CTF - OSINT

SOCIAL ENGINEERING VILLAGE - EKOPARTY 2025

Laura Cordoba

Especialista en ciberseguridad.

Marcos Pablo Russo

Administrador GNU/Linux, Infraestructura, Auditor, SOC, Autodidacta, ex-profesor de la UTNFra Arquitectura y Sistemas Operativos. Creador de la Distribución de Informática Forense CondorLinux y luego Huemul (Centrux).

Ciberseguridad en Mundoe.

Informática Forense en CPCI
Dictado de clase de OSINT en HackAcademy (Ekoparty)

Grupo: xsec (https://xsec.sh/)

https://www.linkedin.com/in/marcos-pablo-russo-57a44514/

Osvaldo Falabella

Consultor IT con más de 15 años en consultorías para el estado, 10 años en el sector privado y más de 15 años de experiencia docencia universitaria y 8 años incursionando y aprendiendo en el área de la ciberseguridad en Ingeniería Social con la utilización de fuentes abiertas, en el ámbito del grupo GIIS (Grupo de Investigación en Ingeniería Social) LINSI UTN FRLP (https://www.linsi.edu.ar/giis/index.html).

CTF OSINT

GIT

https://github.com/marcospr1974/CTF-OSINT

git clone https://github.com/marcospr1974/CTF-OSINT.git

Herramientas

Google Earth:
https://maps.google.es/intl/es_es/earth/download/gep/agree.html

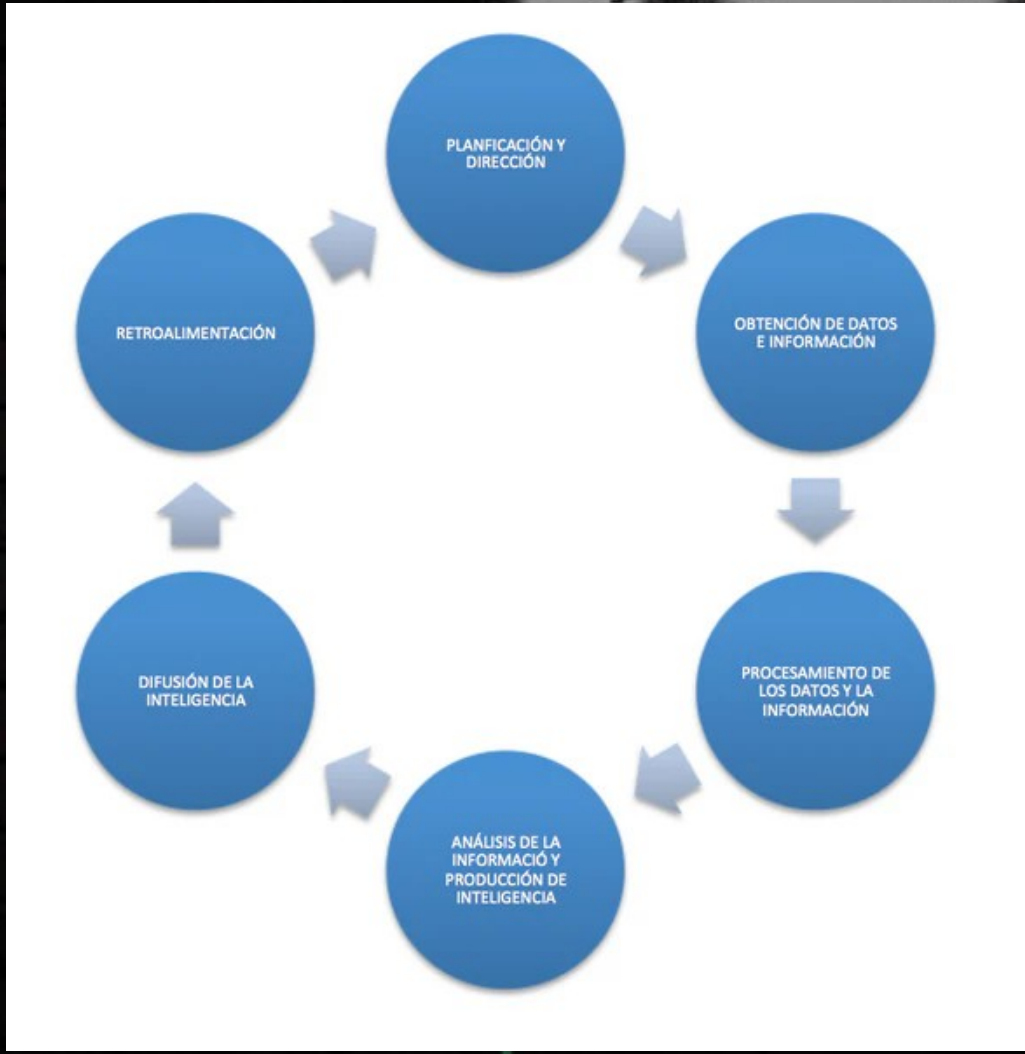
¿Qué es **Osint ?**

OSINT se refiere a la obtención de información desde fuentes abiertas (públicamente accesibles sin requerir autorización previa) la cual será analizada pudiendo luego utilizarse con distintos objetivos como por ejemplo:

- Investigaciones judiciales (injurias, amenazas, extorsiones, etc).
- Seguridad pública
- Monitoreo de amenazas
- Monitoreo de eventos públicos
- Investigaciones corporativas
- Inteligencia competitiva

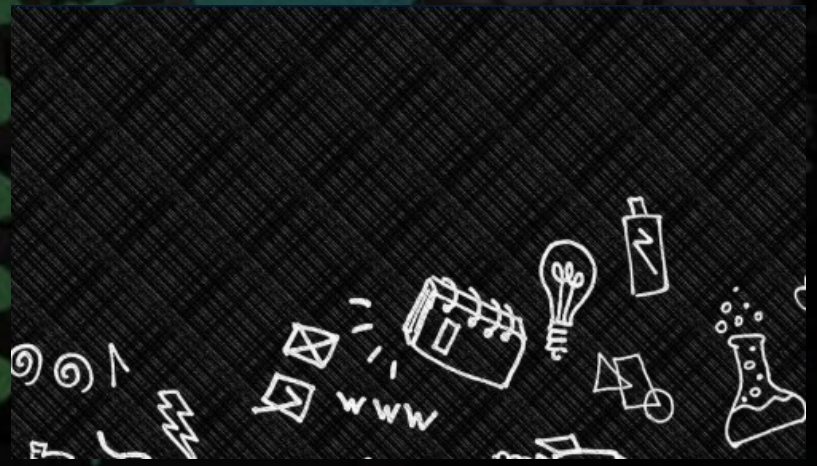
Fuentes de Inteligencia

- Inteligencia Humana (HUMINT).
- Inteligencia de Imágenes (IMINT).
- Inteligencia de Señales (SIGNT).
- Inteligencia de Redes Sociales (SOCMINT)
- Inteligencia de Reconocimiento y Signatura (MASINT).
- Inteligencia de Fuentes Abiertas (OSINT).


PLANFICACIÓN Y DIRECCIÓN
OBTENCIÓN DE DATOS E INFORMACIÓN
PROCESAMIENTO DE LOS DATOS Y LA INFORMACIÓN
ANÁLISIS DE LA INFORMACIÓ Y PRODUCCIÓN DE INTELIGENCIA
DIFUSIÓN DE LA INTELIGENCIA
RETROALIMENTACIÓN

Fuentes de Inteligencia

En la investigación se tomará un individuo como objetivo a modo de ejemplo con el fin de explicar las etapas de la investigación. Como también se hará uso de las información pública expuesta utilizando OSINT



CTF 01

Translated from Arabic by Google

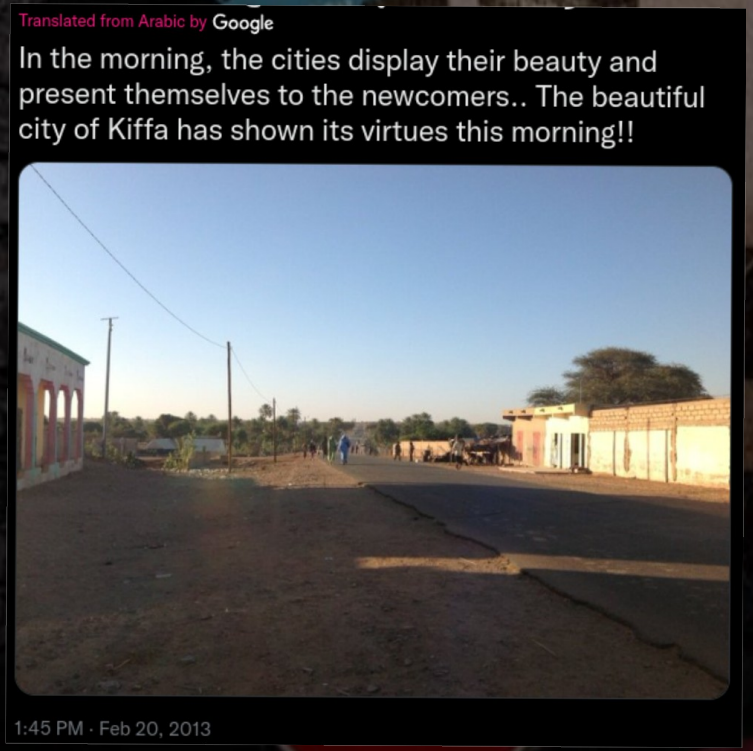
In the morning, the cities display their beauty and present themselves to the newcomers.. The beautiful city of Kiffa has shown its virtues this morning!!

1:45 PM · Feb 20, 2013

DESCRIPCIÓN - CTF 01

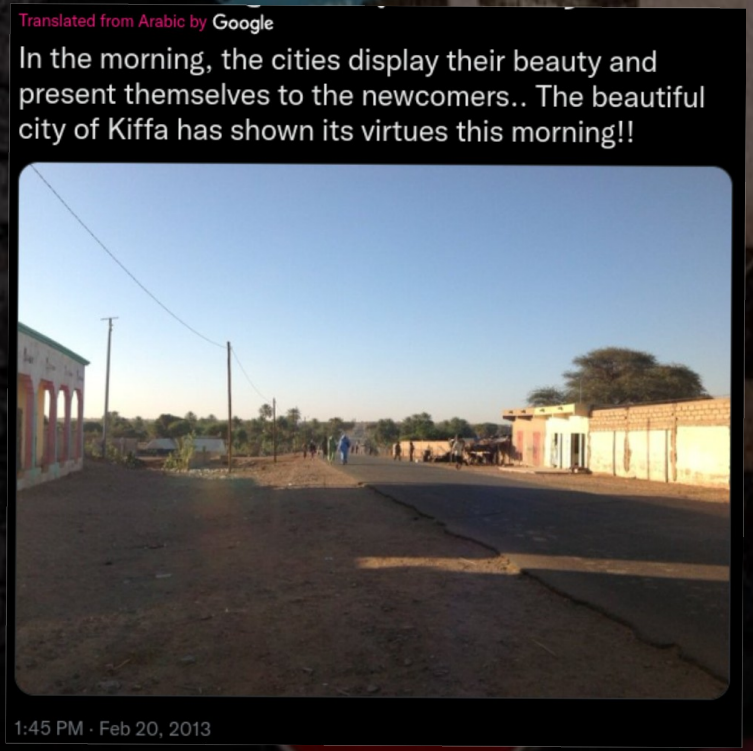
A continuación, puede ver una captura de pantalla de un tuit con una foto. Contiene toda la información necesaria para encontrar la ubicación exacta.

Por favor, indique las coordenadas de donde se tomó la foto.



OBSERVACIONES - CTF 01

- Vemos una carretera asfaltada.
- Construcción del lado derecho.
- Otra construcción del lado izquierdo.
- Al final de la carretera se ve mucha vegetación.
- En el Twitter indica la ciudad de **Kiffa**.
- También aparece una fecha **1:45 PM – Feb 20, 2013**.
- Idioma **Árabe**.

