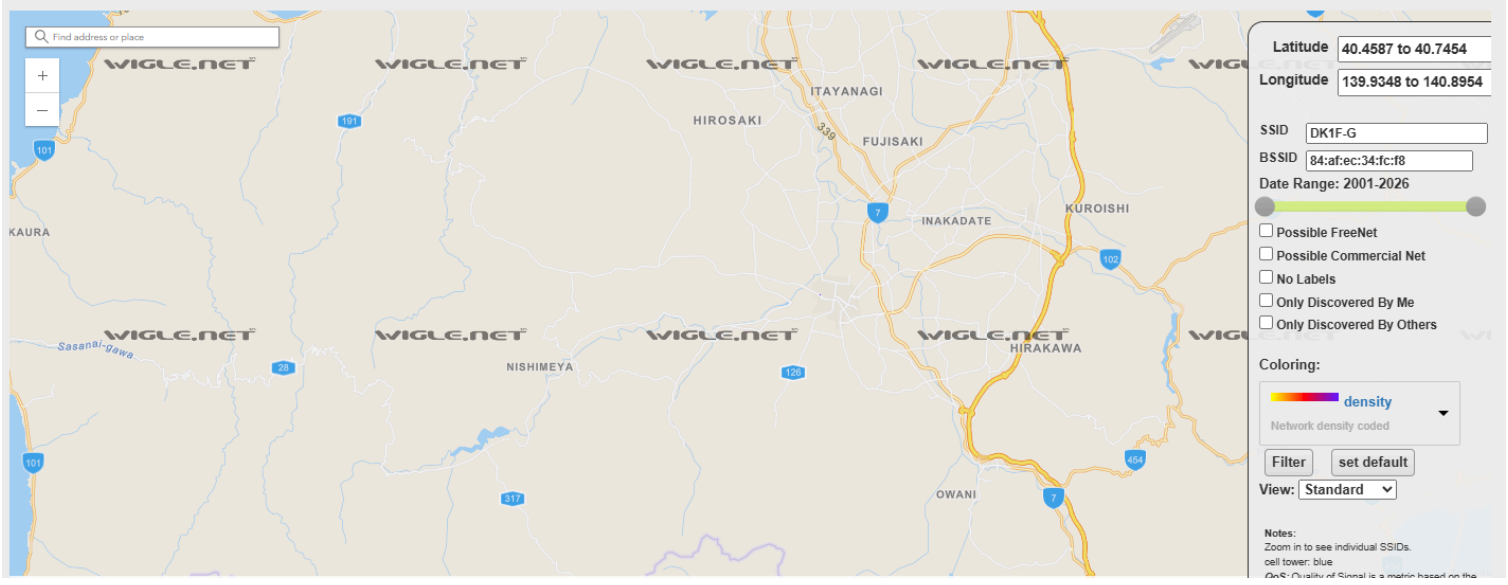
```
Saving here so I do not forget

School WiFi Computer Lab:       GTRI-Device             GTgfettt44221@
Mcdonalds:                      Buffalo-G-19D0-1        Macdonalds2020
School WiFi:                    GTvisitor               GTFree123
City Free WiFi:                 HIROSAKI_FREE_Wi-Fi     H_Free934!
Home WiFi:                      DK1F-G                  Fsdf324T@@
```

