WRITE-UP OSINT
Eau salée

Challenge 1:

Un de vos amis vient de vous contacter. Après avoir fait une nuit blanche en regardant des vidéos sur de supposés monstres marins et leur bruit très mystérieux, il ne se rappelle plus du nom de celui qui l'avait terrorisé mais il se rappelle que le son avait été entendu pendant la même saison que la sortie du premier Men in Black en France.

Il aimerait aussi investiguer sur l'agence gouvernementale qui a découvert ce "monstre".

Votre mission si vous l'acceptez: Récupérez le nom du "bruit" et celui de l'agence gouvernementale en question.

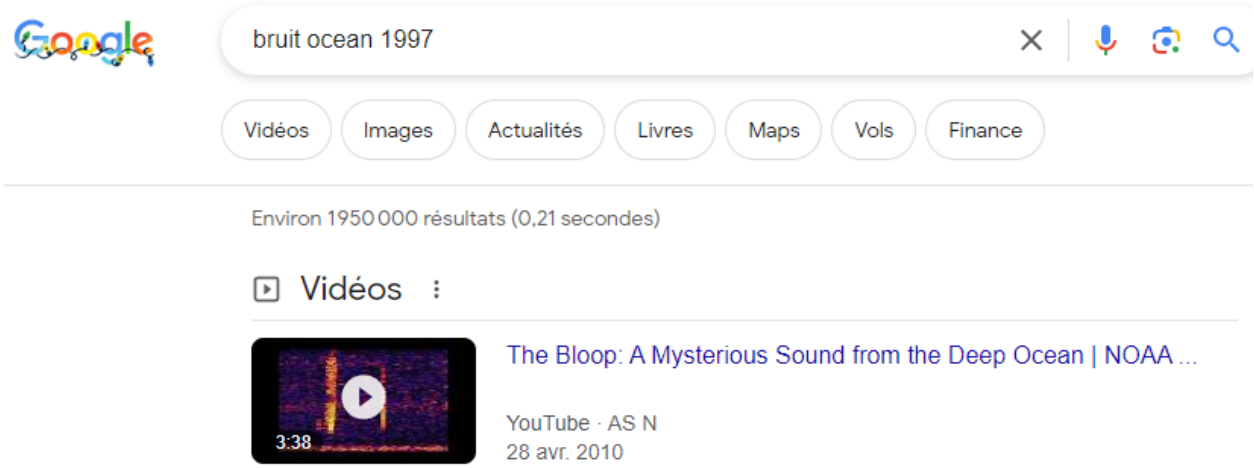
De quel autre monstre (fictif) était-il proche géographiquement ? L'agence gouvernementale ne pense pas que le "bruit" venait réellement d'un monstre, quelle est la cause la plus probable selon elle ?

Format du flag:
dracula_regional-chocolatine-and-petit-pain-administration_frankenstein_volcan

———

Solution:

On parle d'un bruit qui a été entendu lors de la sortie du premier Men in Black en France.
Men in black en France est sorti en 1997.
Avec les informations que l'on a, on peut en déduire que l'on cherche un bruit maritime en 1997, avec cette recherche google "bruit ocean 1997", on trouve le **Bloop**.



Sur le wikipédia du Bloop (https://fr.wikipedia.org/wiki/Bloop) on trouve que c'est la **National Oceanic and Atmospheric Administration** qui a découvert ce bruit.
Dans la catégorie "Dans la culture populaire", on voit qu'il y avait une rumeur sur la proximité de **Cthulhu**.
La cause est dans le premier paragraphe du Wikipédia, c'est un énorme **iceberg**.

Flag: bloop_national-oceanic-and-atmospheric-administration_cthulhu_iceberg

Challenge 2:

Cthulhu a été aperçu lors de la destruction d'une ville en 2015, quelle ville a été détruite ?

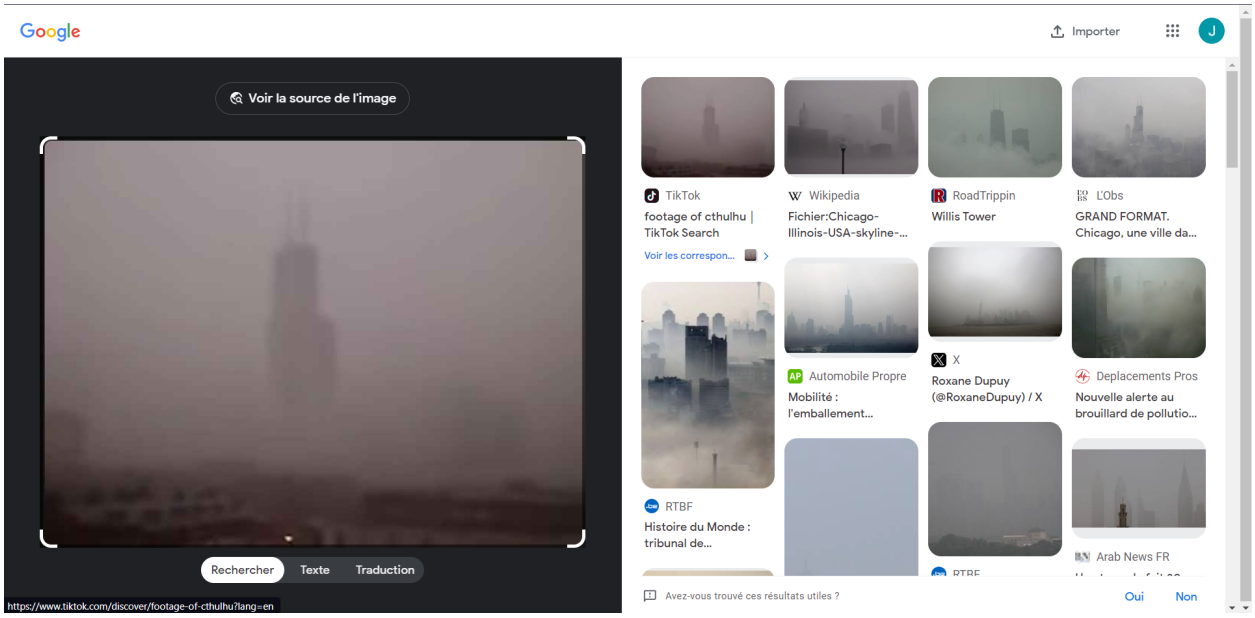
Quand est-ce que Lovecraft a imaginé pour la première fois Cthulhu ?

