

## 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.

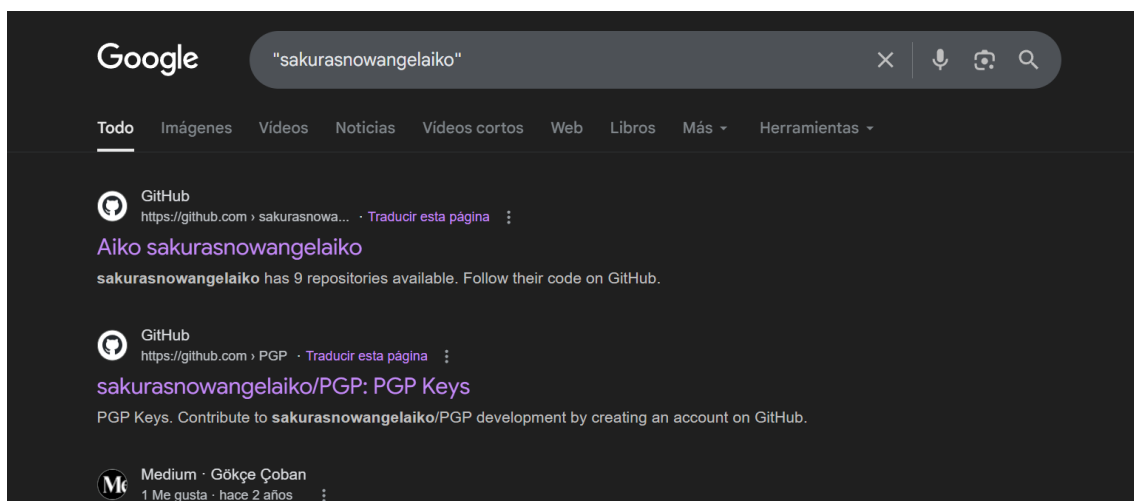
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!-- Created with Inkscape (http://www.inkscape.org/) -->

<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"
        offset="1"
        style="stop-color:#ffffff;stop-opacity:1;" />
    </linearGradient>
  </defs>
</svg>
```

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.

sakurasnowangelaiko

Overview Repositories 9 Projects Packages Stars



**Aiko**  
sakurasnowangelaiko

Follow

185 followers · 0 following

**Pinned**

**cpuminer** Public

Forked from pooler/cpuminer

CPU miner for Litecoin and Bitcoin

Assembly ☆ 2 🍴 7

**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

**PGP** Public

PGP Keys

☆ 8 🍴 24

**xmrig** Public

Forked from xmrig/xmrig

RandomX, CryptoNight, AstroBWT and Argon2 CPU/GPU miner

C++ 🍴 1

Una vez estas dentro del documento PGP te aparece esto:

sakurasnowangelaiko Create publickey df43e68 · 5 years ago 1 Commit

publickey	Create publickey	5 years ago
-----------	------------------	-------------

Una vez entras dentro de publickey accedes a esto:



Code

Blame

41 lines (40 loc) · 2.39 KB



