

### What username does the attacker go by?

Respuesta: **SakuraSnowAngelAiko**

La primera pista que se nos presenta es una imagen en una url, la cual analizaremos con cualquier herramienta que nos permita acceder a sus metadatos.



https://exifmeta.com

i6be6a191/TryHackMe/Sakura/sakurapwnedletter.svg GO

RAW	EXIF	SVG	SVG-inkscape	SVG-sodipodi	XMP
<b>System:FileName</b>					
<b>System:FileSize</b>		850125			
<b>System:FileModifyDate</b>		2021:04:15 18:33:45+00:00			
<b>System:FileAccessDate</b>		2021:04:15 18:33:45+00:00			
<b>System:FileinodeChangeDate</b>		2021:04:15 18:33:45+00:00			
<b>System:FilePermissions</b>		644			
<b>File:FileType</b>		SVG			
<b>File:FileTypeExtension</b>		SVG			
<b>File:MIMEType</b>		image/svg+xml			
<b>SVG:XmInns</b>		http://www.w3.org/2000/svg			
<b>SVG:imageWidth</b>		116.29175mm			
<b>SVG:imageHeight</b>		174.61578mm			
<b>SVG:ViewBox</b>		0 0 116.29175 174.61578			
<b>SVG:SVGVersion</b>		1.1			
<b>SVG:iD</b>		svg8			
<b>SVG:MetadataID</b>		metadata5			
<b>SVG-inkscape:Version</b>		0.92.5 (2060ec1f9f, 2020-04-08)			
<b>SVG-inkscape:Export filename</b>		/home/SakuraSnowAngelAiko/Desktop/pwnedletter.png			
<b>SVG-inkscape:Export xdpi</b>		96			
<b>SVG-inkscape:Export ydpi</b>		96			
<b>SVG-sodipodi:Docname</b>		pwnedletter.svg			
<b>XMP:cc:WorkFormat</b>		image/svg+xml			
<b>XMP:cc:WorkType</b>		http://purl.org/dc/dcmitype/StillImage			
<b>XMP:cc:WorkTitle</b>					

### What is the full email address used by the attacker?

Respuesta: **SakuraSnowAngel83@protonmail.com**

https://www.namechecker.com

namechecker Home Domains Help

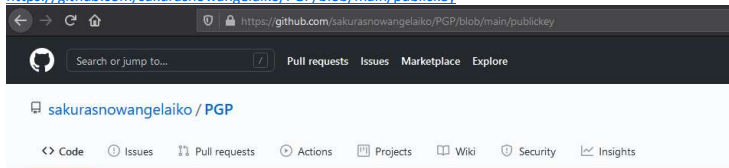
SakuraSnowAngelAiko

.com Available! ✓	Facebook Available! ✓	Twitter Error! !	Tumblr Available! ✓	Reddit Unavailable! ✗
Slack Available! ✓	Twitch Available! ✓	.net Available! ✓	myspace Available! ✓	YouTube Available! ✓
Meetup Available! ✓	Pinterest Available! ✓	Dribbble Available! ✓	.org Available! ✓	Github Unavailable! ✗
Vimeo Available! ✓	ello Error! !	Feedburner Available! ✓	Foursquare Available! ✓	Deviantart Available! ✓
.io Available! ✓	aboutme Available! ✓	lickr Available! ✓	Wordpress Available! ✓	Blogger Available! ✓
Venmo Available! ✓	Cash App Available! ✓	ifttt Available! ✓	mix Available! ✓	deviantart Available! ✓

Load More

Al realizar OSINT sobre el nombre descubrimos un repositorio de GITHUB con el usuario en cuestión. Al enumerar los repositorios originales (no los FOLKed) encontramos una llave pública.

