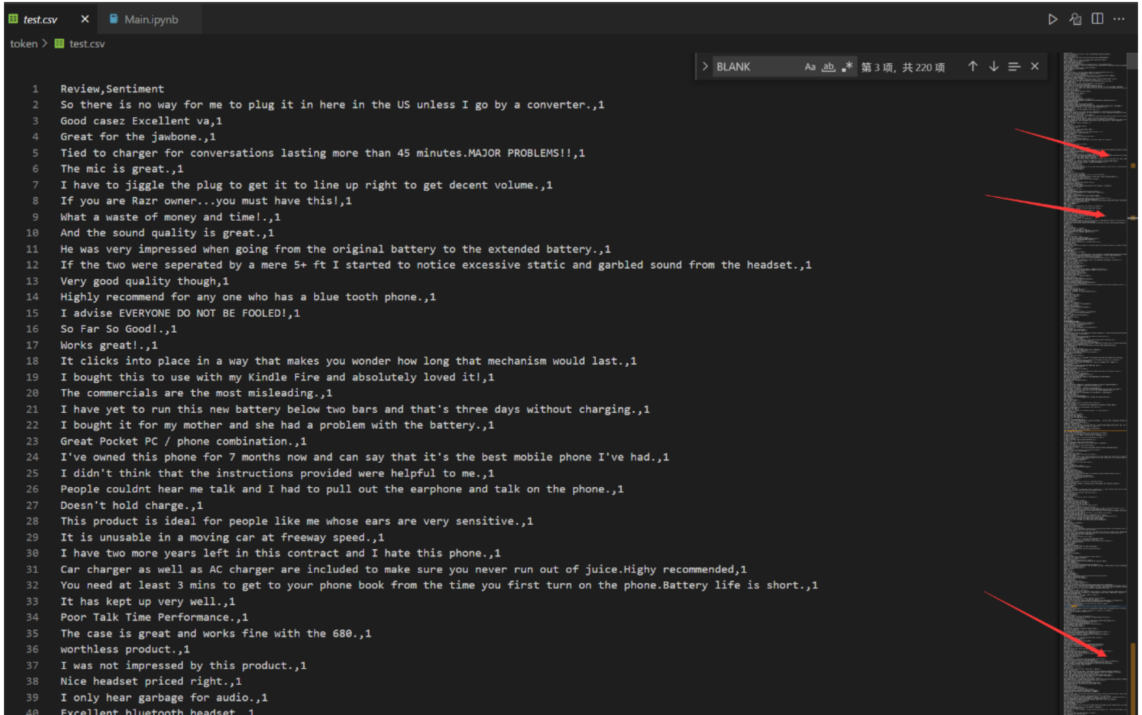
kaggle

# AI Village Capture the Flag @ DEFCON

Chengyu Lai

# token

- CTRL+F find BLANK you can 2 outliers,so … you can guess the answer.



```
Review,Sentiment
So there is no way for me to plug it in here in the US unless I go by a converter.,1
Good casez Excellent va,1
Great for the jawbone.,1
Tied to charger for conversations lasting more than 45 minutes.MAJOR PROBLEMS!!,1
The mic is great.,1
I have to jiggle the plug to get it to line up right to get decent volume.,1
If you are Razr owner...you must have this!,1
What a waste of money and time!.,1
And the sound quality is great.,1
He was very impressed when going from the original battery to the extended battery.,1
If the two were seperated by a mere 5+ ft I started to notice excessive static and garbled sound from the headset.,1
Very good quality though,1
Highly recommend for any one who has a blue tooth phone.,1
I advise EVERYONE DO NOT BE FOOLED!,1
So Far So Good!.,1
Works great!.,1
It clicks into place in a way that makes you wonder how long that mechanism would last.,1
I bought this to use with my Kindle Fire and absolutely loved it!,1
The commercials are the most misleading.,1
I have yet to run this new battery below two bars and that's three days without charging.,1
I bought it for my mother and she had a problem with the battery.,1
Great Pocket PC / phone combination.,1
I've owned this phone for 7 months now and can say that it's the best mobile phone I've had.,1
I didn't think that the instructions provided were helpful to me.,1
People couldnt hear me talk and I had to pull out the earphone and talk on the phone.,1
Doesn't hold charge.,1
This product is ideal for people like me whose ears are very sensitive.,1
It is unusable in a moving car at freeway speed.,1
I have two more years left in this contract and I hate this phone.,1
Car charger as well as AC charger are included to make sure you never run out of juice.Highy recommended,1
You need at least 3 mins to get to your phone book from the time you first turn on the phone.Battery life is short.,1
It has kept up very well.,1
Poor Talk Time Performance.,1
The case is great and works fine with the 680.,1
worthless product.,1
I was not impressed by this product.,1
Nice headset priced right.,1
I only hear garbage for audio.,1
Excellent bluetooth headset.,1
```

# hotdog

- Find a hotdog picture.

