

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.

The screenshot shows a Google search results page. The search term "sakurasnowangelaiko" is entered in the search bar. The top result is a GitHub profile for "Aiko sakurasnowangelaiko", which has 9 repositories available. Below this, another result is "sakurasnowangelaiko/PGP: PGP Keys". At the bottom of the page, there is a snippet from a Medium post by "Gökçe Çoban" with 1 like.

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

The screenshot shows a GitHub profile page for the user 'sakurasnowangelaiko'. The profile picture is a white circle with a teal cross pattern. The user has 185 followers and 0 following. There are four pinned repositories displayed:

- cpuminer** (Public) - Forked from pooler/cpuminer. CPU miner for Litecoin and Bitcoin. Assembly language, 2 stars, 7 forks.
- IO** (Public) - No description provided. 4 stars, 3 forks.
- Mailpile** (Public) - Forked from mailpile/Mailpile. A free & open modern, fast email client with user-friendly encryption and privacy features. Python language, 2 stars, 2 forks.
- xmrig** (Public) - Forked from xmrig/xmrig. RandomX, CryptoNight, AstroBlitz and Argon2 CPU/GPU miner. C++ language, 1 star, 1 fork.
- PGP** (Public) - PGP Keys. 8 stars, 24 forks.

Una vez estas dentro del documento PGP te aparece esto:

The screenshot shows a GitHub commit history for the repository 'publickey'. The commit was made by 'df43e68' 5 years ago. The commit message is 'Create publickey'. The commit details show the file 'Create publickey' was added 5 years ago.

Una vez entras dentro de publickey accedes a esto:

PGP / publickey



sakurasnowangelaiko Create publickey

Code

Blame

41 lines (40 loc) · 2.39 KB



```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----  
2  
3 mQGNBGALrAYBDACsGmhcjKRelsBCNxwWvP5mN7saMKsKzDwGOCBBMViON52nqRyd  
4 HivLsWdwN2UwRX1fJoxCM5+QlxRpzrJ1kIgAXGD23z0ot+S7R7tZ8Yq2HvSe5JJL  