<https://github.com/sakurasnowangelako/PGP/blob/main/publickey>



main PGP / publickey

sakurasnowangelako Create publickey

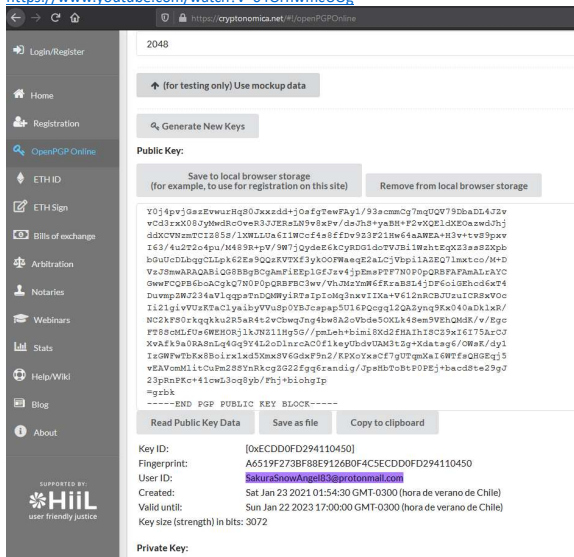
1 contributor

41 lines (40 sloc) 2.39 KB

```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3 mQNBGALrAYBDAcs6mhCjKRe1sBCIXwlvP5mN7saMksKzDwGOCB89VlON5ZnqRyd
4 HivLskidwN2UwK1FJoxCf5+Q1xRpr71KiGaXGDQ23z0ot+S7R7tZBYq2HySe53JL
5 FzoCjCh1VsvWfNIPIYFcuFbwj7zv8AG00s9rBjSt1EHaxX6rt3z6UJ24n+82Vn9
6 L1x8V1hIU9QFj6AyyvX735Z51zWhEYNG0msurDpahvIwjqEChVa4thyVIAOg7p5Fm
7 t6TzxhSPHNIAtCDIYL1mdonRDQ3VrtG55/dTNbzDgVAg1388EEH00d+Vq0Tpu
8 fN84nKFep52czHvK8krNY1tLS2yYxHUFa5FYvhh9F12RUGQ5bC1hA1zKSP26mEh
9 HPFmxrvStovco1s4f1t0A6bf+Gbkx0J+HJugvU2ibexRvyyoKT3NonhcF5bftz/D5
10 65tORyd150+11LLry15Xf612R8HPf7AATsuH4+a0xoVarhgCF2b7C90kqDpe301
```

Dado que previamente había visto el video de OSINTDojo sobre llaves públicas. Logré utilizar una herramienta online para resolver esta pregunta.

<https://www.youtube.com/watch?v=64OrnwmUOg>



What is the attacker's full real name?

Respuesta: **Aiko Abe**

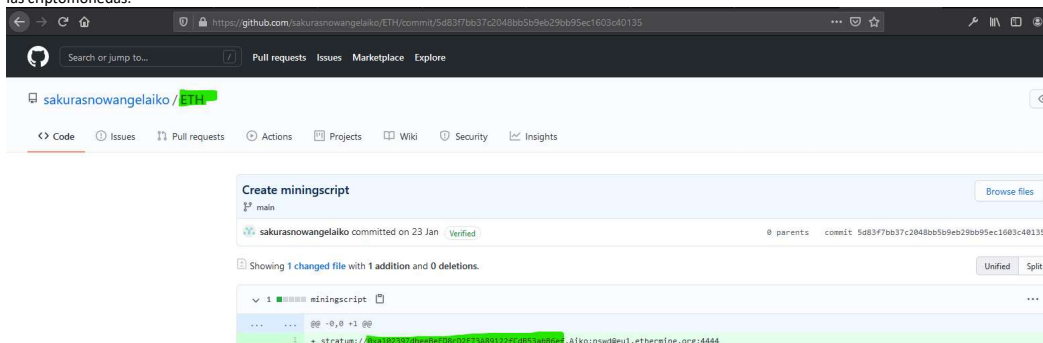
Encontrado también desde google, llegando a LinkedIn

<https://www.linkedin.com/in/sakurasnowangelako/>

What cryptocurrency does the attacker own a cryptocurrency wallet for?

Respuesta: **Ethereum**

En otro de los repositorios de Github encontramos varios que indican que el usuario está interesado en las criptomonedas.



Al observar en un summit, encontramos varios datos de valor para la investigación

What is the attacker's cryptocurrency wallet address?

Respuesta: **0xa102397dbecBeFD8c2f73A89122fcdB53abB6ef**

En la pregunta anterior encontramos también la respuesta a esta.