Format du flag: paris_2023

———————————————————————————————————————

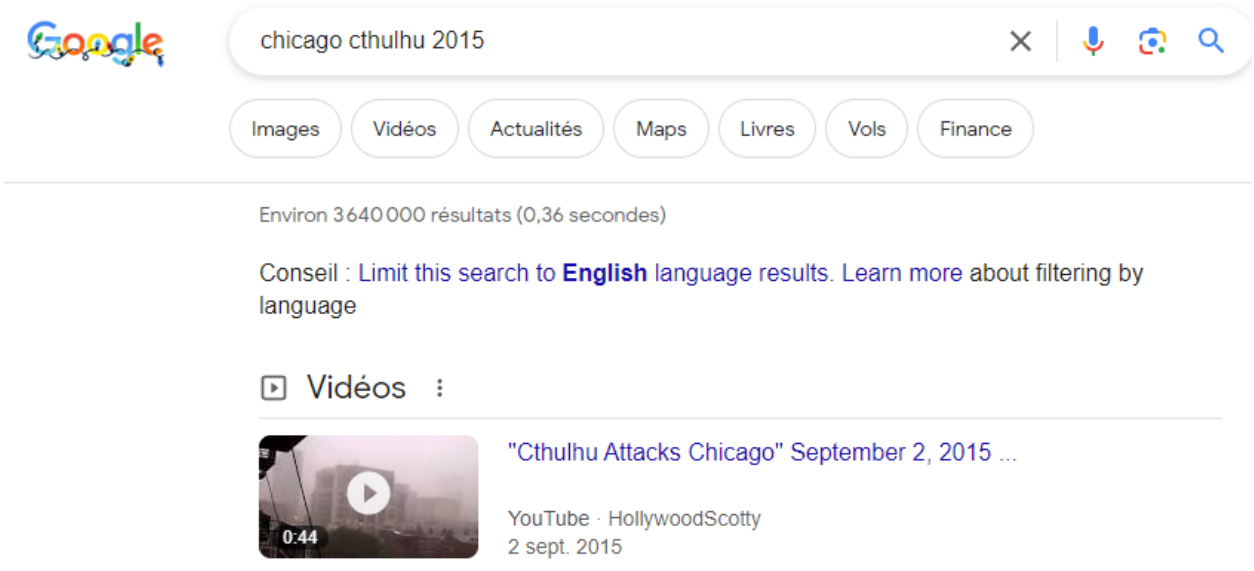
Solution:

En faisant une recherche inversée par image sur google, on a:



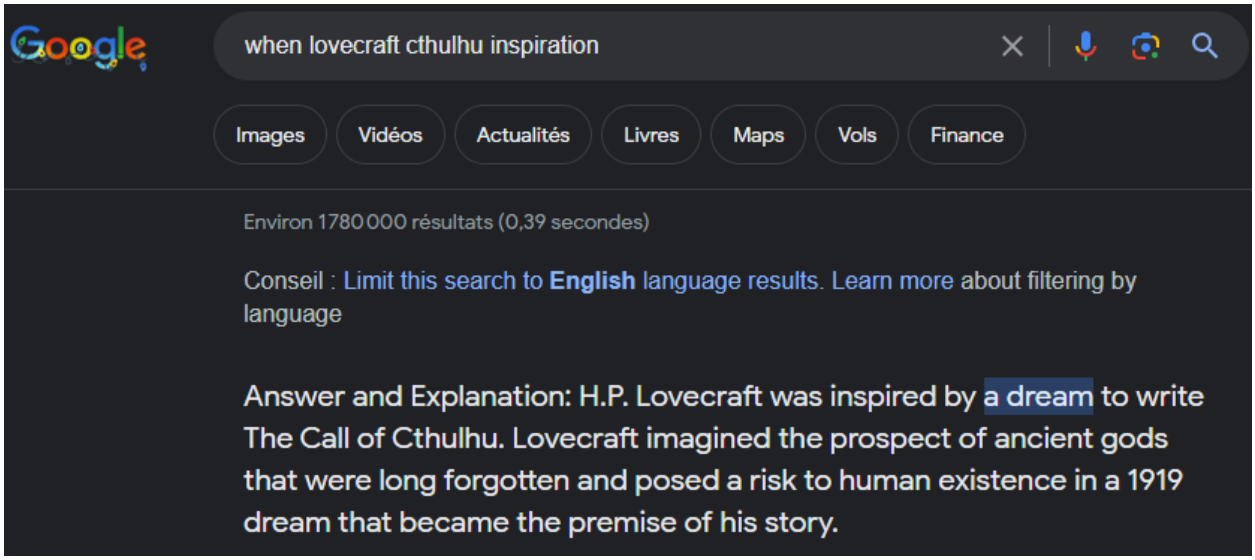
On voit que l'on parle de **Chicago**, plus précisément, la Willis Tower.

On vérifie en cherchant "chicago cthulhu 2015" sur Google:



La vidéo (https://www.youtube.com/watch?v=FkcDoUE8_Ec) correspond bien à notre image.

Pour savoir quand Lovecraft avait imaginé Cthulhu, il fallait chercher d'où venait son inspiration:



On peut essayer de vérifier l'information avec une source plus "sûre" (Wikipédia n'est pas 100% sûre mais c'est une bonne source quand même).
Sur la page Wikipedia de L'appel de Cthulhu (https://fr.wikipedia.org/wiki/L%27Appel_de_Cthulhu), dans la catégorie "Inspiration" on voit qu'il s'est inspiré d'un rêve qu'il a eu en 1919.

Flag: chicago_1919

Challenge 3:

L'agence ne pense pas que ce soit un monstre...cependant ce n'est peut-être pas le cas de tout le monde, quel est le nom COMPLET (avec le nom intermédiaire) de la personne faisant parti de l'agence, interviewé par la CNN, qui émet un doute sur l'origine du bruit ?

Ce serait utile si on pouvait la contacter via un numéro de téléphone...il me semble qu'il vit en Oregon, ça commencerais par 541 donc...

Son adresse mail personnelle (gmail) nous permettrait d'échanger avec lui s'il ne répond pas au téléphone...