```
1  -----BEGIN PGP PUBLIC KEY BLOCK-----
2
3  mQGNBGALrAYBDACsGmhCjKRelSBCNXwWvP5mN7saMKsKzDwGOCBBMVion52nqRyd
4  HivLsWdwN2UwRXlfJoxCM5+QlxRpzrJlkIgAXGD23z0ot+S7R7tZ8Yq2HvSe5JJL
5  FzoZjCph1VsvMfNIPYFcufbwjJzvBAG00Js0rBj5t1EHaXK6rtJz6UMZ4n+B2Vm9
6  LIx8VihIU9QfjGAyyvX735ZS1zMHyNGQmusrDpahvIwjqEChVa4hyVIA0g7p5Fm
7  t6TzxhSPhNIpAtCDIYL1WdonRDgQ3VrtG5S/dTNbzDGdvAg13B8EEH00d+Vq0Tpu
8  fnR4GnKFep52czHVkBkrNY1tL5zyYxHUFaSFYWh9FI2RUGQ5bCiHAizKSP26mFeH
9  HPFmxrvStovcols4f1tOA6bF+GbkkDj+MUgvrUZWbeXbRvyoKTJNonhcf5bMz/D5
10  6StORyd150+iiLLRyi5Xf6I2RRHPfp7A4TsuH4+a0xoVaMxgCFZb7cMXNqDpeJ01
11  /idzm0HUKCiP6Z0AEQEAAQgU2FrdXJhU25vd0FuZ2VsODNACjVdG9ubWfPbC5j
12  b22JAdQEewEKAD4WlQSmUZ8n0/i0kSaw9MXs3Q/S1BEEUAUCYAusBgIbAwUJA8Hp
13  ugULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAKCRDs3Q/S1BEEUP/9C/0b6aWqhTr7
14  0Jgf68KnS8nTXLJeoI5S9+moP/GVvw1dsfLoHkJYXuIc/fne2Y1y4qjvEd5CtAIs
15  rQReXno1yyqCW52e70YsQ9Sgg0JG4o7r0VoJkNzuHDWQ944yhGk6zjC54qHba6+
16  37F9erDy+xRQS9BSgEFF2C60Fe00i+vpOWipqYAc1VGaUxHNRvYn8Fu01sIRTIo7
17  10LRlbuHvgZvDIRR11dyFbF8B7oxrZZe9eWQGURjXEVg07nh1V5UzekRv7qLsVyg
18  sTV3mxodvxgw3KmrXU9FsFSKY9Cdu8vN9IvFJWQJj++rnzyyTUCUmxSB9Y/L9wRx
19  4+7D5pfV1e4bG0ZKY+KQqipYypUX1AFMHeb2RKVvjK5DzMDq6CQs73jqj/vlYdp4
20  kNsucdZKEKn2eVjJion750vE5cus0l0jZuR93+w5Cmf4q6DhpXSUT1AP016R1eue
21  8mPTmCra9dEmzAMsnLEPSPXN5tZdxcDqHvvIDtj8M3l2iRyD6v1NeZa5AY0EYAus
22  BgEMAN4mK70jRDxwnjQd8AJ5133VncYT43gehVmkKaZOAFaxoZtmR6oJbiTwj+b1
23  fV1I1XP51I80JBZ2YPEvLEBhuqeFQjEIG4Suk3p/HUaIXaVhiIJFRzoxoIZGM1Mh
24  XKRsqc3Zd3LLg1Gir7smKSMv8qIlgnZZrOTcpwX9Qh90d/MqtCRyg5Rt8FibtKFI
25  Y0j4pvjGszEvwurHqS0Jxxzdd+j0sfgTewFAy1/93scmmCg7mqUQV79DbadL4JZv
26  vCd3rxX08JyMwdRcOveR3JJERSLN9v8xPv/dsJhS+yaBH+F2vXQEldXE0azwdJhj
27  ddXCVNzmTCIZ85S/1XWLLUa6I1WCcf4s8ffDv9Z3F21Hw64aAWEA+H3v+tvS9pxv
28  I63/4u2T2o4pu/M489R+pV/9W7jQydeE6kCyRDG1doTVJB1iWzhtEqXZ3ssSZXpb
29  bGuUcDLbqgCLLPk62Es9QQzKVTF3yk00FWaeqE2aLCjVbp11AZEQ7lmxtco/M+D
30  VzJSmwARAQABiQG8BBgBCgAmFIEEp1GfJzv4jpEmsPTF7N0P0pQRBFAFAMAlRAYC
31  GwwFCOPB6boACgkQ7N0P0pQRBFBFC3wv/VhJMzYmW6fKraBSL4jDF6oiGEhcd6xT4
```

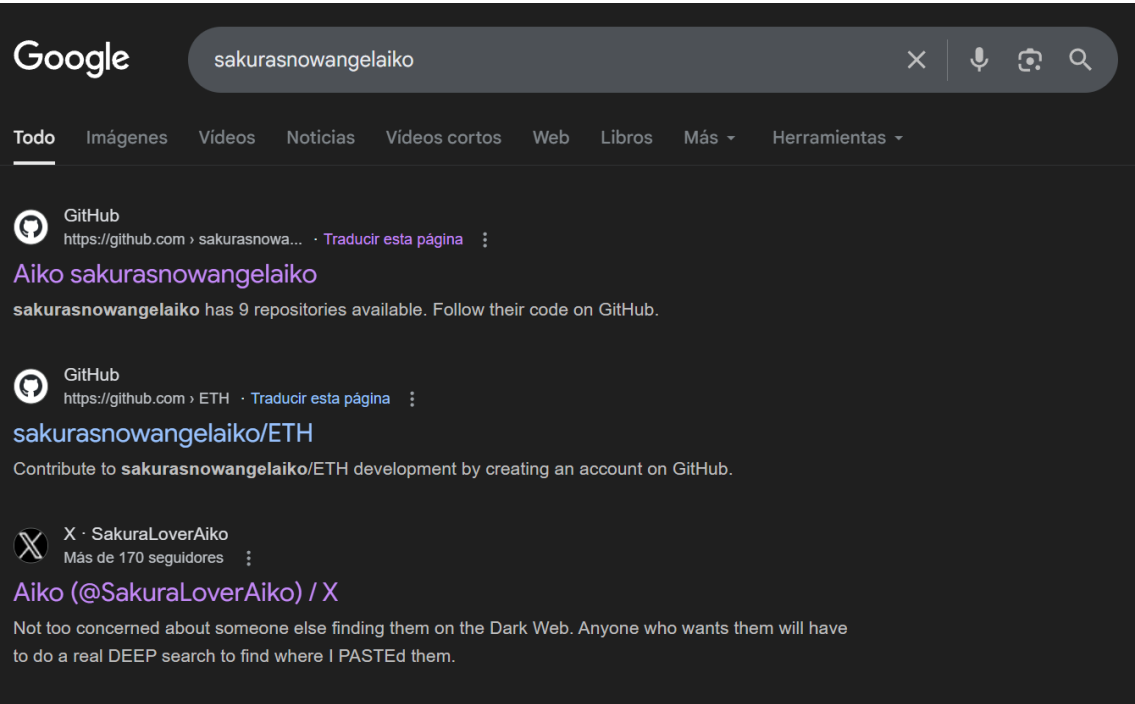
Que se trata del texto que tienes que decodificar en PGP.

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 User ID Packet (0xd)
6c 38 33 40 70 72 6f 74 6f 6e 6d 61 69 6c 2e 63
6f 6d
cipherTypeByte: "180"
length: "32"
userId: "SakuraSnowAngel83@protonmail.com"

89 01 d4 04 13 01 0a 00 3e 16 21 04 a6 51 9f 27 Signature Packet (0x2)
3b f8 8e 91 26 b0 f4 c5 ec dd 0f d2 94 11 04 50
a5 a7 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77
```