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

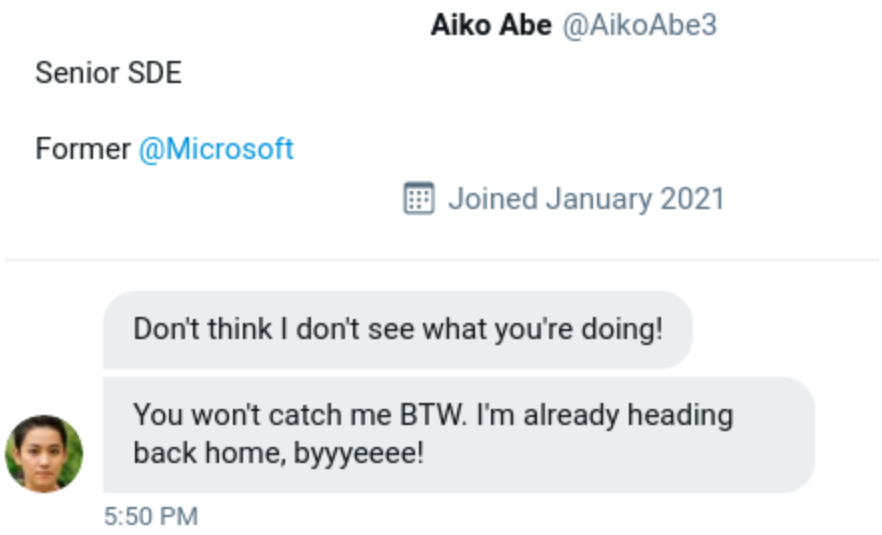
> Based on their tweets, it appears our cybercriminal is indeed heading home as they claimed. Their Twitter account seems to have plenty of photos which should allow us to piece together their route back home. If we follow the trail of breadcrumbs they left behind, we should be able to track their movements 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 to the image THM provided earlier, all we get from it that he was still out of Japan during January.

