

Bonus- Fishing

Saturday, December 23, 2023

4:36 PM

Difficulty: 1

Fishing Guide: Catch twenty different species of fish that live around Geese Islands. When you're done, report your findings to Poinsettia McMittens on the Island of Misfit Toys.

Difficulty: 4

Fishing Mastery: Catch at least one of each species of fish that live around Geese islands. When you're done, report your findings to Poinsettia McMittens.

CONVERSATION w/ Elf	<p><u>Poinsettia McMittens (Squarewheel Yard)</u></p> <p>Hoy small fry, nice work! Now, just imagine if we had an automatic fish catcher? It would be as ingenious as me on a good day! I came across this fascinating article about such a device in a magazine during one of my more glamorous fishing sessions. If only I could get my hands on it, I'd be the undisputed queen of catching them all!</p> <p>** ----- Response after completing challenge ----- **</p> <p>You managed to catch every fish? You're like the fishing version of a Christmas miracle! Now, if only you could teach me your ways... but then again, I'm already pretty fabulous at everything I do.</p> <p>From <https://2023.holidayhackchallenge.com/badge?section=conversation&id=poinsettiamcmittens></p>
HINTS	<p>Fishing Machine</p> <p>From: Poinsettia McMittens Objective: BONUS! Fishing Guide</p> <p>There are a variety of strategies for automating repetitive website tasks. Tools such as AutoKey and Autofit allow you to programmatically examine elements on the screen and emulate user inputs.</p> <p>From <https://2023.holidayhackchallenge.com/badge?section=hint&id=hintFishing2></p> <p>I Am Become Data</p> <p>From: Poinsettia McMittens Objective: BONUS! Fishing Guide</p> <p>One approach to automating web tasks entails the browser's developer console. Browsers' console allow us to manipulate objects, inspect code, and even interact with websockets.</p> <p>From <https://2023.holidayhackchallenge.com/badge?section=hint&id=hintFishing3></p>

MY WORK AND ANSWER

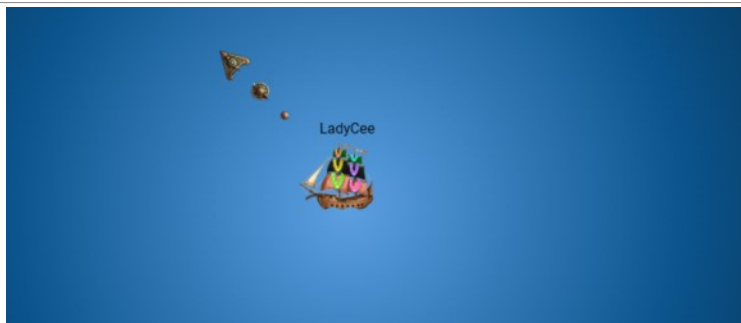
Early on in the challenge, I begun fishing manually. It was enjoyable and a nice way to take a break from the challenges. I didn't consider the challenge until after I had secured the bonus challenge achievement. At this stage, I hadn't decided if I would complete this bonus challenge. I continued to fish as I did this when I needed a break from a challenge and before long I had amassed 100 fish! Then 169! So yeah, I was in this one to win even while I still had nearly half of the challenges to complete.

I checked for hints from other players and realized my leisurely fishing would not capture that last and elusive fish, the rare *Piscis Cyberneticus Skodo*. I was able to confirm the total fish count (171). With only one left to reel in, I didn't waste time with web sockets. Instead, I began chasing the trail of a heat map with plans to locate him and catch him as I had the other fish.

Fishing for fun: At first, I was casting my line but didn't realize I needed to wait for a bite. So, I was throwing my line out and almost immediately reeling it in before being prompted to "Reel it in!".

Once I realized how the fishing functioned in this challenge, I took more care as I fished on the open seas and near the ports, and even in channels.

The fishing proved to be surprisingly relaxing and I especially enjoyed the crazy names, descriptions and variety in the



waters. So I found myself fishing a lot.

I quickly completed the bonus fishing guide challenge, which prompted me to explore what was needed to complete the other portion of the fishing challenge.

Now in the challenge to win: I reviewed the source code in the frame while sailing. And there was a reference, apparently mistakenly left by the developer, that revealed where I could find information on the fish index.