5 FzoZjCph1VsvMfnIPYFcufbwjJzvBAG00Js0rBj5t1EHaXK6rtJz6UMZ4n+B2Vm9  
6 Lix8VihIU9QfjGAyyvX735ZS1zMhEyNGQmusrDpahvIwjjqEChVa4hyVIA0g7p5Fm  
7 t6TzxhSPhNIpAtCDIYL1WdonRDgQ3VrtGSS/dTNbzDGdvAg13B8EEH00d+VqOTpu  
8 fnR4GnKFep52czHVkBkrNY1tL5ZyYxHUFaSfYWh9FI2RUGQSbCihAIzKSP26mFeH  
9 HPFmxrvStovcols4f1t0A6bF+GbkkDj+MUgvrUZwbeXbRvyoKTJNonhcF5bMz/D5  
10 6St0Ryd150+iiLLRyi5XF6I2RRHPfp7A4TsuH4+aOxoVaMxgCFZb7cMXNqDpeJ01  
11 /idzm0HukCiP6Z0AEQEAAbQgu2FrDXjhU25vd0FuZ2VsODNaCHJvdG9ubWFpbC5j  
12 b22JAdQEEwEKAD4WIQSmlUZ8n0/i0kSaw9MXs3Q/S1BEEUAUCYAusBgIbAwUJA8Hp  
13 ugULCQgHAgnYVCgkICwIEFgIDAQIeAQIXgAAKCRDs3Q/S1BEEUP/9C/0b6aWQhTr7  
14 0Jgf68KnS8nTXLJeoi5S9+moP/GVvw1dsfLoHkJYXuIc/fne2Y1y4qjvEdSCtAIs  
15 rqReXnolyyqCWS2e70YsQ9Sgg0JG4o7r0VojKJNzuHDWQ944yhGk6zjC54qHba6+  
16 37F9erDy+xRQS9BSgEFF2C60Fe00i+vp0WipqYAc1VGaUxHNrVYn8Fu01sIRTIo7  
17 10LR1bUHVgZvDIRR11dyFbF8B7oxrZZe9eWQGURjXEVg07nh1V5UzekRv7qLsVyg  
18 sTV3mxodvxgw3KmrxFsFSKY9Cdru8vN9IvFJWQQj++rnzyyTUCUmxB9Y/L9wRx  
19 4+7DSpfV1e4bGOZKY+KQqipYypUX1AFMHeb2RKVvjK5DzMDq6CQs73jqq/v1Ydp4  
20 kNsucdZKEKn2eVjJIon750vE5cus0l0jZuR93+w5Cmf4q6DhpXSUT1AP016R1eue  
21 8mPTmCra9dEmzAmSnLEPSPXN5tzdxzDqHvvIDtj8M3l2iRyD6v1NeZa5AY0EYAus|  
22 BgEMAN4mK70jRDxwnjQd8AJS133VncYT43gehVmKaZOAFaxoZtmR6oJbiTwj+b1  
23 fV1I1XP51I80JBZ2YPEvLE8huqeFQjEIG4Suk3p/HUaIXaVhiIjFRzoxoIZGM1Mh  
24 XKRsqc3zd3LLg1Gir7smKSMv8qI1gnZZr0TcpwX90h90d/MqtCRyg5Rt8FibtKFI  
25 Y0j4pvjGsZEvwurHqS0Jxxzdd+j0sfgTewFAy1/93scmmCg7mqUQV79DbaDL4JZv  
26 vCd3rxX08JyMwdRcOveR3JJERsLN9v8xPv/dsJhS+yaBH+F2vXQEldXE0azwdJhj  
27 ddXCVNzmTCIZ85S/1XWLLUa6I1WCcf4s8ffDv9Z3F21Hw64aWEA+H3v+tv59pxv  
28 I63/4u2T2o4pu/M489R+pV/9W7jQydeE6kCyRDG1doTVJBi1WzhtEqXZ3ssSZXpb  
29 bGuUcDLbqgCLLpk62Es9QQzKVTXF3yk00FWaeqE2aLCjVbpi1AZEQ7lmxtco/M+D  
30 VzJSmwARAQABiQG8BBgBCgAmFiEEplGFJzv4jpEmsPTF7N0P0pQRBFACAmALrAYC  
31 GwwFCQPB6boACgkQ7N0P0pQRBFBC3wv/VhJMzYmW6fKraBSL4iDF6oiGEhcd6xT4
```

