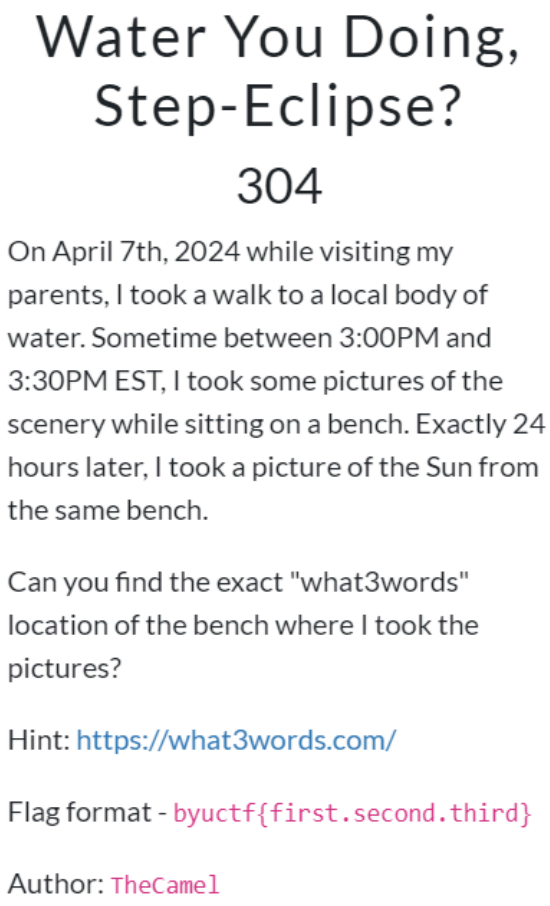
OSINT CHALLENGES

BYUCTF 2024

by: meadow

In May 2024, me and my Team **World Wide Flags** competed in the BYUCTF. I want to provide writeups for the OSINT challenges *Water You Doing, Step-Eclipse?* and *Records*.

Water You Doing, Step-Eclipse?