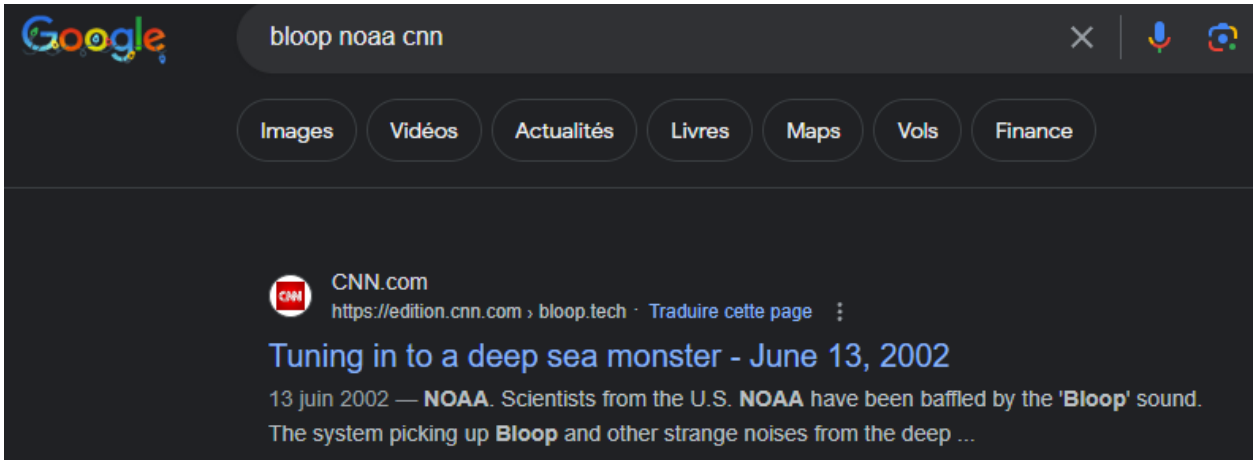
Combien de fenêtres a-t-il remplacé il y a 2 ans ?

Format du flag: john-fitzgerald-kennedy_541-XXX-XXXX_johnfkennedy@gmail.com_4

———

Solution:

En cherchant sur Google, “bloop noaa cnn”, on tombe sur cet article de 2002:



https://edition.cnn.com/2002/WORLD/sailing/06/13/bloop.tech/index.html

Dans cet article, on voit que deux scientifiques sont mentionnés, Christopher Fox et Phil Lobel.

Philip Lobel ne pense pas que ce soit une créature comme le calamar géant.

However Phil Lobel, a marine biologist at Boston University, Massachusetts, doubts that giant squid are the source of Bloop.

Il apparaît aussi sur le Wikipédia:

Autres explications [modifier | modifier le code]

- Certains scientifiques postulent que ce son pourrait être émis par un énorme et encore non découvert calamar géant ou pieuvre, ou une nouvelle espèce de poisson ou baleine encore plus grand que la baleine bleue[3]. Phil Lobel, un biologiste de l'Université de Boston, conteste ces hypothèses, soulignant que les céphalopodes connus n'ont pas de membranes gazeuses nécessaires pour produire ce genre de son, et qu'un cétacé doit faire surface pour respirer et aurait déjà dû être repéré[4].

Christopher Fox, quant à lui, est dubitatif quant à la nature du bruit.

Scientist Christopher Fox of the U.S. National Oceanic and Atmospheric Administration's Acoustic Monitoring Project at Portland, Oregon, has given the signals names such as Train, Whistle, Slowdown, Upsweep and even Gregorian Chant.

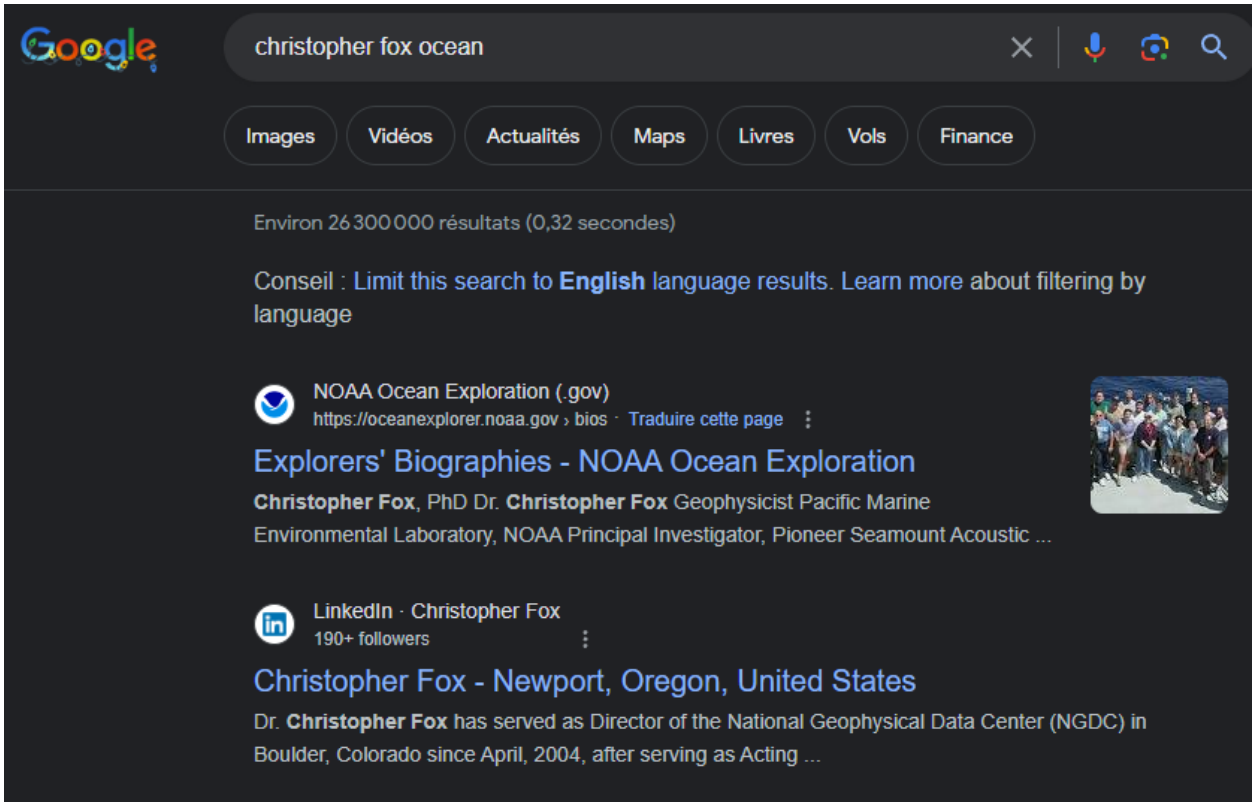
He told New Scientist that most can be explained by ocean currents, volcanic activity -- Upsweep was tracked to an undersea South Pacific mountain that had not been identified as "live."