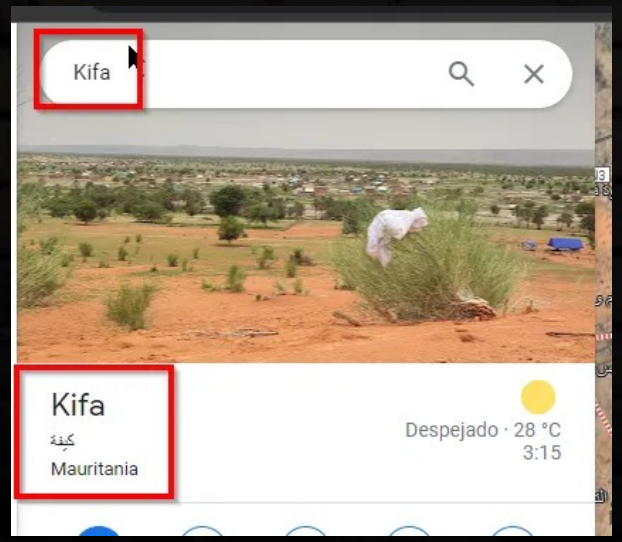


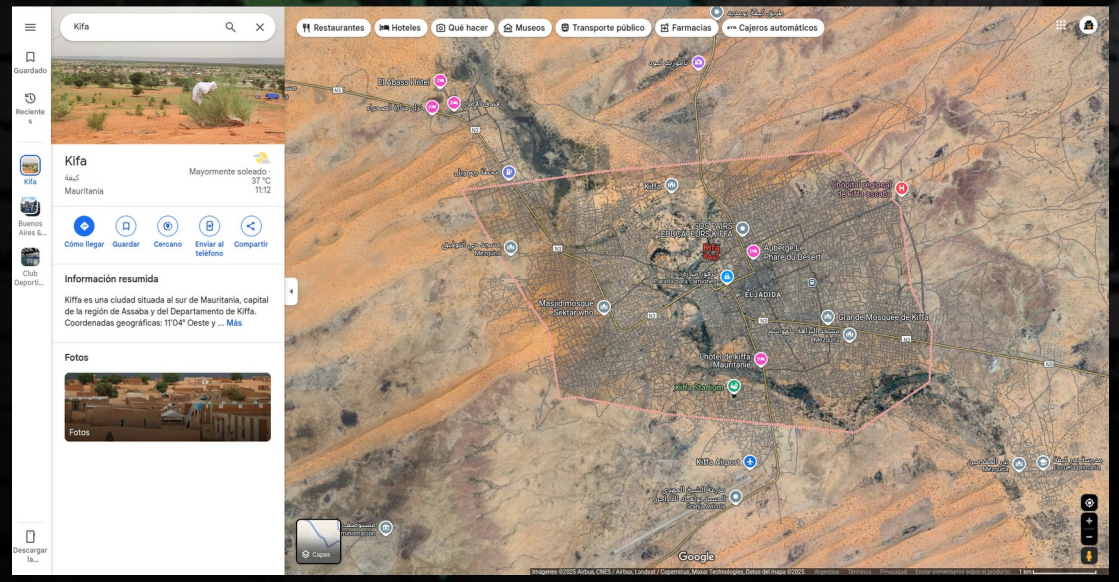
IDEAS - CTF 01

- Búscar la imagén en google image.
- Verificar si contiene metadatos con **FotoForensics** o **exiftools**.
- Buscar en **Google Maps** mediante el nombre de la ciudad **Kiffa** o en **Google Earth**.

SOLUCIÓN - CTF 01

- Buscar en **Google Maps** mediante el nombre de la ciudad **Kifa** y el primero que aparece es **Kifa Mauritania**, donde lo pondremos en visión satélite



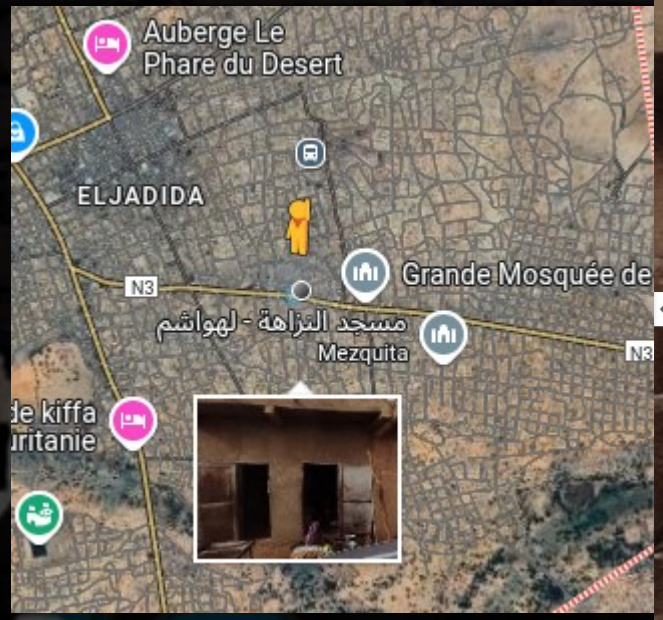


SOLUCIÓN - CTF 01

- Observamos que tenemos **N3** que es la carretera la cual se encuentra pavimentada, que se encuentra en color amarillo.

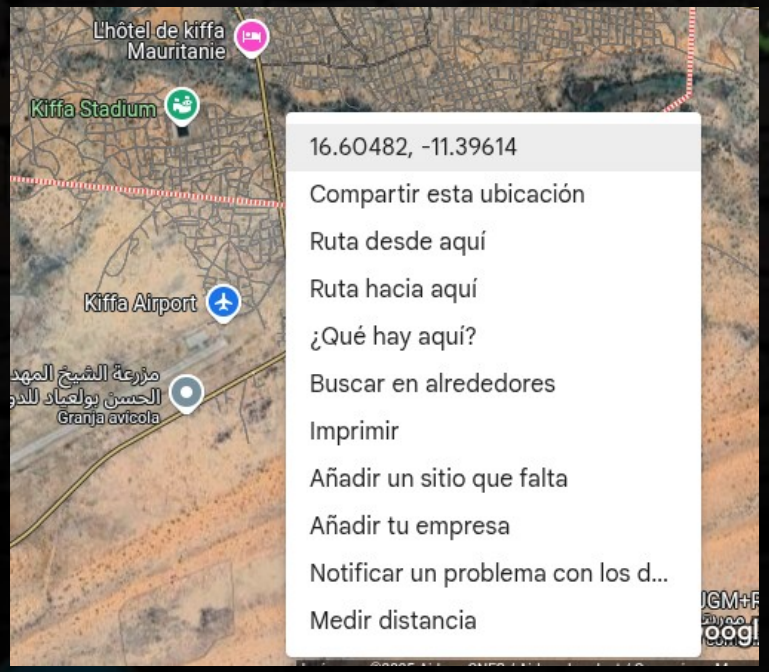
SOLUCIÓN - CTF 01

- Podemos observar que en el Twitter dice que fue en el año 2013, a la fecha veremos que no hay tanta vegetación y más edificación.



SOLUCIÓN - CTF 01

- Salimos y nos situamos donde vemos que hay vegetación y con el botón izquierdo nos aparece un submenú donde copiamos las coordenadas y lo llevamos a **Google Earth**.



SOLUCIÓN - CTF 01

- Empezamos a recorres hasta encontrar donde fue sacada la foto. Como observamos luego de muchos años cambia completamente.

CTF 02

DESCRIPCIÓN - CTF 02

La foto se compartió en redes sociales. Muestra claramente una estación de tren.

Responder las siguientes preguntas

a) ¿ Cómo se llama la estación de tren que se ve en la foto ?

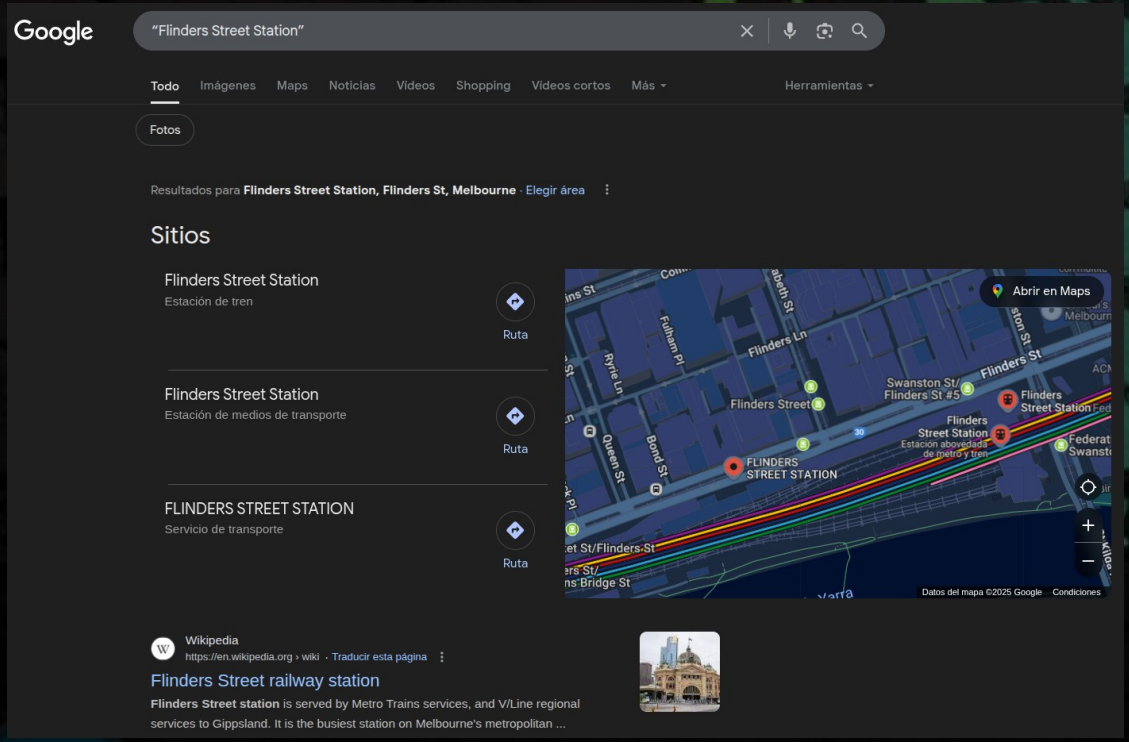
b) ¿ Cuál es el nombre y la altura de la estructura más alta que se ve en la foto ?

IDEAS - CTF 02

- Ver bién la imaǵen (agrandarla).
- Búscar la imagén en google image.
- Verificar si contiene metadatos con **FotoForensics** o **exiftools**.
- Buscar en **Google Maps** mediante el nombre de la ciudad **Kiffa** o en **Google Earth**.