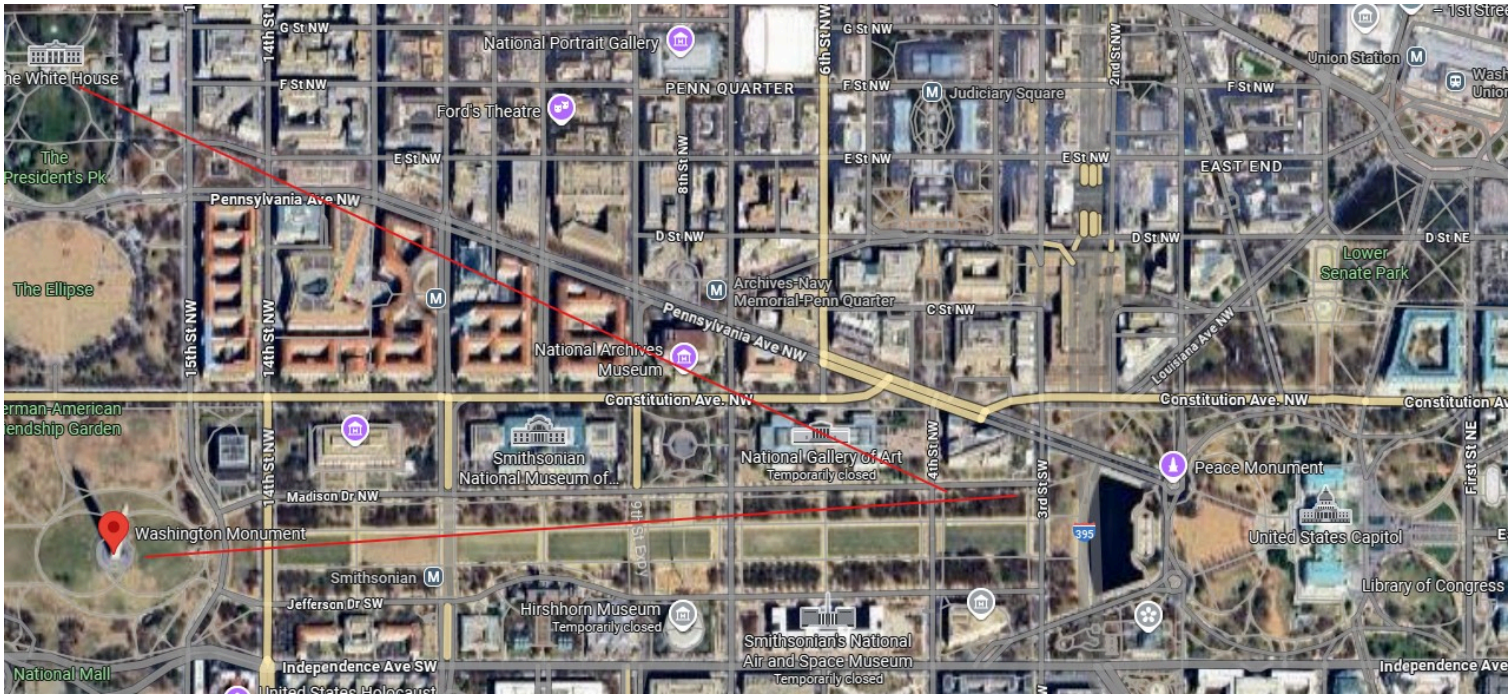


I scrolled through his tweets until Jan tweet, and that was the only lead.

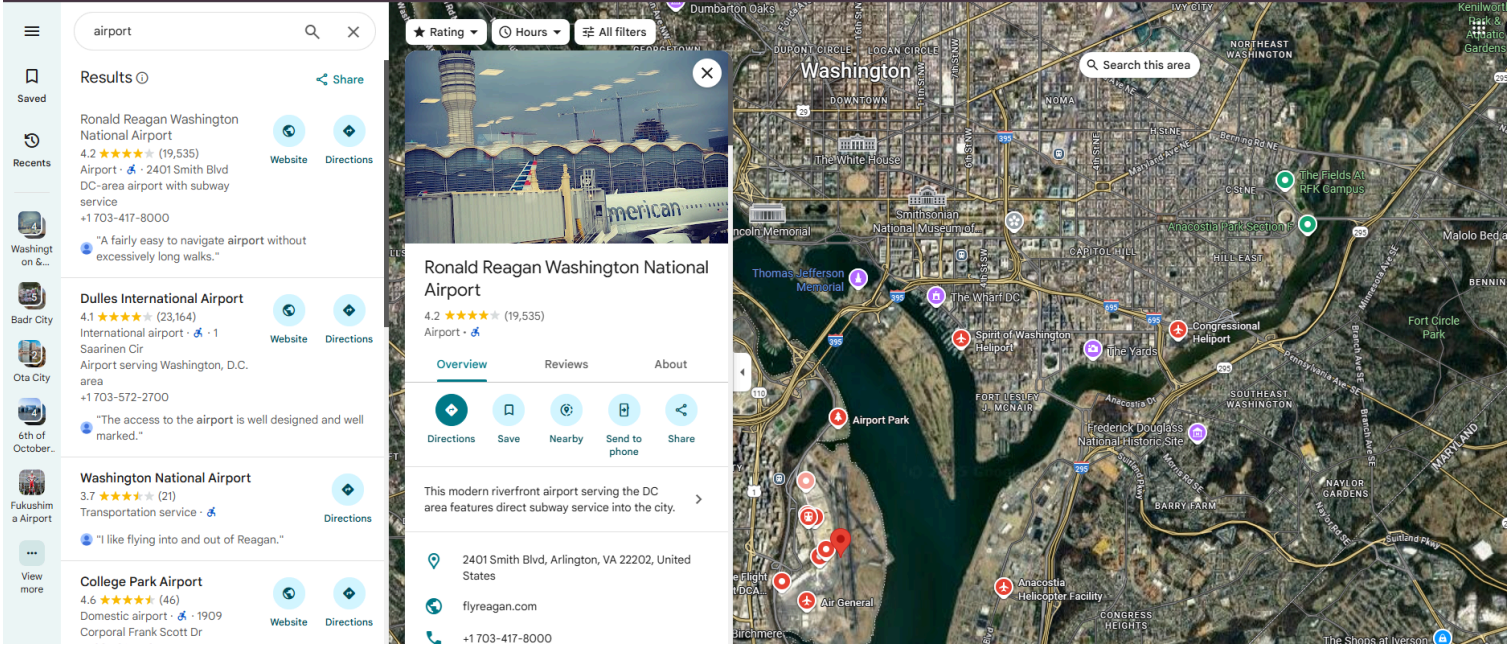
I noticed the Monument in the back, I couldn't think of any place but Washington DC.

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.