"The sound waves are almost like voice prints. You're able to look at the characteristics of the sound and say: 'There's a blue whale, there's a fin whale, there's a boat, there's a humpback whale and here comes and earchquake," he says.

But some sounds remain a mystery he says. Like Bloop -- monster of the deep?

Nous sommes sur la bonne piste mais malheureusement, Christopher Fox n'est pas son nom complet.

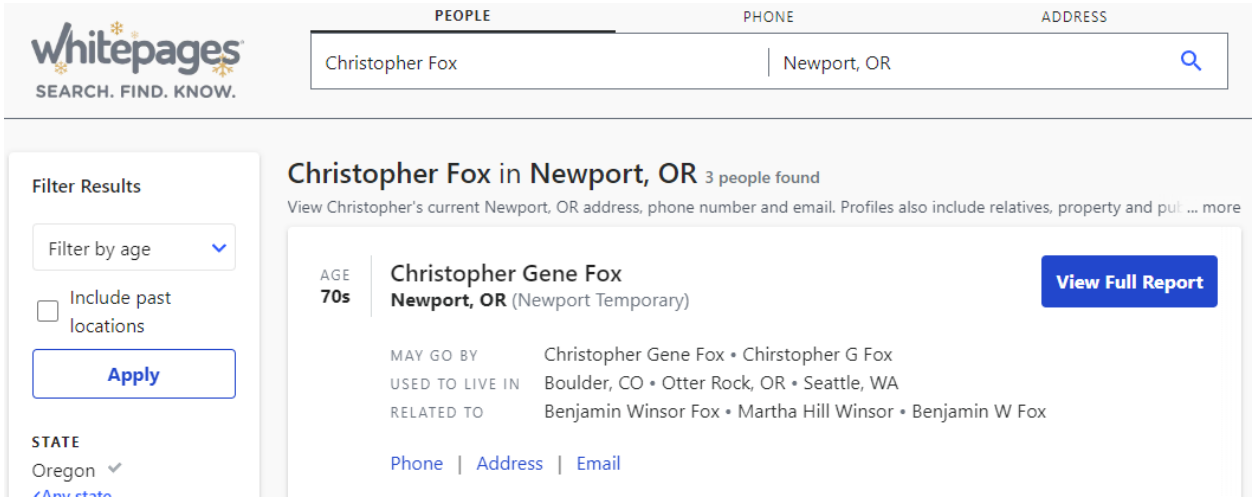
En cherchant "christopher fox ocean", on trouve son compte LinkedIn (https://www.linkedin.com/in/christopher-fox-4589945a/), il habite à Newport dans l'Oregon.



L'énoncé nous confirmait que le chercheur habitait dans l'Oregon.

Avec un outil comme [Fast People Search.com](), on peut chercher toutes les personnes dans une zone géographique (aux États-Unis).

On peut aussi utiliser [Whitepages]() pour trouver son nom complet, une fois le nom complet nous pouvons faire un dork sur son nom pour récupérer tous les résultats d'outils en ligne.



[True People Search]() pour toutes les informations (https://www.truepeoplesearch.com/find/person/px40n6nlrlu92l6294nn6)

On tombe alors sur son profil: (Fast People Search - Christopher Fox)

Sur le profil, on voit qu'il s'appelle **Christopher Gene Fox**.

On trouve aussi son numéro de téléphone (le plus probable en tout cas)

(541) 264-8091 (numéro rattaché aussi à sa femme)

Son adresse mail gmail (**chrisgfox1@gmail.com**).

Et en faisant une recherche avec cette adresse mail sur Epieos, on récupère son compte sur Google maps, il a laissé un avis il y a 2 ans en disant qu'il avait changé 14 fenêtres.

On confirme que c'est bien son adresse mail avec la photo de profil similaire à celle de LinkedIn.

Google Maps de Christopher Fox

Flag: christopher-gene-fox_541-264-8091_chrisgfox1@gmail.com_14

Challenge 4:

Vous avez réussi à le contacter mais il ne voulait pas révéler ses secrets à n'importe qui, il veut vous voir dans la vraie vie, dans un café de sa ville plus précisément, mais il est resté mystérieux: "C'est un café qui est à moins de 200 mètres d'un point d'eau potable et à moins de 2 km d'un terrain de foot, si vous êtes vraiment à la recherche de la vérité, vos talents de détectives vous mèneront à moi, je prendrais un Mimosa..."

Combien vaut (en dollars) le Mimosa dans ce café ? Combien de fautes d'orthographes il y a-t-il sur les cépages français servis dans ce café (dans la catégorie Fine Wine)? Combien valait une omelette au fromage dans ce café le 26 décembre 2010 (arrondi au centime, en euro de l'époque) ?

Format du flag: 5_6_5.55

Solution:

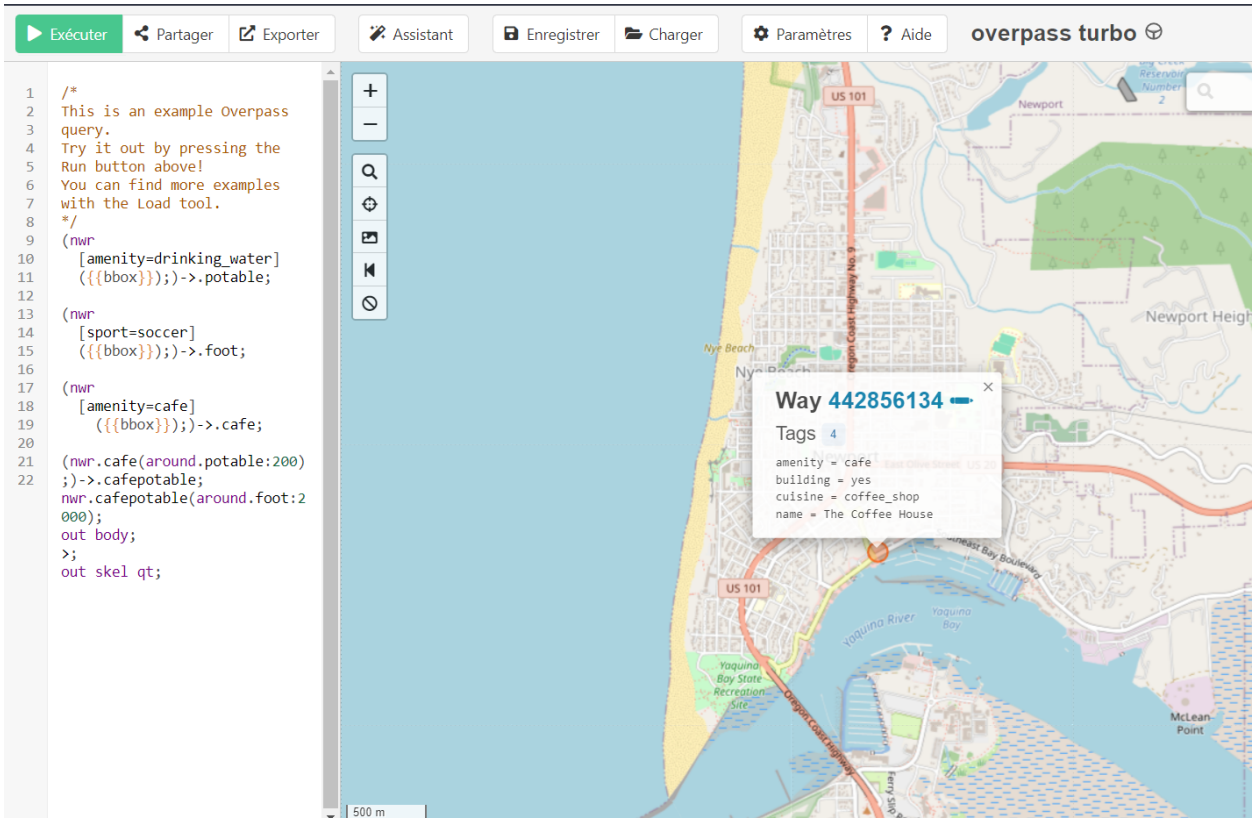
On sait que Christopher habite à Newport dans l'Oregon, donc il faut chercher dans cette ville. On peut utiliser l'outil Overpass Turbo pour ce genre de requêtes:

```
(nwr
  [amenity=drinking_water]
  ({{bbox}});)->.potable;

(nwr
  [sport=soccer]
  ({{bbox}});)->.foot;

(nwr
  [amenity=cafe]
    ({{bbox}});)->.cafe;

(nwr.cafe(around.potable:200);)->.cafepotable;
nwr.cafepotable(around.foot:2000);
out body;
>;
out skel qt;
```



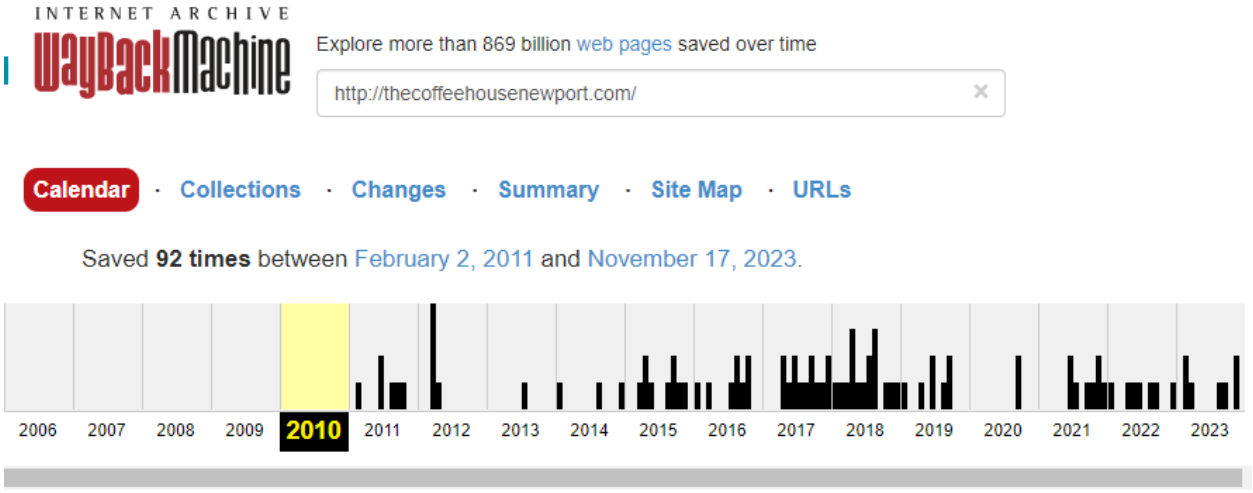
The Coffee House est donc le café recherché (https://www.thecoffeehousenewport.com/menu)

Dans le menu, on voit le Mimosa qui est à **9$**.

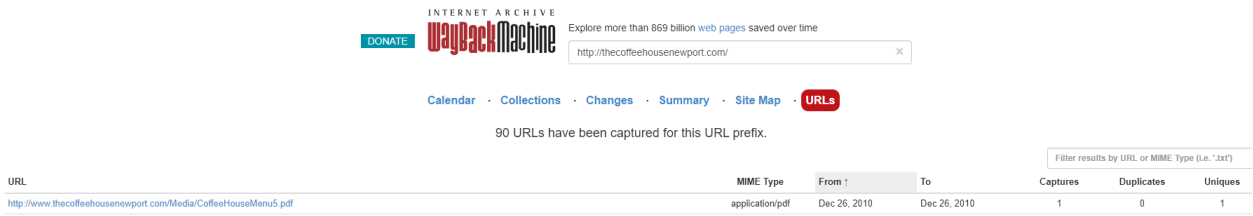
Dans la catégorie “Fine Drinks”, on voit **3** fautes d’orthographes: 2 “Sauvingon”, 1 “Riésling” (Sauvignon pour la première erreur, et pas d’accent sur Riesling en temps normal).

Pour l’omelette au fromage, on va sur Wayback Machine.

Bizarrement, pas d’archive en 2010…



Cependant, en allant dans la catégorie URLs et en triant par date on récupère le [PDF du menu]




Breakfast Menu - *See Our Menu Board for Daily Specials*

Omelets:

Cheese $6.95

On voit que l'omelette au fromage est donc à 6,95$.

