RACTF2020 Writeup – Mad CTF Disease

```
Todo:
[x] Be a cow
[x] Eat grass
[x] Eat grass
[x] Eat grass
[ ] Find the flag
```

350 Points

In this challenge, a picture of a cow was provided:

I ran the image through the usual tools (binwalk, strings) but found nothing. So I decided to download Stego Toolkit by Dominic Breuker (https://github.com/DominicBreuker/stego-toolkit), a docker image that has plenty of built in steganography tools. I ran it using the following command:

sudo docker run -it dominicbreuker/stego-toolkit /bin/bash

Once in, I transferred the image to the server using pythons SimpleHTTPServer module, and ran the image through stegoveritas. The first result returned something of interest:

```
root@f171aa7d0c11:/data# stegoveritas cow.jpg
Running Module: SVImage
+------------------+------+
|   Image Format   | Mode |
+------------------+------+
| JPEG (ISO 10918) | RGB  |
+------------------+------+
Found something with StegHide: /data/results/steghide_4f3dae4985bf32dcb5f46aa14dd3f97d.bin
Running Module: MultiHandler
```

Opening this file, I found an odd looking string of text:

After showing this to a team member, they identified it as COW language (https://esolangs.org/wiki/COW). So after a quick read on that I went to find an interpreter for COW, and stumbled upon Try It Online (https://tio.run/) which had a compiler for COW. I put the extracted COW code into the COW interpreter and got the flag:

ractf{exp3rt-mo0neuv3r5}