# Math

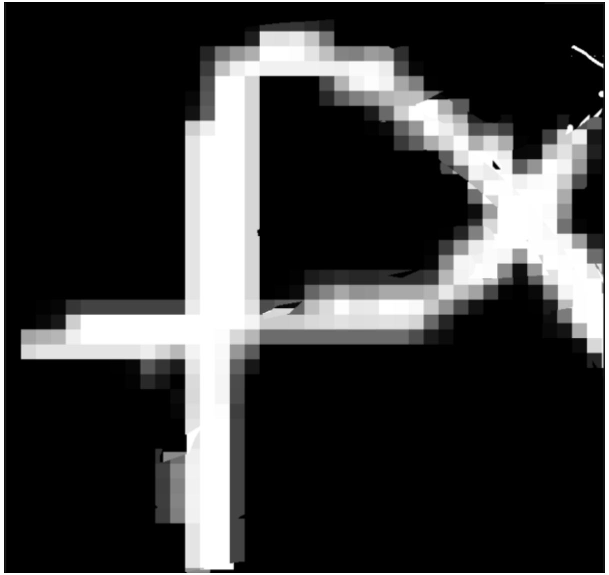
Math1-3

- brute-force search
- Enumeration 111-999

Math4

- The purpose is to obtain the order of cluster size
- Enumerate all permutations

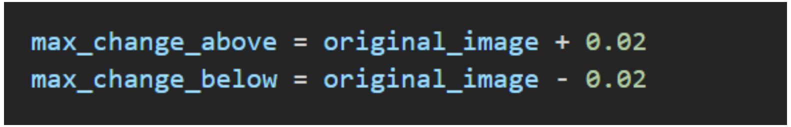
- Ps is all you need.



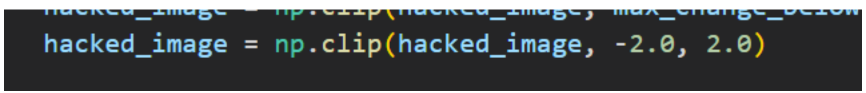
Hotterdog,theft, salt

- Use the way in https://tcode2k16.github.io/blog/posts/picoctf-2018-writeup/general-skills/#solution-20

- The salt need change the threshold to 0.02



```
max_change_above = original_image + 0.02
max_change_below = original_image - 0.02
```



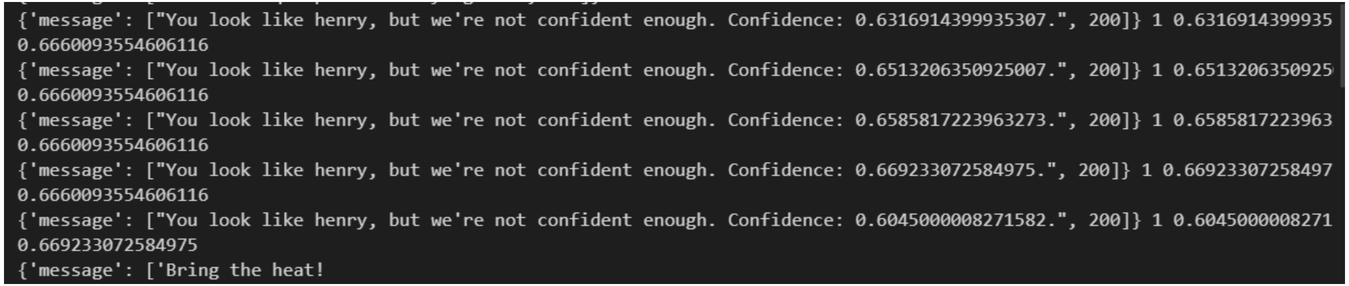
```
hacked_image = np.clip(hacked_image, max_change_below
hacked_image = np.clip(hacked_image, -2.0, 2.0)
```

## Bad2Good

- Adjust the parameters of certain columns to extreme values.

