DÍA D - EJERCICIO FINAL - CTF OSINT

Prerrequisitos

Crear cuenta: https://tryhackme.com/login

Sakura Room

https://tryhackme.com/room/sakura

Introducción:

Esta sala está diseñada para probar una amplia variedad de técnicas OSINT diferentes. Con un poco de investigación, la mayoría de los practicantes principiantes de OSINT deberían poder completar estos desafíos. Esta sala os llevará a través de una investigación OSINT de muestra en la que se os pedirá que identifiquéis información relevante para ayudar a atrapar a un ciberdelincuente. Cada sección incluirá algún pretexto que os ayudará a orientaros en la dirección correcta, así como una o más preguntas que deberán responderse para continuar con la investigación. NOTA: Todas las respuestas se pueden obtener mediante técnicas OSINT pasivas. NO intentéis ninguna técnica activa, como comunicarse con los propietarios de cuentas, restablecer contraseñas, etc., para resolver estos desafíos.

Escenario:

El Dojo de OSINT recientemente fue víctima de un ciberataque. Parece que no hay daños importantes y no parece haber ningún otro indicador significativo de compromiso en ninguno de nuestros sistemas. Sin embargo, durante el análisis forense, nuestros administradores encontraron una imagen dejada por los ciberdelincuentes. ¿Quizás contenga algunas pistas que nos permitan determinar quiénes fueron los atacantes?... Pruebas:

Task 1 - INTRODUCTION

¡Aparece la palabra en el propio documento para que empieces el ejercicio!

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

Task 2 - TIP-OFF

Me he descargado la imagen que proporciona el documento que es esta:

Después le he dado clic derecho y le he dado a clic en el botón de Ver código fuente de la página.

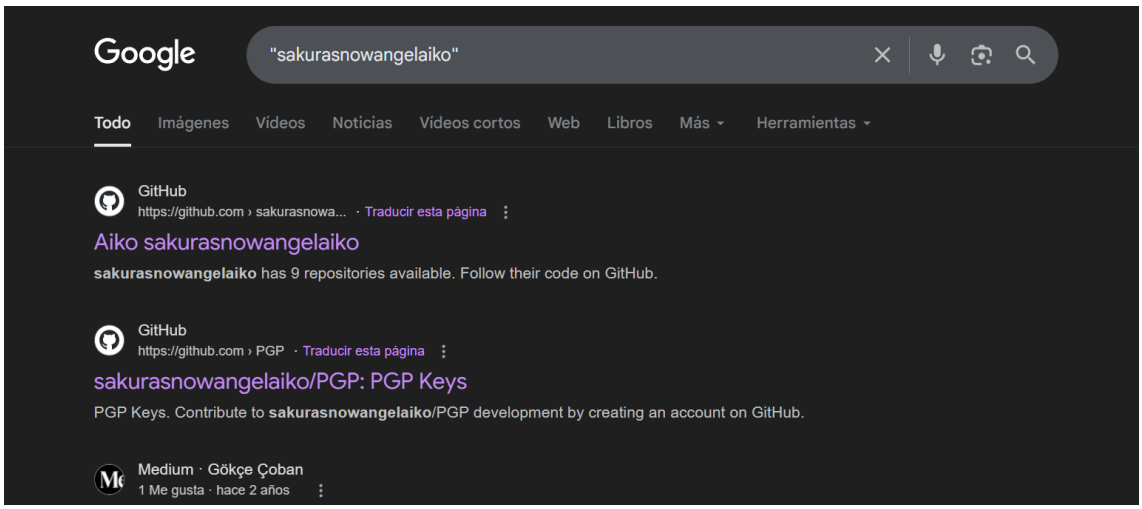
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!-- Created with Inkscape (http://www.inkscape.org/) -->