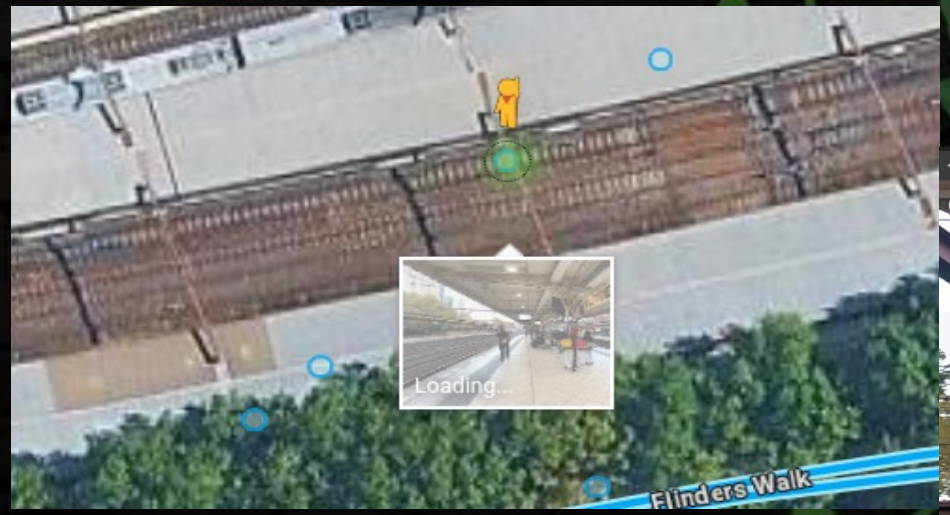
SOLUCIÓN - CTF 02

- Búscamos en Google “Flinders Street Station”)



SOLUCIÓN - CTF 02

- Búscamos en Google “Flinders Street Station”) y de ahí abrimos Google Maps.



google.com/maps/place/FLINDERS+STREET+STATION/@-37.8217823,144.9653492,272m/data=!3m1!1e3!4m15!1m8!3m7!1s0x6ad6437076a71161:0x87fa8...

FLINDERS STREET STATION

Guardado

Recientes

FLINDERS STREE...

Buenos Aires &...

Kifa

Club Deporti...

Descargar la...

FLINDERS STREET STATION

4,6 ★★★★★ (183)

Servicio de transporte · ♿

Vista general | Reseñas | Información

Cómo llegar | Guardar | Cercano | Enviar al teléfono | Compartir

Flinders St, Melbourne VIC 3000, Australia

5XJ7+HG Ciudad de Melbourne, Victori Australia

Copiar Plus Code

esta empresa

Tu actividad de Google Maps

Añadir una etiqueta

Sugerir un cambio

Añadir la información que falta

Añadir número de teléfono del sitio

Restaurantes | Hoteles | Qué hacer | Transporte público | Aparcamientos | Farmacias | Cajeros automáticos

Southbank Apartments (45) ...trellas

Southgate Ave

Southgate Express
Tienda de alimentación

Southgate Pharmacy

IBM Australia
JB Hi-Fi
Corporate Office
Google Pixel
9 Pro Range

Mercure Melbourne Southbank
3.9 (496)
Hotel de 4 estrellas

Riverside Quay

Gainsville Furniture
Entertainment
Cabinets – Gainsvil...

Southgate Ave

City Road Public Purposes Reserve

Fanning St

Oaks Melbourne Southbank Suites
4.1 (638)
Hotel de 4 estrellas

Fawkner St

Cook Street Reserve

FOCUS Apartments by Central Equity

Adina Apartment Hotel Melbourne Southbank
Hotel in Melbourne

Kavanagh St

Mapa | Relieve | Tráfico | Transporte público | En bicicleta | Más

Google

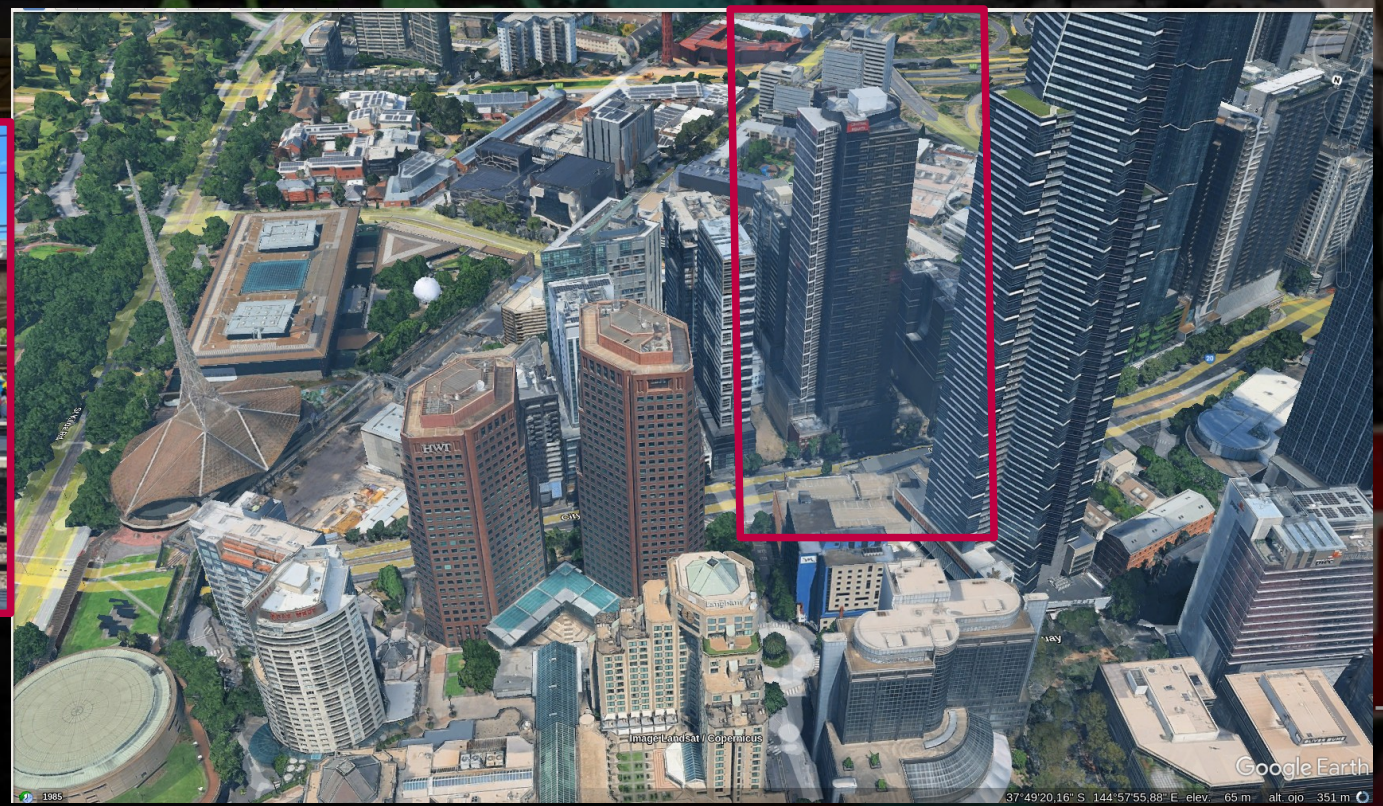
Imágenes ©2025 Airbus, Maxar Technologies, Vexcel Imaging US, Inc. Datos del mapa ©2025 Google Argentina Términos Privacidad Enviar comentarios sobre el producto 20 m

SOLUCIÓN - CTF 02

- Si nos acercamos al edificio más alto podemos observar que es de “IBM”.

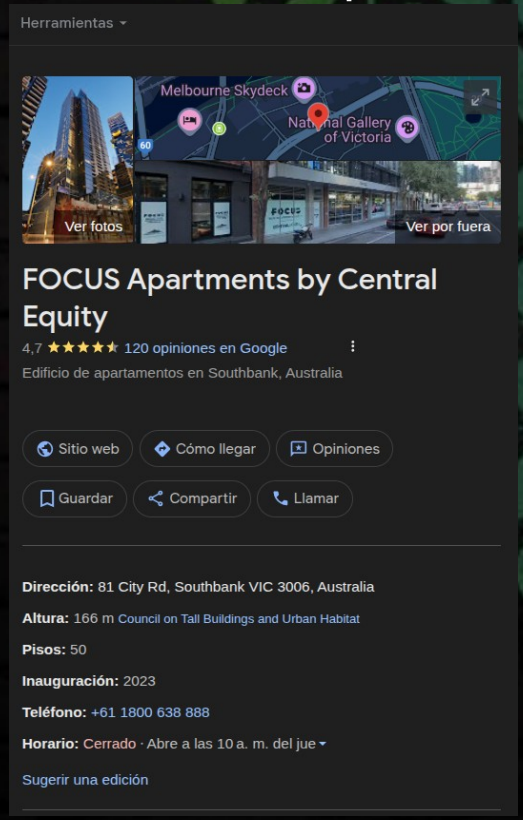
SOLUCIÓN - CTF 02

- Vamos a Google Earth y buscamos “FLINDERS STREET STATION”



SOLUCIÓN - CTF 02

- Buscamos en Google “altura focus apartaments by central equity australia”
- Altura 166 metros.



SOLUCIÓN - CTF 02

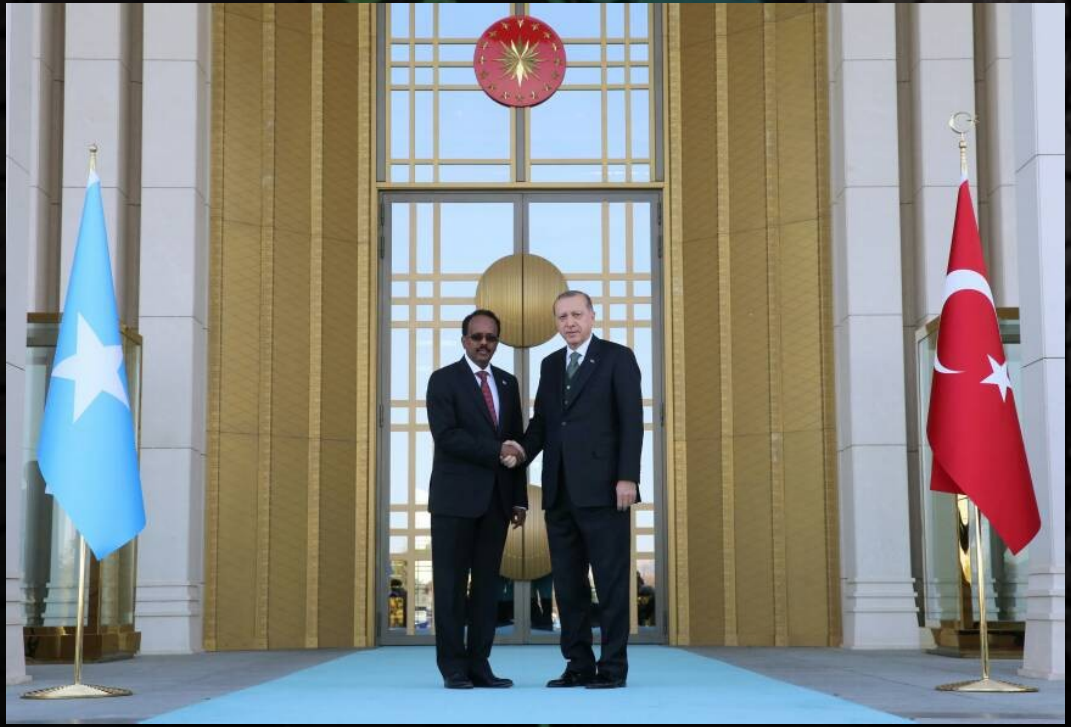
- a) ¿ Cómo se llama la estación de tren que se ve en la foto ?

  “Flinders Street”

- b) ¿ Cuál es el nombre y la altura de la estructura más alta que se ve en la foto ?

  Focus Apartaments By Central Equity - 166 metros

CTF 03



DESCRIPCIÓN - CTF 03

En abril de 2017, Mohamed Abdullahi Farmaajo, entonces presidente de Somalia, visitó Turquía. Una agencia de noticias publicó una foto donde se le ve estrechando la mano a Recep Tayyip Erdoğan, presidente del país. El artículo no reveló dónde se tomó la foto.

Hay que averiguar el nombre y las coordenadas del lugar que se ve a continuación.