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 aa ah ac af a7 1h a2 a5 aa c1 a9 ha a5
```

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

Google

sakurasnowangelaiko

X | 🎤 | 📸 | 🔍

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](https://twitter.com/SakuraLoverAiko) :

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.

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.

Aiko @SakuraLoverAiko · 30 ene. 2021

Silly me, I forgot to introduce myself!

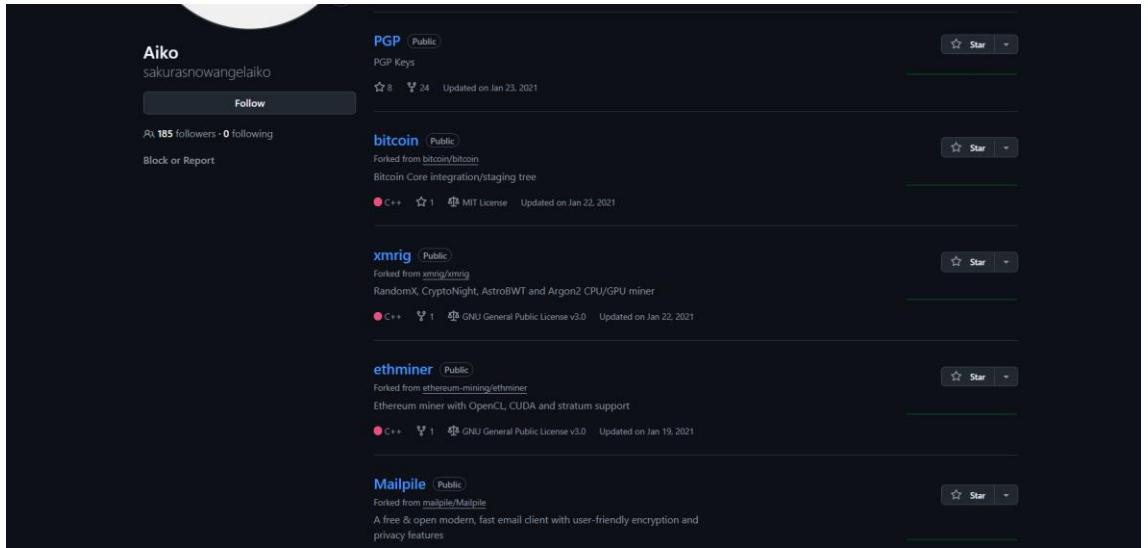
Hi there! I'm [@AikoAbe3!](#)

Reply Retweet Like 17 Quote Bookmarks Share

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

Task 4 - UNVEIL

1.

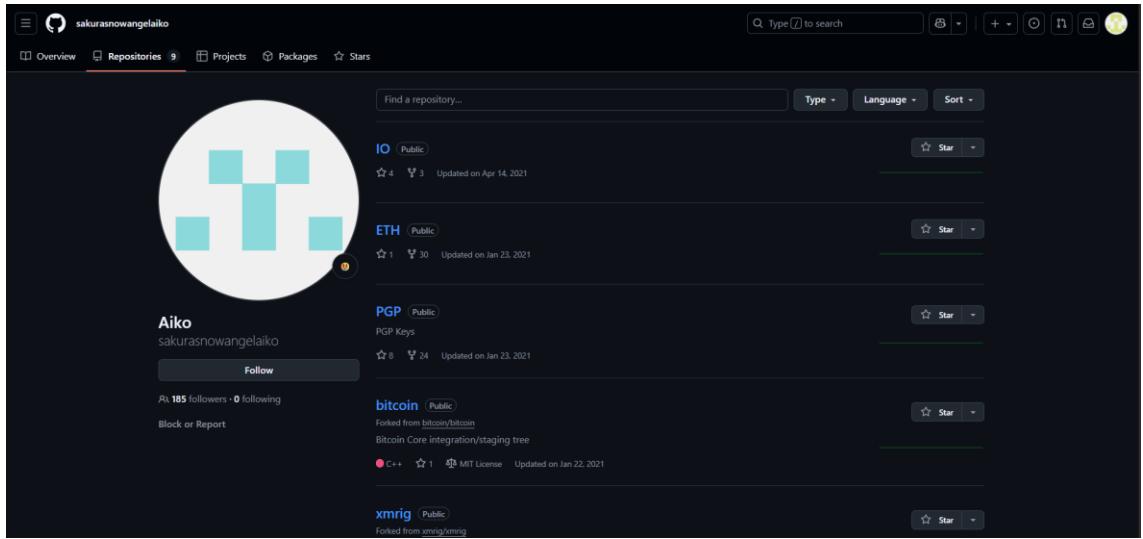


A screenshot of a GitHub user profile for 'Aiko' (sakurasnowangelaiko). The profile shows 185 followers and 0 following. The user has forked several repositories:

- PGP** [Public] - PGP Keys, updated on Jan 23, 2021. Stars: 8, Forks: 24.
- bitcoin** [Public] - Forked from bitcoin/bitcoin, Bitcoin Core integration/staging tree. Stars: 1, Forks: 1, MIT License, Updated on Jan 22, 2021.
- xmrig** [Public] - Forked from xmrig/xmrig, RandomX, CryptoNight, AstroBlitz and Argon2 CPU/GPU miner. Stars: 1, Forks: 1, GNU General Public License v3.0, Updated on Jan 22, 2021.
- ethminer** [Public] - Forked from ethereum-mining/ethminer, Ethereum miner with OpenCL, CUDA and stratum support. Stars: 1, Forks: 1, GNU General Public License v3.0, Updated on Jan 19, 2021.
- Mailpile** [Public] - Forked from mailpile/Mailpile, A free & open modern, fast email client with user-friendly encryption and privacy features. Stars: 1, Forks: 1, Updated on Jan 19, 2021.

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



A screenshot of a GitHub user profile for 'Aiko' (sakurasnowangelaiko). The profile shows 185 followers and 0 following. The user has forked several repositories:

- IO** [Public] - updated on Apr 14, 2021. Stars: 4, Forks: 3.
- ETH** [Public] - updated on Jan 23, 2021. Stars: 1, Forks: 30.