<svg
   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">>
  <defs
     id="defs2">
    <linearGradient
       id="linearGradient905-3"
       inkscape:collect="always">
      <stop
         id="stop901"
         offset="0"
         style="stop-color:#ffffff;stop-opacity:1;" />
      <stop
         style="stop-color:#ffffff;stop-opacity:0.14509804;"
         offset="0.86251646"
         id="stop916" />
      <stop
         id="stop903"
```

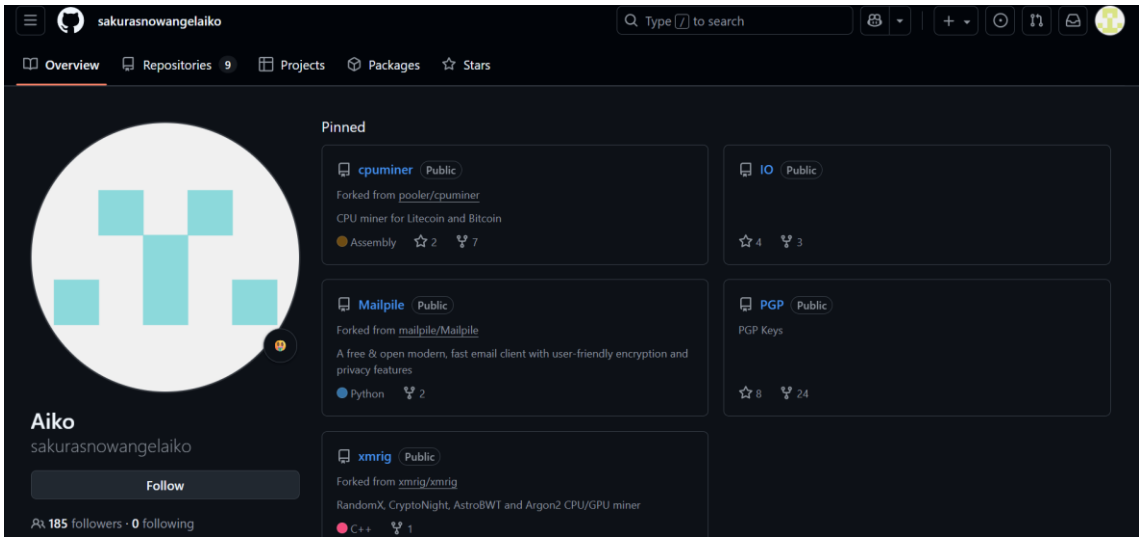
Y donde te he marcado en rojo me aparecía el nombre de usuario.

Task 3 - RECONNAISSANCE

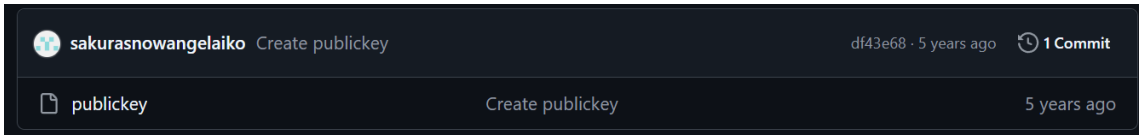
Primero he puesto con Google Dorcks el parámetro "sakurasnowangelaiko" y me ha salido su cuenta de GitHub.



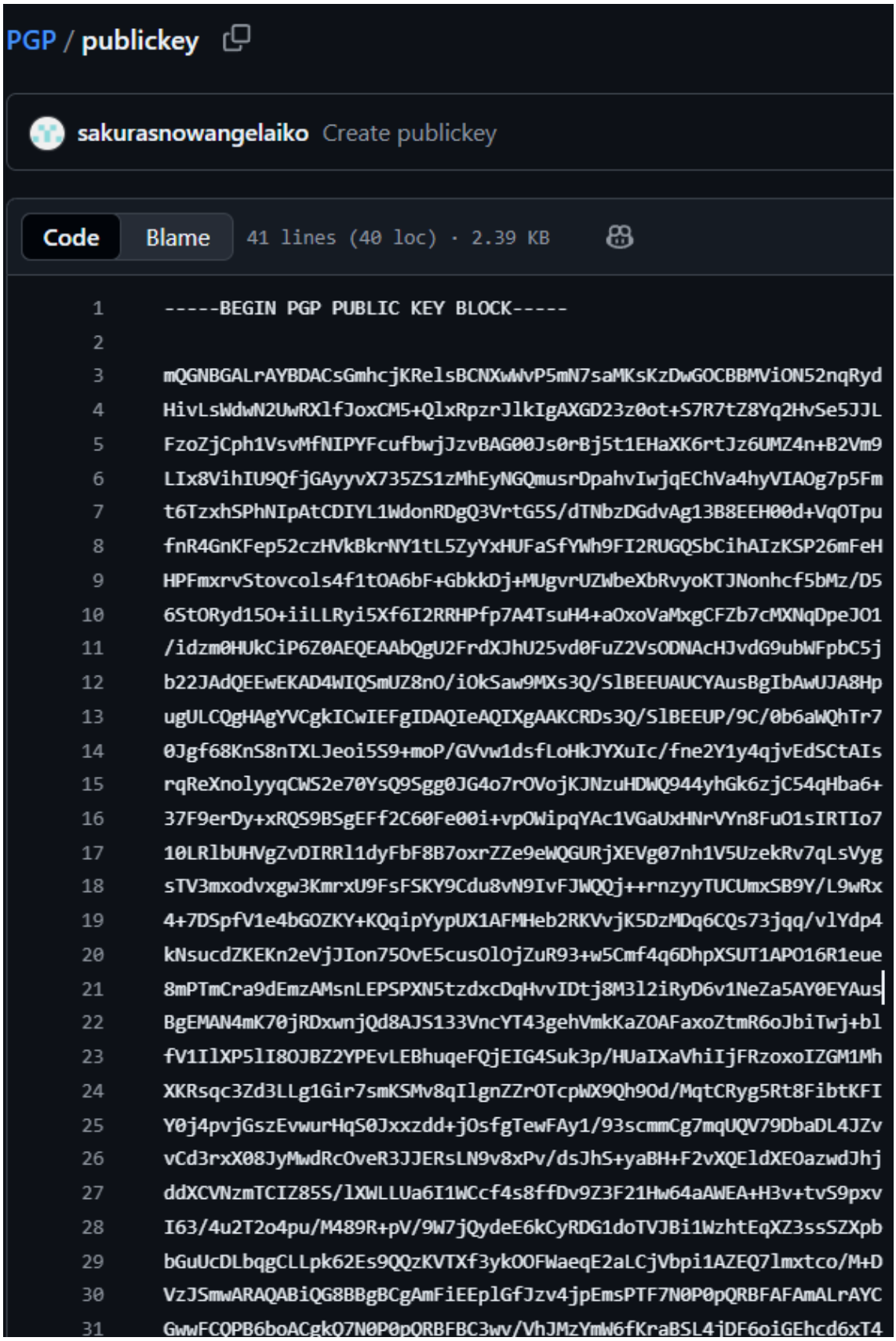
Después de estar un buen rato indagando por su perfil, me he dado cuenta de que había que entrar en este repositorio.



Una vez estas dentro del documento PGP te aparece esto:



Una vez entras dentro de publickey accedes a esto:



Que se trata del texto que tienes que decodificar en PGP.

Lo he pasado por una herramienta de Google y me ha decodificado el texto y dado el resultado:

```
b4 20 53 61 6b 75 72 61 53 6e 6f 77 41 6e 67 65
6c 38 33 40 70 72 6f 74 6f 6e 6d 61 69 6c 2e 63
6f 6d
```

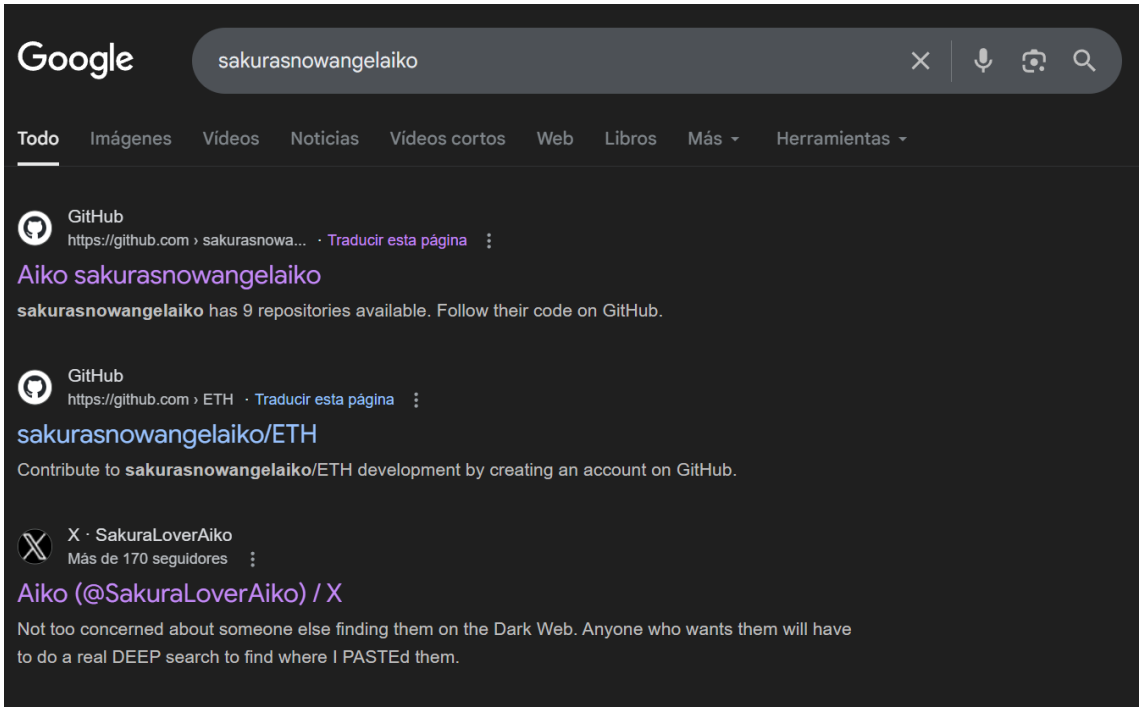
User ID Packet (0xd)

```
cipherTypeByte: "180"
length: "32"
userId: "SakuraSnowAngel83@protonmail.com"
```