IDEAS - CTF 03

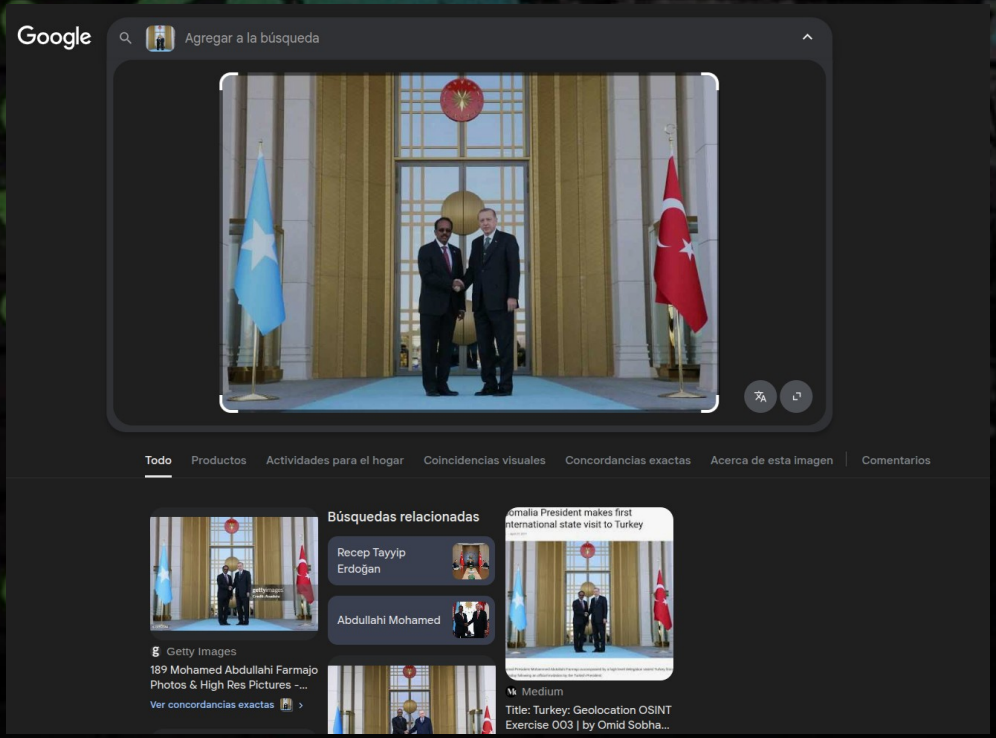
- Ver bién la imaǵen (agrandarla).
- Búscar la imagén en google image.
- Buscar en **Google Maps** y **Google Earth**.

OBSERVACIONES - CTF 03

- El presidente de Somalia, visitó Turquía.
- El presidente de Somalia, se reúne con el presidente turco Recep Tayyip Erdoğan.
- Banderas de ambos países.
- Un edificio con pilares blancos y plateados, una gran puerta dorada con 3 diseños circulares redondos (1 rojo,2 dorados).

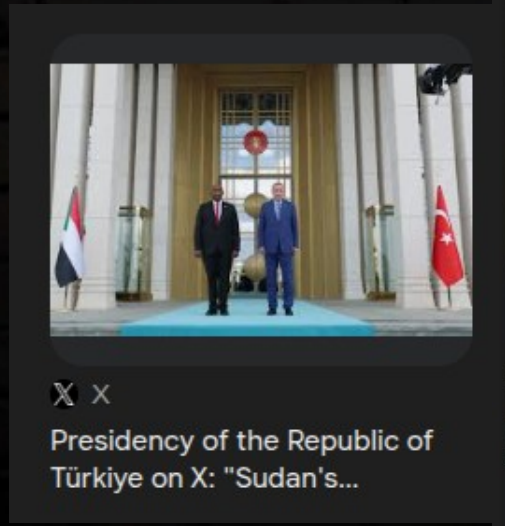
SOLUCIÓN - CTF 03

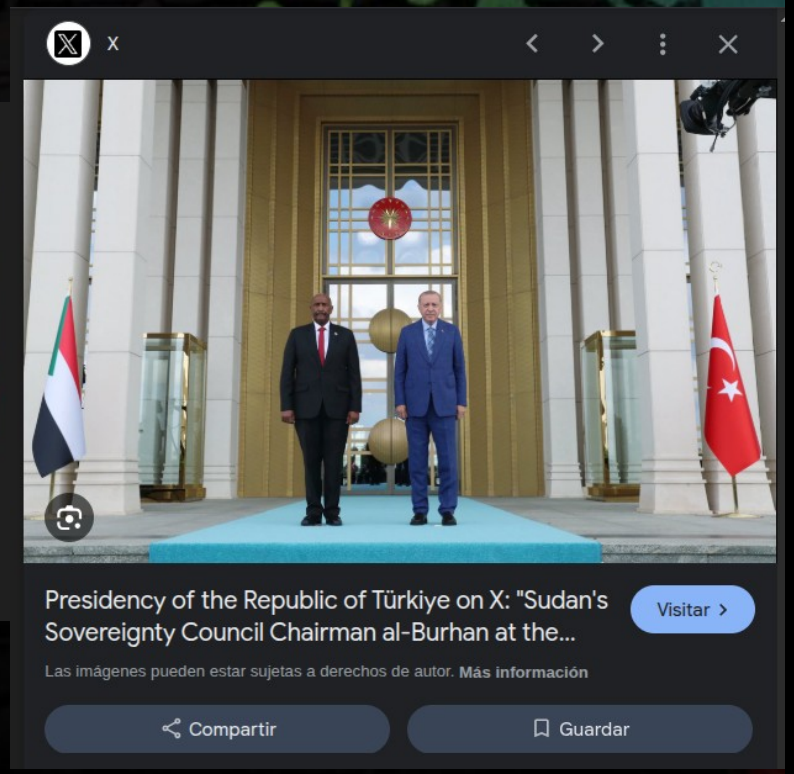
- Buscamos en Google Image.