El correo es: **SakuraSnowAngel83@protonmail.com**



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

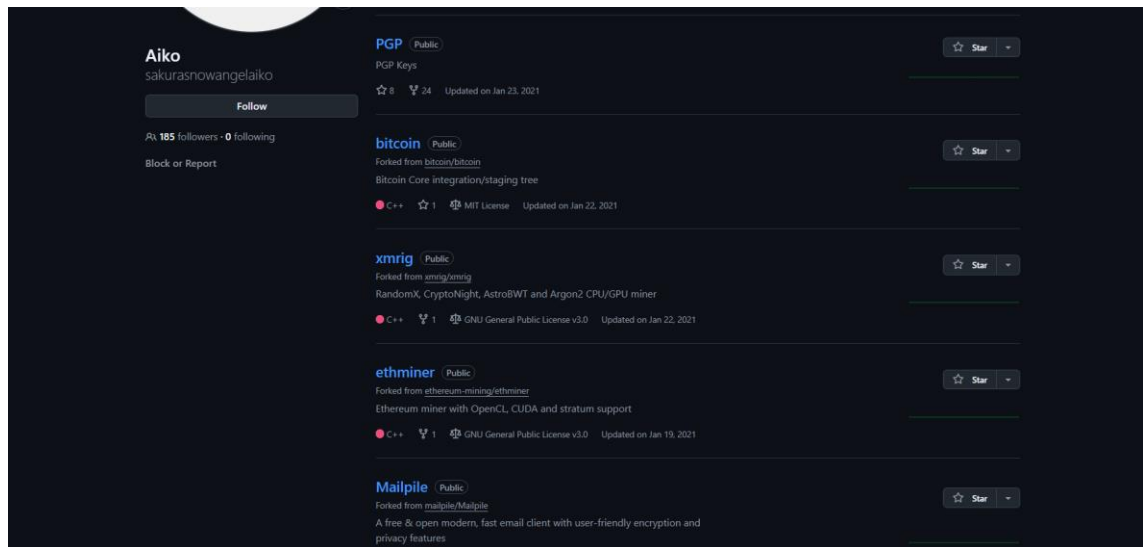
Una vez he accedido a su cuenta y he bajado en sus posts me he encontrado con este “tweet” suyo.