```
89 01 d4 04 13 01 0a 00 3e 16 21 04 a6 51 9f 27
3b f8 8e 91 26 b0 f4 c5 ec dd 0f d2 94 11 04 50
```

Signature Packet (0x2)

El correo es: SakuraSnowAngel83@protonmail.com



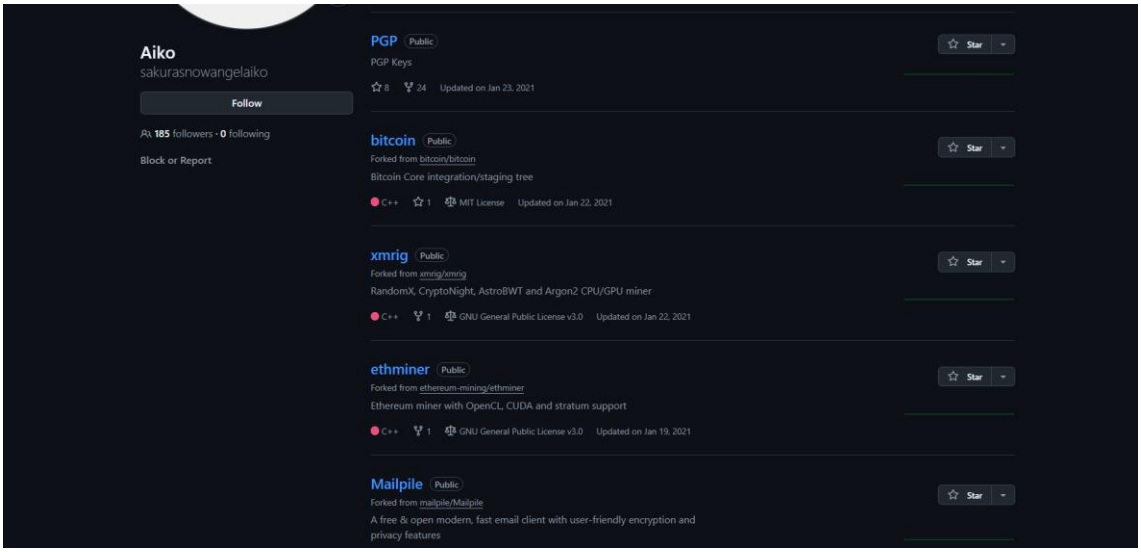
He buscado su nombre de GitHub en Google y me ha aparecido una cuenta de X suya.

Una vez he accedido a su cuenta y he bajado en sus posts me he encontrado con este “tweet” suyo.

He probado en TryHackMe poner el nombre Aiko Abe y me ha dado respuesta correcta.

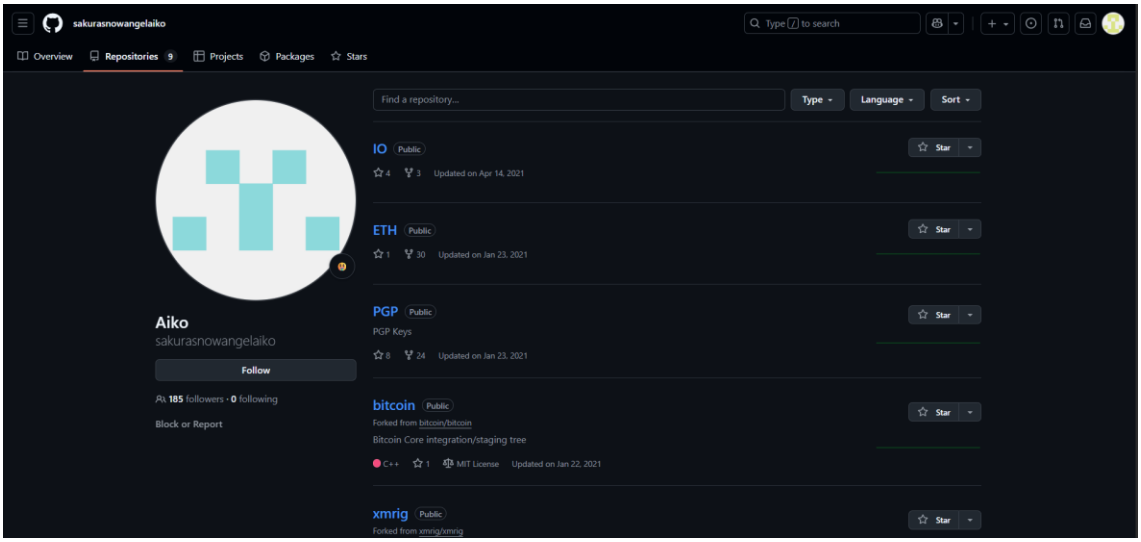
Task 4 - UNVEIL

1.

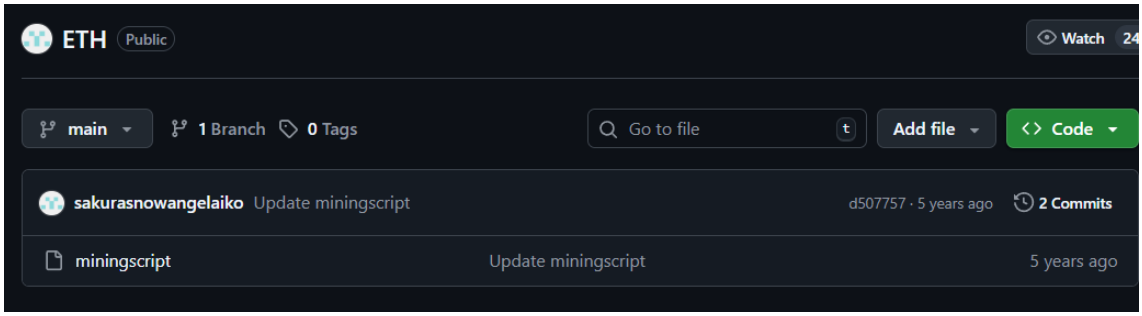


Me he metido en sus repositorios de GitHub y me ha aparecido ese con el titulo de ethminer y debajo que trabaja con Ethereum y lo he puesto en el ejercicio y me ha aparecido correcto.