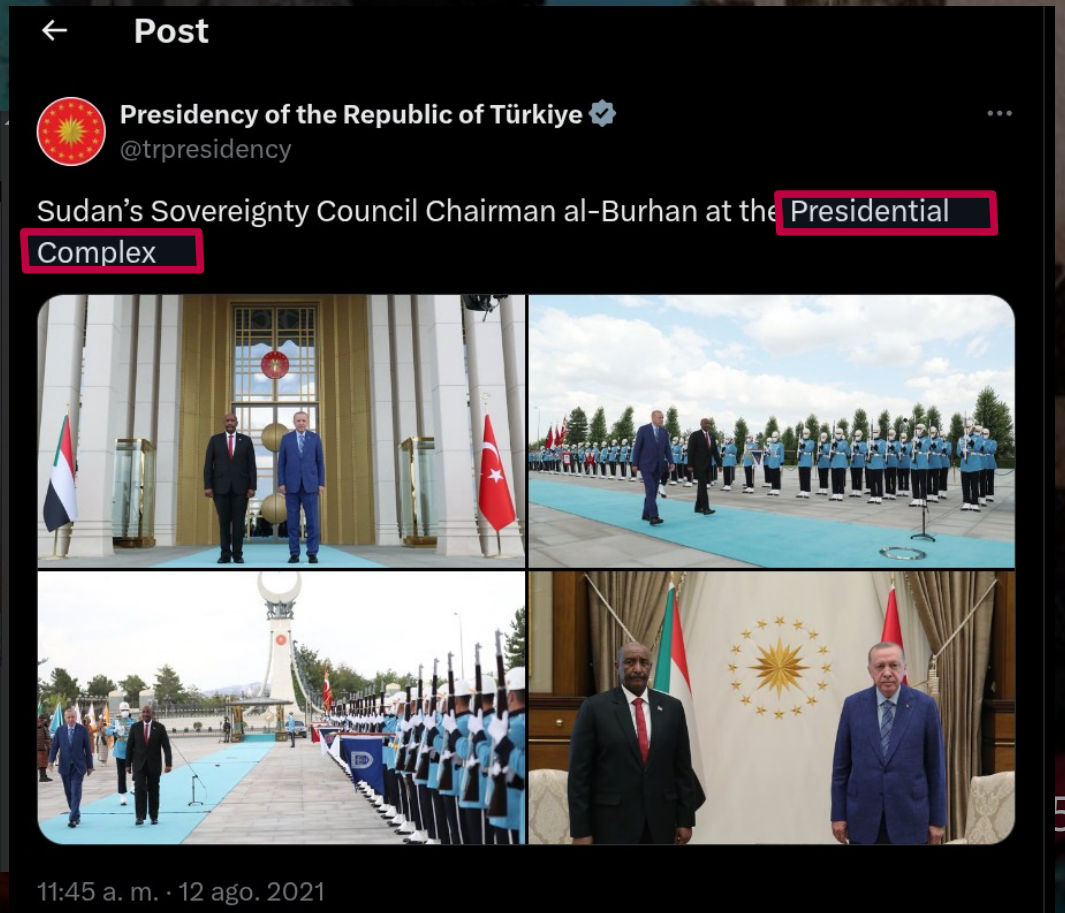


SOLUCIÓN - CTF 03

- Nos fijamos en las páginas de **X (ex twitter)**

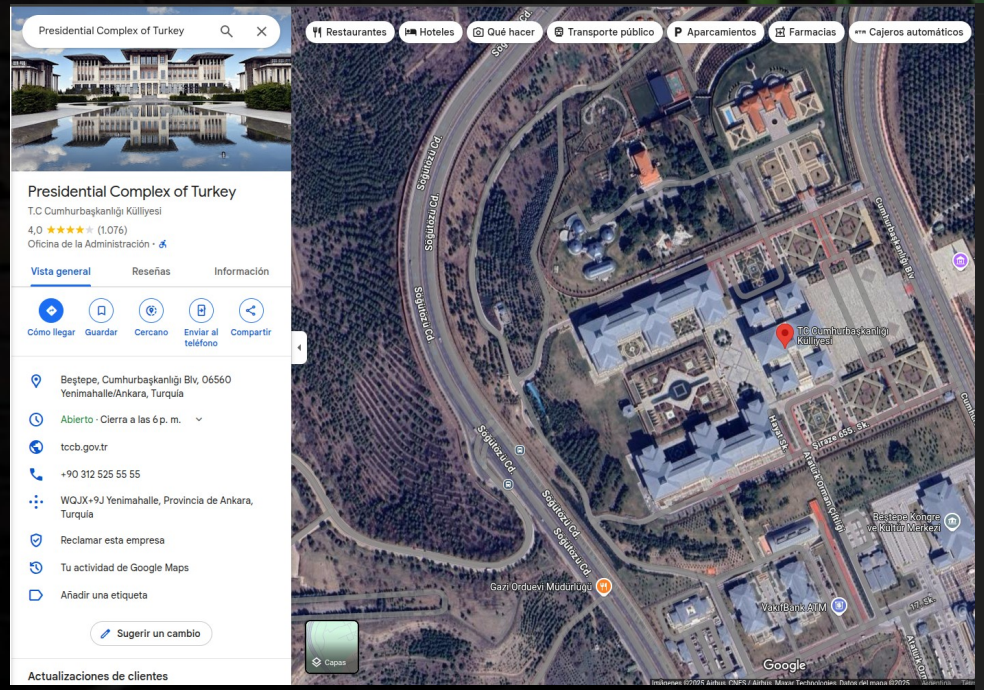


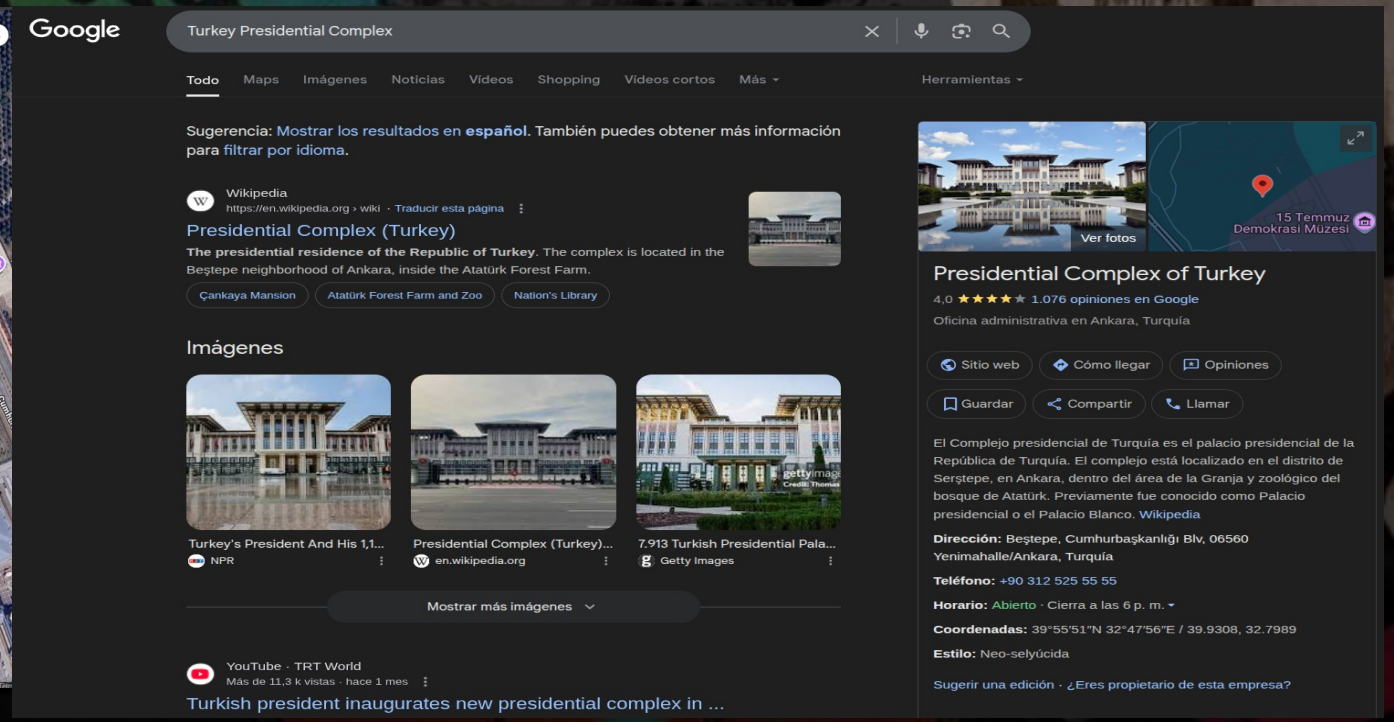




SOLUCIÓN - CTF 03

- Buscamos en Goolge Maps – **Turkey Preseidental Complex**.

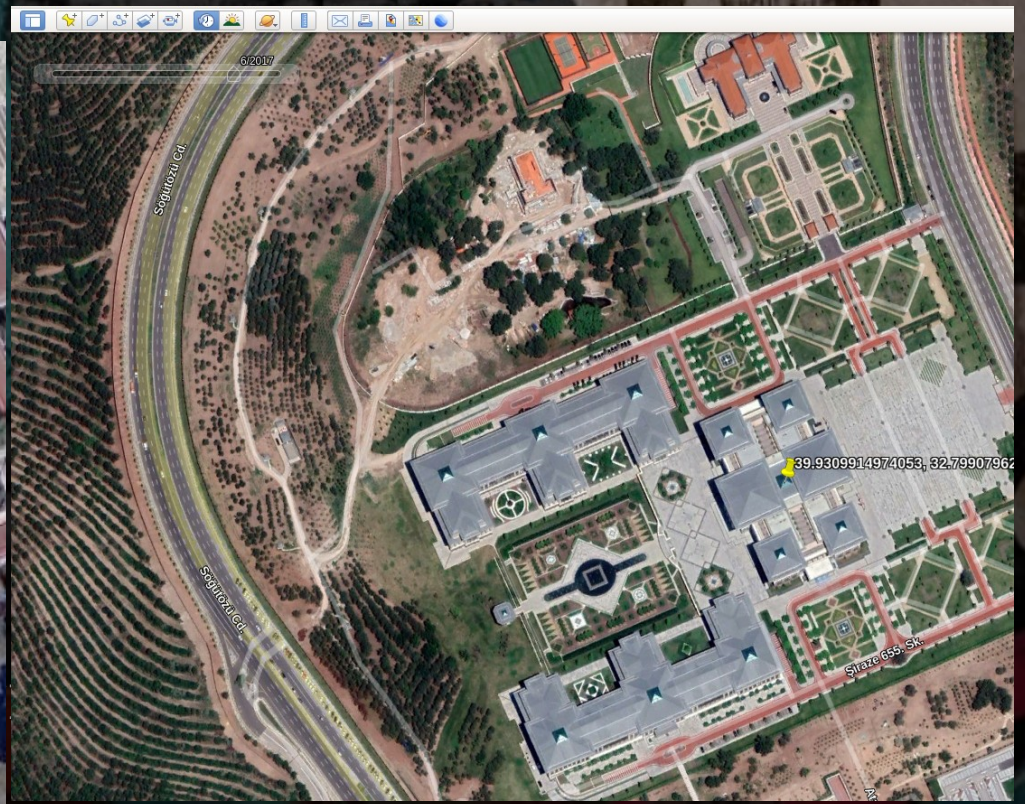




Buscamos en Goolge – **Turkey Preseidental Complex** y vamos a imágenes. Para verificar.

SOLUCIÓN - CTF 03

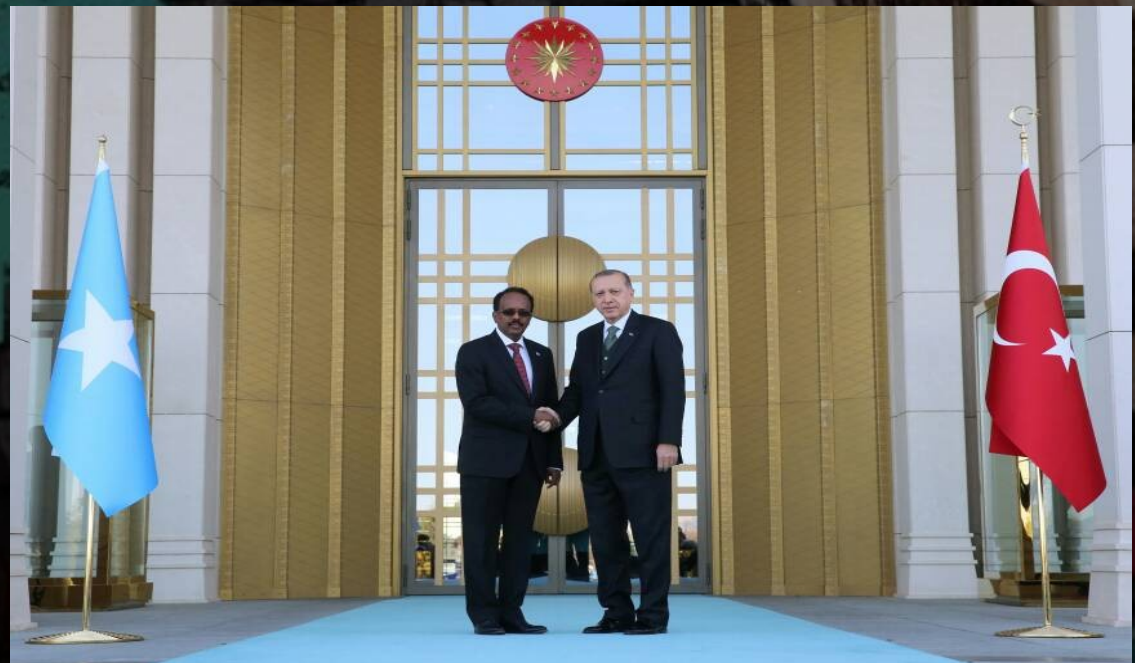
- Desde Goolge Maps copiamos las coordenadas para ponerlo en **Google Earth**



SOLUCIÓN - CTF 03

Hay que averiguar el nombre y las coordenadas del lugar que se ve a continuación.

- El nombre del es: **Preseidental Complex en Turkey**
- Las coordenadas son: **39.93097, 32.79907**



CTF 04

DESCRIPCIÓN - CTF 04

Esta es una foto de un complejo turístico ubicado en una isla:

a) ¿ Cuál es el nombre del complejo turístico ?

b) ¿ Cuáles son las coordenadas de la isla ?

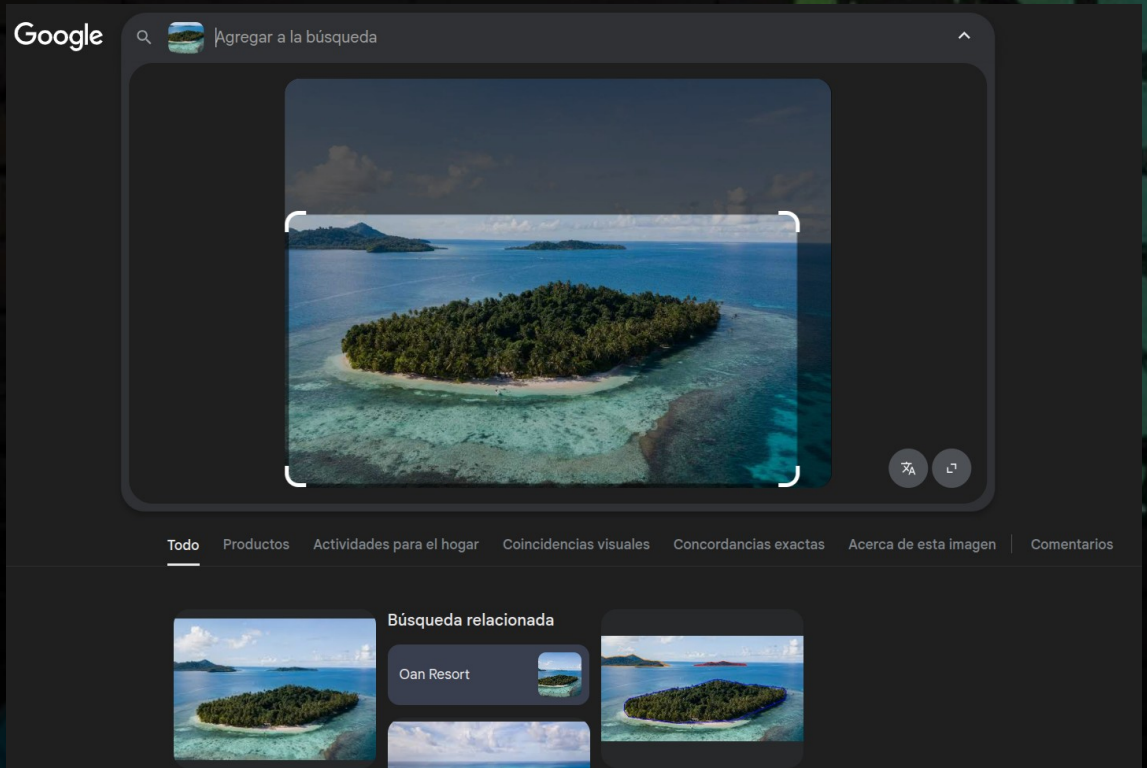
c) ¿ En qué dirección cardinal estaba orientada la cámara cuando se tomó la foto ?

IDEAS - CTF 04

- Búscar la imagén en **Google Image**.
- Buscar en **Google Maps** y **Google Earth**.