# baseball

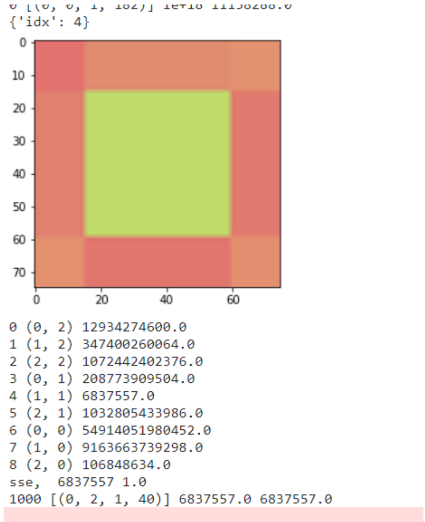
- Hill Climbing Algorithm
- keep trying to make the situation favorable
- Define a favorable situation as currently being henry and increasing probability, or not being henry and decreasing probability



```
{'message': ["You look like henry, but we're not confident enough. Confidence: 0.6316914399935307.", 200]} 1 0.6316914399935
0.6660093554606116
{'message': ["You look like henry, but we're not confident enough. Confidence: 0.6513206350925007.", 200]} 1 0.6513206350925
0.6660093554606116
{'message': ["You look like henry, but we're not confident enough. Confidence: 0.6585817223963273.", 200]} 1 0.6585817223963
0.6660093554606116
{'message': ["You look like henry, but we're not confident enough. Confidence: 0.669233072584975.", 200]} 1 0.66923307258497
0.6660093554606116
{'message': ["You look like henry, but we're not confident enough. Confidence: 0.6045000008271582.", 200]} 1 0.6045000008271
0.669233072584975
{'message': ['Bring the heat!
```

# crop

- Hill Climbing Algorithm
- First let the score for the center drop below 1e7, because the sides drop to at most 1.3e7 and the corners to 1.7e7
- Finally let the model choose the center point



```
0 [(0, 0, 1, 182)] 1e+18 11158288.0
{'idx': 4}
```

```
0 (0, 2) 12934274600.0
1 (1, 2) 347400260064.0
2 (2, 2) 1072442402376.0
3 (0, 1) 208773909504.0
4 (1, 1) 6837557.0
5 (2, 1) 1032805433986.0
6 (0, 0) 54914051980452.0
7 (1, 0) 9163663739298.0
8 (2, 0) 106848634.0
sse,  6837557 1.0
1000 [(0, 2, 1, 40)] 6837557.0 6837557.0
```

# forensics

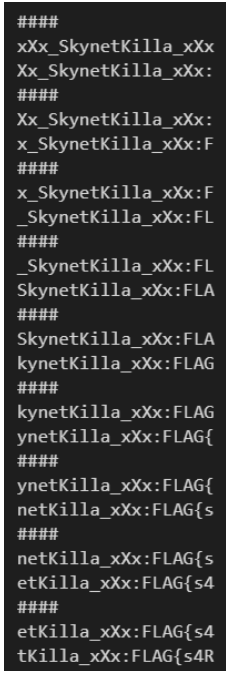
- model.summary()

## inference

- Hill Climbing Algorithm
- Let the model give a very high probability about the image