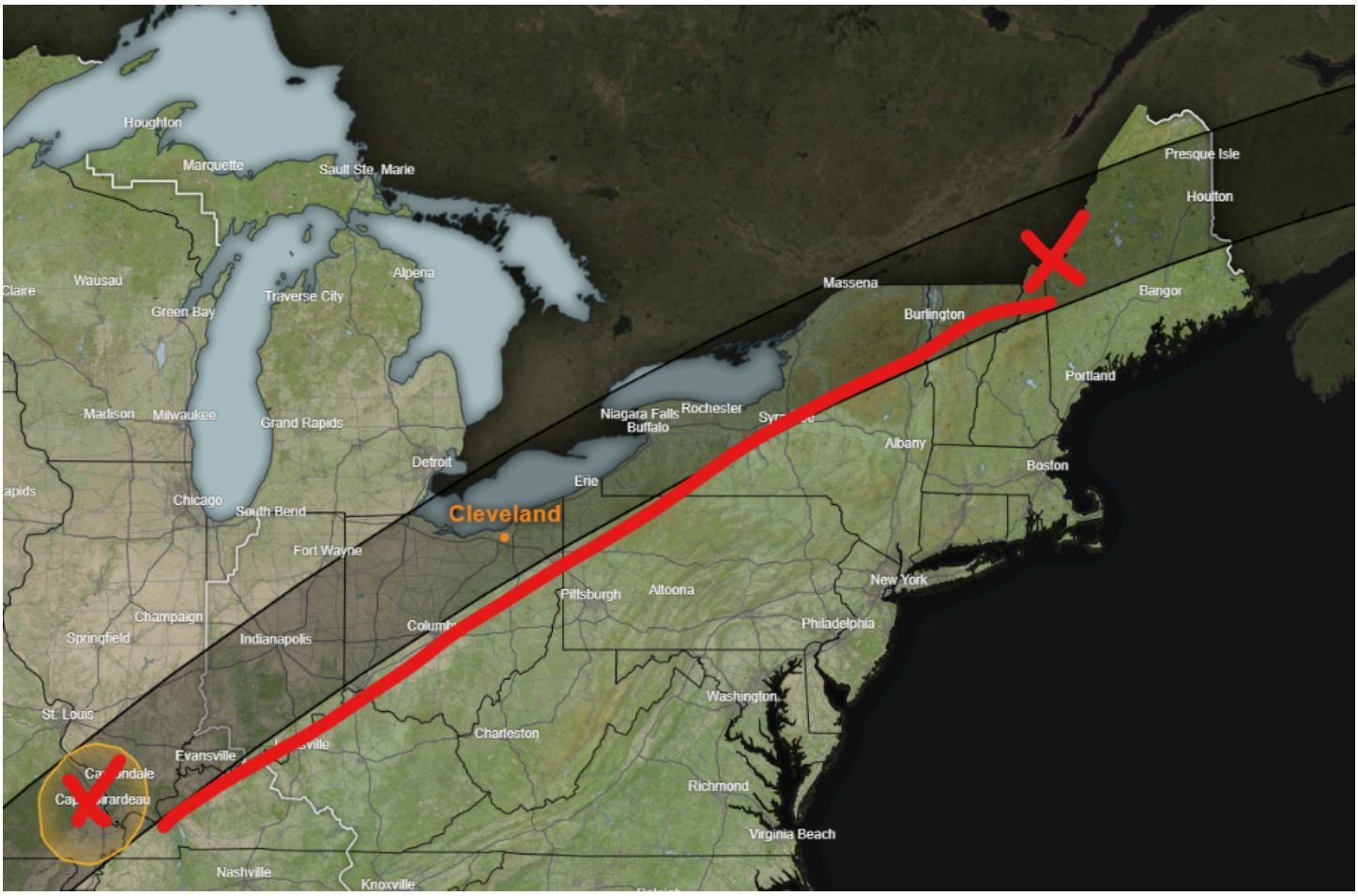


Attached to the challenge are 3 photos:

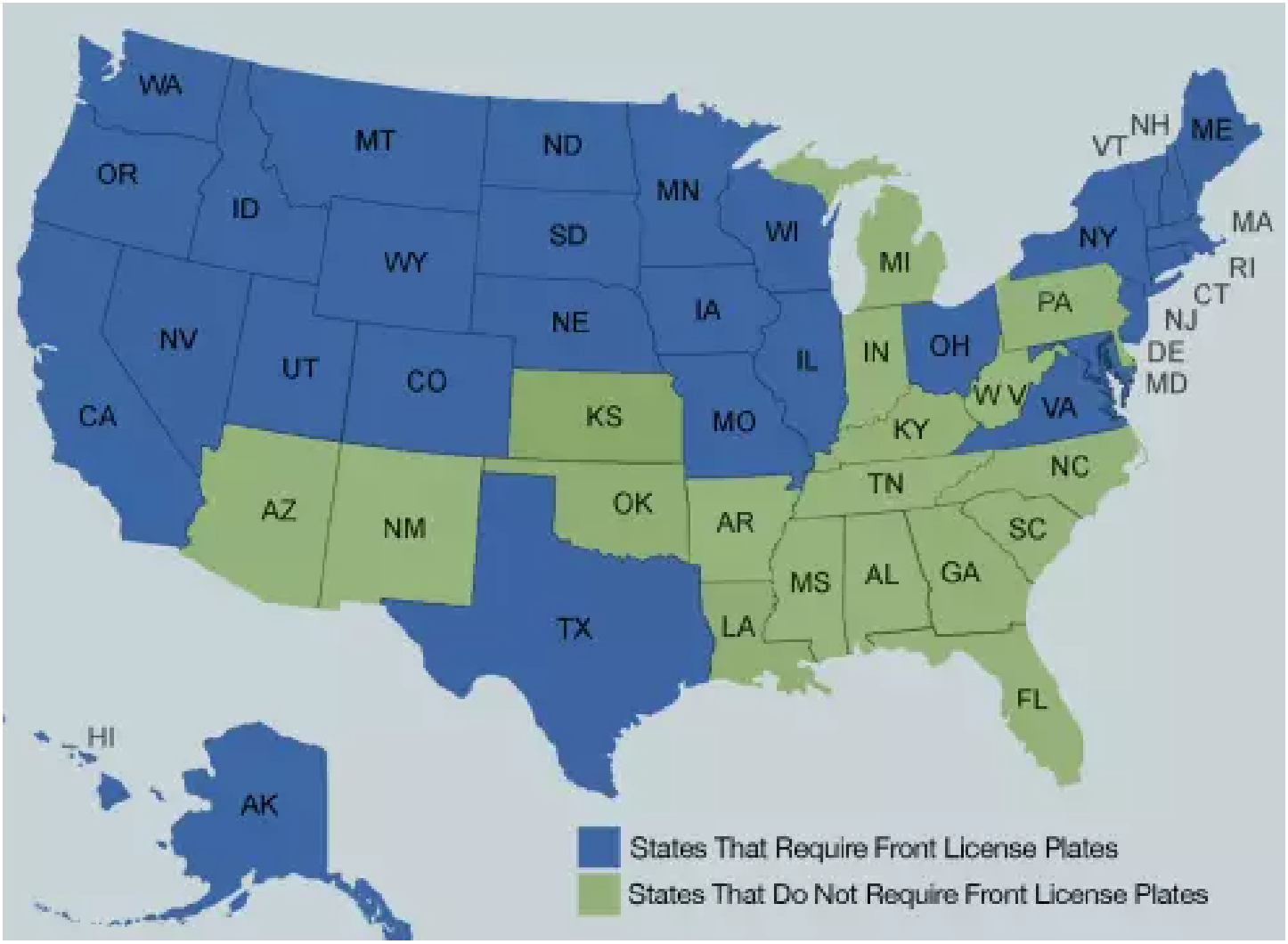
Based on the challenge description we find out that the photo of the full solar eclipse was taken on April 8th, 2024 between 3PM and 3:30PM EST.