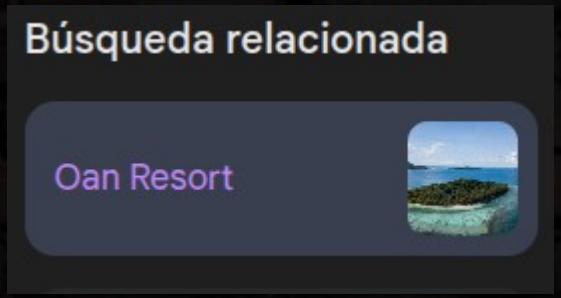
SOLUCIÓN - CTF 04

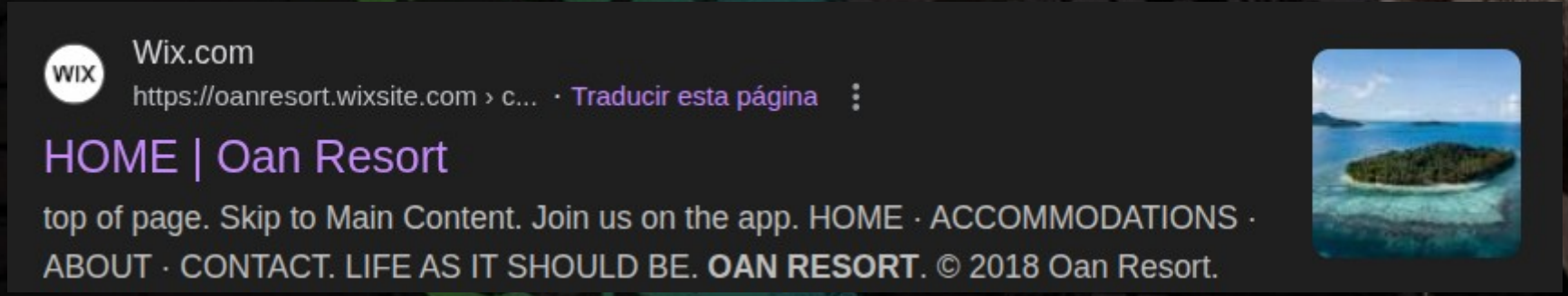
- Buscamos en Google Image.

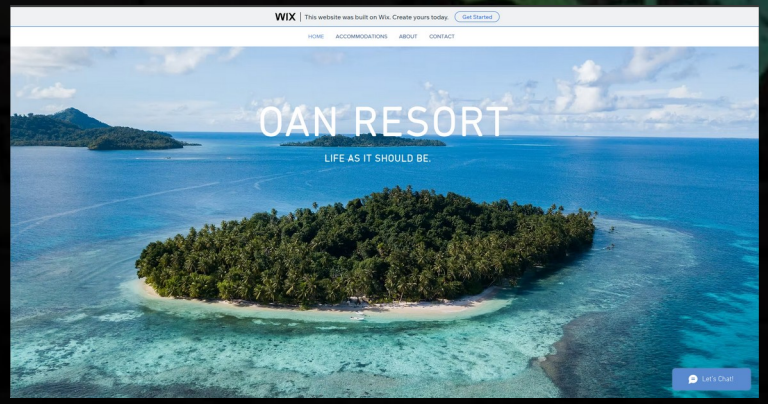


SOLUCIÓN - CTF 04

- Buscamos en Google Image.





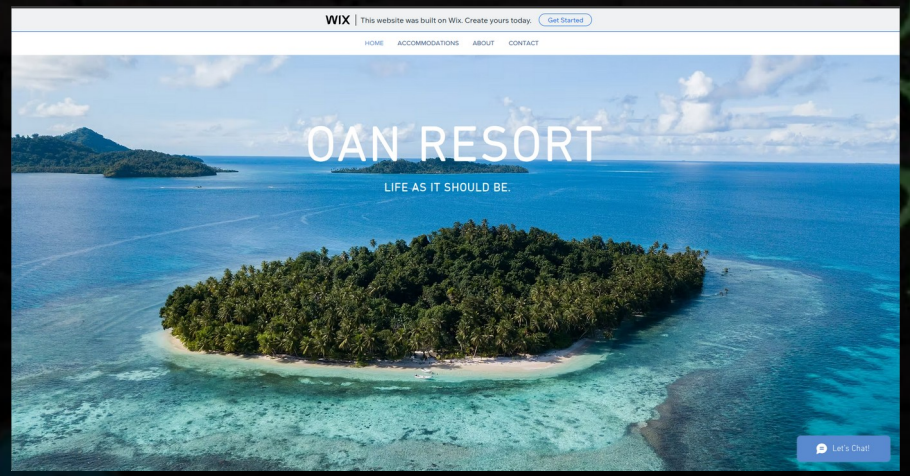


SOLUCIÓN - CTF 04

Esta es una foto de un complejo turístico ubicado en una isla:

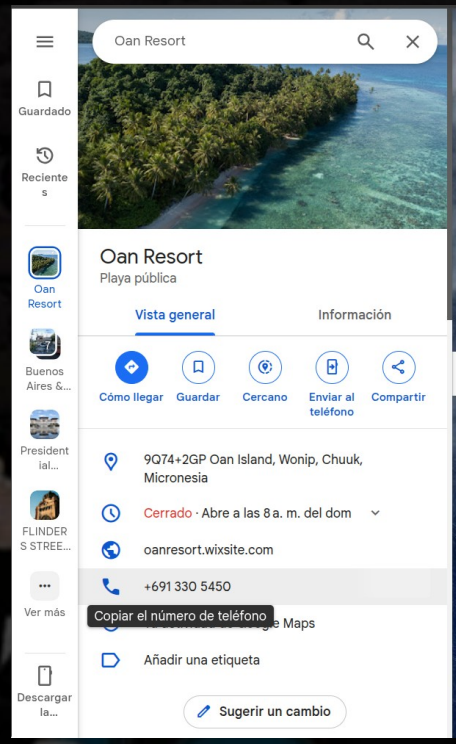
- a) ¿ Cuál es el nombre del complejo turístico ?

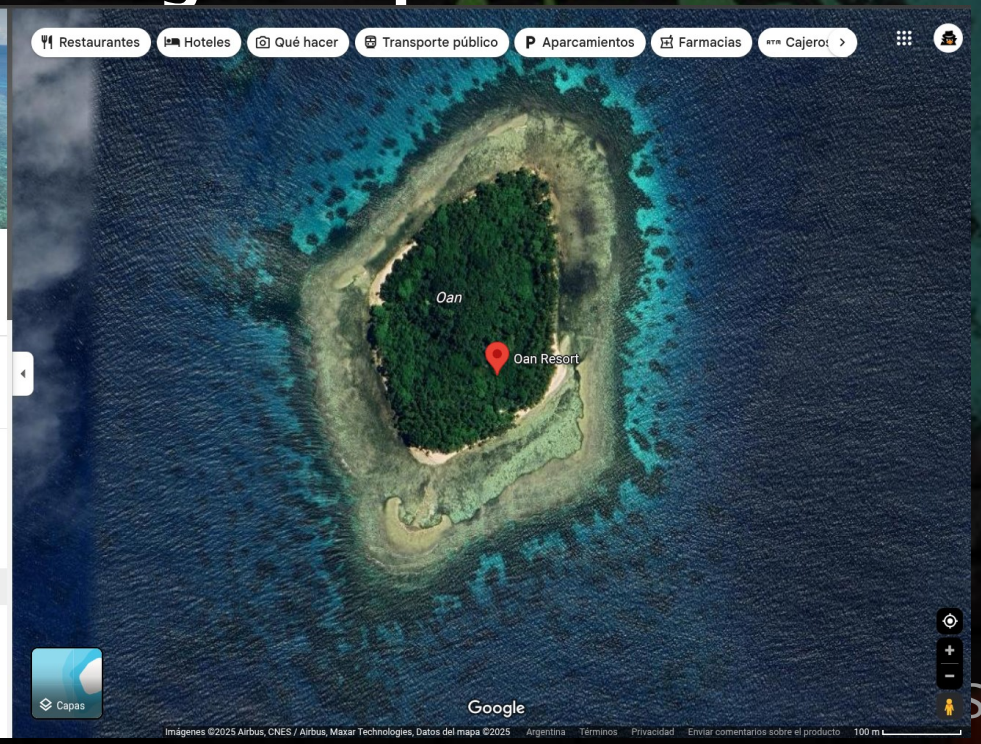
OAN RESORT

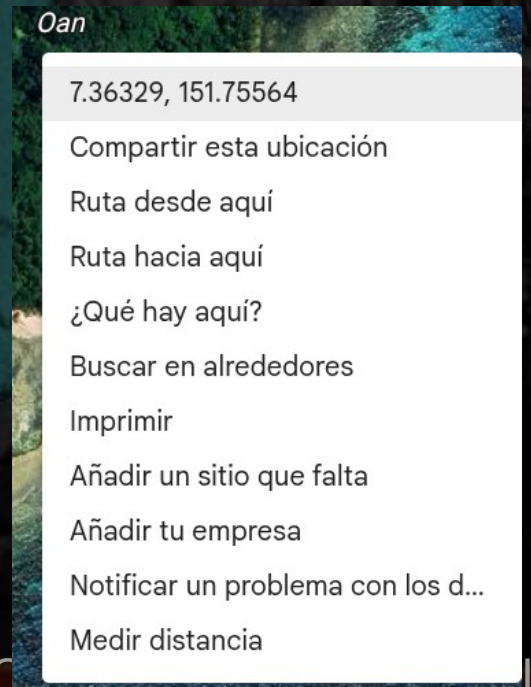


SOLUCIÓN - CTF 04

Buscamos en **Google Map OAN RESORT.**



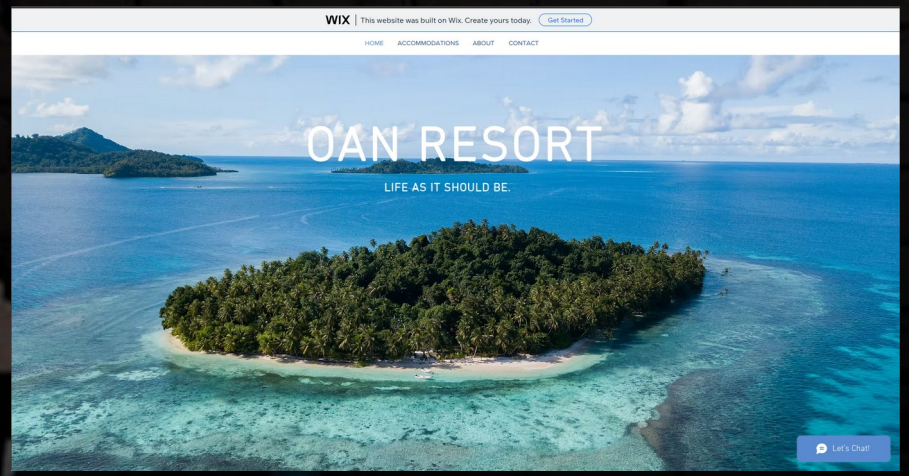




SOLUCIÓN - CTF 04

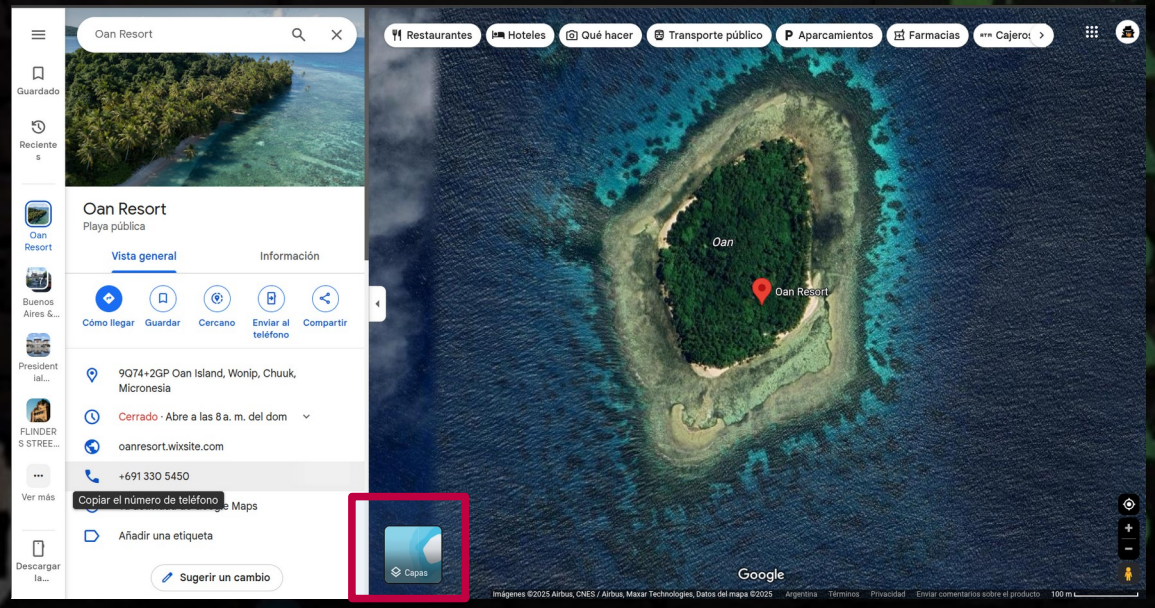
b) ¿ Cuáles son las coordenadas de la isla ?