What mining pool did the attacker receive payments from on January 23, 2021 UTC?

En internet hay varios exploradores de criptomonedas.. Es una de las ventajas que tiene el sistema. Se puede auditar sin necesidad de mucho esfuerzo. Al poner en el buscador la wallet del sospecho, encontramos todas sus transacciones. De las cuales podremos sacar esta respuesta y la siguiente.

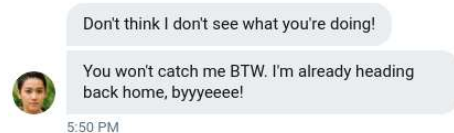
[illegible]

Respuesta: **Tether**

	<a href="#">0xc057104cc5637d9d5e...</a>	<a href="#">11678837</a>	84 days 15 hrs ago	<a href="#">0xa102397dbeebefd8cd...</a>	OUT	<a href="#">Tether: USDT Stablecoin</a>	0 Ether	0.00131045
	<a href="#">0xf6fdb0b2d865907e1e...</a>	<a href="#">9806922</a>	373 days 8 hrs ago	<a href="#">0xa102397dbeebefd8cd...</a>	OUT	<a href="#">Tether: USDT Stablecoin</a>	0 Ether	0.000131105

What is the attacker's current Twitter handle?

**Aiko Abe** @AikoAbe3  
Senior SDE  
Former @Microsoft  
Joined January 2021



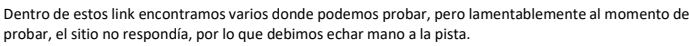
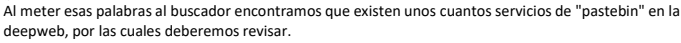
De la imagen entregada por los investigadores, tenemos un user de twitter, que no logramos encontrar directamente, dado que indica que no existe, pero al buscarlo como una palabra tenemos un resultado sorprendente, reconociendo aquí a nuestra imagen



Respuesta: [depastedihrn3jtw.onion/show.php?md5=0a5c6e136a98a60b8a21643ce8c15a74](http://depastedihrn3jtw.onion/show.php?md5=0a5c6e136a98a60b8a21643ce8c15a74)

Al revisar los post del actual Twitter, encontramos varias pistas que nos permitirán ir avanzando en la búsqueda de nuestro sospechoso.

El primero apunta a una ruta en la deepweb. Las letras en mayúscula son las que nos indican a qué no podríamos estar refiriendo.



depastedfhn3jw.onion/.how.php?end5e

# DeepPaste

Your Deep-Shit Hoster for special shit

---

Results for 0a5c6e136a98a60b8a21643ce8c15a74:

## Regular WiFi and Passwords

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

```
saving here so I do not forget
School WiFi Computer Lab: 6TRI-Device 6TGfett14421@
McDonalds: 6urfaio-c-1906-1 mcdm1m192620
School WiFi: 6Vax1s1c 6TFP69321
City Free WiFi: 6HER0AM1_Free_Wi-Fi H_Free9341
Home WiFi: 6CCP-6 6uF324708
```

Luego de obtener el DeepPaste, el contenido del texto indica credenciales y nombre de SSID. Esto nos lleva a consultar a la mundialmente conocida [wifile.net](http://wifile.net), el google de las redes wifi. Al escribir el SSID en la búsqueda avanzada, logramos encontrar un resultado que nos apunta a Japón. Además nos entrega la MAC address que nos pide la pregunta.



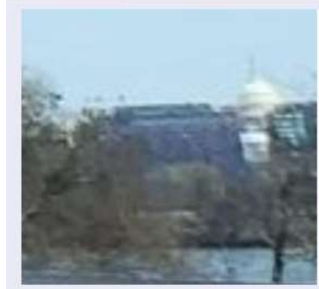
getting on their flight?

Respuesta: Dca

La imagen a investigar la encontramos en el twitter actual del sospechoso, en la cual muestra un puente, un avión, y un árbol de cerezas..

La búsqueda reversa no lleva a muchos resultados útiles, por lo cual debí hacer zoom para ir identificando dónde podría llegar a ser el lugar..