- PGP** [Public] - PGP Keys, updated on Jan 23, 2021. Stars: 8, Forks: 24.
- bitcoin** [Public] - Forked from bitcoin/bitcoin, Bitcoin Core integration/staging tree. Stars: 1, Forks: 1, MIT License, Updated on Jan 22, 2021.
- xmrig** [Public] - Forked from xmrig/xmrig. Stars: 1, Forks: 1.

Hay que acceder al apartado que dice 2 Commits.

The screenshot shows a GitHub repository named 'ETH'. It has 1 branch and 0 tags. There are two commits:

- sakurasnowangelaiko** Update miningscript · d507757 · 5 years ago · 2 Commits
- sakurasnowangelaiko** miningscript · 5 years ago

Después una vez lo has presionado te sale esto:

Commits on Jan 23, 2021

Update miningscript
sakurasnowangelaiko authored on Jan 23, 2021
12 comments, Verified, d507757

Create miningscript
sakurasnowangelaiko authored on Jan 23, 2021
58 comments, Verified, 5d83f7b

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.

miningscript

...	@@ -1 +1 @@
1	- stratum://0xa102397dbeefBeFD8cD2F73A89122fCdB53abB6ef.Aiko:pswd@eu1.ethermine.org:4444
1	+ stratum://ethwallet.workerid:password@miningpool:port

Aquí tienes la solución de la dirección de la cartera del atacante que es 0xa102397dbeefBeFD8cD2F73A89122fCdB53abB6ef, 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

For 0xa102397dbeeBeFD8cD2F73A89122fCdB53abB6ef

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	▼ ▾
①	Transaction Hash	Method ⓘ	Block	Age	From	To	Amount	Txn Fee					
②	0x9e8561bcd8...	Transfer	23183604	47 days ago	0x0Db9f16...3CdD2c157	IN 0xa102397d...B53abB6ef	0.000232149 ETH	0.00004581					
③	0xe8d1c31e9b...	Transfer	20149437	471 days ago	0xa102397d...B53abB6ef	OUT 0x2264783b...Af1b1F82B	0.132432361 ETH	0.000084					
④	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.

Aiko
@SakuraLoverAiko
Se unió el enero de 2021
1 Siguiendo 172 Seguidores

Posts Respuestas Multimedia

Aiko @SakuraLoverAiko · 24 ene. 2021
Checking out some last minute cherry blossoms before heading home!

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

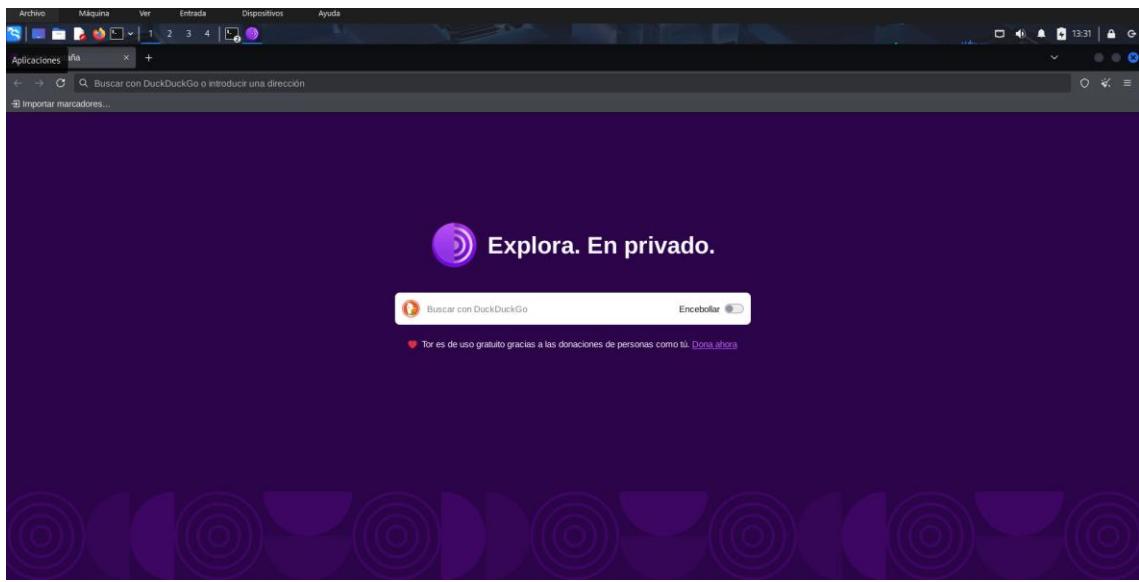
5.2