Googling for “solar eclipse 2024 8 april” we can use this site: https://science.nasa.gov/eclipses/future-eclipses/eclipse-2024/where-when/

to exactly determine where the full eclipse was visible during the time we are interested in:



The second photo from the challenge shows a car that has no front license plate, so we can determine that we have to look in a state where this is actually permitted:



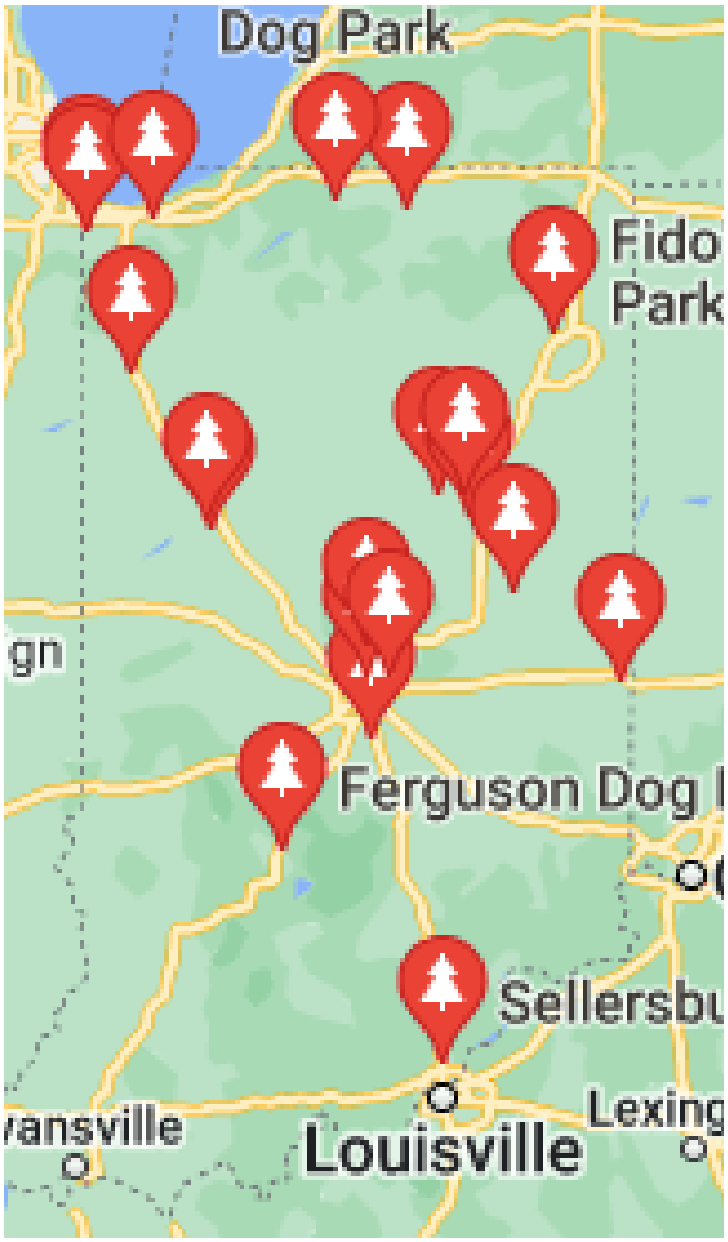
From the path the eclipse traveled we can determine that the state we are looking for can only be **Indiana** or a tiny part of **Pennsylvania.**

I quickly dismissed PA because I didn't see any bodies of water that seemed fitting, instead focusing in Indiana.