Nos encontramos con estas pequeñas pistas que nos orientan.



Encontramos una cúpula y un monumento.. Lo que se parece mucho al capitolio de washington, así que deberemos averiguar si es cierto.

Googleamos por unas imágenes referenciales y da que sí era posible.

Este es el lugar por donde entraremos para realizar la visita al Capitolio que es gratuita. Así que allá vamos.



Luego al buscar por el aeropuerto mas cercano de washington, ya encontramos el código que necesitamos.

https://www.latamairlines.com/cl/es

Vuelos Hoteles Paquetes Seguros

Ida y Vuelta Economy 1 p

wash Ing

Washington DC, DCA - Estados Unidos  
R Reagan Nat

Washington DC, IAD - Estados Unidos  
Dulles Intl.

What airport did the attacker have their last layover in?

Respuesta: HND

La búsqueda inversa de la imagen esta vez sí dio resultados positivos, identificando un aeropuerto que claramente era el que buscábamos



About 2 results (0.78 seconds)



Image size:  
443 × 523

No other sizes of this image found.

Possible related search: **jai sakura lounge**

<https://www.jal.co.jp> > inter > service > lounge ▾

**Lounge Service - JAL International Flights**

First Class Lounge, Sakura Lounge list — Tokyo International Airport (Haneda) **Sakura Lounge** - Narita International Airport First Class ...

<https://www.jal.co.jp> > dom > service > lounge > hnd ▾

**SAKURA LOUNGE (Haneda Airport Domestic Lounge) - JAL ...**

Use Sakura Lounge for 3,000 yen per person. For a small fee, gain access to JAL's Sakura Lounge during business trips or special commemorative trips.

Desde la wikipedia logré encontrar el código correspondiente al aeropuerto.

[https://en.wikipedia.org/wiki/List\\_of\\_airports\\_in\\_Japan](https://en.wikipedia.org/wiki/List_of_airports_in_Japan)

**Airports** [ edit ]

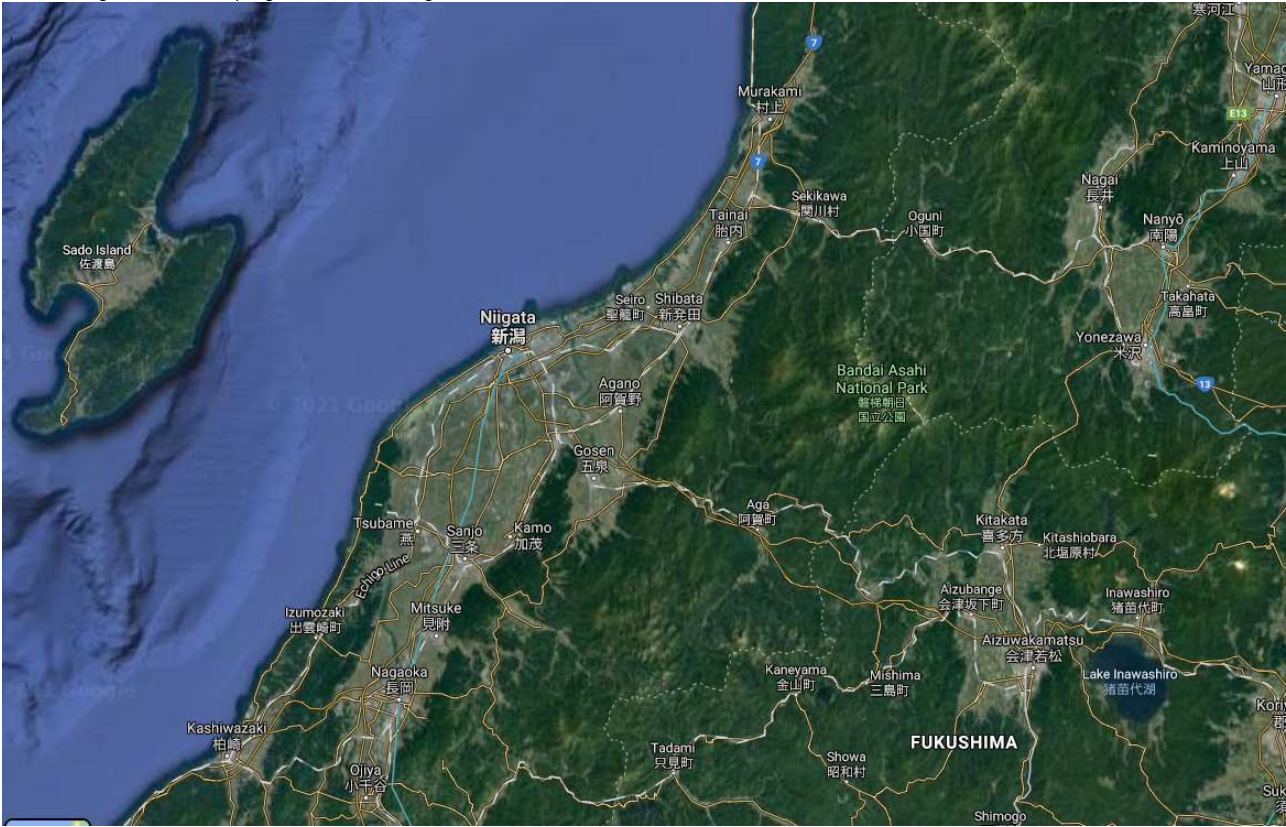
Airport name	Municipality	Prefecture	Island	ICAO	IATA	Classification
Kansai International Airport	Izumisano / Tajiri / Sennan	Osaka	Honshu	RJBB	KIX	First-class
Narita International Airport	Narita	Chiba	Honshu	RJAA	NRT	First-class
Chubu Centrair International Airport	Tokoname	Aichi	Honshu	RJGG	NGO	First-class
Tokyo International Airport	Ōta	Tokyo	Honshu	RJTT	<b>HND</b>	First-class