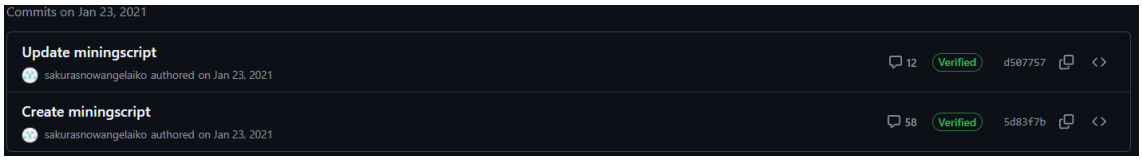
2. Hay que meterse en el repositorio de ETH



Hay que acceder al apartado que dice 2 Commits.



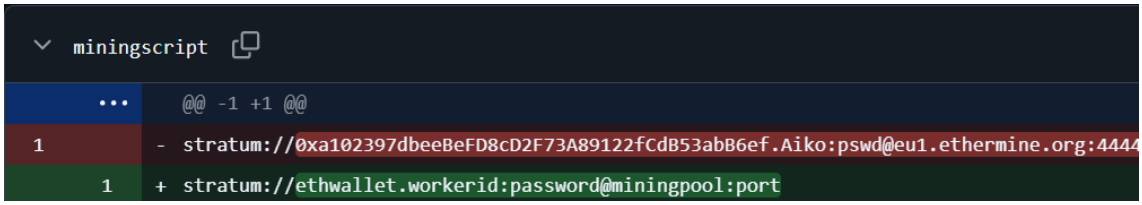
Después una vez lo has presionado te sale esto:



Primero nos sale ya la fecha en que se creó la Wallet.

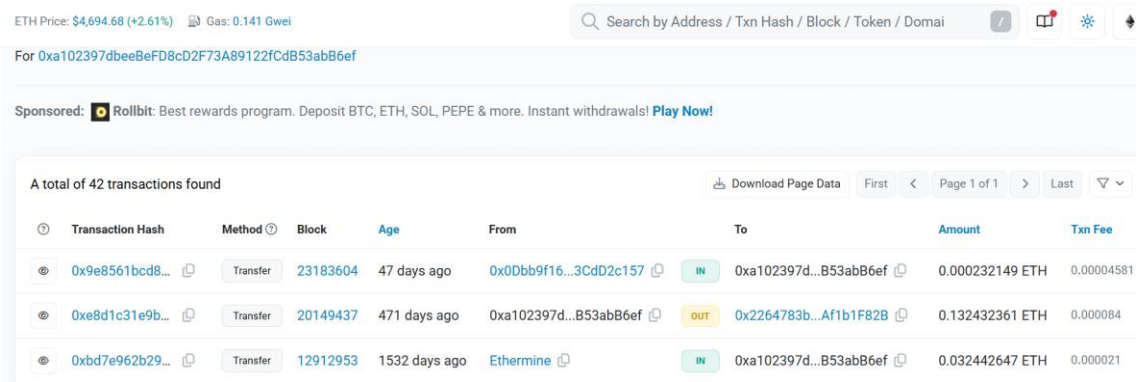
Nos metemos en el primero, en el “Update minigscript”.

Una vez estás dentro te aparece esto.



Aquí tienes la solución de la dirección de la cartera del atacante que es 0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef, el grupo de minería del que recibió los pagos que es Ethermine.

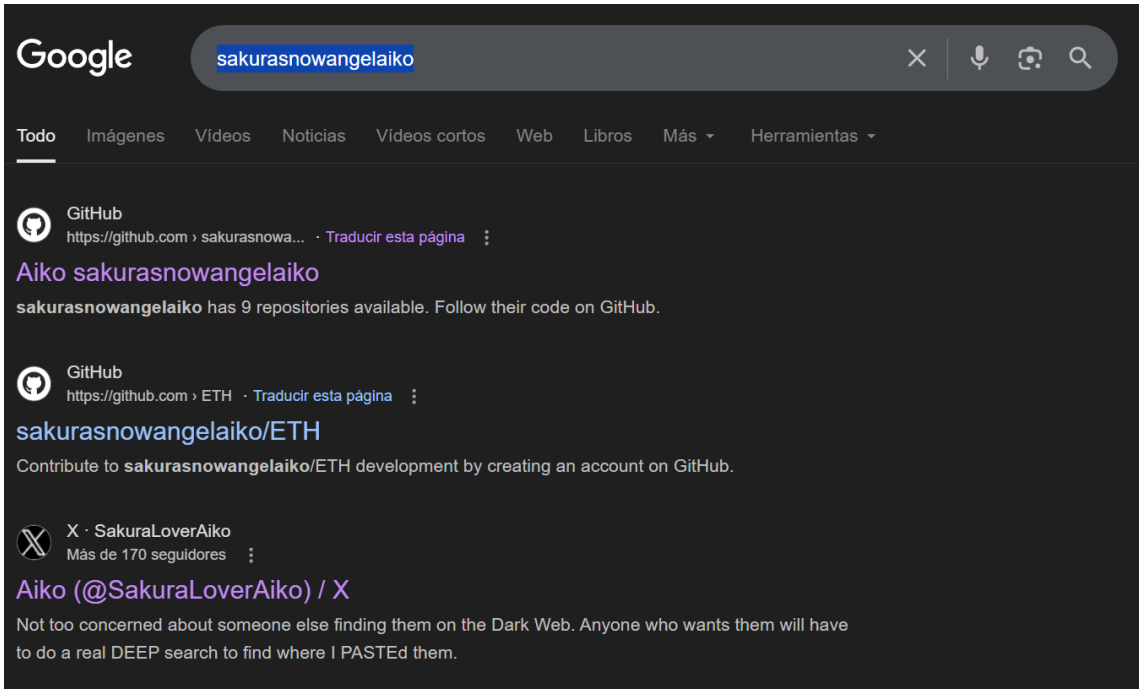