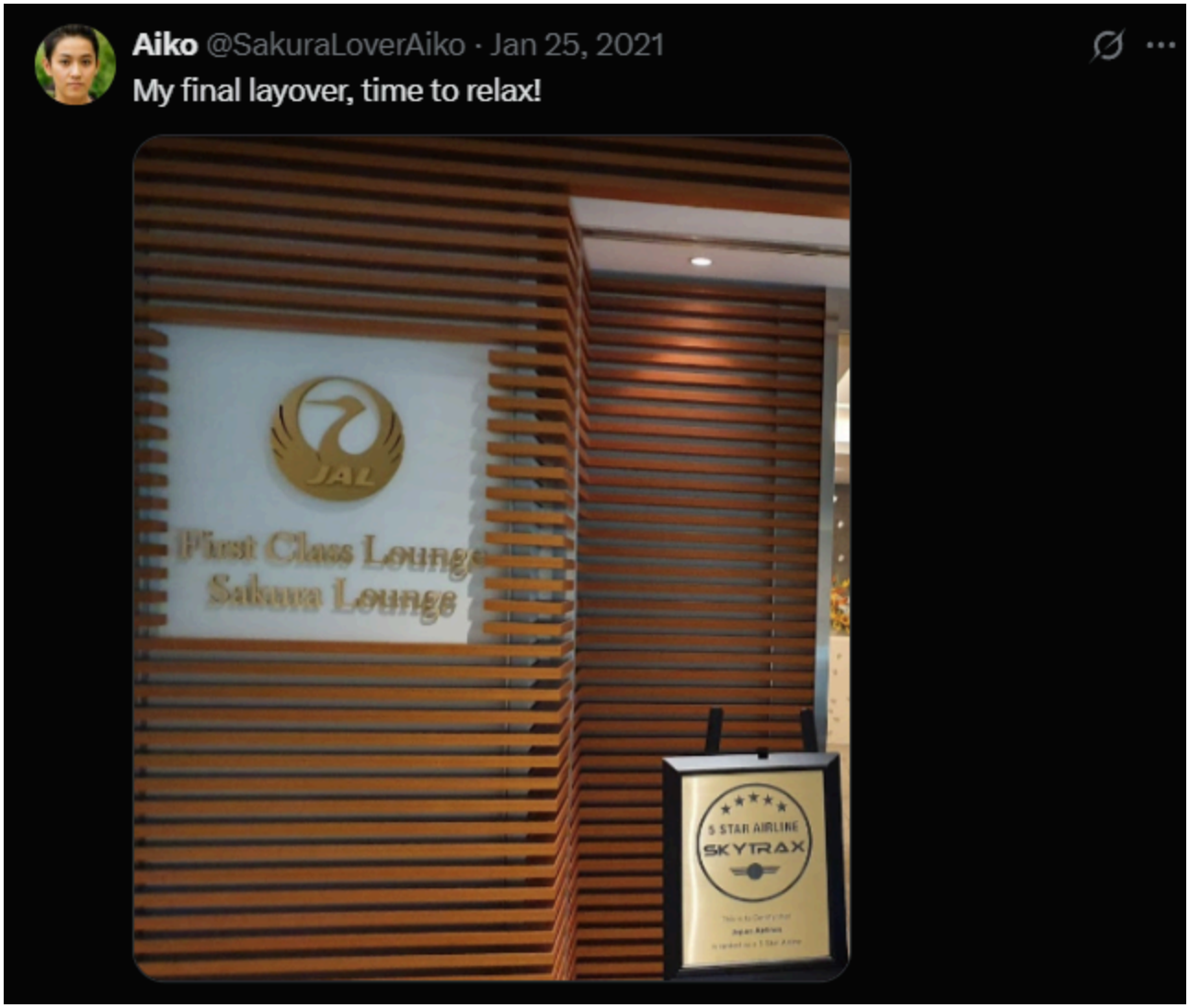
I tried drawing some crookie lines to simulate where were the photo taken from, so I tried searching for all the airports in the area, and the closest one was "Ronald Reagan Washington National Airport(DCA)"