```
(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 ~]# ls
tor-browser tor-browser-linux-x86_64-14.5.7.tar.xz

[root@kali ~]# ./start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach' ...
[root@kali ~]# 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://zerobinftagjpeeebbvvyzjcqyjpmjvynj5qlexwyxe7l3vqejxnqv5qd.onion/?cd484d8f2fd1cc00#jbAhOJplt4+o6K+3YT2P4dlLoy+kCWX25B+9Xa/qC0o=>

A screenshot of the ZeroBin.net website. The header features the site's logo and the tagline 'Because ignorance is bliss'. It provides links to 'Tor OnionSpace' and 'Onion V3'. The main content area displays a list of pasted data entries. One entry is highlighted, showing a long string of characters: 9a5ce136a98a60bb8a21643ce8c15a74. Below this, there are several other entries with names like 'School WiFi Computer Lab', 'McDonalds G...', 'School WiFi', 'City Free WiFi', and 'Home WiFi'. Each entry has a 'Clone' button and a 'Raw text' link.

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.

The screenshot shows a Google search interface. The search bar contains the query "que monumento es". Below the search bar, there are tabs for "Todo", "Productos", "Coincidencias visuales", "Acerca de esta imagen", and "Comentarios". A blue diamond icon indicates that the result is "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 encyclopédie libre

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

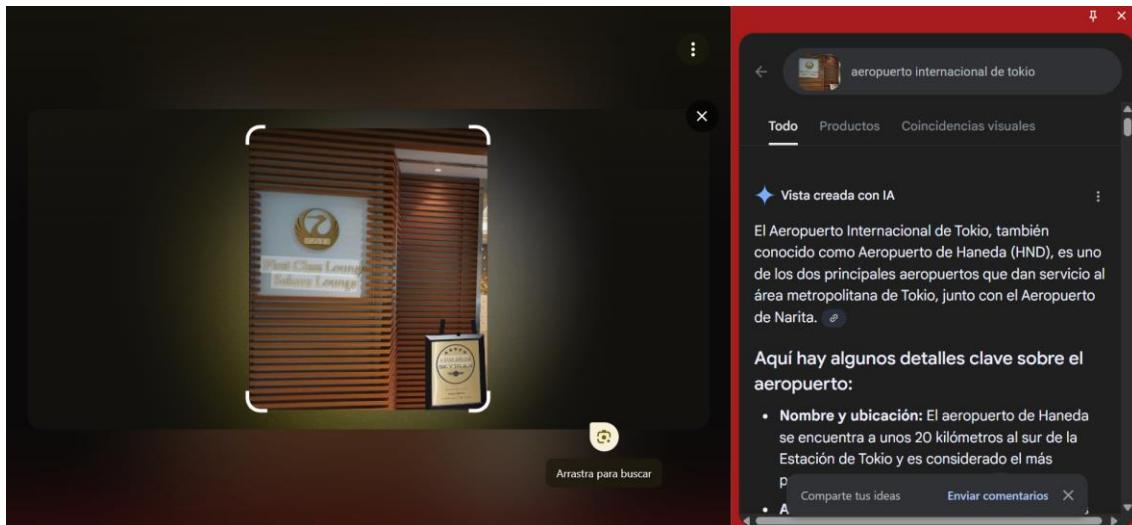
Wikipedia

Guía completa de monumentos nacionales en Washington D.C.