Para ver que otra criptomoneda intercambio el atacante he buscado en Google webs para ver movimientos de direcciones de carteras de criptomonedas me ha dado como resultado Etherscan.



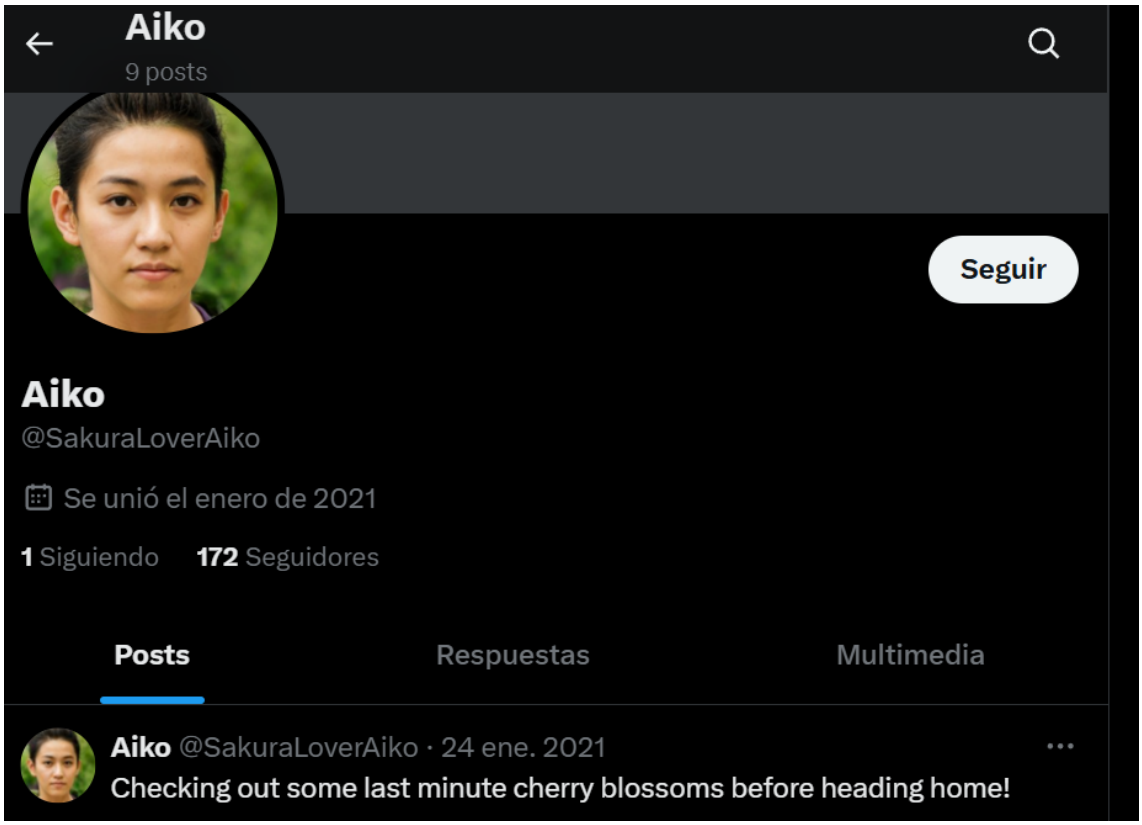
Una vez he accedido poniendo la dirección de la cartera en la Web, me aparecía Ethermine que es la solución.

Task 5 - TAUNT

He puesto en el buscador de Google “sakurasnowangelaiko”

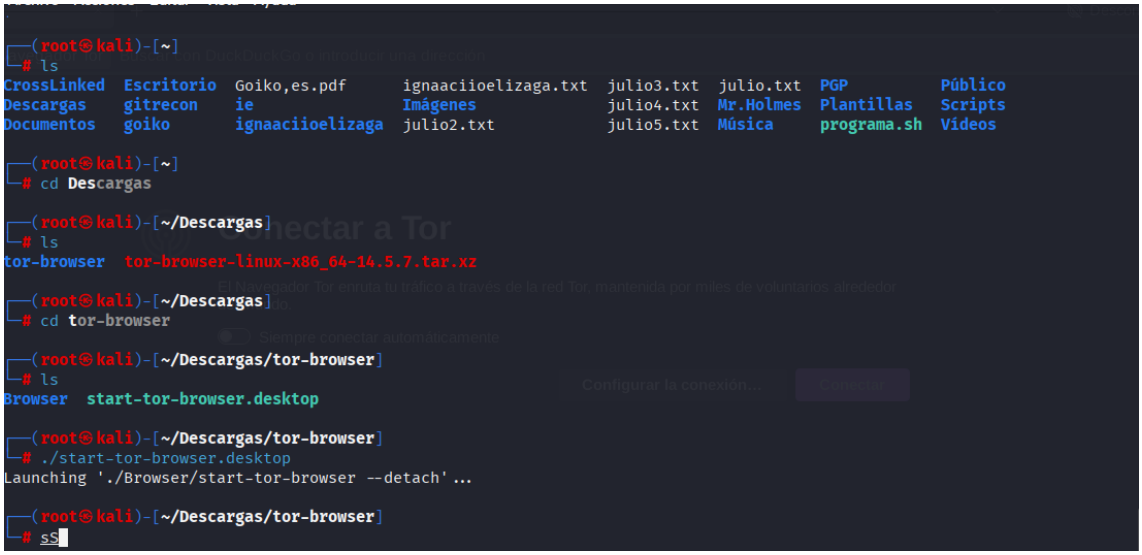


Me he metido en el tercer enlace que es de su cuenta de Twitter y he introducido el nombre que es quitando el signo de “@” y era ese el nombre.

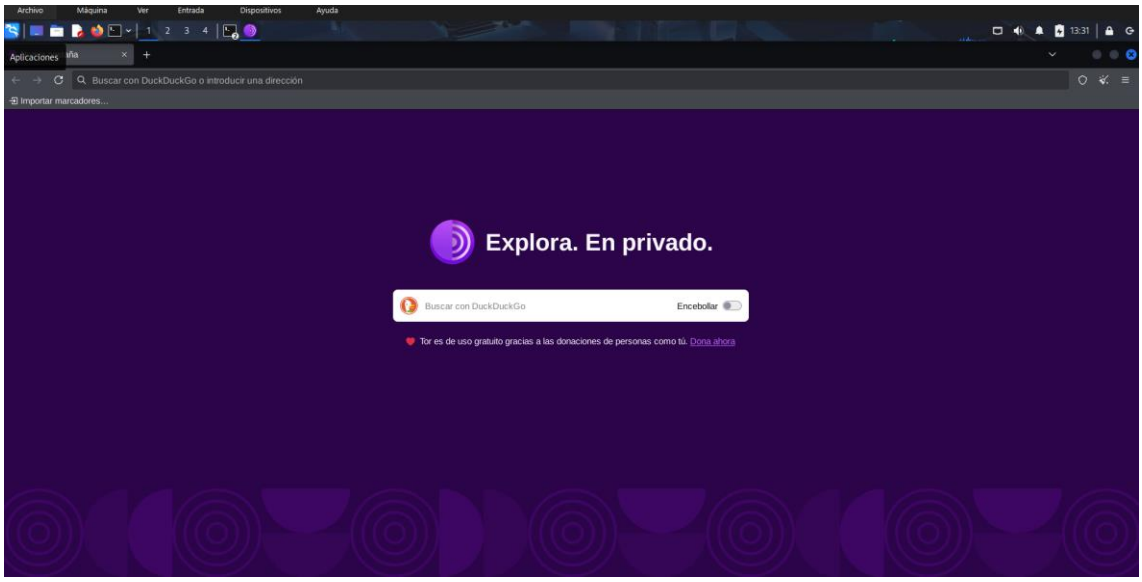


Ahí me aparece en el arroba su nombre y lo he probado quitándolo y me ha funcionado.