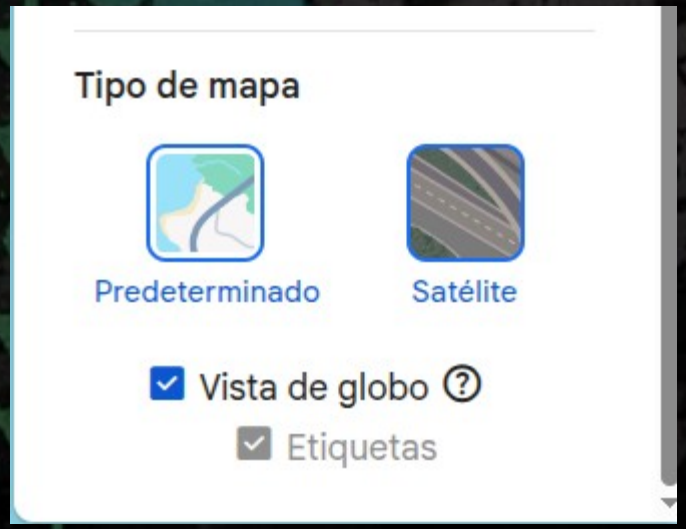
7.363285069812649, 151.75564168871873



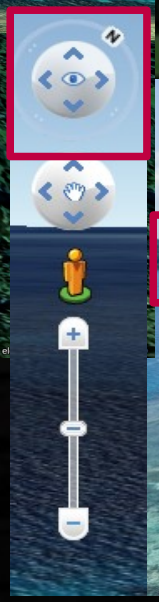
SOLUCIÓN - CTF 04

Buscamos en **Google Map OAN RESORT**.





SOLUCIÓN - CTF 04



SOLUCIÓN - CTF 04

c) ¿ En qué dirección cardinal estaba orientada la cámara cuando se tomó la foto ?

Noreste

CTF 05

DESCRIPCIÓN - CTF 05

La imagen a continuación es una captura de pantalla de una cámara en vivo del zoológico. Se tomó el 15 de enero del 2023 alrededor de las 14:00 hora local.

a) ¿ En qué zoológico se encuentran estos osos polares ?

b) ¿ Cuál era la temperatura al momento de la captura de la pantalla ?

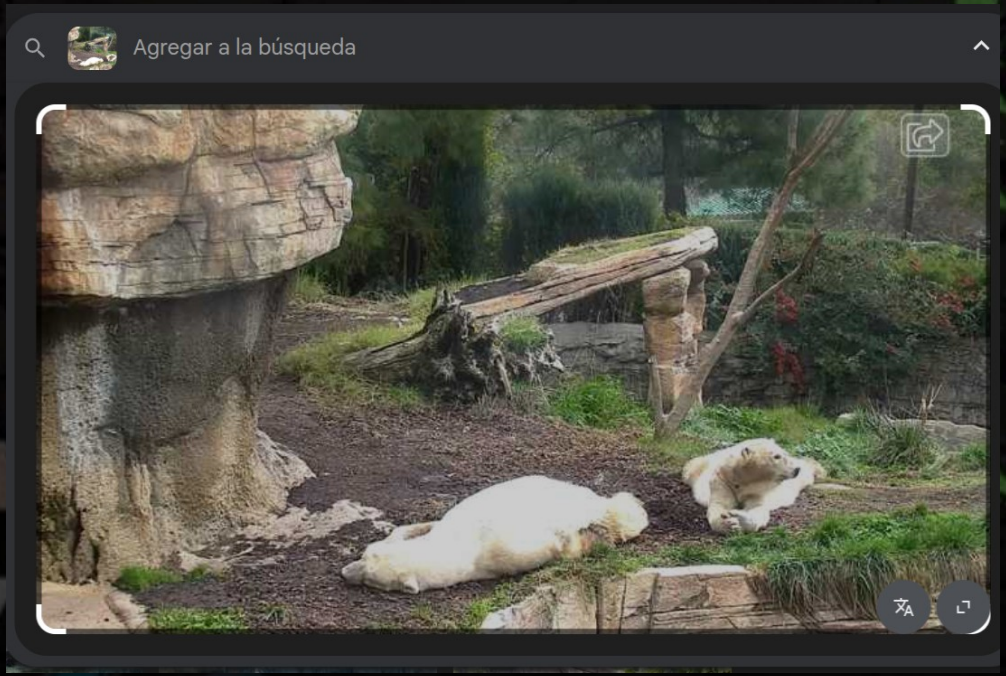
c) ¿ Cuáles eras las coordenadas exactas del lugar donde se encontraban lo osos ?

IDEAS - CTF 05

- Búscar la imagén en **Google Image**.
- Buscar en **Google Maps** y **Google Earth**.

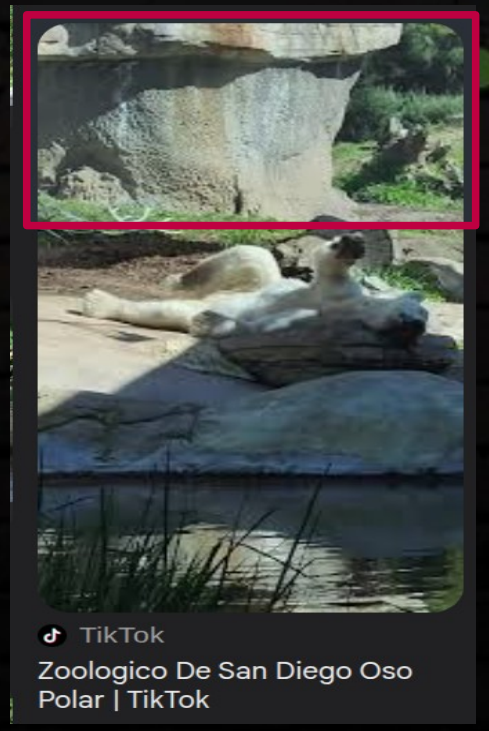
SOLUCIÓN - CTF 05

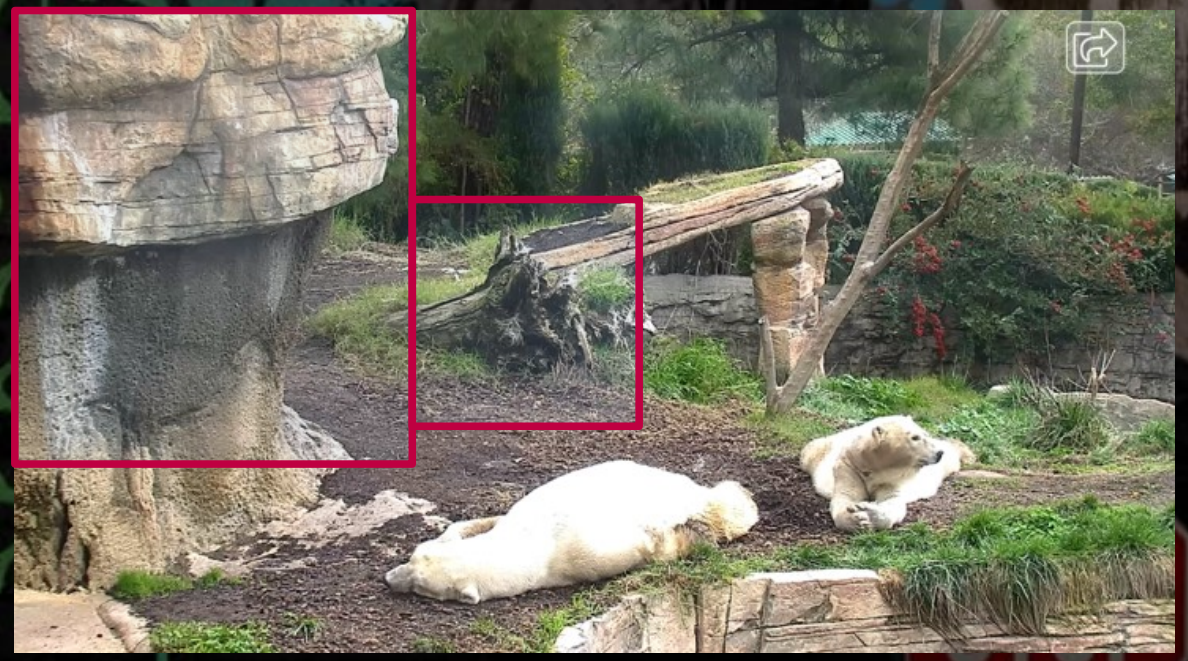
Buscamos en **Google Image**.



SOLUCIÓN - CTF 05

Buscamos en **Google Image**.





SOLUCIÓN - CTF 05

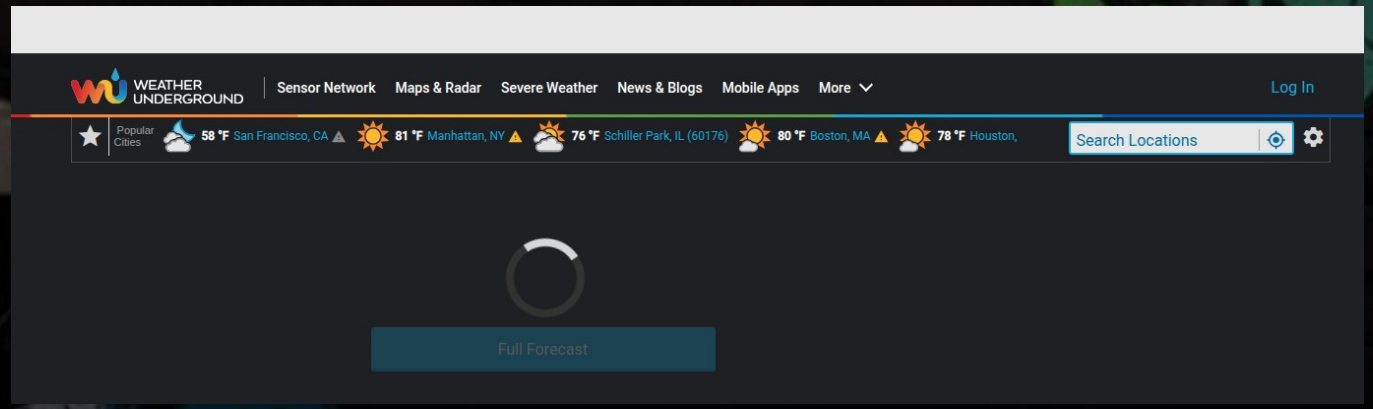
a) ¿ En qué zoológico se encuentran estos osos polares ?