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

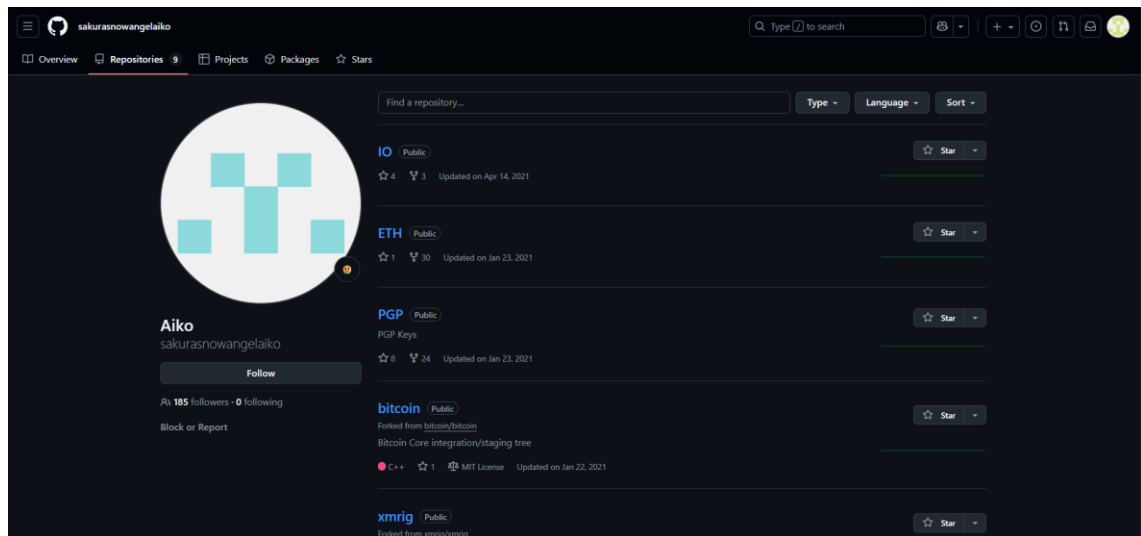
## Task 4 - UNVEIL

1.

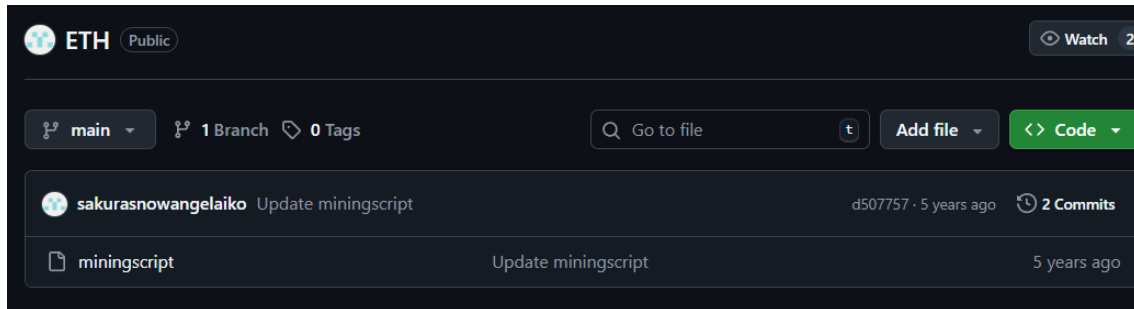


Me he metido en sus repositorios de GitHub y me ha aparecido ese con el título de ethminer y debajo que trabaja con Ethereum y lo he puesto en el ejercicio y me ha aparecido correcto.