5.2

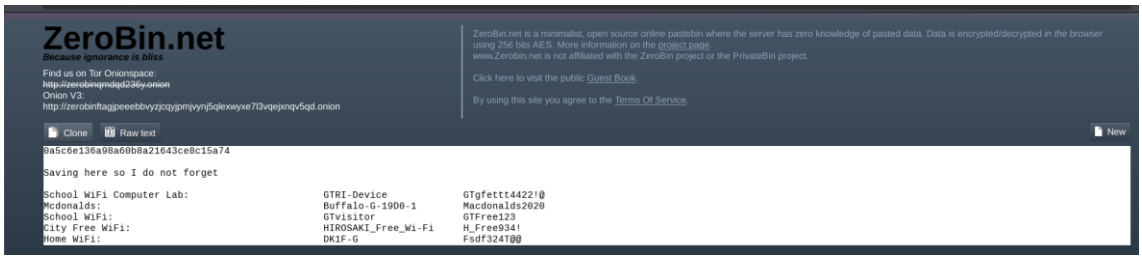


Con estos comandos e iniciado Thor.



Aquí como se puede ver ya estamos dentro de la Dark Weeb.

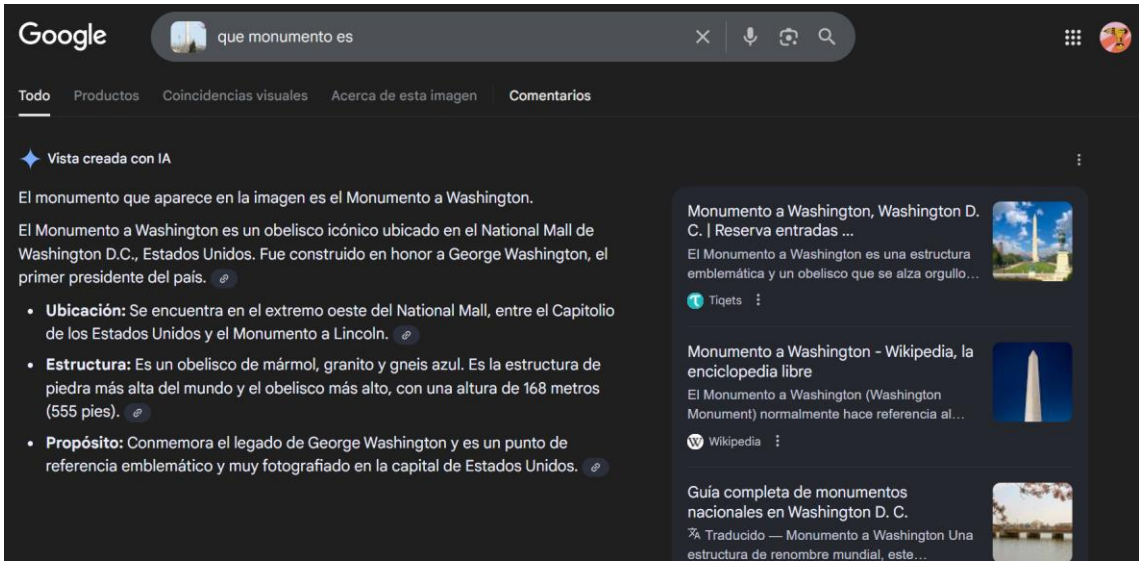
Ahora he introducido la URL que tenemos en slack que es: http://zerobinftagjpeeebbvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/?cd484d8f2fd1cc00#jbAhOJpIt4+o6K+3YT2P4dlLoy+kcWX25B+9Xa/qC0o=



Ahí aparece un numero que lo he convertido a BSSID.

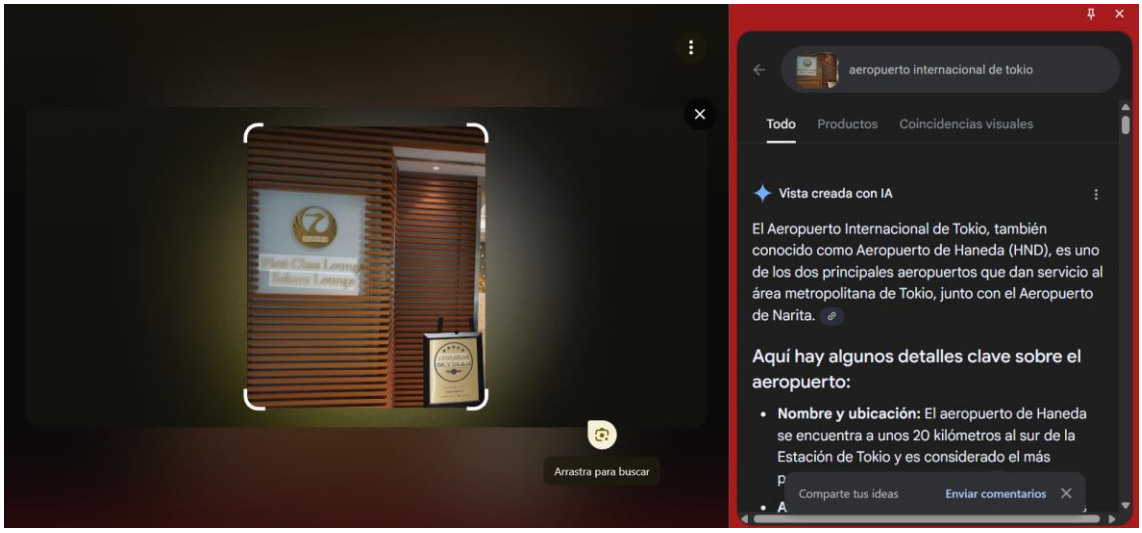
Task 6 - HOMEBOUND

En esta imagen publicada por el atacante se puede ver de frente un monumento con forma de palo, se lo he metido al Google lean y me ha dicho dónde estaba.

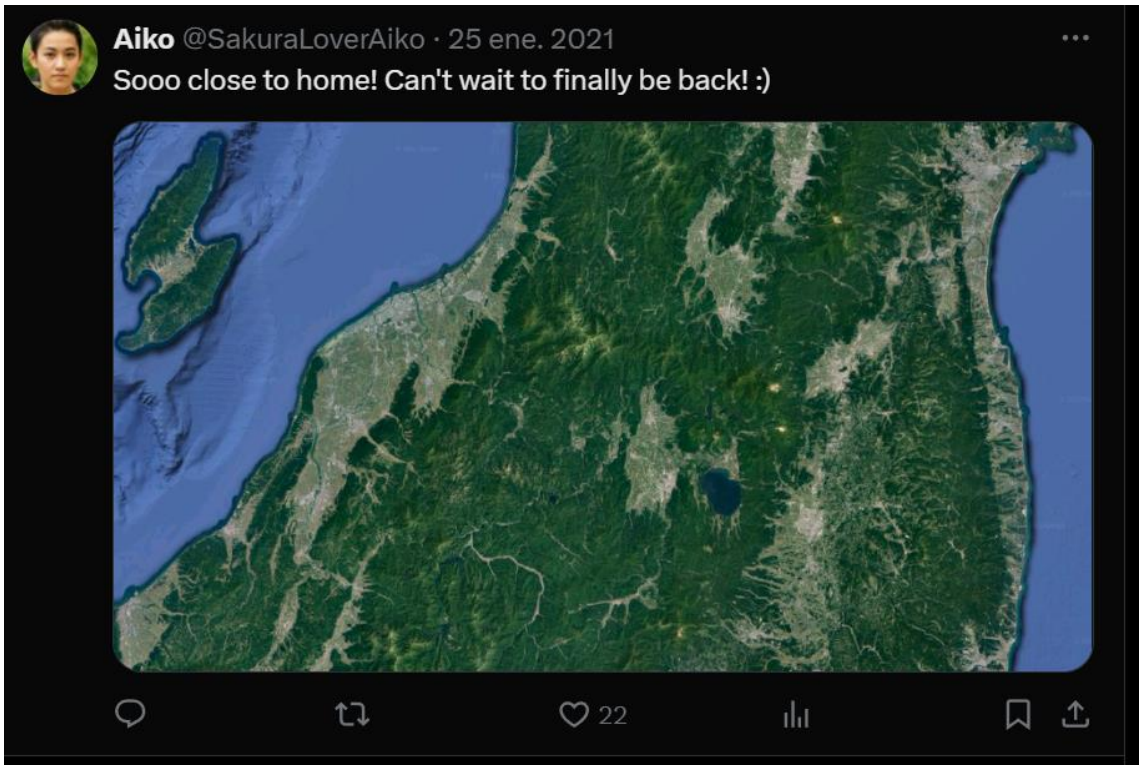