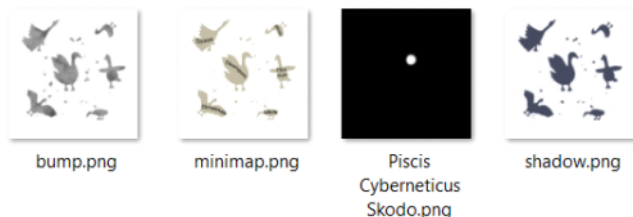
A href = fishdensityref.html

[\[DEV ONLY\] Fish Density Reference \(holidayhackchallenge.com\)](https://2023.holidayhackchallenge.com/sea/fishdensityref.html)

<https://2023.holidayhackchallenge.com/sea/fishdensityref.html>

<h3>Piscis Cyberneticus Skodo</h3>

I used the location map for the *Piscis Cyberneticus Skodo* (i.e., fishdensityref.html) and using MS PowerPoint, I overlayed it with three (3) other image files (locations of which I found in the html code) to create the image to the right.



Stretching each to equal length, the newly layered map clearly revealed the location of the elusive fish, as denoted by the white circle.

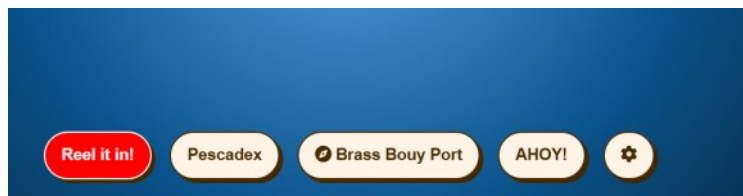
Armed with this intel, I set sail for the location of where this elusive fish swam.

I journeyed to the spot, where I found two other boats there who likely were doing the same thing.

I anchored a respectable distance from them, in the neck of the goose and cast my line.

Only after a few minutes, I had the last fish!

Ahoy!!!



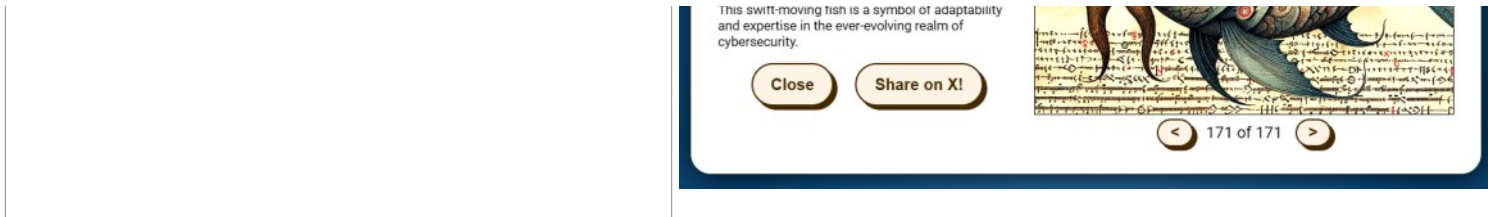
```
▼ #document (https://2023.holidayhackchallenge.com/sea/?dock5lip=3f30ebd6-1470-43f9-9c59-
c2acdf3ad6da&r=0.4547050779659785)
<!DOCTYPE html>
▼ <html lang="en">
  <head>
  </head>
  <body>
    <!-- <a href='fishdensityref.html'>[DEV ONLY] Fish Density Reference</a> --> == $0
    <div class="overlay"></div>
    <div class="ui">
      <button class="quitrace" style="display: none;">Exit Race</button>
      <button class="castreel" style="display: block;">Cast Line</button>
      <button class="reelitin" style="display: none;">Reel it in</button>
      <button class="openpescadex" style="display: block;">Pescadex</button>
      <button class="setbearing"></button>
      <button class="sayAhoy">AHoy!</button>
      <button class="settingsBtn">
        <i class="fas fa-cog">
      </button>
    </div>
    <div class="cotd"></div>
    <div class="shortcuts"></div>
    <div class="port-label"></div>
    <div class="settings"></div>
    <div class="wrapper hidden"></div>
    
    <canvas tabindex="1" width="600" height="923">
    <script src="https://cdn.jsdelivr.net/npm/notifyjs@3.10.0/notify.min.js" integrity="sha512-
467grL09I/fq86LVDz186uaxuAhFzyjC9906CC1vghM1YAs+DqCgRvHtZIKX+o91R0F2bro6qniyeCMEQ="
crossorigin="anonymous" referrerpolicy="no-referrer"></script>
    <script type="application/javascript" src="https://cdn.jsdelivr.net/npm/chance/1.1.11/c
hance.min.js" integrity="sha512-Mvo/gaGrTVzN9i+swfStIsSkBkzMsTRgMdES58uVoV5WP9/SfJgoR+G1QIYMS4RC
f62DiAn/3R/Im3q/GHnNg==" crossorigin="anonymous" referrerpolicy="no-referrer"></script>
    <script> window.SEA_WS_HOST = 'wss://2023.holidayhackchallenge.com/sail'; </script>
    <script type="application/javascript" src="js/client.js?nocache=27060298323552"></script>
  </body>
```



You caught a Piscis Cyberneticus Skodo!