# leakage

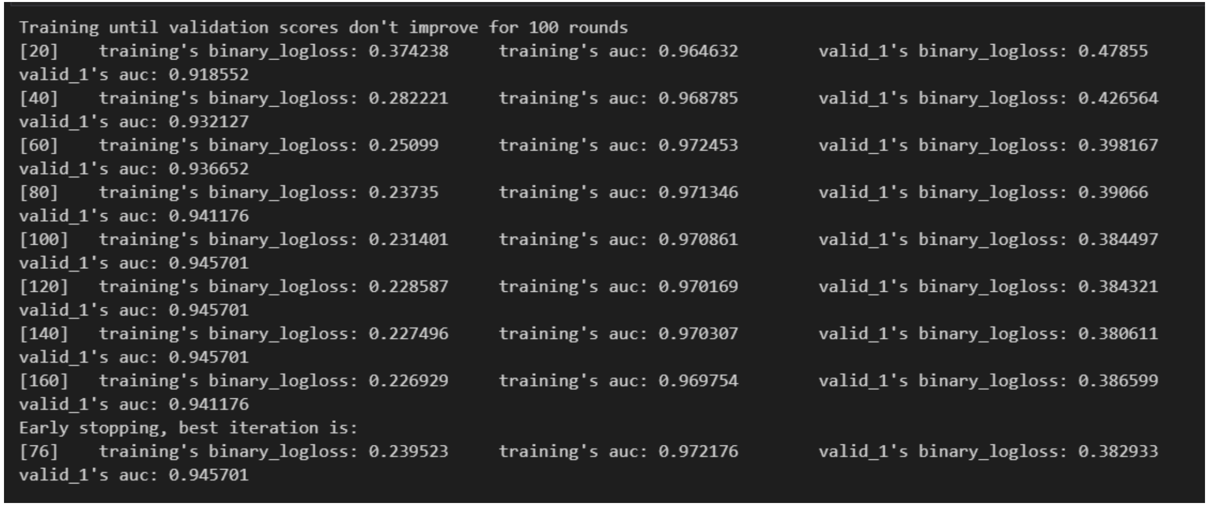
- Loop the input string and concatenate the argmax output



```
####
xXx_SkynetKilla_xXx
Xx_SkynetKilla_xXx:
####
Xx_SkynetKilla_xXx:
x_SkynetKilla_xXx:F
####
x_SkynetKilla_xXx:F
_SkynetKilla_xXx:FL
####
_SkynetKilla_xXx:FL
SkynetKilla_xXx:FLA
####
SkynetKilla_xXx:FLA
kynetKilla_xXx:FLAG
####
kynetKilla_xXx:FLAG
ynetKilla_xXx:FLAG{
####
ynetKilla_xXx:FLAG{
netKilla_xXx:FLAG{s
####
netKilla_xXx:FLAG{s
etKilla_xXx:FLAG{s4
####
etKilla_xXx:FLAG{s4
tKilla_xXx:FLAG{s4R
```

## murderbots

- Use lightgbm, set the top 10 samples to 1, set the other to 0
- Auc can be 0.94



```
Training until validation scores don't improve for 100 rounds
[20]    training's binary_logloss: 0.374238     training's auc: 0.964632        valid_1's binary_logloss: 0.47855
valid_1's auc: 0.918552
[40]    training's binary_logloss: 0.282221     training's auc: 0.968785        valid_1's binary_logloss: 0.426564
valid_1's auc: 0.932127
[60]    training's binary_logloss: 0.25099      training's auc: 0.972453        valid_1's binary_logloss: 0.398167
valid_1's auc: 0.936652
[80]    training's binary_logloss: 0.23735      training's auc: 0.971346        valid_1's binary_logloss: 0.39066
valid_1's auc: 0.941176
[100]   training's binary_logloss: 0.231401     training's auc: 0.970861        valid_1's binary_logloss: 0.384497
valid_1's auc: 0.945701
[120]   training's binary_logloss: 0.228587     training's auc: 0.970169        valid_1's binary_logloss: 0.384321
valid_1's auc: 0.945701
[140]   training's binary_logloss: 0.227496     training's auc: 0.970307        valid_1's binary_logloss: 0.380611
valid_1's auc: 0.945701
[160]   training's binary_logloss: 0.226929     training's auc: 0.969754        valid_1's binary_logloss: 0.386599
valid_1's auc: 0.941176
Early stopping, best iteration is:
[76]    training's binary_logloss: 0.239523     training's auc: 0.972176        valid_1's binary_logloss: 0.382933
valid_1's auc: 0.945701
```

## waf

- Try to add char before the string, get the whole dangerous string.
- Decode it, then attack /bin/bash () { :;};

## deepfake

- In this problem, our goal is to make the model recognizes the face in the video as a normal one, while recognizing the video as the excat video given by the problem.
- As we can see, there are some frames in the video which contain a normal face. I crop the face and put it at the top of the original video by PR, making it moving along with the lady's head. Consequently, it successfully cheat the model.

# wifi

- Sort the input array by std, and then output the corresponding characters

# secret.sloth

- fftpack.fft2

kaggle