Now I actually spent several hours scanning the state manually for places that seemed fitting. Not very effective but it got the job done 😉 I spotted the distinct pier shape:

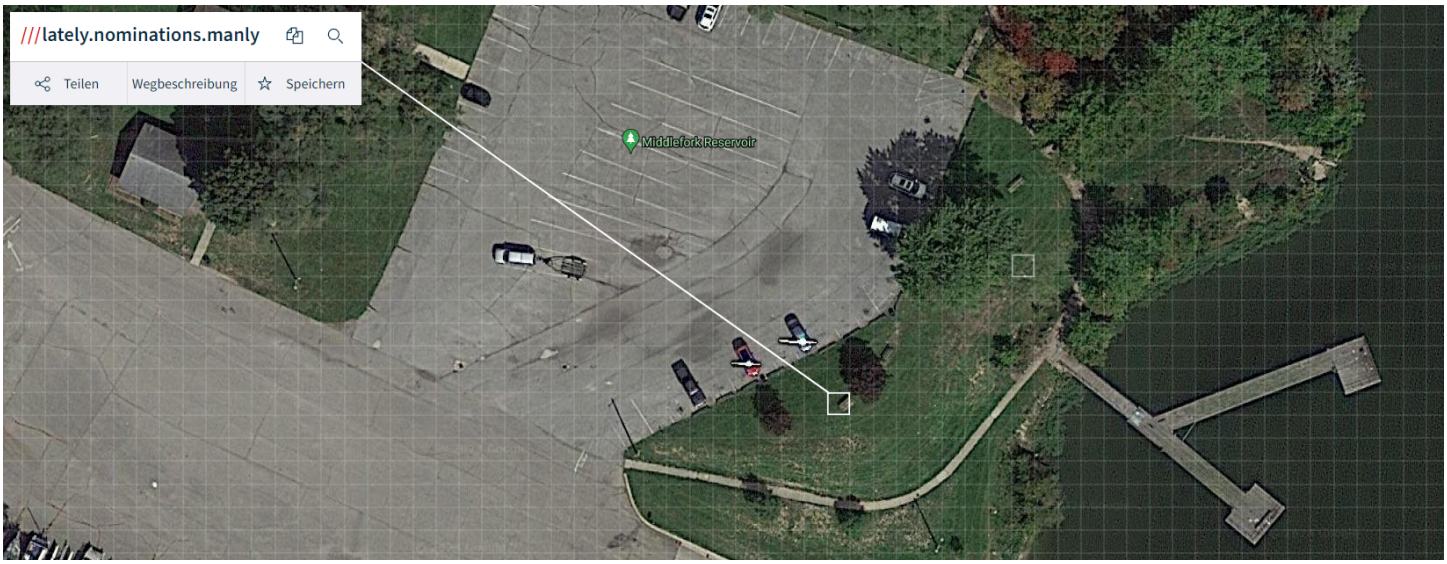
This was the right place but later I discovered that we could have narrowed down that place even more. Again looking at the second photo, in the left background part we see a kind of park that looks like a **dog training park.**

Googling **dog park Indiana** we find ourselves with only a few results:



Checking these takes hardly any time at all and like this we can quickly spot our desired place.

We need to pinpoint the exact bench where the photos were taken. For the flag we don’t need coordinates, but a what3words location. Hopping onto **what3words.com** we can determine the exact square:



We finally get our flag: **byuctf{lately.nominations.manly}**

Records

Records

499

Deep within the labyrinthine corridors of the DNS records for `cyberjousting.com` lies a trove of clandestine data, shrouded in mystery and guarded by digital sentinels. Concealed within the intricate web of cyberspace, this critical information holds the key to unlocking secrets of paramount importance.

Author: `welshdragon`

This challenge caused some headaches 😝 We got really close but actually only solved this one after the CTF ended.

After LOTS of rabbit holes we do a DNS Record Lookup at **viewdns.info** finally find out that there should be a www. subdomain:

WWW Record Tests

Status	Test Case	Information
ℹ	WWW record	www.cyberjousting.com A records are:
✔	WWW A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.
✖	WWW CNAME lookup	Oops! You don't have a CNAME entry or an A record for your WWW record. This means that no-one will see your site when they visit www.cyberjousting.com!

This is a lead! Doing a DNS Record Lookup for **www.cyberjousting.com** we find a TXT record.

DNS Records for www.cyberjousting.com
==========

Name	TTL	Class	Type	Priority	Data
www.cyberjousting.com.	14400	IN	TXT		"Ynl1Y3Rme0RONV9SM2Nvbl9NNDV0M3J9"
www.cyberjousting.com.	14400	IN	RRSIG		TXT 8 3 14400 20240607222920 20240516222920 34059 cyberjousting.com. HofdKo5x6GbGMPBLOI+Y2/IWiZCdNxOn9qXsdyvUefyYkBj/Tne80gtb GOUj6ffUSnOhFewtRERZOiGaWhjtAyUnHK50VTFDL9VlfarRmxvwWK9T K0sVVGTDbI6FwESibV1+025SZNt4dToBV8vFOw3dSgiLWzV9/GgaYOSQ MCQ=

Decoding the base64 finally rewards us with the flag:

byuctf{DN5_R3con_M45t3r}