Piscis Cyberneticus Skodo, a unique fish adorned with a fedora, glasses, a moustache, and a goatee, thrives in the digital depths of cyber seas. Renowned for its love of Coke Zero, this fish symbolizes a blend of classic and modern tastes. A master of penetration testing, it navigates complex network labyrinths with ease, uncovering hidden vulnerabilities. Remarkably, it possesses the unusual ability to walk swiftly on land, a trait that defies its aquatic nature and sparks intrigue.





Comments of Interest from other Players

Pesadex Count: Html code shows there are 171 fish

- Different fish are found in different areas.
- There may be a fish that can only be found in a limited area.
 - the rare guy? Piscis Cyberneticus Skodo

Overlaying the heatmap

Find heatmap based on hidden note - The note doesn't lie at all. It's where it points at

Looking at the fish heat-maps, it seems that only 1 fish cannot be caught everywhere

- there's a pretty good chance that you'll catch like almost all of them as long as you're in one of the hotspots on the heatmaps
 - Film Noir islands will probably get you 95%
- i had to move around a bit to get the last like 4 or 5 fishes, but yeah most you can get almost anywhere

Okay, I found the images but they all seem to be blurred? Is that intentional?

- It could be, just look through them and you might find a way to interpret them
- Find source file: There is a clue in | | one the source files

Take the heat maps and overlay them on the minimap

convert -compose over -background none 'fishy.png' 'minimap.png' -layers flatten 'wherefindfishy.png'

Looking at heatmap of "Piscis Cyberneticus Skodo", it is clear that white is better.

I found the heat map, but I was having trouble grabbing the minimap and being able to overlay the heat map to get the exact position on the mini map. and both images are different sizes, so I calculated the pixels and this distance of the location in percentage to the maps edge. It was simple math and ended up getting me close enough to the right location to find the last fish.

- Will probably be fun for you to know that i just replaced assets/minimap.png with heatmap png in browser dev tools and drive the boat to a huge bright spot on the minimap

- i just replaced assets/minimap.png with heatmap png in browser dev tools and drive the boat to a huge bright spot on the mini map | |

- some folks actually overlayed the heatmaps over minimap properly too

I added an image tag and made it 0.5 opacity, same size :) | | low tech approach

set theory, you should know what you've caught from the json, and you have your fish-list, then look at those maps?

Use the source

- The brighter the better!!!
- You can overlay the hYup, i relaced it in js for the sea. minimap.png for the fishes heatmap pngotspot map and the minimap. T hen the location is easy to find
- i don't think that looks as nice as overlaying the 2 images, just set the opacity of the heatmap lower i used gimp

Interact with websockets

Getting started with socat, a multipurpose relay tool for Linux - If you need an advanced sysadmin tool for your toolbox, this is the one. Socat allows for bidirectional data transfers from one location to another.

From <<https://www.redhat.com/sysadmin/getting-started-socat>>

This is working quite nicely! websockets only fishing script: <https://imgur.com/a/14cyzkq>

Other hacks

Checking 10 times per second in js whether the cast button is visible or the reel in button is red and then i click 'em. works great for letting it run in the background!

Hypothetically speaking, if that's the hash in the file name....

```
└─(marlas@marlaskali)-[~/hhc2023]
└─$ ./auto-fisher.py -u marlas
Enter your Holiday Hack Challenge password (will be hidden):
[+] Successfully logged in!
[+] Bumbleberry Floatfish was caught!
[+] The Speckled Whisker-Spoon Puffer was caught!
[+] Pistachio Pizzafin Puffinfly was caught!
[+] The ChocoChandelier Goldnipper was caught!
[+] Gumball Guppygator was caught!
```

When in your chair you don't have to fish too far for it, like Skywalker, ||use the source Luke||.

Power Automate makes easy work of this...but it's getting harder to get new fish

Was anyone able to get their code to work using the color change of the button? I have mine going with code that Bard helped me write, but it's still a little janky. It's working to catch fish slowly though.

webdeveloper console and javascript is what i used
It was just javascript in the console for me. Found the context I needed with Inspect and then told chatGPT what I needed to do re: playing the game. It spit out a function that worked out of the gate.