Il faut donc convertir cette somme en dollars en euros de l'époque (https://www.exchangerates.org.uk/historical/find-exchange-rate-history-for-26_12_2010)

On fait 6,95 * 0,7646 = 5,31397, arrondi au centime = **5,31**

Flag: 9_3_5.31

Challenge 5:

Enfin, vous voilà devant lui...comme annoncé, il est en train de siroter son Mimosa, vous commencez à l'interroger mais malgré votre présence devant lui, vous voyez qu'il ne peut pas être direct et vous donner toutes les réponses à vos questions.

Vous allez devoir chercher vous même, le chercheur à la retraite vous donne quand même quelques indications: "Rends-toi à la prochaine soirée pyjama organisé par l'aquarium du coin...avec de la chance tu verras les copains du Dr Brent, on l'a plus vu depuis octobre 2018"

"Le spécimen qui t'intéresse a été tagué lors de la même expédition que Breton. Tu comprendras en voyant le mastodonte que c'est pas une grand-mère comme les autres."

Quel est le nom scientifique du Dr Brent ? Lors de quelle expédition le mastodonte a-t-il été taggé ? Combien de kilogrammes pèse-t-il ?

Une fois vos réponses acquises, vous comprenez que vos recherches ne mènent à rien et que vous vous êtes fait mener en bateau depuis le début, le chercheur voulait juste partager sa passion de l'océan avec un détective à la recherche de la vérité comme vous.

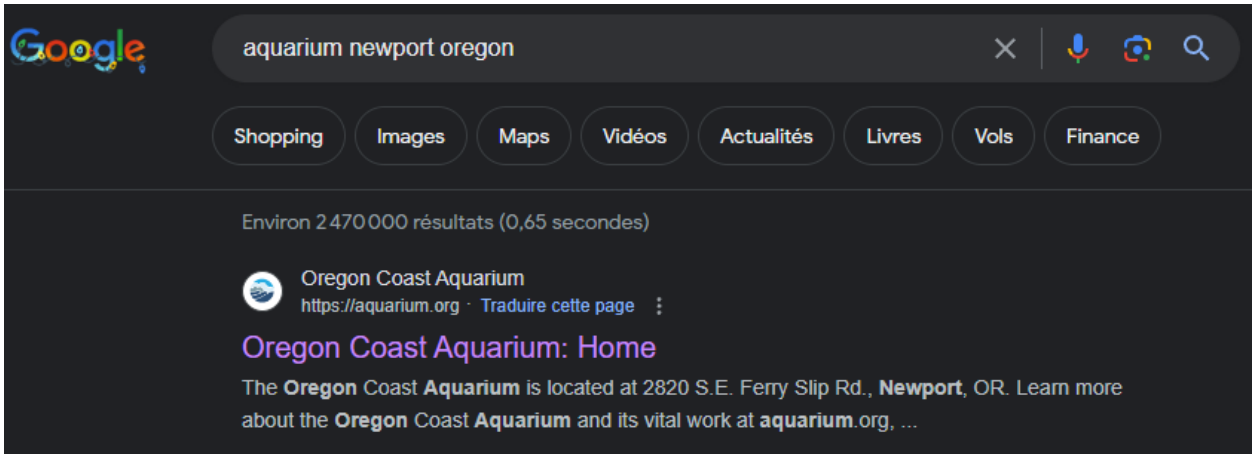
Même si vous aviez la vérité devant vos yeux, dans un élan de scepticisme, la fougue de l'imaginaire et du mystérieux s'était emparée de vous. Malheureusement, la vérité est quelques fois ennuyante, il n'y a donc pas de monstre à l'horizon...

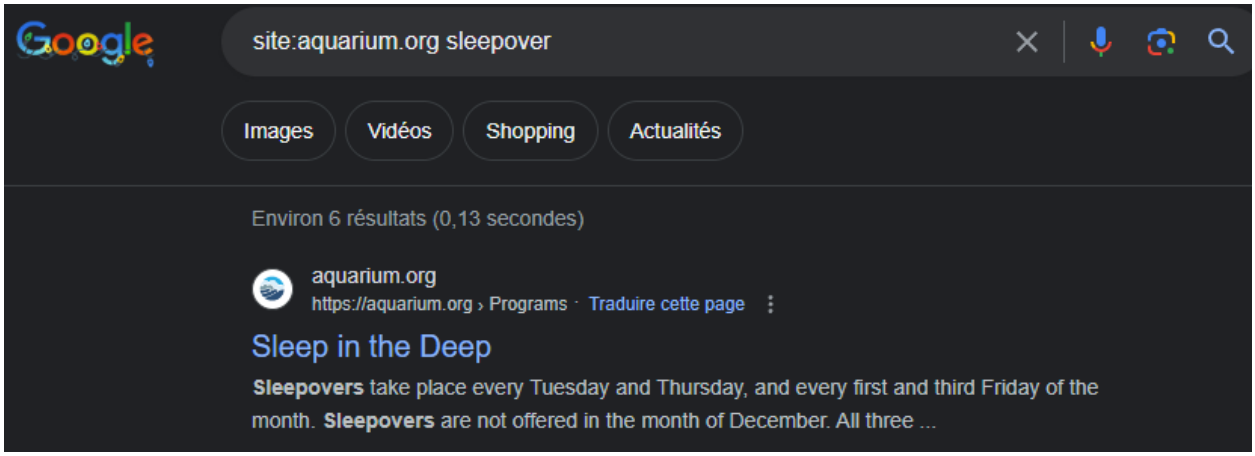
Format du flag: homo-sapiens_isla-nublar-2015_1460

———————————————————————————————————————

Solution:

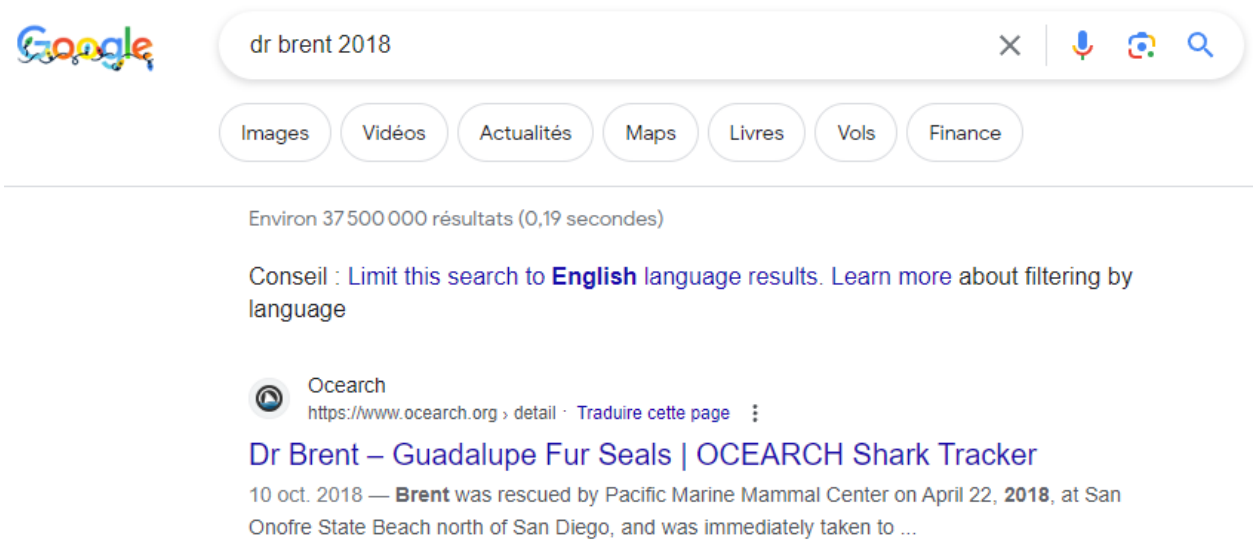
Le chercheur nous parle d'une soirée pyjama à l'aquarium le plus proche.





La soirée pyjama permet donc de voir les animaux de l'aquarium (la prochaine session est le 2 janvier 2024 pour information).

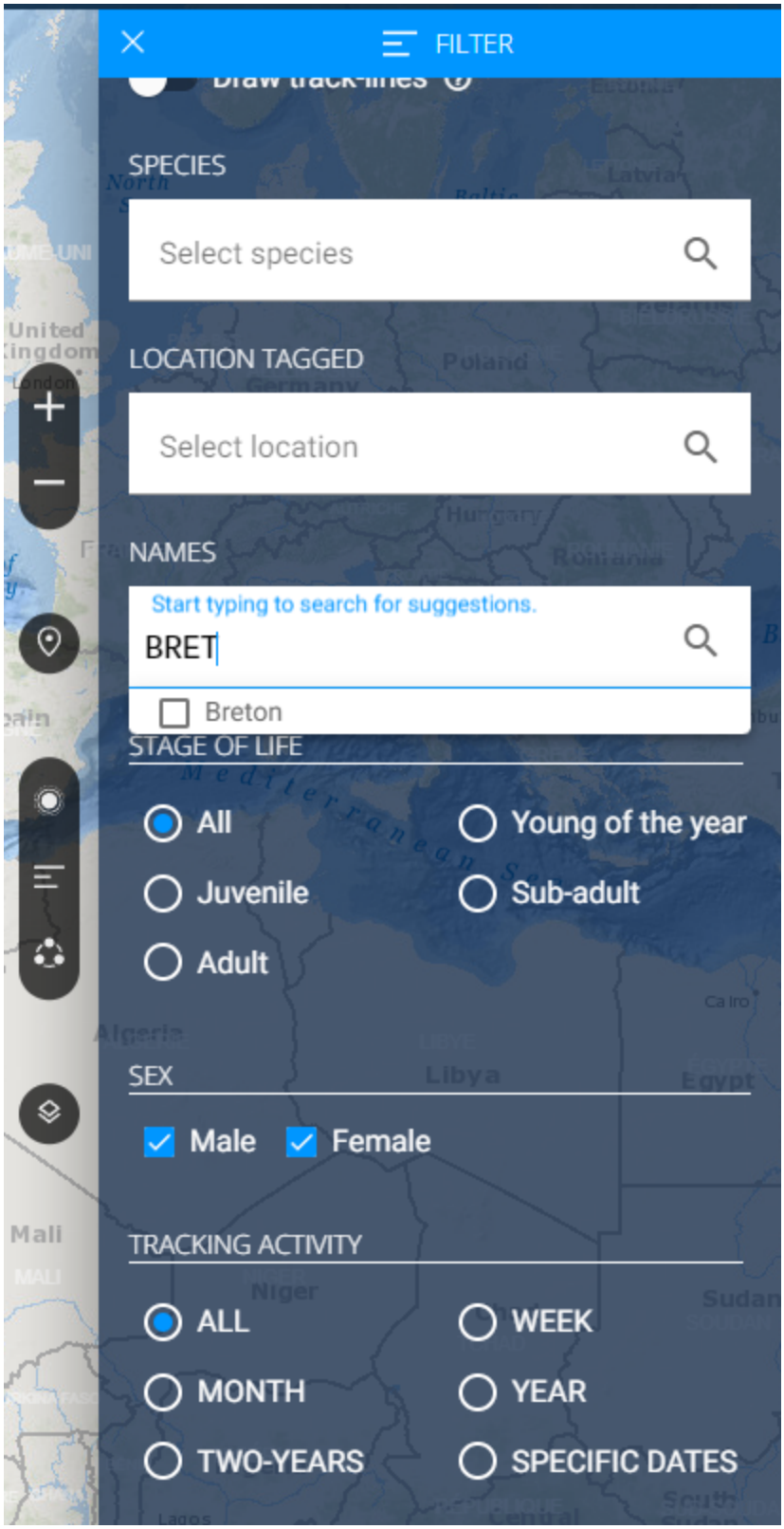
En cherchant:



On voit que le Dr. Brent n'est pas un humain en réalité mais un phoque !
En allant sur la page du Dr. Brent, on récupère son nom scientifique: **arctocephalus townsendi.**

Reprenons l'énoncé pour chercher les mots-clés pour la suite de la question:

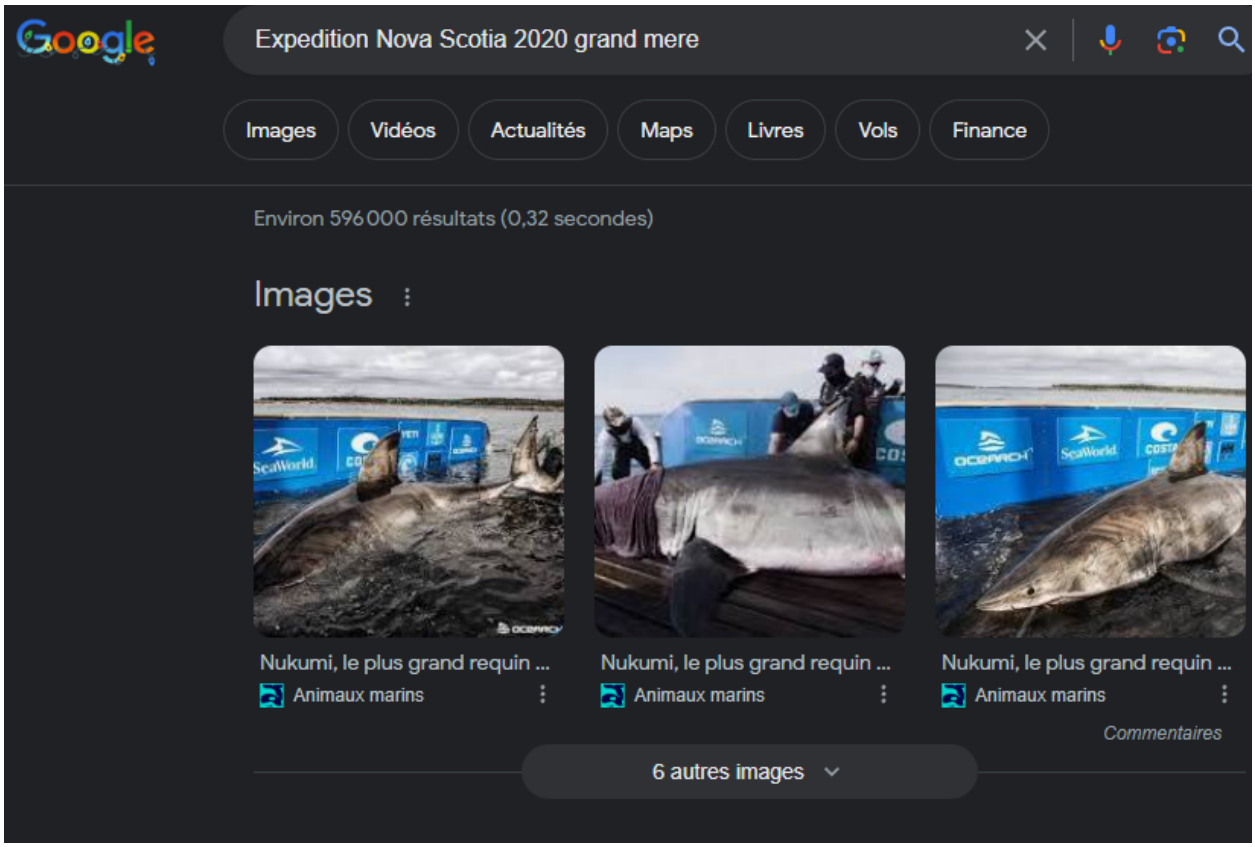
""Le **spécimen** qui t'intéresse a été **tagué** lors de la **même expédition** que **Breton**. Tu comprendras en voyant le **mastodonte** que c'est pas une **grand-mère** comme les autres."
Si on s'intéresse au site utilisé pour le Dr. Brent, on comprend que c'est un site d'une organisation qui tague la localisation des animaux marins.
En restant sur le même site, on peut filtrer et faire des recherches par nom d'animal.



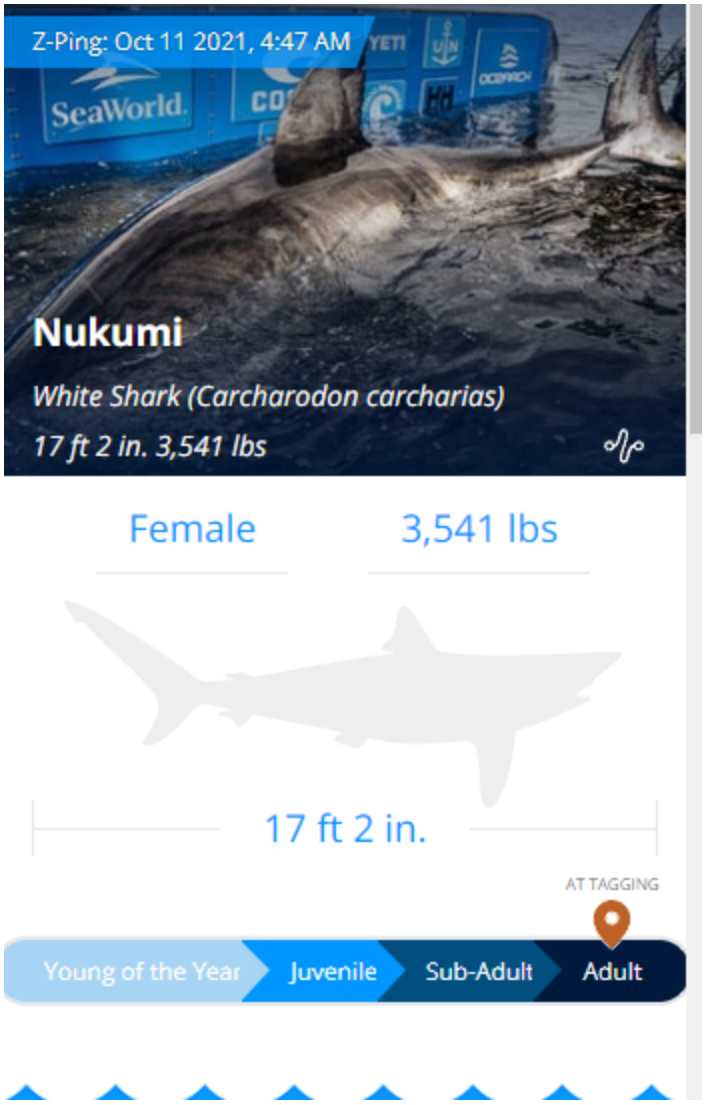
On récupère le profil de [Breton], dans “About Breton” on apprend qu’il a été tagué pendant

l'expédition **Nova Scotia 2020**.

En cherchant "Expédition Nova Scotia 2020 grand mere":



On voit Nukumi" (ce qui veut dire grand-mère en Mik'maw). En revenant sur Ocearch on va chercher Nukumi



En faisant la conversion 3541 lbs -> 1606 kilos, Nukumi, reine de l'océan, fait **1606** kg.

Flag: arctocephalus-townsendi_nova-scotia-2020_1606