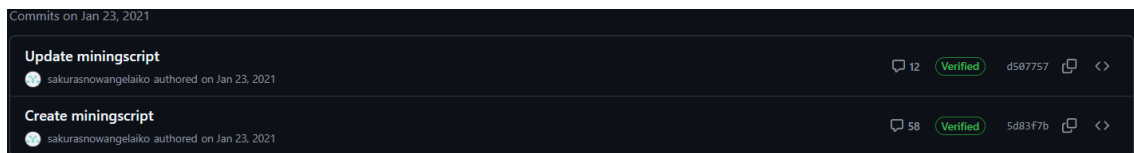
2. Hay que meterse en el repositorio de ETH



Hay que acceder al apartado que dice 2 Commits.



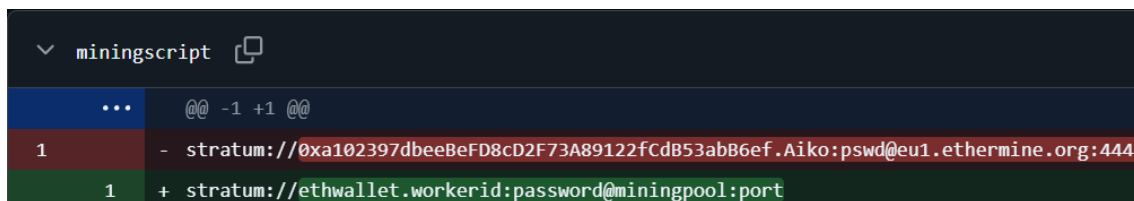
Después una vez lo has presionado te sale esto:



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

Nos metemos en el primero, en el "Update miningscript".

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.



ETH Price: \$4,694.68 (+2.61%) Gas: 0.141 Gwei

Search by Address / Txn Hash / Block / Token / Domai

For 0xa102397dbeeBFD8cD2F73A89122fCdB53abB6ef

Sponsored: Rollbit: Best rewards program. Deposit BTC, ETH, SOL, PEPE & more. Instant withdrawals! [Play Now!](#)

A total of 42 transactions found

Download Page Data First < Page 1 of 1 > Last

Transaction Hash	Method	Block	Age	From	To	Amount	Txn Fee
0x9e8561bcd8...	Transfer	23183604	47 days ago	0x0Dbb9f16...3CdD2c157	IN 0xa102397d...B53abB6ef	0.000232149 ETH	0.00004581
0xe8d1c31e9b...	Transfer	20149437	471 days ago	0xa102397d...B53abB6ef	OUT 0x2264783b...Af1b1F82B	0.132432361 ETH	0.000084
0xbd7e962b29...	Transfer	12912953	1532 days ago	Ethermine	IN 0xa102397d...B53abB6ef	0.032442647 ETH	0.000021

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”