I Used wscat, burp, and browser dev console for recon to gather and understand the messages going over websockets. And python with websockets module to automate it

[6:02 PM]KDP: I used burp and the browser console to explore and locate the heat maps then used the console to use the maps and automate fishing

my automation script in python? I can login, I think I can reel and cast but that's about it, I can't seem to get responses to those actions. I can't see an easy way to filter/sort the ws in burp to try to piece them together and there are soooo many of them.

i need help from where i could start as i opened page sources and cannot access fish/assets?

[12:57 AM]JPMinty (Jai Minton): Look into the network websocket traffic with burpsuite or in your network developer tools or manually start fishing using the UI and look at how you could automate the clicks. For information on the fish look for any comments on the web page

finally figured out that by adding 2 lines of code, it will auto catch fish for me

[11:45 AM]g0|df!ng3Я: now to get the last fish the Fizzgiggle Frizzlefin

I've been poking around the WS and JS, and spotted the WS flow - info about the catch/reel, local area, players, ports etc. But nothing about heatmaps or the other fish

I have automated my crew, but am out of ideas on finding the last few fish. I see mention of a heatmap but can someone help steer me to where I can find such goodness? TY!

- look at the hint again for the challenge, and check out dev tools while you're at sea
- it helps if i fish in the right location as well -- now with the heat map and finally overlaying it, i was in the wrong place

Did you inspect the right place? there are only two buttons you need to care for, if only focus on the ||html|| parts, like i did, and don't involve with ||websockets|| which would probably be more straight encompassing.

Fire up Burp and take a look at the websocket traffic

So as mentioned several times in this chat there is **one fish that has a small location where it may be caught.**

The image names are derived from the fish names for all fish except for this one fish.

I tried generating a few ideas based on the fish's namesake to see if maybe there was a fun original name I could gleam with no luck. Chances are it was just changed for the sake of being a rare fish and make it harder to view when people connected the name/value setup. Would be fun to find out if this value was based off of something like a fun name originally tied more closely to its namesake.

automation really was really a necessity on this one as well as the hints the elf gave.

heard an elf named Poinsettia McMittens who spoke of a forgotten language for this specific kind of task. (check if you have a hint in your badge provided by Poinsettia McMittens for this challenge). - also leveraging AI is encouraged, if programming is not your cup of tea

do have a hint but it just says check the HTML. if i can get more info though I'll definitely look at using AI
- maybe it's relative to where you found that

Is there a quick way to identify which fish are in my pescadex and which I don't have so I can figure out which heat maps to look at?

[6:51 AM]jevan: consider having ChatGPT or Bard to write you a script that compares JSON blobs

There are Linux tools that are made for this. Just gotta clean up the lists. Sorting then manually looking would take longer but would work.

Dear AI of choice, create me a Python program that creates a nice collage from 171 fish images. 3, 2, 1, done. I love it 🐟

Really trying to figure out why `||canFish` is set to false when I connect via websocket, but true when I connect via gui... Everything else working. `||` check under assets/

[2:24 PM]TMX25519: I'm still looking for that

never done browser automation before but was able to get working code running in minutes using a Bard query.

- may be some broken fish scripts out there; see [image.png \(979×1113\) \(discordapp.net\)](#)

There's 171.

I use the heat maps to move around to the best spots for each fish type

[8:26 AM]TMX25519: Use AI tools to generate the script for you once you know how the buttons functions.

Since the pescadex only has the ones you've caught, couldn't you write a script to make a list of the ones you have, make a list of all of them from the page of heatmaps, and then do a remove operation on the heatmap list `||`?

Any way to get a list of fish I've already caught? I know about the heat map, but curious to know which I have yet to catch. The "pescadex" only appears to list one fish at a time.

[12:29 PM]joergen: Check your websocket traffic. This data is transferred as message type i:

Woo! Found the `||density reference images||`!

You can hold down the anchor brake (spacebar) to break out of a loop

If you mean the 'select evaluation context' box, yeah, I've been careful about that one.

[10:49 AM]Wraith 5: HAH! I made it automatically click the 'reel it in' button!

have successfully made it automatically fish! I have caught 4 22 65 (not counting repeats) fish in a row without pressing a button!

Poor lil Jace...

so got two ways forward.... once is using `pynput.mouse` and another with `pure js` in the chrome console. right now the `js` method is cleaner as it uses a `mutation observer` to know when to reel.

oh i see u on the map... it's about 20 lines so not too bad. responding to mutation and re-casting was quicker than the 1.5sec sleep on the autoclicker.

Have you looked at the heatmap? I'm sure you'll get it just fishing around

<https://arnydo.gitlab.io/2023-hhc-pescadex/>

From <<https://discord.com/channels/783055461620514818/783055463083671627>>