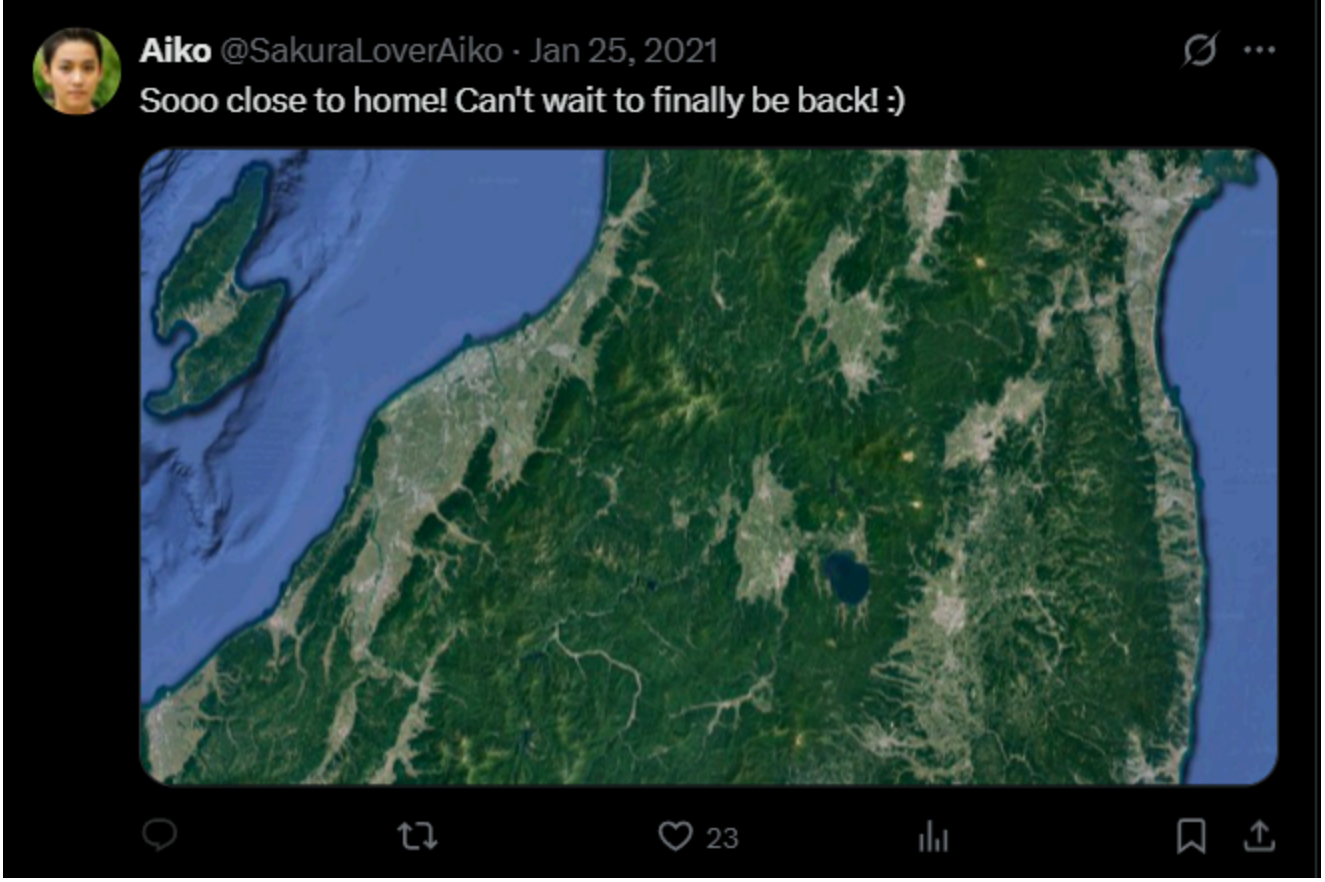
So, the closest airport to the location the attacker shared a photo from prior to getting on their flight is {**DCA**}.

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.



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**}.



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. ↩