Google sakurasnowangelaiko

Todo Imágenes Vídeos Noticias Vídeos cortos Web Libros Más Herramientas

GitHub  
https://github.com > sakurasnowa... · Traducir esta página

**Aiko sakurasnowangelaiko**  
sakurasnowangelaiko has 9 repositories available. Follow their code on GitHub.

GitHub  
https://github.com > ETH · Traducir esta página

**sakurasnowangelaiko/ETH**  
Contribute to sakurasnowangelaiko/ETH development by creating an account on GitHub.

X · SakuraLoverAiko  
Más de 170 seguidores

**Aiko (@SakuraLoverAiko) / X**  
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.

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

```
(root@kali) - [~]
# ls
CrossLinked  Escritorio  Goiko.es.pdf  ignaacioelizaga.txt  julio3.txt  julio.txt  PGP  Público
Descargas    gitrecon    ie            Imágenes            julio4.txt  Mr.Holmes  Plantillas  Scripts
Documentos   goiko       ignaacioelizaga  julio2.txt          julio5.txt  Música     programa.sh  Videos

(root@kali) - [~]
# cd Descargas

(root@kali) - [~/Descargas]
# ls
tor-browser  tor-browser-linux-x86_64-14.5.7.tar.xz

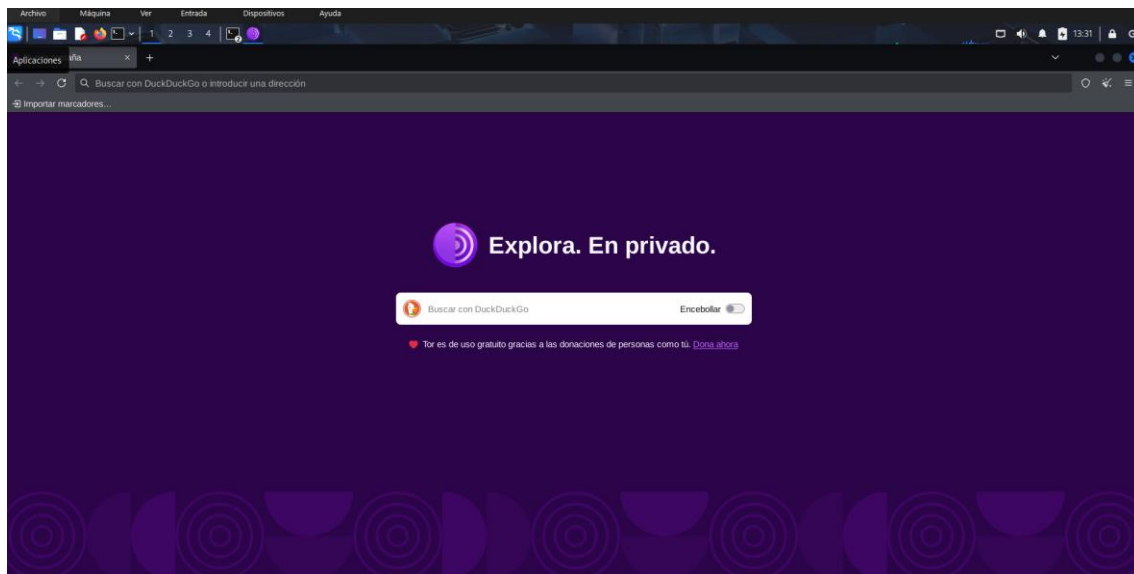
(root@kali) - [~/Descargas]
# cd tor-browser

(root@kali) - [~/Descargas/tor-browser]
# ls
Browser  start-tor-browser.desktop

(root@kali) - [~/Descargas/tor-browser]
# ./start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach' ...

(root@kali) - [~/Descargas/tor-browser]
# ss
```

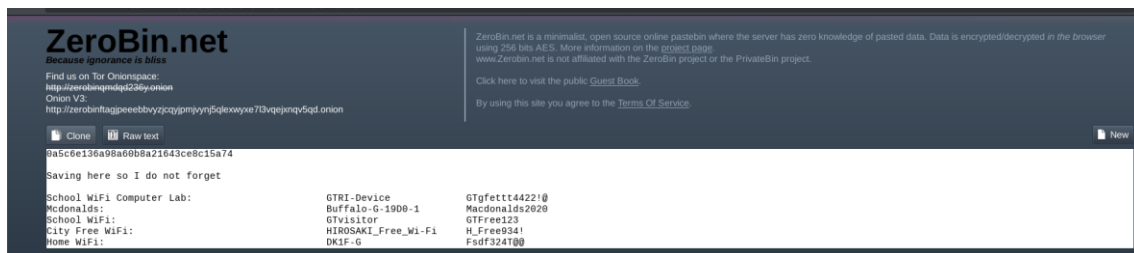
Con estos comandos e iniciado Thor.



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

Ahora he introducido la URL que tenemos en slack que es:

<http://zerobinftagjpeeebbvyzjcqyjpmyjynj5qlexwyxe7l3vqejxnqv5qd.onion/?cd484d8f2fd1cc00#jbAhOJplt4+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.

Google

Todo Productos Coincidencias visuales Acerca de esta imagen Comentarios

♦ Vista creada con IA

El monumento que aparece en la imagen es el Monumento a Washington.