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

Respuesta: **Lake inawashiro**

Dada la experiencia que teníamos a este punto, encontrar este lago fue juego de niños..

Tracé una ruta entre HND y la ubicación final del sospechoso (basado en wigle) y ya pude buscar fácilmente la figura de la Isla SADO y luego hacer match con el lago buscado.

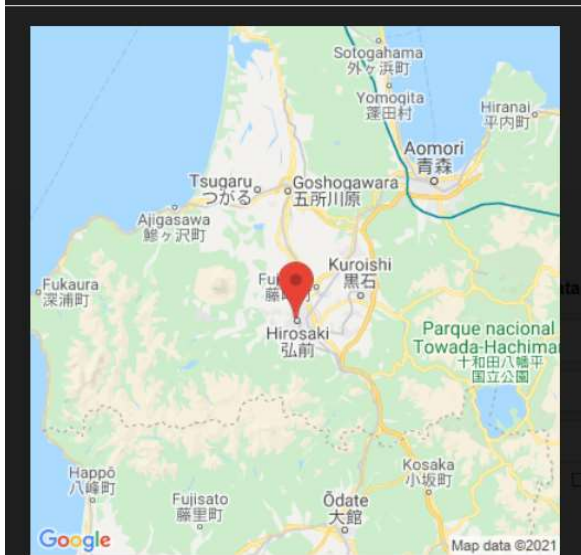


What city does the attacker likely consider "home"?


Respuesta: **Hirosaki**

Este respuesta la teníamos de varias anteriores.. Desde wigle.net podíamos pinchar en el mapa e instantáneamente nos indicaba la ciudad donde estaba el access point del sospechoso.

## Network Location



**Click for interactive map**



106

Sakura Room

Use a variety of OSINT techniques to solve this room created by the OSINT Dojo.

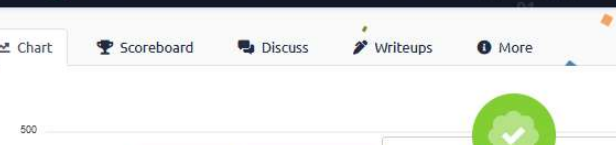
Chart


Scoreboard

Discuss

Writeups

More





Congratulations

You've completed the room!

Share on Twitter

Share on Facebook

in Share on LinkedIn

87







430023

 Users

20

 Rank