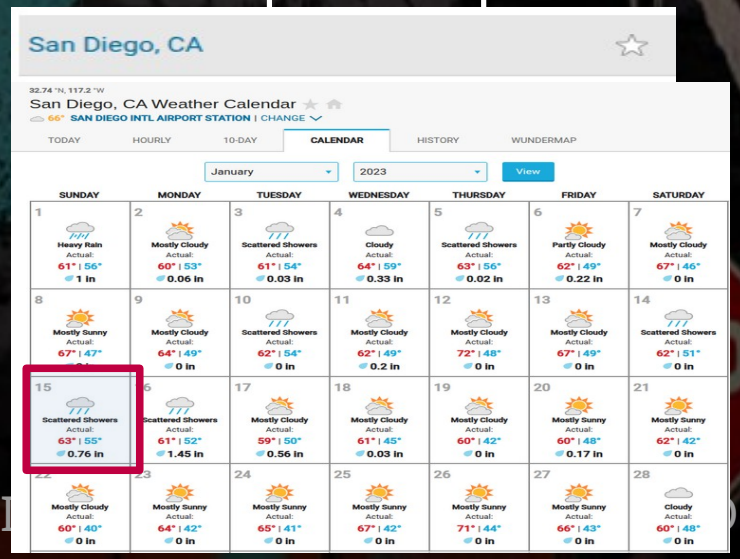
Zoológico De San Diego

SOLUCIÓN - CTF 05

Para saber la temperatura, sabes que la fecha fue tomada el **15 de enero del 2023 alrededor de las 14:00 hora local.**

Para esto vamos a la URL: **https://www.wunderground.com/** que nos permite indicar una fecha determinada.

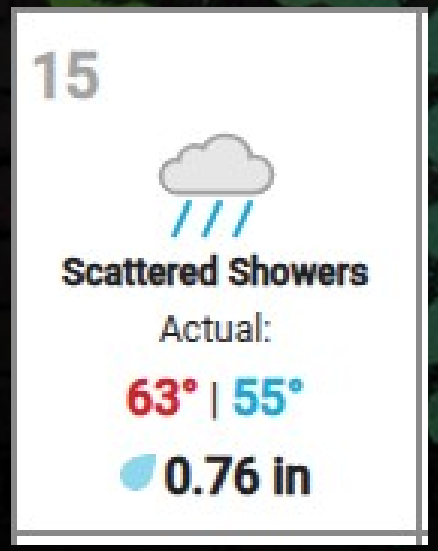




SOLUCIÓN - CTF 05

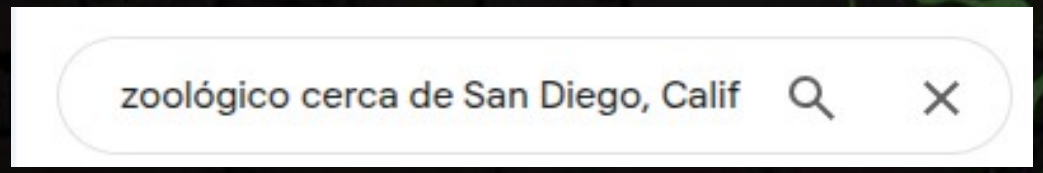
b) ¿ Cuál era la temperatura al momento de la captura de la pantalla ?

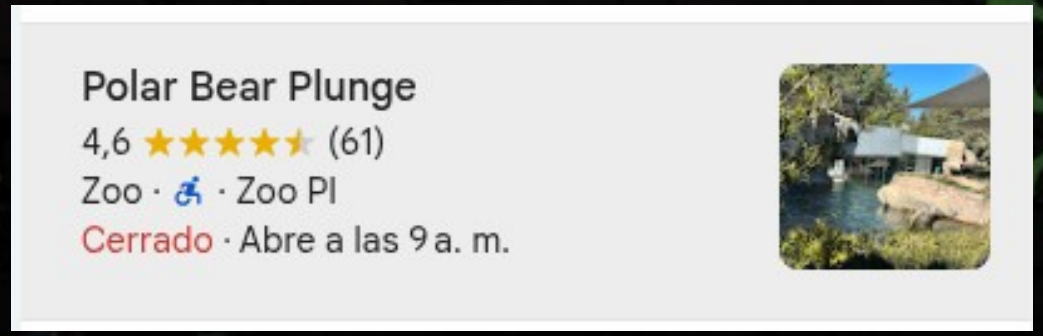
63 Grados

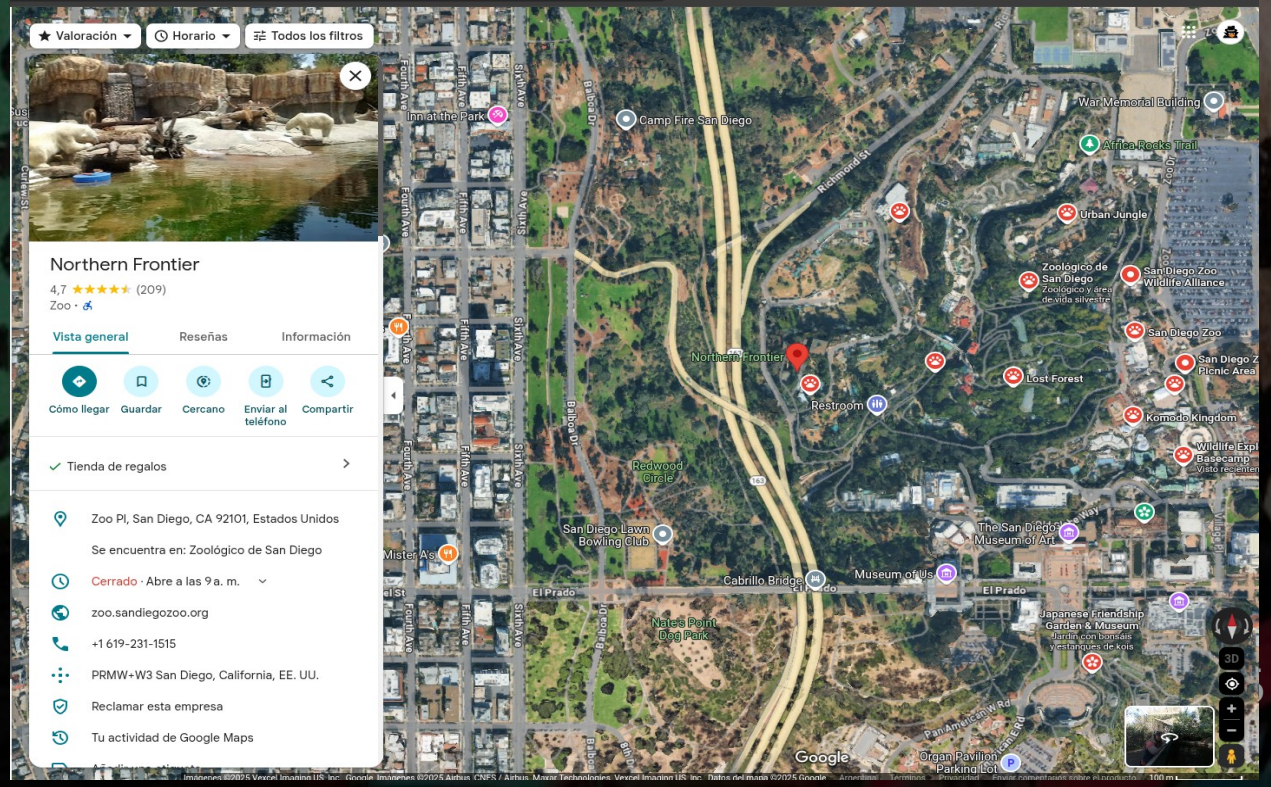


SOLUCIÓN - CTF 05

Buscamos en **Google Maps donde** buscamos **Zoológico San Diego California.**

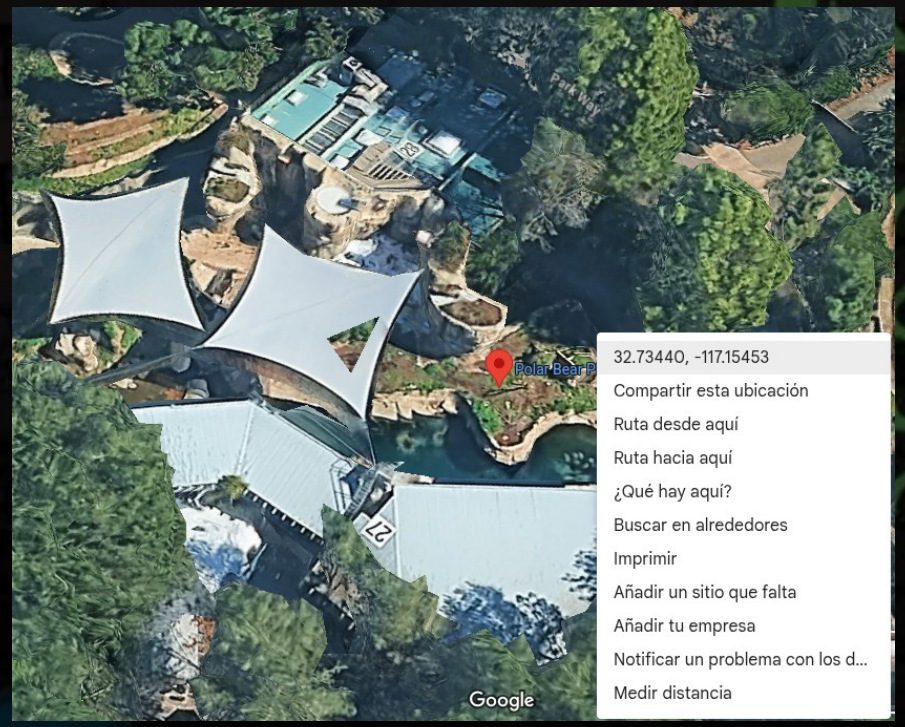


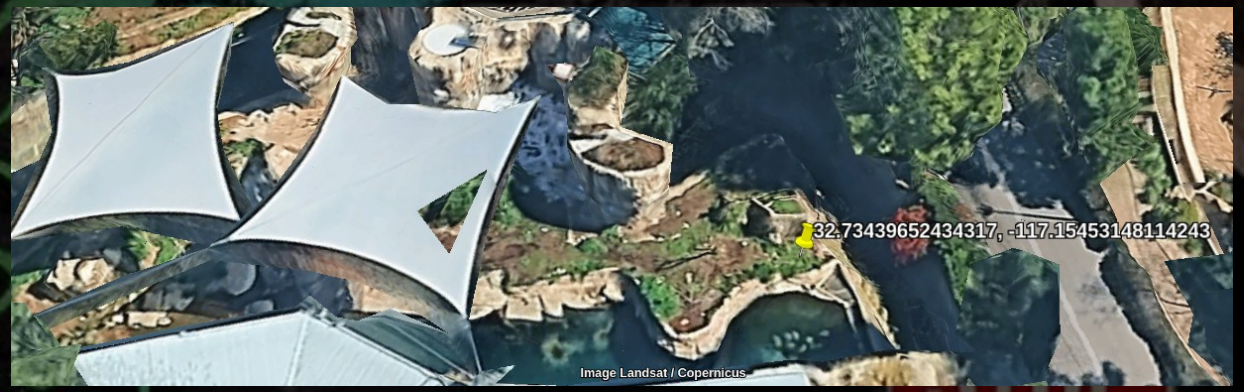




SOLUCIÓN - CTF 05

Copiamos las coordenadas para llevarloa **Google Earth.**





SOLUCIÓN - CTF 05

c) ¿ Cuáles eras las coordenadas exactas del lugar donde se encontraban lo osos ?

32.73440, -117.1543

MUCHAS GRACIAS