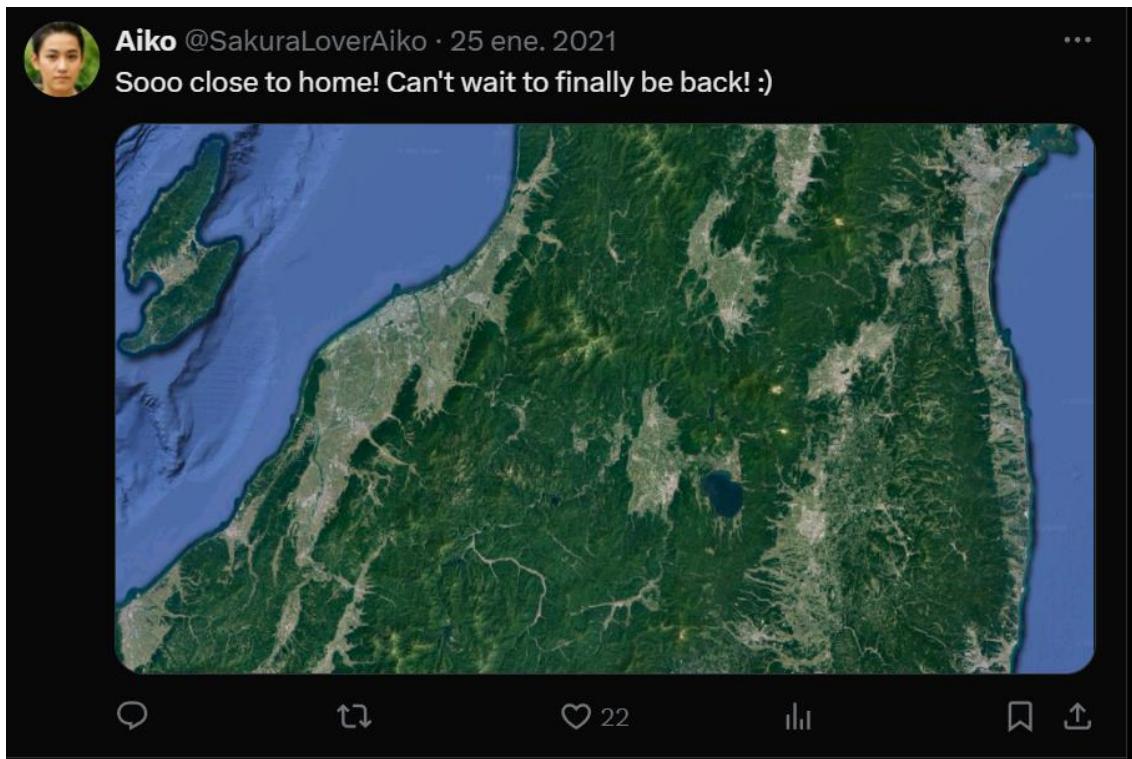
Traducido — Monumento a Washington Una estructura de renombre mundial, este...

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

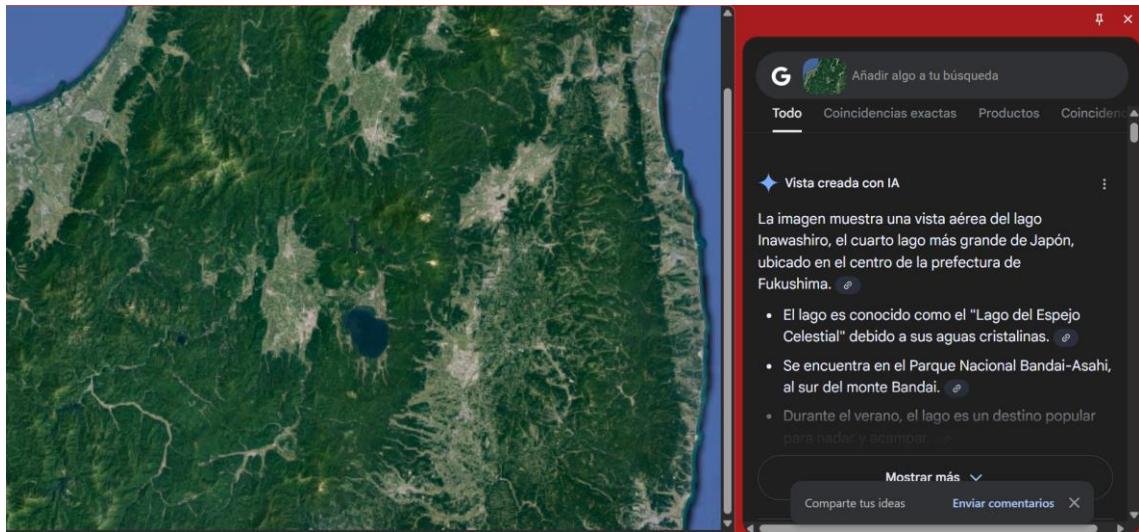
Para la respuesta del segundo, he metido la imagen en Google lean y me ha dicho directamente que aeropuerto era y buscando el código de 3 dígitos me ha salido que era NHD.



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.

Network	Device	MAC Address
School WiFi Computer Lab	STRI Device	67gfFeltt44221#
McDonalds	Buffalo-G-1800-5	Macdonalds29200
School WiFi	Visitor	679ree123
City Free WiFi	#HIROSAKI_Free_Wi-Fi	R_Free0341
Home WiFi	DEIF-G	Fsef32410#

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.