El Monumento a Washington es un obelisco icónico ubicado en el National Mall de Washington D.C., Estados Unidos. Fue construido en honor a George Washington, el primer presidente del país.

- **Ubicación:** Se encuentra en el extremo oeste del National Mall, entre el Capitolio de los Estados Unidos y el Monumento a Lincoln.
- **Estructura:** Es un obelisco de mármol, granito y gneis azul. Es la estructura de piedra más alta del mundo y el obelisco más alto, con una altura de 168 metros (555 pies).
- **Propósito:** Conmemora el legado de George Washington y es un punto de referencia emblemático y muy fotografiado en la capital de Estados Unidos.

**Monumento a Washington, Washington D. C. | Reserva entradas ...**

El Monumento a Washington es una estructura emblemática y un obelisco que se alza orgullo...

Tickets

**Monumento a Washington - Wikipedia, la enciclopedia libre**

El Monumento a Washington (Washington Monument) normalmente hace referencia al...

Wikipedia

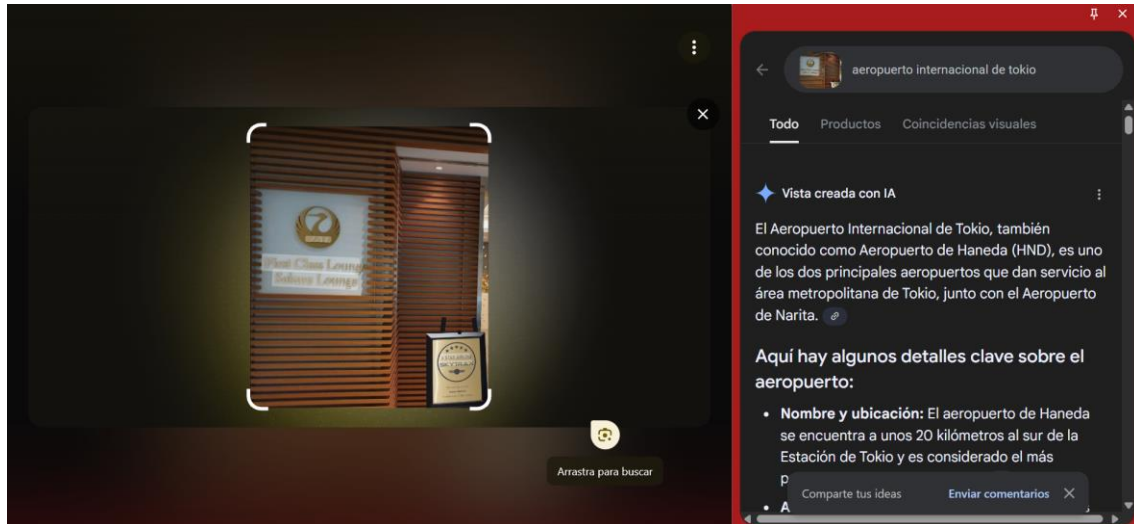
**Guía completa de monumentos nacionales en Washington D. C.**

Traducido — Monumento a Washington Una estructura de renombre mundial, este...