He buscado cual era el aeropuerto mas cercano a esa ubicación en Google y me ha salido la respuesta.

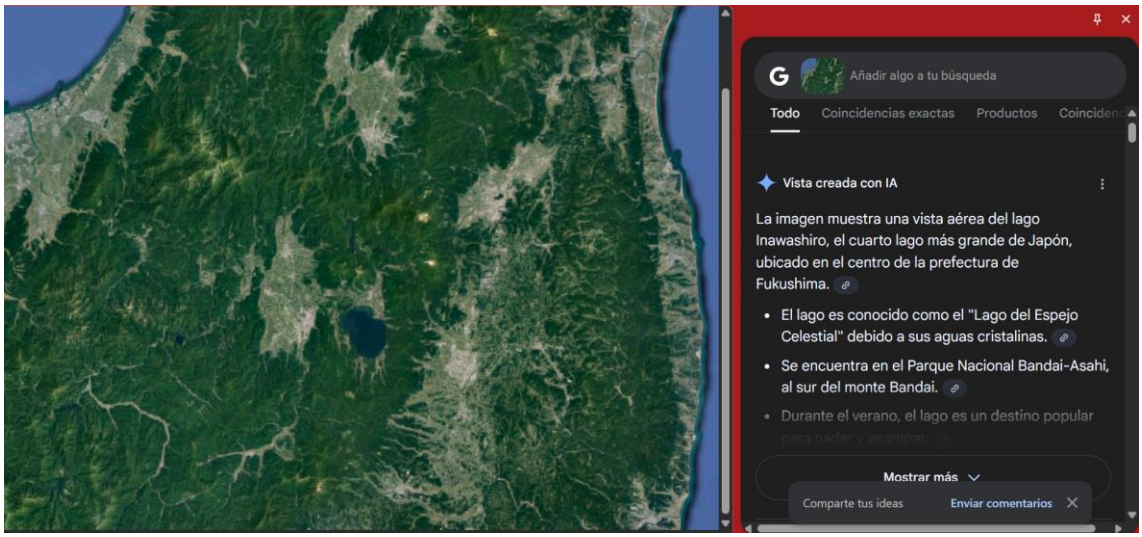
Para la respuesta del segundo, he metido la imagen en Google lean y me ha dicho directamente que aeropuerto era y buscando el código de 3 dígitos me ha salido que era NHD.



Para el Tercero he encontrado esta foto en su perfil de Tiktok y salía esta publicación.



La he metido en Google leans y me ha salido el nombre del lago.



Con esto ya tenía la respuesta.

Por último, la ciudad que el autor considera como su hogar es: Hirosaki.

Donde he subrayado en rojo dentro de esta captura se aprecia la wifi gratis de la ciudad en la que vive y así se averigua la respuesta.