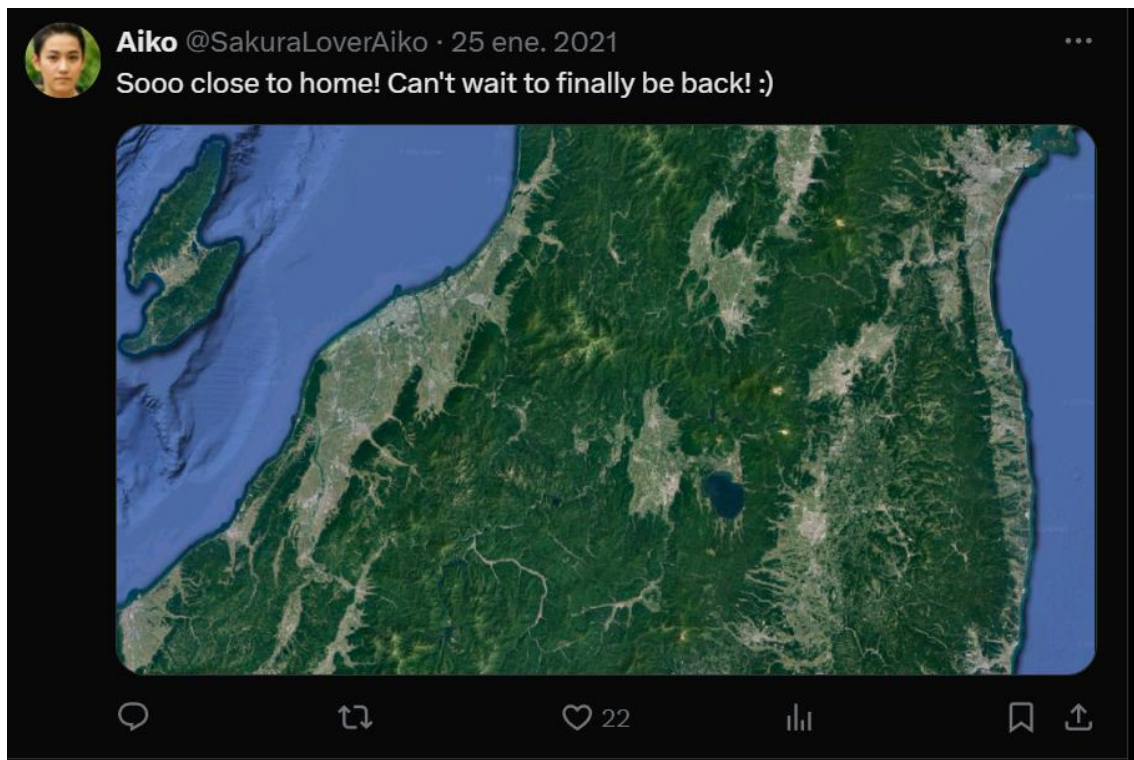


He buscado cual era el aeropuerto mas cercano a esa ubicación en Google y me ha salido la respuesta.

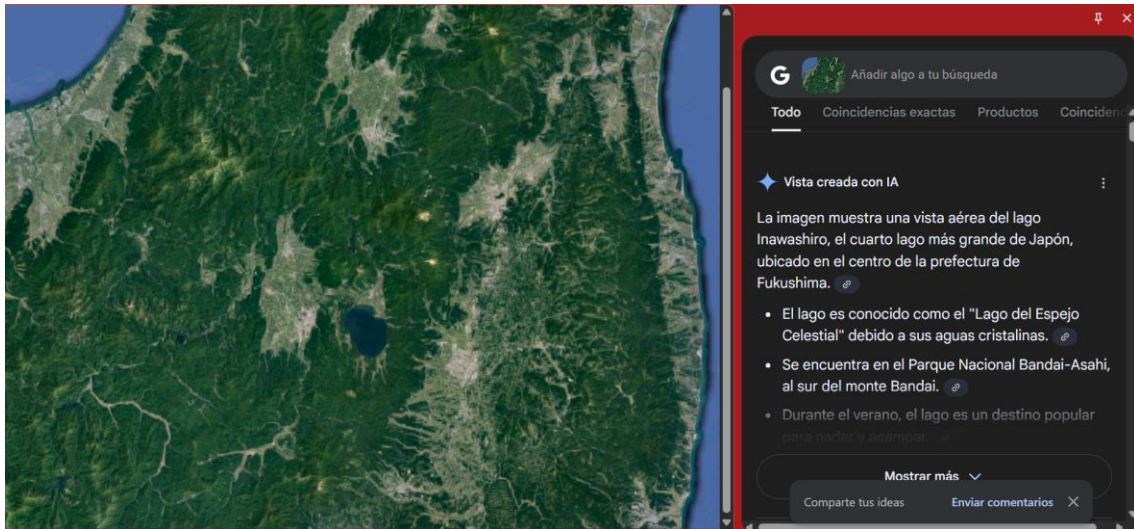
Para la respuesta del segundo, he metido la imagen en Google lean y me ha dicho directamente que aeropuerto era y buscando el código de 3 dígitos me ha salido que era NHD.



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.